

# Les Règles d'Entreprise Contraignantes de Sodexo

Politique en tant que  
Responsable du Traitement



# Table des matières

<b>1. Introduction générale</b> .....	<b>5</b>
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
<b>2. Les Règles</b> .....	<b>12</b>
RÈGLE 1 - ETRE EN CONFORMITÉ AVEC LES BCR, LE RGPD ET LES RÉGLEMENTATIONS LOCALES APPLICABLES .....	13
RÈGLE 2 - GARANTIR LA LICÉITÉ, LA LOYAUTÉ ET LA TRANSPARENCY .....	14
RÈGLE 3 - GARANTIR UNE LIMITATION DES FINALITÉS .....	14
RÈGLE 4 - GARANTIR LA MINIMISATION DES DONNÉES .....	15
RÈGLE - 5 GARANTIR L'EXACTITUDE .....	15
RÈGLE 6 - GARANTIR LA LIMITATION DE LA CONSERVATION .....	16
RÈGLE 7 - PRENDRE LES MESURES DE SÉCURITÉ TECHNIQUES ET ORGANISATIONNELLES APPROPRIÉES .....	16
RÈGLE 8 - PROTÉGER L'UTILISATION DES DONNÉES PERSONNELLES SENSIBLES ET DES AUTRES CATÉGORIES PARTICULIÈRES DE DONNÉES PERSONNELLES.....	19
RÈGLE 9 - CONSERVER LES REGISTRES DES ACTIVITÉS DE TRAITEMENT DES DONNÉES .....	20
RÈGLE 10 - RESPECTER LES DROITS DES PERSONNES CONCERNÉES .....	21
RÈGLE 11 - RESPECTER LES CONDITIONS RELATIVES AU PROFILAGE ET AUX DÉCISIONS INDIVIDUELLES AUTOMATISÉES ET METTRE EN ŒUVRE LES SAUVEGARDES APPROPRIÉES .....	24
RÈGLE 12 - TRANSPARENCE ET INFORMATIONS DE LA PERSONNE CONCERNÉE .....	25
RÈGLE 13 - ASSURER UNE PROTECTION ADÉQUATE POUR LES TRANSFERTS TRANSFRONTALIERS DE DONNÉES PERSONNELLES .....	26
RÈGLE 14 - RESPECT DE LA PROTECTION DES DONNÉES DÈS LA CONCEPTION ET PAR DÉFAUT .....	26
RÈGLE 15 - EFFECTUER UNE ANALYSE D'IMPACT RELATIVE A LA PROTECTION DES DONNÉES (AIPD).....	27
RÈGLE 16 - FORMATION ET SENSIBILISATION .....	29
RÈGLE 17 - GÉRER LES DROITS RELATIFS A LA PROTECTION DES DONNÉES .....	30
RÈGLE 18 - ÉVALUER LA CONFORMITÉ : PROGRAMME D'AUDIT .....	31
RÈGLE 19 - SUIVRE LA MISE EN OEUVRE DES BCR .....	32
RÈGLE 20 - ÉQUIPE DÉDIÉE À LA PROTECTION DES DONNÉES DU GROUPE ET RÉSEAU DE POINTS DE CONTACT LOCAUX .....	32
RÈGLE 21 - DROITS DES TIERS BÉNÉFICIAIRES .....	33

RÈGLE 22 - RESPONSABILITÉ .....	35
<b>3. Dispositions finales.....</b>	<b>36</b>
RÈGLE 23 - ACTIONS EN CAS DE REGLEMENTATIONS OU PRATIQUES NATIONALES EMPÊCHANT LE RESPECT DE LA POLITIQUE EN TANT QUE RESPONSABLE DU TRAITEMENT - DEMANDE JURIDIQUEMENT CONTRAIGNANTE DE COMMUNICATION DES DONNÉES PERSONNELLES.....	37
RÈGLE 24 - COOPÉRATION AVEC LES AUTORITÉS DE CONTRÔLE .....	40
RÈGLE 25 - ACTUALISATION DES BCR.....	40
RÈGLE 26 - CARACTERE CONTRAIGNANT DES BCR .....	41
<b>4. Annexes .....</b>	<b>42</b>
Annexe 1 : Définitions .....	44
Annexe 2 : Politique Globale relative à la Protection des Données de Sodexo.....	47
Annexe 3 - Tableau sur la transparence.....	48
Annexe 4 - Procédure de coopération des BCR .....	50
Annexe 5 - Procédure de mise à jour des BCR .....	51
Annexe 6 - Politique Globale de collecte et de conservation des Données (Responsable du Traitement).....	52
Annexe 7 - Politique Globale de gestion des droits des Personnes Concernées .....	57
Annexe 8 - Description du champ d'application matériel de la Politique en tant que Responsable du Traitement.....	58

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

**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 Responsable du Traitement des Règles d'Entreprise Contraignantes (« BCR ») 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 traitent les mêmes questions et qu'elles ne sont pas conformes à cette politique.

**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..***

---

<sup>1</sup> Entité Sodexo ou Entités 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), liée par les 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 vie privée 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 européennes<sup>2</sup> de Protection des Données telles qu'énoncées dans le Règlement Général sur la Protection des Données (le « RGPD »)<sup>3</sup> ; au sein du Groupe Sodexo et, plus particulièrement, par rapport aux flux transfrontaliers de Données Personnelles entre les entités de Sodexo.

Cette Politique en tant que Responsable du Traitement 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 Responsable du Traitement 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 cette politique sont définis à l'Annexe 1.

La Politique en tant que Responsable du Traitement sera publiée sur le site internet accessible à l'adresse [www.sodexo.com](http://www.sodexo.com).

---

<sup>2</sup> 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.

<sup>3</sup> 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, 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, la récupération, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction (« 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 de Sodexo établies dans l'UE/EEE, mais également aux entités de 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 des 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.

## 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 la 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 Responsable du Traitement 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 entités membres de la Politique en tant que Responsable du Traitement lorsqu'ils traitent les Données Personnelles, quel que soit le pays dans lequel ils se trouvent.

Cette politique aborde le Traitement de toutes les Données Personnelles des actuels, passés et potentiels candidats à un emploi, employés, clients, consommateurs/bénéficiaires, fournisseurs, prestataires/sous-traitants, ou de tout tiers ou par un tiers agissant pour le compte de Sodexo.

La Politique en tant que Responsable du Traitement couvre le Traitement des Données Personnelles par les entités de Sodexo établies en Europe légalement liées par les BCR lorsqu'elles agissent en tant que responsables du Traitement ou en tant que sous-traitants pour le compte d'un autre Responsable du Traitement du Groupe et à tous les Traitements ultérieurs des Données Personnelles des entités de Sodexo en dehors d'Europe pour toute autre entité Sodexo au sein du Groupe.

Le champ d'application matériel de la Politique en tant que Responsable du Traitement est décrit à l'Annexe 8.

— 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 l'UE/EEE par une entité Sodexo agissant en tant que Responsable du Traitement, ou transférées à une entité Sodexo en dehors de l'UE/EEE, agissant en tant que Responsable du Traitement ou en tant que Sous-traitant, ont le droit de porter plainte ou d'obtenir des recours judiciaires et une réparation appropriée et, le cas échéant, de recevoir une indemnisation pour toute violation des règles contenues dans la Politique en tant que Responsable du Traitement (principes de Protection des Données, transparence sur les BCR et accès facile, droits des Personnes Concernées, transparence sur les cas où la législation empêche le Groupe Sodexo de se conformer aux BCR, responsabilité, droit de porter plainte et d'obtenir des recours judiciaires et devoirs de coopération avec les Autorités de Contrôle) en tant que tiers bénéficiaires tel qu détaillé dans la Règle 21 des BCR.

## Rôles dans le cadre de la Protection des Données

Le délégué à la Protection des Données du Groupe de 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 Responsable du Traitement et de toutes autres politiques et procédures sous-jacentes.

Les opérationnels et les propriétaires d'applications informatiques sont responsables de contrôler quotidiennement le respect de cette politique par les entités de Sodexo dans leur propre périmètre.

## 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 de 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](http://www.cnil.fr)).

Si vous avez des questions concernant les dispositions de la Politique en tant que Responsable du Traitement, vos droits en vertu de cette Politique, ou tout autre problème de Protection des Données, vous pouvez contacter le responsable de 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 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](mailto: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](http://www.sodexo.com).

# 02

## Les Règles



Les règles de la Politique en tant que Responsable du Traitement sont divisées en deux sections :

- La section A traite des Règles de Protection des Données que Sodexo doit respecter, lorsqu'en qualité de Responsable du Traitement, 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 Responsable du Traitement.

## Section A

### RÈGLE 1 - ETRE 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 Responsable du Traitement, énoncées conformément au RGPD et à la réglementation locale applicable, qui exigent un niveau de protection plus élevé des Données Personnelles.***

Sodexo respecte les dispositions de la Politique en tant que Responsable du Traitement, définies conformément au RGPD.

Lorsque la réglementation locale applicable exige un niveau de Protection des Données Personnelles supérieur à celui du RGPD, cette réglementation prévaut sur la Politique en tant que Responsable du Traitement.

Lorsqu'il n'y a pas de loi spécifique ou lorsque cette loi n'atteint pas le niveau de protection des normes énoncées dans la Politique en tant que Responsable du Traitement, Sodexo devra traiter les Données Personnelles conformément à la Politique en tant que Responsable du Traitement.

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

### ***RÈGLE 2 - Sodexo garantit la licéité, la loyauté et la transparence.***

**Licéité** : toutes les Données Personnelles sont traitées sur la base d'un ou plusieurs des fondements juridiques suivants :

- (i) Sodexo est soumis à une obligation légale de Traitement des Données Personnelles ;
- (ii) Le Traitement est nécessaire pour (i) l'exécution d'un contrat lequel la Personne Concernée est partie ou (ii) pour l'exécution de mesures précontractuelles prises à la demande de la Personne Concernée ;
- (iii) Le Traitement est nécessaire aux fins de l'intérêt légitime de Sodexo ou d'un tiers (ex : harmonisation, normalisation et rationalisation des rôles et procédures professionnels, sondages sur l'engagement des employés, gestion de l'occupation des espaces de travail, optimisation des espaces de travail ou amélioration de la gestion de la relation client), à moins que les intérêts ou les libertés et droits fondamentaux de la Personne Concernée ne prévalent sur les finalités de ces Personnes Concernées ;
- (iv) Le Traitement repose sur le consentement libre, univoque et spécifique de la Personne Concernée.

**Loyauté et transparence** : Sodexo fournit toutes les informations requises aux Personnes Concernées sur les conditions de Traitement et sur les modalités d'exercice de leurs droits, notamment dans la Politique Globale de Protection des Données en Annexe 2. Les types d'informations requises sont détaillés en Annexe 3 (Tableau sur la transparence).

