Délibération n° 2023-142 du 21 décembre 2023 portant approbation des règles d'entreprise contraignantes (BCR) « responsable du traitement » du groupe SODEXO

(Demande d'approbation n° 20005716)

La Commission nationale de l'informatique et des libertés (ci-après « la CNIL »),

Saisie par la société Sodexo SA au nom et pour le compte du groupe Sodexo (ci-après « Sodexo ») d'une demande d'approbation de ses BCR « responsable du traitement » ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données ou RGPD), notamment ses articles 47, 57 et 64 ;

Vu la décision de la CJUE C-311/18 Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian Schrems, du 16 juillet 2020 ;

Vu les recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE, du 18 juin 2021 ;

Vu les recommandations 1/2022 sur la demande d'approbation et sur les éléments et principes à inclure dans les BCR responsable de traitement (article 47 RGDP), du 20 juin 2023 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Sur la proposition de Mme Anne DEBET, commissaire, et après avoir entendu les observations de M. Damien MILIC, commissaire du Gouvernement,

Formule les observations suivantes :

1. En vertu de l'article 47-1 du RGPD, la CNIL approuve des règles d'entreprise contraignantes (« BCR ») sous réserve que celles-ci répondent aux exigences prévues par cet article.

2. La mise en œuvre et l'adoption de BCR par un groupe d'entreprises visent à fournir des garanties aux responsables de traitement et aux sous-traitants établis sur le territoire

de l'Union européenne (« UE ») afin qu'un niveau de protection uniforme soit appliqué aux données transférées vers des pays tiers, et ce, indépendamment du niveau de protection conféré par chacun de ces pays tiers.

3. Toutefois, avant de mettre en application ces BCR, il incombe à l'exportateur de données situé dans un État membre, le cas échéant en collaboration avec l'importateur de données, d'apprécier si le niveau de protection requis par le droit de l'UE est respecté dans le pays tiers de destination, y compris dans les situations de transferts ultérieurs. Cette évaluation doit être effectuée afin de déterminer si les garanties établies par les BCR peuvent être respectées dans la pratique, compte tenu des circonstances du transfert et des conflits qui peuvent exister entre les exigences du droit du pays tiers et les droits fondamentaux. Si tel n'est pas le cas, l'exportateur de données situé dans un État membre, le cas échéant en collaboration avec l'importateur de données, doit évaluer s'il peut prévoir des mesures supplémentaires pour assurer un niveau de protection substantiellement équivalent à celui garanti au sein de l'UE. La mise en œuvre des mesures supplémentaires relève de la responsabilité de l'exportateur, y compris après l'approbation des BCR par l'autorité compétente. Par conséquent, ces mesures supplémentaires ne font pas partie des éléments analysés dans le cadre de la procédure d'approbation des BCR.

4. Dans le cas où l'exportateur de données établi dans un État membre n'est pas à même de prendre des mesures supplémentaires suffisantes pour assurer un niveau de protection substantiellement équivalent à celui garanti dans l'UE, il ne peut y avoir de transfert de données à caractère personnel vers le pays tiers en vertu des BCR. Par conséquent, l'exportateur de données est tenu de renoncer, de suspendre ou de mettre fin au transfert de données à caractère personnel. Dans la même logique, lorsque l'exportateur prend connaissance de nouveaux développements touchant à la protection des données dans un pays tiers qui diminuent le niveau de protection attendu ; il est tenu de suspendre ou mettre fin au transfert concerné.

5. Conformément à la procédure de coopération décrite par le document de travail WP263 rev.01[1], la documentation relative aux BCR « responsable du traitement » du groupe a été instruite par les services de la CNIL en qualité d'autorité compétente, puis par les services de deux autres autorités de protection des données agissant en qualité de co-examinatrices. Ces BCR ont également été revues par les autorités de protection des données des pays membres de l'Espace économique européen (« EEE ») en application de la procédure d'approbation mise en place par le Comité européen de la protection des données (« CEPD »).