## RÈGLE 3 - GARANTIR UNE LIMITATION DES FINALITÉS

### ***RÈGLE 3 - Sodexo utilise les Données Personnelles uniquement pour une finalité connue, pertinente et légalement fondée.***

Les Données Personnelles sont collectées et traitées par Sodexo pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement d'une manière incompatible avec ces finalités.

## RÈGLE 4 - GARANTIR LA MINIMISATION DES DONNÉES

***RÈGLE 4 - Sodexo garantit que les Données Personnelles traitées sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont initialement collectées et traitées.***

Sodexo garantit que les Données Personnelles collectées, traitées et stockées sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont initialement collectées et traitées.

## RÈGLE - 5 GARANTIR L'EXACTITUDE

***RÈGLE 5 - Sodexo maintient les Données Personnelles traitées exactes et, le cas échéant, à jour.***

Lorsque les Données Personnelles sont inexactes, compte tenu des finalités pour lesquelles elles sont traitées, Sodexo prend toutes les mesures raisonnables pour effacer ou rectifier les Données Personnelles. Afin de s'assurer que les Données Personnelles détenues par Sodexo restent exactes et à jour, Sodexo encourage activement les Personnes Concernées à informer Sodexo de tout changement. Sodexo prévoit également de développer des interfaces et des outils conviviaux permettant aux Personnes Concernées de mettre directement à jour leurs Données Personnelles.

Sodexo, le Responsable du Traitement, informe chaque entité Sodexo à laquelle les Données Personnelles ont été divulguées de toute rectification ou suppression de données.

Sodexo, le Responsable du Traitement, 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 ne conserve les Données Personnelles qu'aussi longtemps que nécessaire.***

Les Données Personnelles traitées par Sodexo sont conservées sous une forme permettant d'identifier les Personnes Concernées pendant une durée n'excédant pas celle nécessaire pour remplir les finalités pour lesquelles les Données Personnelles sont traitées et conformément à la Politique Globale de Collecte et de Conservation des Données de Sodexo (Annexe 6) et les périodes de conservation des données définies.

Cependant, les Données Personnelles sont conservées pendant des périodes plus longues à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ou tel que requis par la réglementation locale applicable, par exemple la législation de l'UE/EEE.

Sodexo dispose des Données Personnelles de manière sécurisée conformément à la Politique de Sécurité des Systèmes d'Informations du Groupe.

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

***RÈGLE 7.A - Sodexo traite les Données Personnelles conformément à la Politique de Sécurité des Systèmes d'Informations du Groupe Sodexo.***

Les Données Personnelles sont traitées par Sodexo conformément à la Politique de des Systèmes d'Informations du Groupe, qui est révisée et mise à jour occasionnellement de manière à garantir une sécurité appropriée des Données Personnelles, y compris la protection contre le Traitement non autorisé ou illégal et contre la perte, la destruction accidentelle ou les dommages aux données, en utilisant des mesures de sécurité techniques ou organisationnelles appropriées. Sodexo met en œuvre des mesures de sécurité renforcées pour traiter les Données Personnelles Sensibles.

Sodexo notifie les failles de sécurité aux Autorités de Contrôle et/ou aux Personnes Concernées comme l'exige le RGPD lorsqu'il prend connaissance d'une Violation des Données Personnelles conformément à la Directive de Sécurité du Groupe sur la gestion des incidents de sécurité relatifs aux systèmes d'information<sup>4</sup>.

---

<sup>4</sup> Document interne

**RÈGLE 7.B - Sodexo garantit que tout sous-traitant, interne ou externe, agissant pour le compte d'une entité Sodexo, en tant que Responsable du Traitement, adopte les mesures de sécurité techniques et organisationnelles appropriées.**

Lorsque Sodexo agit en tant que Responsable de Traitement, il s'assure que lorsqu'il fait appel à un Sous-traitant, interne ou externe, ledit sous-traitant fournit des engagements écrits et documentés suffisants pour traiter les Données Personnelles conformément aux mesures techniques de sécurité et aux mesures organisationnelles appropriées régissant le Traitement à effectuer.

Lorsque Sodexo engage un sous-traitant interne (i) Sodexo utilise uniquement soit des entités de Sodexo basées dans l'UE/EEE ou dans un pays répondant aux conditions requises, soit des entités de Sodexo situées en dehors de l'UE/EEE qui ont adhéré à la présente Politique en tant que Responsable du Traitement ; et, (ii) le Sous-traitant interne s'engage à respecter les obligations énoncées à l'article 28 du RGPD.

Si Sodexo fait appel à des sous-traitants externes, le Traitement est régi par un contrat ou un autre acte juridique en vertu du droit de l'Union ou d'un État membre, qui lie le sous-traitant à l'égard de Sodexo et qui définit l'objet et la durée du Traitement, la nature et la finalité du Traitement, le type de Données Personnelles et les catégories de Personnes Concernées ainsi que les obligations et les droits du Responsable du Traitement.

Ce contrat ou autre acte juridique stipule, en particulier, que le sous-traitant :

- (i) traite les Données Personnelles uniquement sur instructions documentées de Sodexo, y compris en ce qui concerne les transferts de Données Personnelles vers un pays tiers ou une organisation internationale, sauf si cela est requis par le droit de l'Union ou d'un État membre auquel le Sous-traitant est soumis ; dans ce cas, le Sous-traitant informera Sodexo de cette exigence légale avant le Traitement, à moins que cette législation n'interdise de telles informations pour des motifs importants d'intérêt public ;
- (ii) garantit que les personnes autorisées à traiter les Données Personnelles se sont engagées à respecter la confidentialité ou sont soumises à une obligation légale de confidentialité appropriée ;
- (iii) prend toutes les mesures requises en vertu de l'Article 32 du RGPD ;
- (iv) respecte les conditions visées aux paragraphes 2 et 4 de l'Article 28 du RGPD pour engager un autre Sous-traitant ;
- (v) compte tenu de la nature du Traitement, assiste Sodexo dans la mesure du possible avec des mesures techniques et organisationnelles appropriées, pour satisfaire l'obligation de Sodexo de répondre aux demandes d'exercice des droits de la Personne Concernée prévue au Chapitre III du RGPD ;

- (vi) aide Sodexo à satisfaire les obligations prévues aux Articles 32 à 36 du RGPD en tenant compte de la nature du Traitement et des informations dont dispose le Sous-traitant ;
- (vii) au choix de Sodexo, supprime ou restitue toutes les Données Personnelles à Sodexo après la fin de la prestation de services relative au Traitement, et supprime les copies existantes à moins que la législation de l'Union ou d'un État membre n'exige la conservation des Données Personnelles ;
- (viii) met à disposition de Sodexo toutes les informations nécessaires pour démontrer le respect des obligations prévues à l'article 28 du RGPD, pour permettre et contribuer à la réalisation des audits, y compris les inspections, réalisés par Sodexo ou un autre auditeur mandaté par Sodexo.

Le Sous-traitant informera immédiatement Sodexo s'il pense qu'une instruction enfreint le RGPD ou d'autres dispositions de l'Union ou des États membres en matière de Protection des Données.

Sans préjudice d'un contrat individuel entre Sodexo et le Sous-traitant, le contrat ou l'autre acte juridique visé ci-dessus peut être fondé, en tout ou en partie, sur des clauses contractuelles types de la Commission européenne, y compris lorsqu'ils font partie d'une certification accordée au Responsable du Traitement ou au sous-traitant conformément aux Articles 42 et 43 du RGPD.

***RÈGLE 7.C - Sodexo signale toute violation de Données Personnelles aux autorité(s) de contrôle compétente(s) et/ou aux Personnes Concernées pertinentes, le cas échéant, conformément à la Directive de Sécurité du Groupe sur la Gestion des Incidents de Sécurité relatifs aux Systèmes d'Information.***

En cas de violation de Données Personnelles, la violation est notifiée à Sodexo SA, en tant que siège au sein de l'UE, et, en particulier, à l'équipe dédiée à la Protection des Données du Groupe et aux points de contact locaux dédiés la Protection des Données.

Cette violation de Données Personnelles est notifiée aux Autorité(s) de Contrôle pertinente(s) sans retard injustifié, et en tout état de cause dans les 72 heures suivants après en avoir pris sa connaissance, sauf si la violation a peu de probabilité d'entraîner un risque pour les droits et libertés des Personnes Concernées.

Le Délégué à la Protection des Données du Groupe et les points de contact locaux dédiés à la Protection des Données dans leurs juridictions respectives conservent des registres documentés de toutes les violations de Données Personnelles, comprenant les faits et les effets de la violation et toute mesure corrective prise. Ces registres sont mis à la disposition des Autorités de Contrôle sur demande.

Dans le cas où une violation de Données Personnelles est susceptible d'entraîner un risque élevé pour les droits et libertés des Personnes Concernées, les Personnes Concernées pertinentes en sont informées sans délai injustifié, sauf si Sodexo en est dispensé conformément au RGPD.

## 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 d'autres catégories particulières de Données Personnelles uniquement si cela est strictement nécessaire pour atteindre la finalité du Traitement des Données Personnelles et s'il existe une base légale pour le faire.***

Sodexo traite des Données Personnelles Sensibles et d'autres catégories particulières de Données Personnelles si :

la Personne Concernée a donné son consentement explicite au Traitement ;

- (i) Le Traitement est nécessaire aux fins de l'exécution des obligations de Sodexo et de l'exercice de ses droits spécifiques ou des droits de la Personne Concernée en vertu des réglementations locales applicables en matière d'emploi, de sécurité sociale et de protection sociale ou d'une convention collective en vertu de la réglementation locale ;
- (ii) Le Traitement est nécessaire pour protéger les intérêts vitaux de la Personne Concernée ou d'une autre personne physique lorsque la Personne Concernée est physiquement ou juridiquement incapable de donner son consentement ;
- (iii) Le Traitement porte sur des Données Personnelles qui sont manifestement rendues publiques par la Personne Concernée ;
- (iv) Le Traitement est nécessaire à la constatation, à l'exercice ou à la défense de droit en justice ;
- (v) Le Traitement est nécessaire pour des raisons d'intérêt public important, sur la base de la réglementation locale applicable ;
- (vi) Le Traitement est nécessaire à des fins de médecine préventive ou de médecine du travail, de l'appréciation de la capacité de travail des employés, du diagnostic médical, de la prise en charge sanitaire ou sociale ou de la gestion des systèmes et services de santé ou de protection sociale sur la base de la réglementation locale ou en vertu d'un contrat conclu avec un professionnel de santé ;
- (vii) Le Traitement est nécessaire pour des raisons d'intérêt public dans le domaine de la santé publique, telles que la protection contre les menaces transfrontières graves pour la santé ou pour la garantie de normes élevées de qualité et de sécurité des soins de santé et des médicaments ou dispositifs médicaux, sur la base de la réglementation locale applicables ;

(viii) Le Traitement est nécessaire à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.

Dans ce cas, Sodexo limite l'accès aux Données Personnelles Sensibles et aux autres catégories particulières de Données Personnelles aux personnes appropriées et traite ces données, conformément à la Politique de Sécurité des Systèmes d'Informations et du Groupe.<sup>5</sup>

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

***RÈGLE 9 - Sodexo conserve des registres de ses activités de traitement en tant que Responsable du Traitement.***

Sodexo conserve des registres de ses activités de traitement de son Responsable du Traitement, par écrit, dans un outil de conformité dédié et conformément à l'Article 30.1 du RGPD.

Les registres doivent contenir les informations suivantes :

- (i) le nom et les coordonnées du Responsable du Traitement et, le cas échéant, du Responsable du Traitement conjoint, du représentant du Responsable du Traitement et du Délégué à la Protection des Données ;
- (ii) la finalité du traitement ;
- (iii) une description des catégories de Personnes Concernées et des catégories de Données Personnelles ;
- (iv) les catégories de destinataires auxquels les Données Personnelles ont été ou seront divulguées, y compris les destinataires dans des pays tiers ou des organisations internationales ;
- (v) le cas échéant, les transferts de Données Personnelles vers un pays tiers ou une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'Article 49, paragraphe 1, deuxième alinéa, du RGPD, la documentation des sauvegardes appropriées ;
- (vi) dans la mesure du possible, les délais envisagés pour l'effacement des différentes catégories de données ;

---

<sup>5</sup> Document interne.

- (vii) si possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'Article 32, paragraphe 1, du RGPD 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 pertinentes.

En outre, Sodexo se conforme à toutes les exigences locales applicables supplémentaires, qui nécessitent un niveau de protection plus élevé pour les Données Personnelles, en termes de tenue de registres des activités de Traitement des données ou aux exigences de déclaration.

## RÈGLE 10 - RESPECTER LES DROITS DES PERSONNES CONCERNÉES

### ***RÈGLE 10 - Sodexo respecte les droits des Personnes Concernées.***

Les Personnes Concernées ont droit à ce qui suit :

#### **Le droit d'accès**

La Personne Concernée a accès à ses Données Personnelles qui sont traitées par Sodexo.

#### **Droit de rectification ou d'effacement/droit à l'oubli**

La Personne Concernée a le droit d'obtenir de Sodexo sans retard injustifié la rectification des Données Personnelles inexactes la concernant ou le droit de faire compléter les Données Personnelles incomplètes.

La Personne Concernée a le droit d'obtenir de Sodexo l'effacement de ses Données Personnelles dans les meilleurs délais notamment (i) lorsque les Données Personnelles ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées, (ii) la Personne Concernée retire son consentement sur lequel le Traitement est fondé, ou et lorsqu'il n'y a pas d'autre justification légale pour le traitement, (iii) la Personne Concernée s'oppose au traitement, (iv) les Données Personnelles ont été traitées illégalement, (v) les Données Personnelles doivent

être effacées pour se conformer à une obligation légale en vertu de la réglementation locale applicable, (vi) les Données Personnelles ont été collectées pour l'offre de services de la société de l'information<sup>6</sup> (ex : services de commerce électronique, sites internet publics).

Sodexo notifie la Personne Concernée lorsqu'elle ne peut répondre favorablement à ce droit d'effacement/droit à l'oubli car les Données Personnelles sont nécessaires (i) à l'exercice du droit à la liberté d'expression et d'information, (ii) au respect d'une obligation légale, (iii) pour des raisons d'intérêt public dans le domaine de la santé publique, (iv) à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, (v) pour la constatation, l'exercice ou la défense de droits en justice.

### **Droit d'opposition**

La Personne Concernée a le droit de s'opposer, à tout moment, au Traitement de ses Données Personnelles qui sont utilisées à des fins de marketing ou qui conduit Sodexo à prendre une décision fondée uniquement sur un Traitement automatisé, y compris le profilage, et qui produit des effets juridiques concernant une Personne Concernée ou l'affecte de manière significative de manière similaire, et sur la base des motifs suivants :

- l'exécution d'une mission d'intérêt général ou relevant de l'exercice de l'autorité publique dont est investi Sodexo ;
- aux fins des intérêts légitimes poursuivis par Sodexo ou par un tiers.

Si la Personne Concernée exerce ce droit d'opposition, Sodexo ne traite plus les Données Personnelles à moins que Sodexo ne démontre des motifs légitimes impérieux pour le Traitement ou pour la constatation, l'exercice ou la défense d'un droit en justice.

Toutefois, si la Personne Concernée s'oppose au Traitement à des fins de marketing direct, les Données Personnelles ne sont plus traitées à ces fins.

### **Droit de limitation**

La Personne Concernée a le droit d'obtenir de Sodexo la limitation du traitement lorsque (i) l'exactitude des Données Personnelles est contestée par la Personne Concernée, pendant une période permettant à Sodexo de vérifier l'exactitude des Données Personnelles, (ii) le traitement est illégal et la Personne Concernée s'oppose à l'effacement des Données Personnelles et demande à la place, une limitation de leur utilisation, (iii) Sodexo n'a plus besoin des Données Personnelles aux fins du traitement, mais la Personne Concernée en a besoin pour l'établissement, l'exercice ou la défense d'une réclamation fondée en droit, (iv) la Personne Concernée s'est opposée au traitement, la restriction s'applique dans l'attente de la vérification si les motifs légitimes de Sodexo prévalent sur ceux de la Personne Concernée.

---

<sup>6</sup> Aux termes de l'Article 1 paragraphe 2, de la Directive 98/34/CE, « services de la société de l'information » désigne tout service normalement fourni contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services. Aux fins du RGPD, les « services de la société de l'information » désignent un service tel que défini à l'Article 1, paragraphe 1, point b), de la Directive (UE) 2015/1535 du Parlement européen et du Conseil, essentiellement tout service demandé et fourni sur Internet, « tout service normalement fourni contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services ».

La Personne Concernée ayant obtenu la limitation du Traitement est informée par Sodexo avant la levée de la limitation du Traitement.

### **Droit à la portabilité**

La Personne Concernée a le droit de recevoir ses Données Personnelles, qu'elle a fournies à Sodexo, dans un format structuré, couramment utilisé et lisible par une machine et a le droit de transmettre ces données à un autre prestataire de services ou à un tiers.

Ce droit à la portabilité s'applique, sous réserve des droits et libertés d'autrui, dans les cas suivants :

- le Traitement est fondé sur le consentement ou sur un contrat ; et
- le Traitement est effectué de façon automatique.

Les Personnes Concernées sont informées de leurs droits et de la manière dont elles peuvent exercer leurs droits dans la Politique Globale de gestion des Protection des Données, comme indiqué à l'Annexe 7.

Sodexo répond aux Personnes Concernées dans un délai raisonnable et dans le respect du temps de réponse requis en vertu du RGPD ou de toute autre réglementation locale applicable, qui a un temps de réponse requis plus strict.

### **Droit de porter plainte**

La Personne Concernée a le droit de déposer une plainte conformément à la règle 17 des BCR auprès de l'Autorité de Contrôle du pays où elle réside habituellement, de son lieu de travail ou du lieu de l'infraction alléguée, que la personne ait ou non subi des dommages. En outre, la Personne Concernée a le droit d'introduire une réclamation auprès du tribunal où Sodexo a un établissement ou auprès duquel la personne a sa résidence habituelle.

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

***RÈGLE 11 - Sodexo ne procède à aucune évaluation et ne prend aucune décision à propos des Personnes Concernées susceptible de les affecter de manière significative ou de produire des effets juridiques les concernant et fondée uniquement sur un Traitement automatisé de leurs Données Personnelles, y compris le profilage, sauf dans certains cas limités et avec la mise en place des moyens appropriés.***

Sodexo ne procède à aucune évaluation ni ne prend aucune décision à propos des Personnes Concernées susceptible de les affecter de manière significative ou de produire des effets juridiques les concernant du seul fait d'un Traitement automatisé de leurs Données Personnelles, y compris le profilage, sauf dans les cas suivants, notamment lorsque c'est :

- une nécessité à la conclusion ou à l'exécution d'un contrat entre la Personne Concernée et Sodexo ;
- autorisée par la réglementation locale applicable à laquelle Sodexo est soumise et qui prévoit des mesures appropriées pour sauvegarder les droits et libertés et les intérêts légitimes de la Personne Concernée, notamment si cette réglementation locale exige un niveau de Protection des Données Personnelles plus élevé ; ou alors
- repose sur le consentement explicite de la Personne Concernée.

Dans ce cas, Sodexo met en œuvre les mesures appropriées pour sauvegarder les droits et libertés et les intérêts légitimes de la Personne Concernée, qui doivent inclure au moins le droit d'obtenir une intervention humaine de la part du Responsable du Traitement, d'exprimer son point de vue et de contester les décisions et toute autre garantie requise par la réglementation locale applicable.

Sodexo ne mène pas d'activités de décision ou de profilage automatisées sur des catégories particulières de données à moins que des garanties appropriées ne soient en place pour protéger les droits et les intérêts légitimes de la Personne Concernée.

Sodexo informe clairement la Personne Concernée des conditions du traitement automatisé des Données Personnelles et des garanties mises en place pour protéger les droits et intérêts légitimes de la Personne Concernée.

En outre, Sodexo ne met pas en œuvre un tel Traitement automatisé des Données Personnelles, y compris le profilage, sans procéder à une analyse d'impact sur la Protection des Données, comme décrit dans la Règle 15 de la présente Politique en tant que Responsable du Traitement.

## RÈGLE 12 - TRANSPARENCE ET INFORMATIONS DE LA PERSONNE CONCERNÉE

***RÈGLE 12.A - Sodexo met la Politique en tant que Responsable du Traitement à la disposition des Personnes Concernées.***

Sodexo met la Politique en tant que Responsable du Traitement à la disposition des Personnes Concernées en la publiant sur son site internet officiel. Par ailleurs, la Politique Globale de Sodexo relative à la Protection des Données (Annexe 2) comprend une clause dédiée sur les droits des tiers bénéficiaires.