6. L'instruction des BCR « responsable du traitement » du groupe permet de conclure que celles-ci sont conformes aux critères imposés par l'article 47-1 du RGPD et le document de travail WP256 rev.01[2], notamment parce que les BCR susmentionnées :

[1] Approuvé par le CEPD le 25 mai 2018.

[2] Les WP256 rev.01 et WP264 sont remplacés par les Recommandations 1/2022 du CEPD. Cependant, étant donné que les BCR « responsable du traitement » du groupe

i. sont rendues juridiquement contraignantes par un contrat intra-groupe et imposent une obligation claire à chaque entité liée, y compris à leurs employés, de les respecter (Règle 26 des BCR et contrat intra-groupe) ;

ii. confèrent expressément des droits aux personnes concernées leur permettant de s'en prévaloir en tant que tiers bénéficiaires via les Règles 10 et 21 des BCR ;

iii. répondent aux exigences prévues par l'article 47-2 du RGPD :

a) la structure et les coordonnées du groupe d'entreprises et de chacune des entités liées sont détaillées dans le formulaire de soumission qui a été fourni dans le cadre de l'instruction du dossier ;

b) les transferts ou l'ensemble des transferts de données, y compris les catégories de données à caractère personnel, les types de traitements et leurs finalités, les types de personnes concernées et les pays tiers en question sont précisés en annexe 8 des BCR ;

c) la nature juridiquement contraignante, tant interne qu'externe, des BCR est reconnue par la Règle 26 des BCR et les dispositions du contrat intra-groupe ;

d) l'application des principes généraux relatifs à la protection des données, notamment la limitation de la finalité, la minimisation des données, la limitation des durées de conservation des données, la qualité des données, la protection des données dès la conception et la protection des données par défaut, la base juridique du traitement, le traitement de catégories particulières de données à caractère personnel, les mesures visant à garantir la sécurité des données, ainsi que les exigences en matière de transferts ultérieurs à des organismes qui ne sont pas liés par les règles d'entreprise contraignantes, sont visés aux Règles 2, 3, 4, 5, 6, 7, 8, 13 et 14 des BCR ;

e) les droits des personnes concernées à l'égard du traitement et les moyens d'exercer ces droits, y compris le droit de ne pas faire l'objet de décisions fondées exclusivement sur un traitement automatisé, y compris le profilage, conformément à l'article 22 du RGPD, le droit d'introduire une réclamation auprès de l'autorité de contrôle compétente et devant les juridictions compétentes des États membres conformément aux articles 77 et 79 du RGPD et d'obtenir réparation

avaient déjà atteint le stade de « projet consolidé » visé par l'article 2.4 du WP263 rev.01 au moment de la publication desdites Recommandations, les BCR peuvent être instruites conformément au cadre précédent, sous réserve que le CEPD adopte son avis d'ici la fin d'année 2023 (paragraphe 13 des Recommandations 1/2022).

et, le cas échéant, une indemnisation pour violation des règles d'entreprise contraignantes sont prévus aux Règles 10, 11, 21 et 22 des BCR ;

f) l'acceptation, par le responsable du traitement ou le sous-traitant établi sur le territoire d'un État membre, de l'engagement de sa responsabilité pour toute violation des règles d'entreprise contraignantes par toute entité concernée non établie dans l'UE est précisée à la Règle 22 des BCR ; de même que le principe selon lequel l'exonération, en tout ou en partie, de cette responsabilité peut intervenir uniquement si l'entité responsable prouve que le fait générateur du dommage n'est pas imputable à l'entité en cause ;

g) la manière dont les informations sur les règles d'entreprise contraignantes, notamment en ce qui concerne les éléments mentionnés aux points d), e) et f) de l'article 47.2 du RGPD, sont fournies aux personnes concernées, en sus des informations visées aux articles 13 et 14 du RGPD, est spécifiée à la Règle 12 des BCR ;