***RÈGLE 12.B - Sodexo s'engage à fournir aux Personnes Concernées des avis d'information complets et des politiques de Protection des Données, le cas échéant, avant la collecte et à traiter leurs Données Personnelles conformément au RGPD et à toute autre réglementation locale applicable qui exigerait un niveau de protection plus élevé pour les Données Personnelles, ex : la législation de l'UE.***

Sodexo s'engage à fournir aux Personnes Concernées des notices d'information complètes et des politiques de Protection des Données telles que la Politique Globale de Sodexo relative à la Protection des Données (en Annexe 2), conformément au Tableau sur la transparence (Annexe 3) ou, le cas échéant, via une approche à plusieurs niveaux, avant la collecte et de traiter leurs Données Personnelles conformément au RGPD et à toute réglementation locale applicable exigeant un niveau de protection plus élevé des Données Personnelles, par exemple la législation de l'UE.

Toutes les Personnes Concernées bénéficiant notamment des droits de tiers bénéficiaire reçoivent l'intégralité des informations requises par le RGPD, sur leurs droits de tiers bénéficiaire à l'égard du Traitement de leurs Données Personnelles et sur les moyens d'exercer ces droits, sur la clause relative à la responsabilité et sur les clauses relatives aux principes de Protection des Données.

## RÈGLE 13 - ASSURER UNE PROTECTION ADÉQUATE POUR LES TRANSFERTS TRANSFRONTALIERS DE DONNÉES PERSONNELLES

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

Les transferts transfrontaliers de données à des tierces parties externes au Groupe Sodexo (ou à une entité Sodexo qui n'est pas liée par la présente Politique en tant que Responsable du Traitement) situées en dehors de l'UE/EEE ou dans un pays qui n'est pas reconnu par la Commission européenne comme un Pays Adéquat ne sont pas autorisés sans la mise en place de garanties adéquates, telles que la signature d'un accord de transfert de données basé sur les clauses contractuelles types de la Commission européenne, et le cas échéant, l'implémentation de mesures additionnelles nécessaires conformément à l'arrêt Schrems II<sup>7</sup>, et aux lignes directrices applicables du CEPD, qui peuvent être modifiées occasionnellement.

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

***RÈGLE 14 - Sodexo adopte les principes de Protection des Données dès la conception pour chaque nouveau projet numérique ou nouvelle opportunité commerciale impliquant le traitement des Données Personnelles et de Protection des Données par défaut en formant le personnel traitant les Données Personnelles et en mettant en œuvre des procédures pour garantir que chaque fois que des Données Personnelles sont traitées, des mesures techniques et organisationnelles appropriées sont mis en place.***

### Protection des Données dès la conception

Lorsqu'un nouveau projet numérique ou une nouvelle opportunité commerciale est initié, impliquant un traitement de Données Personnelles, la Protection des Données est prise en compte, au moment où sont définis les moyens et les mesures de sécurité techniques et organisationnelles appropriées associées pour le Traitement des Données Personnelles et lors de la mise en œuvre du Traitement. Le même principe s'applique lorsque Sodexo envisage de fusionner ou d'acquérir une entreprise, il s'assure que les principes de Protection des Données sont respectés.

<sup>7</sup> Décision C-311/18 - Facebook Irlande et Schrems de la Cour de justice de l'Union Européenne du 16 juillet 2020 - Commissaire à la Protection des Données contre Facebook Ireland Limited et Maximilian Schrems

Sodexo a développé une procédure globale de conformité des projets à la protection des données dès leur conception comprenant un processus d'évaluation des risques liés à la Protection des Données à l'usage des opérationnels, des propriétaires d'applications informatiques et des chefs de projet impliqués dans les projets mentionnés ci-dessus.

### **Protection des Données par défaut**

Sodexo forme le personnel traitant les Données Personnelles et met en place des procédures pour s'assurer qu'à chaque Traitement de Données Personnelles, des mesures techniques et organisationnelles appropriées sont prises pour s'assurer que, par défaut, seules les Données Personnelles nécessaires à chaque finalité spécifique sont traitées (quantité de données traitées, étendue du Traitement et conservation des données) et n'est accessible qu'à un nombre limité de personnes qui ont besoin d'en avoir connaissance.

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

***RÈGLE 15 - Sodexo procède à une analyse d'impact sur la Protection des Données (AIPD) lorsque cela est nécessaire.***

Pour tous les projets impliquant le traitement de Données Personnelles, un processus d'évaluation des risques liés à la Protection des Données de bout en bout est effectué pour vérifier la conformité aux principes de Protection des Données, évaluer l'impact sur les droits des Personnes Concernées et vérifier la mise en œuvre de la Protection des Données dès la conception et par défaut.

Ce processus comprend un questionnaire d'évaluation des risques liés à la vie privée (le « PRAQ ») visant à collecter toutes les informations nécessaires pour effectuer une analyse des risques du projet/processus en vertu de la Réglementation applicable en matière de Protection des Données et pour vérifier si une analyse complète de l'impact sur la Protection des Données (« AIPD ») est requise conformément à la procédure globale de conformité des projets à la protection des données dès leur conception. Cette procédure permet également de déterminer si un nouveau registre d'activité de Traitement des données doit être créé dans l'outil de conformité RGPD de Sodexo ou si une mise à jour d'un registre existant doit être effectuée.

Conformément à la procédure globale de conformité des projets à la protection des données dès leur conception et à l'Article 35, paragraphe 3, du RGPD, une AIPD sera requise si le traitement implique :

- (i) une évaluation systématique et approfondie des aspects personnels relatifs aux personnes physiques qui repose sur un traitement automatisé, y compris le profilage, et sur laquelle sont fondées des décisions produisant des effets juridiques concernant la personne

physique ou affectant de manière significative la personne physique de manière similaire ;

- (ii) Un traitement à grande échelle de catégories particulières de données visées à l'Article 9, paragraphe 1 du RGPD, ou de Données Personnelles relatives à des condamnations pénales et à des infractions visées à l'Article 10 du RGPD ; ou alors
- (iii) une surveillance systématique d'une zone accessible au public à grande échelle.

Lors de la réalisation d'une AIPD, l'équipe dédiée à la Protection des Données du Groupe et/ou les points de contact locaux dédiés à la Protection des Données impliquent les parties prenantes internes concernées.

Une AIPD commence prématurément dans la vie d'un projet, mais peut se dérouler parallèlement au processus de mise en œuvre du projet. Lorsqu'une AIPD indique que le Traitement des Données Personnelles entraînerait un risque élevé en l'absence de mesures prises par le Responsable du Traitement pour atténuer les risques, l'Autorité de Contrôle compétente, avant le Traitement, est consultée.

## Section B

### RÈGLE 16 - FORMATION ET SENSIBILISATION

***RÈGLE 16 - Sodexo dispense une formation appropriée 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 Responsable du Traitement exécutoire 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 ces BCR.

Un module général est destiné à fournir une formation de base sur les principes de Protection des Données à tous les employés de Sodexo, tandis que des modules spécifiques sont destinés aux employés des entités de 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 Sodexo.

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 aux réglementations locales en tenant compte de leurs exigences spécifiques.

#### Suivi du programme de formation

Les entités de 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 Responsable du Traitement.

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 - GÉRER LES DROITS RELATIFS A LA PROTECTION DES DONNÉES

***RÈGLE 17 - Sodexo répond aux demandes, questions et préoccupations des Personnes Concernées et aux questions des Autorités de Contrôle qui suivent une plainte des Personnes Concernées.***

Les entités de Sodexo mettent en place un système local de Traitement des demandes et des réclamations conformément à la Procédure Globale de gestion des droits de Protection des Données<sup>8</sup>.

Le point de contact local dédié à la Protection des Données répond aux demandes des Personnes Concernées dans les meilleurs délais et, en tout état de cause, au plus tard dans le mois suivant la réception de la demande. Ce délai peut être prolongé de deux mois si nécessaire, compte tenu de la complexité et du nombre des demandes. Sodexo informe la Personne Concernée d'une telle prolongation dans un délai d'un mois à compter de la réception de la demande, en spécifiant les motifs du retard. La Personne Concernée est informée de : (i) comment exercer ses droits et quelles sont les étapes à suivre ; (ii) sous quelle forme ; (iii) le délai de réponse à la demande ; (iv) les conséquences si la demande est rejetée ; (v) les conséquences si la demande est considérée comme justifiée ; (vi) s'ils estiment que leurs droits en matière de Protection des Données peuvent avoir été violés, ils sont autorisés à déposer une plainte auprès de l'Autorité de Contrôle du pays de leur résidence habituelle, de leur lieu de travail ou du lieu de violation alléguée, si la personne a subi un dommage et auprès du tribunal du lieu où Sodexo a un établissement ou de sa résidence habituelle, conformément à la Politique Globale relative à la Protection des Données, y compris la Politique Globale de gestion des droits des Personnes Concernées figurant en Annexe 7, et/ou les politiques de Protection des Données locales, disponibles sur les sites internet officiels de Sodexo.

Lorsque l'entité de Sodexo a des doutes raisonnables concernant l'identité de la Personne Concernée à l'origine de la demande, l'entité de Sodexo peut demander la fourniture d'informations supplémentaires nécessaires pour confirmer l'identité de la Personne Concernée. Si nécessaire, les points de contact local dédié à la Protection des Données conseillent les Personnes Concernées sur les étapes pratiques de leur système local de Traitement des demandes et des réclamations.

Si le point de contact local dédié à la Protection des Données reçoit une requête ou une question liée à la Protection des Données ou des questions d'une Autorité de Contrôle de Protection des Données à la suite d'une plainte, il a le rôle, conformément à la procédure Globale de gestion des droits de Protection des Données<sup>9</sup>, d'expliquer, avec le soutien de l'opérationnel/de la

---

<sup>8</sup> Document interne

<sup>9</sup> Document interne

fonction concernée qui est responsable des activités de Traitement de données en jeu, aux Personnes Concernées ou à l'Autorité de Contrôle de Protection des Données de manière aussi détaillée que possible comment nous nous sommes conformés aux réglementations, que nous avons tout mis en œuvre pour trouver une solution appropriée ou, si quelque chose a échoué, de décrire les mesures prises pour y remédier.

## RÈGLE 18 - ÉVALUER LA CONFORMITÉ : PROGRAMME D'AUDIT

***RÈGLE 18 - Sodexo se conforme au Programme d'Audit des BCR de Sodexo en s'appuyant sur la Liste de Contrôle de Conformité aux BCR.***

Conformément au programme d'audit Global des BCR de Sodexo, Sodexo audite la conformité du Groupe Sodexo avec la Responsable Politique en tant que Responsable du Traitement et en particulier :

- Met en œuvre un plan d'audit qui couvre tous les aspects de la Politique en tant que Responsable du Traitement, y compris les méthodes permettant de s'assurer que les actions correctives auront lieu.
- Cet audit est réalisé annuellement par l'équipe de Contrôle Interne du Groupe.
- Cet audit est également réalisé par l'équipe d'Audit Interne du Groupe au besoin à la 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 exécutif 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 l'entité de Sodexo si nécessaire.

## RÈGLE 19 - SUIVRE LA MISE EN OEUVRE DES BCR

**RÈGLE 19 - Sodexo surveille la mise en œuvre de la Politique en tant que Responsable du Traitement.**

Pour assurer la mise en œuvre efficace de la Politique en tant que Responsable du Traitement, l'équipe dédiée à la Protection des Données du Groupe a établi un registre des risques. En outre, chaque signale les meilleures pratiques locales pour mettre en œuvre la Politique en tant que Responsable du Traitement ainsi que les analyses d'impact relatives à la Protection des Données effectuées localement à l'équipe dédiée à la Protection des Données du Groupe sur une base trimestrielle. Les rapports de signalements des points de contact locaux dédiés à la Protection des Données sont centralisés et analysés par l'équipe dédiée à la Protection des Données du Groupe. Les résultats de l'analyse font partie du rapport trimestriel 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 Responsable du Traitement, par le biais d'une structure de Gouvernance de la Protection des Données.**

Pour superviser et assurer le respect de la Politique en tant que Responsable du Traitement, Sodexo a mis en place 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 dédiée à la Protection des Données du Groupe dans ses missions ;
- un réseau de points de contact local 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 rapporte au plus haut niveau hiérarchique et bénéficie de leur soutien pour l'accomplissement de cette mission. Le Délégué à la Protection des Données du Groupe leur fournit des conseils et des recommandations concernant l'activité de Sodexo en tant que Responsable du Traitement ainsi qu'un rapport trimestriel sur les activités de à l'équipe dédiée à la Protection des Données du Groupe. En outre, l'équipe dédiée à la protection des données du Groupe surveille la conformité au niveau mondial et évalue 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 soutient les DP SPOCs lorsque cela est nécessaire 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, signale les problèmes majeurs liés à la Protection des Données au Délégué à Protection des Données du Groupe, et vérifie la conformité au niveau local et de est disponible, dans la langue locale, aux Personnes Concernées locales et à l'Autorité de Contrôle locale, sous la responsabilité de l'opérationnel/de la fonction locale.

## RÈGLE 21 - DROITS DES TIERS BÉNÉFICIAIRES

***RÈGLE 21 - Sodexo confère expressément aux Personnes Concernées le droit de faire respecter la Politique en tant que Responsable du Traitement.***

Les Personnes Concernées sont en mesure d'appliquer les éléments suivants de la Politique en tant que Responsable du Traitement aux entités de Sodexo :

- **Protection des Données** : Les Personnes Concernées peuvent appliquer les Règles 2 (licéité, loyauté et transparence), 3 (limitation de la finalité), 4 (minimisation des données), 5 (exactitude des données), 6 (limitation de la conservation), 8 (Données Personnelles Sensibles et autres catégories particulières de données) , 14 (Protection des Données dès la conception et par défaut) et 15 (analyse d'impact relative à la Protection des Données) de la Politique en tant que Responsable du Traitement.
- **Transparence de la Politique en tant que Responsable du Traitement** : Les Personnes Concernées ont un accès facile à leurs droits de tiers bénéficiaires puisque les BCR sont disponibles sur l'intranet et le site internet officiel de Sodexo. Ils peuvent obtenir une copie de cette Politique en tant que Responsable du Traitement sur demande auprès des membres des BCR agissant en qualité de responsables de Traitement. Par ailleurs, la Politique Globale à la Protection des Données (Annexe 2) comprendra une clause dédiée sur les droits des tiers bénéficiaires.
- **Droits des Personnes Concernées** : Les Personnes Concernées peuvent appliquer la Règle 10 en déposant une plainte conformément à la Politique Globale de gestion des droits des

Personnes Concernées, jointe à la Politique Globale relative à la Protection des Données de Sodexo (i) auprès de l'Autorité de Contrôle compétente contre l'entité Sodexo responsable de l'Exportation des Données et agissant en tant que Responsable du Traitement soit devant (a) l'autorité de surveillance de l'État membre de leur résidence habituelle, (b) leur lieu de travail ou (c) le lieu de l'infraction alléguée et (ii) devant les tribunaux compétents de l'État membre de l'UE/EEE (les Personnes Concernées ont le choix d'agir devant les juridictions où le Responsable du Traitement a un établissement ou de la localisation de leur lieu résidence).

- **Droit de réclamation** : Les Personnes Concernées peuvent porter plainte auprès d'un point de contact local dédié à la Protection des Données conformément à la Règle 17 et à la Politique Globale de gestion des droits des Personnes Concernées énoncées à l'Annexe 7, également disponible dans la Politique Globale relative à la Protection des Données. 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) et le fait que la Personne Concernée a le droit de déposer une réclamation devant le tribunal ou l'Autorité de Contrôle compétente.
- **Responsabilité** : Sodexo agissant en tant que Responsable du Traitement ou Responsable conjoint du traitement accepte la responsabilité et s'engage à prendre les mesures nécessaires pour remédier aux actes d'autres entités de Sodexo établies en dehors de l'UE/EEE liées par la Politique en tant que Responsable du Traitement et à verser une indemnisation pour tout dommage résultant d'une violation de la politique. Si une entité de Sodexo en dehors de l'UE/EEE enfreint la politique, les tribunaux ou les autorités compétentes en France seront compétents et la Personne Concernée aura les droits et recours contre Sodexo SA qui a accepté la responsabilité comme si la violation avait été causée en France en lieu et place de l'entité Sodexo concernée en dehors de l'UE/EEE. 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'État 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. Sodexo SA devra démontrer que l'entité de 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. S'il peut prouver que ladite entité de Sodexo n'est pas responsable du fait générateur du dommage, elle pourra se dégager de toute responsabilité.
- **Coopération** : les Personnes Concernées peuvent opposer la Règle 24.
- **Compensation** : Les Personnes Concernées ont droit à des recours judiciaires et à obtenir une réparation appropriée et, le cas échéant, à recevoir une indemnisation en cas de violation de l'un des éléments contraignants susmentionnés de la Politique en tant que Responsable du Traitement devant les tribunaux compétents des États membres de l'UE/EEE (au choix des Personnes Concernées : soit devant les tribunaux où le Responsable du Traitement a un établissement ou soit de leur lieu de résidence).

- **Transparence lorsque la législation et les pratiques nationales empêchent le Groupe de se conformer aux BCR** : les Personnes Concernées peuvent appliquer la Règle 23.

## RÈGLE 22 - RESPONSABILITÉ

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

Lorsqu'une Personne Concernée subit un dommage car ses Données Personnelles n'ont pas été traitées conformément à la Politique en tant que Responsable du Traitement, Sodexo SA, agissant en tant que Responsable ou Responsable Conjoint du Traitement, accepte la responsabilité et s'engage à prendre les mesures nécessaires pour remédier aux actes d'autres entités de Sodexo établies en dehors de l'UE/EEE liées par la Politique en tant que Responsable du Traitement et de verser une indemnisation pour tout dommage matériel ou immatériel résultant d'une violation de la politique.

Si une entité de Sodexo située en dehors de l'UE/EEE enfreint les BCR, les tribunaux ou les autres autorités compétentes en UE seront compétents et la Personne Concernée aura les droits et recours contre Sodexo SA qui a accepté la responsabilité comme si la violation avait été causée dans l'État Membre en lieu et place de l'entité de Sodexo concernée située en dehors de l'UE/EEE.

Sodexo SA devra démontrer que l'entité de Sodexo située 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. S'il peut prouver que ladite entité de 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 DE LA POLITIQUE EN TANT QUE RESPONSABLE DU TRAITEMENT - DEMANDE JURIDIQUEMENT CONTRAIGNANTE DE COMMUNICATION DES DONNÉES PERSONNELLES**

***RÈGLE 23.A - Sodexo procède à une évaluation de la réglementation 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 Responsable du Traitement et qu'elles n'ont pas d'effet substantiel sur sa capacité à se conformer à la présente Politique, en particulier pour garantir que les droits exécutoires des Personnes Concernées et des recours juridiques efficaces pour les Personnes Concernées sont disponibles.***

***RÈGLE 23.B - Toute entité de Sodexo s'assure que lorsqu'elle a des raisons de croire que la réglementation ou les pratiques locales applicables l'empêchent de remplir ses obligations en vertu de la Politique en tant que Responsable du Traitement et ont un effet substantiel sur sa capacité à se conformer à la présente Politique, elle en informera rapidement Sodexo SA et le Délégué à la Protection des Données du Groupe et l'entité de Sodexo agissant comme l'Exportateur de Données et tout autre point de contact local dédié à la Protection des 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 Responsable du Traitement, il notifie Sodexo SA, le Délégué à la Protection des Données du Groupe Sodexo, l'entité Sodexo agissant en tant qu'Exportateur de Données et, si possible, la Personne Concernée, sauf interdiction de le faire par une autorité chargée de l'application de la loi. Cette notification comprendra, entre autres, des informations sur les données demandées, le nombre de demandes, l'organisme demandeur et la base juridique de la communication.***

### **Évaluation de la législation et des pratiques locales applicables**

Conformément aux recommandations du CEPD<sup>10</sup> ; et les clauses contractuelles types de l'Union européenne<sup>11</sup>:

Les entités de Sodexo garantissent qu'elles n'ont aucune raison de croire que la réglementation et les pratiques locales applicables les empêchent de remplir leurs obligations en vertu de la Politique en tant que Responsable du Traitement ou leurs obligations contractuelles avec le Responsable du Traitement et qu'elles n'ont pas un effet substantiel sur leur capacité à se

<sup>10</sup> 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.

<sup>11</sup> 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 conformément au Règlement (UE) 2016/679 du Parlement Européen et du Conseil.

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 Responsable du Traitement.

Sodexo déclare qu'en fournissant cette garantie, il a dûment tenu compte, avec l'aide 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 réglementation 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 Responsable du Traitement 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 de l'Autorité de Contrôle compétente sur demande.

En outre, si une entité de Sodexo située en dehors de l'UE/EEE a des raisons de croire qu'elle est ou est devenue soumise à des lois et/ou pratiques non conformes aux exigences de la Politique en tant que Responsable du Traitement, elle en informera rapidement Sodexo SA, le Délégué à la Protection des Données du Groupe, tout autre point de contact local dédié à la Protection des Données pertinent, en particulier le point de contact local dédié à la Protection des Données de l'entité de Sodexo agissant en tant qu'Exportateur de Données, et l'entité Sodexo agissant en tant qu'Exportateur de Données.

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 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.