h) les missions de tout délégué à la protection des données, désigné conformément à l'article 37 du RGPD, ou de toute autre personne ou entité chargée de la surveillance du respect des règles d'entreprise contraignantes au sein du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, ainsi que le suivi de la formation et le traitement des réclamations sont détaillées aux Règles 16, 17 et 20 des BCR ;

i) les procédures de réclamation sont décrites à la Règle 17 des BCR ;

j) les mécanismes mis en place au sein du groupe d'entreprises pour garantir le contrôle du respect des règles d'entreprise contraignantes sont détaillés à la Règle 18 des BCR. Ces mécanismes prévoient des audits sur la protection des données et des méthodes assurant que des mesures correctrices seront prises pour protéger les droits des personnes concernées. Les résultats de ces contrôles sont communiqués à la personne ou à l'entité visée au point h) ci-dessus et au conseil d'administration de l'entreprise qui exerce le contrôle du groupe d'entreprises, et sont mis à la disposition de l'autorité de contrôle compétente sur demande ;

k) les mécanismes mis en place pour communiquer et consigner les modifications apportées aux règles et pour communiquer ces modifications à l'autorité de contrôle sont précisés à la Règle 25 des BCR ainsi qu'en annexe 5 ;

l) le mécanisme de coopération avec l'autorité de contrôle mis en place pour assurer le respect des règles par toutes les entités du groupe d'entreprises est décrit à la Règle 24 des BCR ainsi qu'en annexe 4. L'obligation de mise à disposition de l'autorité de contrôle des résultats des contrôles des mesures visés au point j) ci-dessus est spécifiée à la Règle 18 des BCR ;

m) les mécanismes permettant de communiquer à l'autorité de contrôle compétente toutes les obligations juridiques auxquelles une entité du groupe d'entreprises est soumise dans un pays tiers qui sont susceptibles d'avoir un effet négatif important sur les garanties fournies par les règles d'entreprise contraignantes sont décrits à la Règle 23 des BCR ;

n) enfin, la Règle 16 des BCR prévoit une formation appropriée en matière de protection des données pour le personnel ayant un accès permanent ou régulier aux données à caractère personnel.

7. Le CEPD a rendu l'avis n°29/2023 en date du 28 novembre 2023, conformément à l'article 64-1-f du RGPD. La Commission a tenu compte de cet avis.

Décide :

8. La CNIL approuve les BCR « responsable du traitement » présentées par le groupe Sodexo, en ce qu'elles fournissent des garanties appropriées pour le transfert de données à caractère personnel conformément aux articles 46-1, 46-2-b, 47-1 et 47-2 du RGPD. Afin de dissiper toute ambigüité, la CNIL rappelle que l'approbation des BCR n'implique pas l'approbation de transferts spécifiques de données à caractère personnel effectués sur la base des BCR. En conséquence, l'approbation des BCR ne peut être interprétée comme une approbation des transferts vers des pays tiers inclus dans les BCR pour lesquels un niveau de protection substantiellement équivalent à celui assuré au sein de l'UE ne peut être garanti.

9. La mise en œuvre des BCR approuvées ne nécessite pas d'autorisation supplémentaire spécifique de la part des autorités européennes de protection des données concernées.

10. Les BCR « responsable du traitement » du groupe Sodexo doivent être mises en conformité avec les Recommandations 1/2022 du CEPD dans le cadre de la mise à jour annuelle de 2024.

11. Conformément à l'article 58-2-j du RGPD, chaque autorité de protection des données concernée dispose du pouvoir d'ordonner la suspension des flux de données adressés à un destinataire situé dans un pays tiers ou à une organisation internationale dans le

cas où les garanties appropriées prévues par les BCR « responsable du traitement » du groupe Sodexo ne seraient pas respectées.

La Présidente

Marie-Laure DENIS

Cette décision peut faire l'objet d'un recours devant le Conseil d'État dans un délai de deux mois à compter de sa notification.