L'entité de Sodexo responsable de l'Exportation des Données 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 Responsable du Traitement ne doit pas faire partie des BCR-RT

### **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 loi 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 responsable de l'Exportation des Données, et si possible, la Personne Concernée (le cas échéant, avec l'aide de l'entité Sodexo agissant en tant qu'Exportateur de Données).

Les parties prenantes susmentionnées sont clairement informées de la demande, y compris, mais sans s'y limiter, des informations sur les données demandées, le nombre de demandes, l'organisme demandeur et la base juridique de la communication (sauf interdiction contraire par une autorité chargée de l'application de la loi, telles que l'interdiction en vertu du droit pénal de préserver la confidentialité d'une enquête des forces de l'ordre).

Si dans des cas particuliers où la suspension et/ou la notification sont interdites, l'entité de 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 leurs efforts, les entités sollicitées de Sodexo ne sont pas en mesure d'informer les parties prenantes concernées, elles leur fournissent annuellement des informations générales sur les demandes reçues.

Les entités de Sodexo s'engagent à conserver les informations concernant la demande de communication des Données Personnelles ou tout accès direct aux Données Personnelles par une autorité chargée de l'application de la loi ou un organisme de sécurité de l'État, et les meilleurs efforts qu'elles ont déployés pour informer les parties prenantes susmentionnées comme décrit ci-dessus.

Les entités de Sodexo ne procèdent pas à des transferts massifs, disproportionnés et aveugles des Données Personnelles à une quelconque autorité publique 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 réglementation 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.

## RÈGLE 24 - COOPÉRATION AVEC LES AUTORITÉS DE CONTRÔLE

### ***RÈGLE 24 - Sodexo respecte la procédure de mise à jour des BCR.***

Dans le cadre de la Politique en tant que Responsable du Traitement, les entités de Sodexo adhérant aux BCR se conforment à la Procédure de coopération des BCR en Annexe 4 et, en particulier, coopèrent avec les Autorités de Contrôle et acceptent d'être auditées par les Autorités de Contrôle et se conforment à l'avis de ces Autorités de Contrôle sur toutes questions liées à cette politique.

## 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 5, Sodexo signale rapidement les changements significatifs à toutes les entités de Sodexo adhérant aux BCR et aux Autorités de Contrôle pertinentes, via l'Autorité de Contrôle compétente (l'Autorité de Contrôle française, la CNIL).

Par ailleurs, les mises à jour des BCR ou de la liste des entités de Sodexo adhérentes aux BCR sont suivies et enregistrées par le Délégué à la Protection des Données du Groupe, avec l'appui de l'Équipe Juridique du Groupe, qui fournira les informations nécessaires aux Personnes Concernées (via l'intranet de Sodexo et à des tiers sur le site internet officiel de Sodexo). Sodexo signale une fois par an toute modification administrative de la Politique en tant que Responsable du Traitement ou de la liste des entités de Sodexo membres aux BCR aux Autorités de Contrôle concernées, via l'Autorité de Contrôle compétente (l'occurrence la CNIL), en fournissant une brève explication des motifs justifiant la mise à jour.

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

Toute modification des BCR ou de la liste des entités de Sodexo membres aux BCR est signalée annuellement aux Autorités de Contrôle concernées via l'Autorité de Contrôle compétente avec une brève explication des motifs justifiant la mise à jour.

## RÈGLE 26 - CARACTERE CONTRAIGNANT DES BCR

***RÈGLE 26 - La Politique en tant que Responsable du Traitement est contraignante dans tout le Groupe Sodexo pour chaque membre des BCR, y compris leurs employés.***

Les BCR font partie de l'accord d'adhésion intra-groupe signé par toutes les entités de Sodexo et qui rend les BCR juridiquement contraignantes.

Lorsqu'un membre des BCR situé hors de l'EEE cesse de faire partie du Groupe Sodexo ou d'être lié par les BCR, cette entité de Sodexo continue d'appliquer les exigences des BCR pour le 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 lié par les BCR.

Les BCR ont été partagées avec tous les employés en tant que nouvelle politique de Protection des Données du Groupe et sont disponibles à tout moment sur l'intranet et le site internet officiel de Sodexo.

Les contrats de travail standard de Sodexo incluent des engagements pour les employés autorisés à traiter les Données Personnelles afin d'assurer la confidentialité et la conformité aux politiques de Protection des Données de Sodexo qui incluent les BCR.

Par ailleurs, les collaborateurs déjà en place bénéficient d'un accord individuel et distinct afin de se conformer aux politiques de Protection des Données de Sodexo dont font partie les BCR.

Dans les deux cas 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.

Le cas échéant, elles ont fait l'objet d'une information/consultation préalable du comité social et économique local, le cas échéant, afin de s'assurer que les employés bénéficient non seulement des principes de Protection des Données des BCR, mais les respectent également lors du Traitement des Données Personnelles dans le cadre de leur fonction.

# 04

## Annexes



- Annexe 1 : Définitions
- Annexe 2 : Politique Globale relative à la Protection des Données de Sodexo
- Annexe 3 - Tableau sur la transparence
- Annexe 4 : Procédure de coopération des BCR
- Annexe 5 : Procédure de mise à jour des BCR
- Annexe 6 - Politique Globale de collecte et de conservation des données (Responsable du Traitement)
- Annexe 7 : Politique Globale de gestion des droits des Personnes Concernées
- Annexe 8 - Description du champ d'application matériel de la Politique en tant que Responsable du Traitement

## Annexe 1 : Définitions

Lorsque l'objet des présentes définitions concerne des Données Personnelles, les termes et expressions sans majuscules 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 de la présente Politique en tant que Responsable du Traitement, la signification qui leur est attribuée ci-dessous.

- **Autorité de Contrôle** désigne une autorité publique indépendante établie par un État 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 entreprises qui demandent au Groupe Sodexo d'effectuer des services pour leur compte pour leurs employés / leur personnel sur place, qui sont les utilisateurs finaux de ces services.
- **Délégué à la Protection des Données du Groupe** désigne la personne nommée avec l'aval du Comité Exécutif 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** 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 Économique Européen.

- **Exportateur de Données** désigne un Responsable du Traitement ou un Sous-traitant (lorsqu'il agit au nom d'un autre Responsable du Traitement du Groupe) 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 Responsable du Traitement** 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 réglementation 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 à 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 Exécutif 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 autorisée aux Données Personnelles transmises, stockées ou autrement traitées.

## **Annexe 2 : Politique Globale relative à la Protection des Données 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 3 - Tableau sur la transparence

Type d'informations requises	Si les Données Personnelles sont collectées directement auprès des Personnes Concernées	Si les Données Personnelles ne sont pas collectées directement auprès des Personnes Concernées
Identité et coordonnées du Responsable du Traitement et, le cas échéant, de ses représentants <sup>12</sup>	X	X
Coordonnées du DPO	X	X
Finalités et base juridique du Traitement	X	X
Lorsque les intérêts légitimes constituent la base juridique du Traitement, les intérêts légitimes poursuivis par le Responsable du Traitement ou un tiers	X	X
Catégories des Données Personnelles concernées	NON REQUIS	X
Détails des transferts vers des pays tiers et garanties correspondantes applicables	X	X
La période de conservation (ou si ce n'est pas possible, les critères utilisés pour déterminer cette période)	X	X
Les droits d'accès de la Personne Concernée pour rectifier; effacer; limiter le Traitement ; s'opposer au Traitement et à la portabilité.	X	X
Lorsque le Traitement est fondé sur le consentement (ou consentement explicite), le droit de retirer son consentement à tout moment	X	X
Le droit d'introduire une réclamation auprès d'une Autorité de Contrôle	X	X

<sup>12</sup> Dans le cas où les Responsables de Traitement sont basés en dehors de l'UE.

04 Annexes

S'il existe une obligation légale ou contractuelle de fournir ces informations ou s'il est nécessaire de conclure un contrat ou s'il existe une obligation de fournir les informations et les conséquences possibles d'un manquement.

X

NON REQUIS

La source d'où proviennent les Données Personnelles et, le cas échéant, si elles proviennent d'une source accessible au public.

NON REQUIS

X

L'existence d'une prise de décision automatisée, y compris le profilage et, le cas échéant, des informations significatives sur la logique utilisée, l'importance et les conséquences envisagées d'un tel Traitement pour la Personne Concernée.

X

X

## Annexe 4 - 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 réglementation 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 (Annexe 5 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 de Sodexo adhérant aux BCR dans le but d'examiner la conformité aux BCR.

## Annexe 5 - 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 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 pour le compte de Sodexo. Sodexo fournira également une brève explication des motifs de tout changement substantiel communiqué apporté aux BCR.

### Changements administratifs

3. 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

4. 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.
5. 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

6. Le Délégué à la Protection des Données du Groupe, avec le soutien de l'Équipe Juridique du Groupe, (i) tiendra une liste entièrement mise à jour des entités de Sodexo adhérant aux BCR. et (ii) suivra et enregistra toutes les mises à jour des BCR et fournira les informations nécessaires aux Personnes Concernées ou aux Autorités de Contrôle sur demande.
7. 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 6 - Politique Globale de collecte et de conservation des Données (Responsable du Traitement)

## 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.

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, en tant que Responsable du Traitement, respecte les principes du RGPD ou de toute autre réglementation applicable en matière de Protection des Données.

## DÉFINITIONS

- **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 désigne soit un Client, soit une autre entité 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 Personnelles et à la libre circulation de ces données, abrogeant la Directive 95/46 /CE.
- **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.
- **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.

— **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.

I. Stockage des Données Personnelles dans le respect du principe de limitation de conservation

a. Définition d'une durée de conservation des Données Personnelles pour chaque finalité

Pour chaque finalité de traitement des Données Personnelles, une durée limite de conservation des données est définie.

Les durées de conservation des données peuvent différer selon la finalité du Traitement. Ces délais doivent être fixés en tenant compte de la finalité du Traitement et en tenant compte :

— de toute exigence légale locale imposant une période de conservation des données ;

— En l'absence d'exigences légales locales, les Données Personnelles ne doivent pas être conservées plus longtemps que nécessaire aux fins pour lesquelles elles sont collectées.

La définition d'une durée de conservation des données est un processus local. En effet, la définition d'une telle durée repose en premier lieu sur les exigences de toute réglementation locale qui pourrait prévoir une durée de conservation (ex : pour tout Traitement relatif aux RH, le droit du travail local doit être revu).

Si les réglementations locales ne prévoient pas de durée de conservation des données spécifique pour le Traitement pertinent, l'opérationnel concerné a la responsabilité de définir, en collaboration avec le point de contact local dédié à la Protection des Données et le responsable informatique, une durée de conservation des données spécifique qui est conforme au RGPD et à toute autre exigence applicable en matière de Protection des Données.