ANNEXE

Les BCR « responsable du traitement » du groupe Sodexo approuvées par la présente décision s'étendent au périmètre décrit ci-après :

a. **Champ d'application.** Ces BCR « responsable du traitement » couvre les traitements des données personnelles par les entités de Sodexo établies au sein de l'EEE 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 de l'EEE pour toute autre entité Sodexo au sein du groupe (annexe 8 des BCR).

b. **États membres de l'EEE depuis lesquels les transferts sont effectués :** Allemagne, Autriche, Belgique, Bulgarie, Chypre, Danemark, Espagne, Finlande, France, Hongrie, Irlande, Italie, Luxembourg, Norvège, Pays-Bas, Pologne, Portugal, République tchèque, Roumanie, Suède (listés en introduction des BCR).

c. **Pays tiers vers lesquels les transferts sont effectués :** 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 (listés en introduction des BCR).

d. **Les finalités des transferts :** ces finalités sont détaillées à l'annexe 8 des BCR. Elles comprennent notamment les finalités suivantes :
   - Gestion du recrutement ;
   - 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 gestion des voyages d'affaires, la gestion de l'annuaire actif, etc.) ;
   - 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 ;
   - Finance, trésorerie et gestion fiscale (y compris mais non limité aux opérations de fusions et d'acquisitions, gestion des actions de performance, consolidation financière, solution de budgétisation et de prévision, y compris le reporting) ;
   - Gestion des risques (audit interne, contrôles internes, etc..) ;

- Gestion de la sécurité des salariés (y compris information et localisation des salariés voyageant ou travaillant à l'étranger, gestion de crise) ;
- 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 ;
- Gestion du support informatique, y compris la gestion de l'infrastructure, la gestion des systèmes et les applications ;
- Gestion de la santé et de la sécurité ;
- 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) ;
- Gestion de la relation client, y compris l'exécution de nos services et de toute autre opération commerciale ;
- Gestion des offres, des ventes et du marketing ;
- Gestion de l'approvisionnement ;
- Communication interne et externe et gestion des événements ;
- 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) ;
- 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) ;
- Mise en place de processus d'éthique et de conformité (afin de se conformer aux exigences applicables).

e. **Catégories de personnes concernées :** ces catégories sont détaillées dans l'annexe 8 des BCR. Elles comprennent :
   - Candidats à une offre d'emploi ;
   - Employés ;
   - Anciens employés ;
   - Clients (clients commerciaux actuels ou potentiels) ;
   - Consommateurs/Bénéficiaires (actuels ou potentiels) ;
   - Fournisseurs/vendeurs (contacts commerciaux) ;
   - Prestataires/sous-traitants (contacts commerciaux) ;
   - Consultants externes ;
   - Autres (visiteurs, occupants du site, etc.).

f. **Catégories de données à caractère personnel transférées :** les catégories sont détaillées dans l'annexe 8 des BCR. Elles comprennent notamment :
   - Données d'identification (état civil, identité) ;

- Vie privée (limitée aux loisirs et autres informations incluses dans les CV, point de contact d'urgence, et informations nécessaires à la gestion du contrat d'assurance maladie pour tous les bénéficiaires) ;
- Vie professionnelle ;
- CV, école, diplôme, formation professionnelles, distinctions, etc.
- Situation économique et financière (ex : attentes salariales) ;
- Situation économique et financière (coordonnées bancaires pour la gestion de la paie) ;
- Données de connexion (ex : informations d'identification à des finalités d'authentification, logs/interaction avec les applications informatiques pertinentes, adresse IP) ;
- Vie privée (numéro de téléphone privé lorsque le salarié n'a pas de téléphone professionnel pour des raisons HLC) ;
- Vie privée (ex : les habitudes de vies) ;
- Vie privée (e-mail personnel pour le marketing direct si la Personne Concernée y a consenti) ;
- Situation économique et financière (revenus, situation financière, situation fiscale, etc.) ;
- Données sensibles : préférences ou restrictions alimentaires ou allergies pouvant révéler indirectement des données de santé ou des croyances religieuses.