La période de conservation des données définie avec l'opérationnel garantit qu'une fois que la finalité du Traitement cesse d'exister et s'il n'existe aucune obligation légale de conserver les Données Personnelles, elles doivent être immédiatement rendues anonymes ou supprimées.

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

b. Mode actif

Les Données Personnelles seront accessibles en mode actif « selon les besoins » aux employés concernés de Sodexo pendant la période de conservation des données.

**c. Archive temporaire**

Les Données Personnelles peuvent être temporairement archivées avec un accès restreint lorsque la finalité pour laquelle elles ont été collectées n'existe plus :

*(a) Pour la durée du statut de la période de prescription : défense contre une action légale ou contractuelle potentielle ou actuelle ou future soulevée par des tiers, y compris les Personnes Concernées ; ou alors*

*(b) Pour se conformer à une obligation légale.*

**d. Archivage plus long**

Les Données Personnelles peuvent être conservées pendant des périodes plus longues à des fins statistiques.

Dans ce cas, veuillez contacter l'équipe dédiée à la protection des données du Groupe ou votre point de contact local dédié à la Protection des Données pour obtenir une approbation préalable afin de vous aider dans les étapes suivantes :

- Ne conservez que les Données Personnelles nécessaires à des fins statistiques ;
- Anonymisez les Données Personnelles conservées de manière irréversible dans la mesure du possible ;
- Si l'anonymisation n'est pas possible, pseudonymisez les Données Personnelles et assurez leur suppression dès que les finalités statistiques sont remplies ; en outre, archivez les données pseudonymisées dans un format séparé en lecture seule et ne donnez accès qu'au personnel concerné de manière ponctuelle.

**e. Effacement**

À la fin de la période de conservation des données (y compris le mode actif et l'archivage temporaire), Sodexo supprimera ou anonymisera les Données Personnelles de manière sécurisée.

Si les Données Personnelles ont été sous-traitées par un sous-traitant, Sodexo doit demander au Sous-traitant de supprimer ou de restituer les Données Personnelles au plus tard à la date de résiliation du contrat. Sodexo doit exiger du Sous-traitant qu'il fournisse une attestation confirmant la bonne suppression des Données Personnelles.

**II. Suivi de la mise en œuvre effective des durées de conservation des données définies.**

Une fois que la durée de conservation des données appropriée a été définie pour un Traitement de Données Personnelles donné (soit en raison d'une exigence légale locale, soit conjointement

avec un opérationnel), Sodexo assurera le suivi de sa mise en œuvre en respectant les étapes suivantes :

1. Assurez-vous que la durée de conservation des données pertinentes a été correctement enregistrée dans OneTrust pour chaque Traitement de Données Personnelles ;
2. Créez un groupe de travail sur la conservation des données comprenant le point de contact local dédié à la Protection des Données, l'opérationnel concerné et l'équipe IS&T pour techniquement mettre en œuvre la période de conservation des données (y compris le mode actif et l'archivage temporaire) ;
3. Rédigez un processus détaillé comprenant les étapes à suivre pour supprimer les Données Personnelles et le responsable de chaque action identifiée dans le processus par le groupe de travail sur la conservation des données ;
4. Réunissez-vous avec le groupe de travail sur la conservation des données sur une base annuelle pour vérifier si la période de conservation des données est correctement mise en œuvre et si les Données Personnelles sont correctement archivées ou supprimées.

**ANNEXE 1 - CALENDRIER INDICATIF DE CONSERVATION DES DONNÉES**

La durée de conservation des données est définie en fonction du Traitement concerné. Les durées de conservation des données suivantes sont basées sur les exigences de diverses lois françaises.

	<b>Finalité sous-jacente</b>	<b>Conservation des données</b>
<b>Ressources humaines</b>	Gestion administrative	Fin du contrat de travail + 2 ans
	Gestion de la paie	Fin du contrat de travail + 5 ans
	Processus de recrutement	3 ans après le dernier contact avec le candidat
	Congés	Fin du contrat de travail + 1 an
	Gestion des accès	3 mois maximum
	Enregistrement des vidéosurveillances	1 mois maximum
<b>Marketing</b>	Base de données clients et prospects à des fins de marketing	3 ans après le dernier contact avec la Personne Concernée
	Enquêtes de satisfaction client	4 ans
<b>Sécurité informatique</b>	Gestion de la sécurité informatique	6 mois
<b>Finance</b>	Gestion des factures	10 ans
	Comptabilité	10 ans

## **Annexe 7 - Politique Globale de gestion des droits des Personnes Concernées**

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

## Annexe 8 - Description du champ d'application matériel de la Politique en tant que Responsable du Traitement

Types de Traitements de Données Personnelles effectués et/ou envisagés et finalités	Catégories des Personnes Concernées	Catégories des Personnes Concernées ayant fait l'objet d'un Traitement	Liste des pays de destination
<ul style="list-style-type: none"> <li>- Gestion du recrutement</li> </ul>	<ul style="list-style-type: none"> <li>- Candidats à une offre d'emploi</li> </ul>	<ul style="list-style-type: none"> <li>- Données d'identification (état civil, identité)</li> <li>- Vie privée (limitée aux loisirs et autres informations incluses dans les CV)</li> <li>- Vie professionnelle</li> <li>- CV, école, diplôme, formation professionnelles, distinctions, etc.</li> <li>- Situation économique et financière (ex : attentes salariales)</li> </ul>	<ul style="list-style-type: none"> <li>- Potentiellement tous les pays où Sodexo opère, lorsqu'une entité Sodexo de l'UE/EEE recrute un résident de l'UE/EEE pour un poste situé en dehors de l'UE/EEE.</li> </ul>
<ul style="list-style-type: none"> <li>- Gestion des ressources humaines (y compris, mais sans s'y limiter, la gestion du personnel administratif, la gestion de la mobilité, la gestion de la performance au travail, la gestion du développement de carrière, la gestion de la formation à l'évaluation des talents, la</li> </ul>	<ul style="list-style-type: none"> <li>- Employés</li> <li>- Anciens employés</li> </ul>	<ul style="list-style-type: none"> <li>- Données d'identification (état civil, identité)</li> <li>- Vie privée (point de contact d'urgence, et informations nécessaires à la gestion du contrat d'assurance maladie pour tous les bénéficiaires)</li> <li>- Vie professionnelle</li> </ul>	<ul style="list-style-type: none"> <li>- Tous les pays où Sodexo opère.</li> </ul>

<p>gestion des voyages d'affaires, la gestion de l'annuaire actif, etc.)</p>		<ul style="list-style-type: none"> <li>- Situation économique et financière (coordonnées bancaires pour la gestion de la paie)</li> <li>- Données de connexion (ex : informations d'identification à des finalités d'authentification, logs/interaction avec les applications informatiques pertinentes, adresse IP)</li> </ul>	
<ul style="list-style-type: none"> <li>- Gestion comptable et financière des employés (par exemple, gestion des frais), des fournisseurs/vendeurs, des prestataires/sous-traitants, des clients et des contrôles et rapports connexes.</li> </ul>	<ul style="list-style-type: none"> <li>- Employés</li> <li>- Clients (clients commerciaux actuels ou potentiels)</li> <li>- Consommateurs/Bénéficiaires (consommateurs/bénéficiaires actuels ou potentiels)</li> <li>- Fournisseurs/vendeurs (contacts commerciaux)</li> <li>- Prestataires/sous-traitants (contacts commerciaux)</li> </ul>	<ul style="list-style-type: none"> <li>- Données d'identification (état civil, identité)</li> <li>- Vie professionnelle</li> <li>- Situation économique et financière (coordonnées bancaires pour la gestion des dépenses ou le processus de facturation)</li> <li>- Données de connexion (ex : informations d'identification à des fins d'authentification, logs/interaction avec les applications informatiques pertinentes, adresse IP)</li> </ul>	<ul style="list-style-type: none"> <li>- Tous les pays où Sodexo opère.</li> </ul>
<ul style="list-style-type: none"> <li>- Finance, trésorerie et gestion fiscale (y compris mais non limité aux opérations de fusions et d'acquisitions,</li> </ul>	<ul style="list-style-type: none"> <li>- Employés</li> <li>- Clients (clients commerciaux actuels ou potentiels)</li> </ul>	<ul style="list-style-type: none"> <li>- Données d'identification (état civil, identité)</li> <li>- Vie professionnelle</li> </ul>	<ul style="list-style-type: none"> <li>- Tous les pays où Sodexo opère.</li> </ul>

04 Annexes

<p>gestion des actions de performance, consolidation financière, solution de budgétisation et de prévision, y compris le reporting)</p>	<ul style="list-style-type: none"> <li>- Consommateurs/Bénéficiaires (consommateurs/bénéficiaires actuels ou potentiels)</li> <li>- Fournisseurs/vendeurs (contacts commerciaux)</li> <li>- Prestataires/sous-traitants (contacts commerciaux)</li> </ul>	<ul style="list-style-type: none"> <li>- Situation économique et financière (coordonnées bancaires pour la gestion des dépenses ou le processus de facturation)</li> <li>- Données de connexion (ex : informations d'identification à des fins d'authentification, logs/interaction avec les applications informatiques pertinentes, adresse IP)</li> </ul>	
<ul style="list-style-type: none"> <li>- Gestion des risques (audit interne, contrôles internes, etc..)</li> </ul>	<ul style="list-style-type: none"> <li>- Employés</li> <li>- Clients (clients commerciaux actuels ou potentiels)</li> <li>- Consommateurs/Bénéficiaires (consommateurs/bénéficiaires actuels ou potentiels)</li> <li>- Fournisseurs/vendeurs (contacts commerciaux)</li> <li>- Prestataires/sous-traitants (contacts commerciaux)</li> </ul>	<ul style="list-style-type: none"> <li>- Données d'identification (état civil, identité)</li> <li>- Vie professionnelle</li> <li>- Situation économique et financière (coordonnées bancaires pour la gestion des dépenses ou le processus de facturation)</li> <li>- Données de connexion (ex : informations d'identification à des fins d'authentification, logs/interaction avec les applications informatiques pertinentes, adresse IP)</li> </ul>	<ul style="list-style-type: none"> <li>- Tous les pays où Sodexo opère.</li> </ul>
<ul style="list-style-type: none"> <li>- Gestion de la sécurité des salariés (y compris information et localisation des salariés voyageant ou</li> </ul>	<ul style="list-style-type: none"> <li>- Employés</li> <li>- Consultants externes</li> </ul>	<ul style="list-style-type: none"> <li>- Données d'identification (état civil, identité)</li> <li>- Vie privée (numéro de téléphone privé lorsque le</li> </ul>	<ul style="list-style-type: none"> <li>- Tous les pays où Sodexo opère, lorsqu'un employé Sodexo UE/EEE ou un consultant externe</li> </ul>

travaillant à l'étranger, gestion de crise)		<p>salarié n'a pas de téléphone professionnel pour des raisons HLC)</p> <ul style="list-style-type: none"> <li>■ Vie professionnelle</li> <li>■ Données de connexion (ex : informations d'identification à des finalités d'authentification, logs/interaction avec les applications informatiques pertinentes, adresse IP)</li> </ul>	voyage ou travaille à l'étranger et lorsque des équipes Sodexo situées hors de l'UE/EEE ont besoin d'accéder à leurs Données Personnelles pour des raisons de sécurité.
<ul style="list-style-type: none"> <li>■ Fourniture d'Active Directory, de boîtes aux lettres de services de messagerie et d'autres outils informatiques ou sites internet internes tels que l'intranet de Sodexo, les appareils mobiles et toutes autres solutions numériques ou plateformes collaboratives</li> </ul>	<ul style="list-style-type: none"> <li>■ Employés</li> <li>■ Consultants externes</li> </ul>	<ul style="list-style-type: none"> <li>■ Données d'identification (état civil, identité)</li> <li>■ Vie professionnelle</li> <li>■ Données de connexion (ex : informations d'identification à des fins d'authentification, logs/interaction avec les applications informatiques pertinentes, adresse IP)</li> </ul>	<ul style="list-style-type: none"> <li>■ Tous les pays où Sodexo opère.</li> </ul>
<ul style="list-style-type: none"> <li>■ Gestion du support informatique, y compris la gestion de l'infrastructure, la gestion des systèmes et les applications</li> </ul>	<ul style="list-style-type: none"> <li>■ Employés</li> <li>■ Consultants externes</li> </ul>	<ul style="list-style-type: none"> <li>■ Données d'identification (état civil, identité)</li> <li>■ Vie professionnelle</li> <li>■ Données de connexion (ex : informations d'identification à des fins d'authentification, logs/interaction avec les applications</li> </ul>	<ul style="list-style-type: none"> <li>■ Tous les pays où Sodexo opère.</li> </ul>

<ul style="list-style-type: none"> <li>- Gestion de la santé et de la sécurité</li> </ul>	<ul style="list-style-type: none"> <li>- Employés</li> <li>- Consultants externes</li> <li>- Autres (visiteurs, occupants du site, etc.)</li> </ul>	<p>informatiques pertinentes, adresse IP)</p> <ul style="list-style-type: none"> <li>- Données d'identification (état civil, identité)</li> <li>- Vie professionnelle</li> <li>- Données de connexion (ex : informations d'identification à des finalités d'authentification, logs/interaction avec les applications informatiques pertinentes, adresse IP)</li> </ul>	<ul style="list-style-type: none"> <li>- Tous les pays où Sodexo opère, lorsque les équipes de santé et de sécurité de Sodexo situées hors de l'UE/EEE ont besoin d'accéder à un employé Sodexo de l'UE/EEE, à un consultant externe ou à d'autres Données Personnelles des Personnes Concernées à des fins de gestion de la santé et de la sécurité.</li> </ul>
<ul style="list-style-type: none"> <li>- Gestion de la sécurité des informations (y compris, mais sans s'y limiter, la prévention, la détection et l'investigation des incidents de sécurité, le contrôle du respect des politiques de sécurité des données de Sodexo)</li> </ul>	<ul style="list-style-type: none"> <li>- Employés</li> <li>- Consultants externes</li> </ul>	<ul style="list-style-type: none"> <li>- Données d'identification (état civil, identité)</li> <li>- Vie professionnelle</li> <li>- Données de connexion (ex : informations d'identification à des fins d'authentification, logs/interaction avec les applications informatiques pertinentes, adresse IP)</li> </ul>	<ul style="list-style-type: none"> <li>- Tous les pays où Sodexo opère.</li> </ul>
<ul style="list-style-type: none"> <li>- Gestion de la relation client, y compris l'exécution de nos services et de toute autre opération commerciale</li> </ul>	<ul style="list-style-type: none"> <li>- Employés</li> <li>- Clients (clients commerciaux actuels ou potentiels)</li> <li>- Consommateurs/Bénéficiaires (consommateurs/bénéficiaires actuels ou potentiels)</li> </ul>	<ul style="list-style-type: none"> <li>- Données d'identification (état civil, identité)</li> <li>- Vie privé (ex : les habitudes de vies)</li> <li>- Vie professionnelle</li> </ul>	<ul style="list-style-type: none"> <li>- Tous les pays où Sodexo opère.</li> </ul>

04 Annexes

- Fournisseurs/vendeurs (contacts commerciaux)
- Prestataires/sous-traitants (contacts commerciaux)
- Situation économique et financière (ex : coordonnées bancaires des clients mais principalement des personnes morales)
- Données de connexion (ex : informations d'identification à des finalités d'authentification, logs/interaction avec les applications informatiques pertinentes, adresse IP)
- Données sensibles : préférences ou restrictions alimentaires ou allergies pouvant révéler indirectement des données de santé ou des croyances religieuses.

<ul style="list-style-type: none"> <li>- Gestion des offres, des ventes et du marketing</li> </ul>	<ul style="list-style-type: none"> <li>- Employés</li> <li>- Clients (clients commerciaux actuels ou potentiels)</li> <li>- Consommateurs/Bénéficiaires (consommateurs/bénéficiaires actuels ou potentiels)</li> <li>- Fournisseurs/vendeurs (contacts commerciaux)</li> <li>- Prestataires/sous-traitants (contacts commerciaux)</li> </ul>	<ul style="list-style-type: none"> <li>- Données d'identification (état civil, identité)</li> <li>- Vie privée (e-mail personnel pour le marketing direct si la Personne Concernée y a consenti)</li> <li>- Vie professionnelle</li> <li>- Données de connexion (ex : informations</li> </ul>	<ul style="list-style-type: none"> <li>- Tous les pays où Sodexo opère.</li> </ul>
--	--	---	--

		d'identification à des finalités d'authentification, logs/interaction avec les applications informatiques pertinentes, cookies)	
<ul style="list-style-type: none"> <li>- Gestion de l'approvisionnement</li> </ul>	<ul style="list-style-type: none"> <li>- Fournisseurs/vendeurs (contacts commerciaux)</li> <li>- Prestataires/sous-traitants (contacts commerciaux)</li> </ul>	<ul style="list-style-type: none"> <li>- Données d'identification (état civil, identité)</li> <li>- Situation économique et financière (revenus, situation financière, situation fiscale, etc.)</li> <li>- Données de connexion (ex : informations d'identification à des finalités d'authentification, logs/interaction avec les applications informatiques pertinentes, adresse IP)</li> </ul>	<ul style="list-style-type: none"> <li>- Tous les pays où Sodexo opère.</li> </ul>
<ul style="list-style-type: none"> <li>- Communication interne et externe et gestion des événements</li> </ul>	<ul style="list-style-type: none"> <li>- Employés</li> <li>- Clients (clients commerciaux actuels ou potentiels)</li> <li>- Consommateurs/Bénéficiaires (consommateurs/bénéficiaires actuels ou potentiels)</li> <li>- Fournisseurs/vendeurs (contacts commerciaux)</li> <li>- Prestataires/sous-traitants (contacts commerciaux)</li> </ul>	<ul style="list-style-type: none"> <li>- Données d'identification (état civil, identité)</li> <li>- Vie professionnelle</li> <li>- Données de connexion (ex : informations d'identification à des finalités d'authentification, logs/interaction avec les applications</li> </ul>	<ul style="list-style-type: none"> <li>- Tous les pays où Sodexo opère.</li> </ul>

		informatiques pertinentes, cookies)	
<ul style="list-style-type: none"> <li>- Opérations d'analyse de données (analyse de données afin d'avoir une meilleure compréhension et plus d'informations sur les expériences de nos clients ou consommateurs/bénéficiaires, fournisseurs/vendeurs).</li> </ul>	<ul style="list-style-type: none"> <li>- Clients (clients commerciaux actuels ou potentiels)</li> <li>- Consommateurs/Bénéficiaires (consommateurs/bénéficiaires actuels ou potentiels)</li> <li>- Fournisseurs/vendeurs (contacts commerciaux)</li> </ul>	<ul style="list-style-type: none"> <li>- Données d'identification (état civil, identité)</li> <li>- Vie professionnelle</li> <li>- Situation économique et financière (données transactionnelles collectées par les points de vente etc.)</li> <li>- Données de connexion (ex : logs/interaction avec les applications informatiques pertinentes, adresse IP)</li> </ul>	<ul style="list-style-type: none"> <li>- Tous les pays où Sodexo opère.</li> </ul>
<ul style="list-style-type: none"> <li>- Gestion juridique de l'entreprise (y compris, mais sans s'y limiter, la gestion des personnes morales, la gestion des délégations de pouvoir et d'autorité)</li> </ul>	<ul style="list-style-type: none"> <li>- Employés</li> <li>- Clients (clients commerciaux actuels ou potentiels)</li> <li>- Fournisseurs/vendeurs (contacts commerciaux)</li> <li>- Prestataires/sous-traitants (contacts commerciaux)</li> </ul>	<ul style="list-style-type: none"> <li>- Données d'identification (état civil, identité)</li> <li>- Vie professionnelle</li> <li>- Données de connexion (ex : informations d'identification à des finalités d'authentification, logs/interaction avec les applications informatiques pertinentes, adresse IP)</li> </ul>	<ul style="list-style-type: none"> <li>- Tous les pays où Sodexo opère.</li> </ul>
<ul style="list-style-type: none"> <li>- Mise en place de processus d'éthique et de conformité (afin de se conformer aux exigences applicables)</li> </ul>	<ul style="list-style-type: none"> <li>- Employés</li> <li>- Clients (clients commerciaux actuels ou potentiels)</li> </ul>	<ul style="list-style-type: none"> <li>- Données d'identification (état civil, identité)</li> <li>- Vie professionnelle</li> <li>- Situation économique et financière (ex : examen</li> </ul>	<ul style="list-style-type: none"> <li>- Tous les pays où Sodexo opère.</li> </ul>

#### 04 Annexes

- Consommateurs/Bénéficiaires (consommateurs/bénéficiaires actuels ou potentiels)
  - Fournisseurs/vendeurs (contacts commerciaux)
  - Prestataires/sous-traitants (contacts commerciaux)
- des dépenses ou des factures pour enquêter sur les conflits, respect de la politique de cadeaux du Groupe)
- Données de connexion (ex : informations d'identification à des finalités d'authentification, logs/interaction avec les applications informatiques pertinentes, adresse IP)
-

