Délibération n° 2023-139 du 21 décembre 2023 portant approbation des règles d'entreprise contraignantes (BCR) « responsable du traitement » du groupe NESTLÉ

(Demande d'approbation n° 20005278)

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

Saisie par la société Nestlé France au nom et pour le compte du groupe Nestlé S.A. (ci-après « Nestlé »), 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 »).

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

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 :

   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 (article 1.1 des BCR et articles 2.1 et 2.2 du contrat intra-groupe) ;

   ii. confèrent expressément des droits aux personnes concernées leur permettant de s'en prévaloir en tant que tiers bénéficiaires via l'article 26.2 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. La liste des entités est accessible depuis le site web du groupe Nestlé ;

      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 2 des BCR ;

      c) la nature juridiquement contraignante, tant interne qu'externe, des BCR est reconnue par l'article 1.1 des BCR ainsi qu'aux articles 2.1 et 2.2 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 articles 5, 6, 7, 8, 9, 10, 16, 17 et 20 des BCR ;

[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 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).

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 Etats membres conformément aux articles 77 et 79 du RGPD et d'obtenir réparation et, le cas échéant, une indemnisation pour violation des règles d'entreprise contraignantes sont prévus aux articles 12, 13 et 26.2 des BCR ;

f) l'acceptation, par le responsable du traitement ou le sous-traitant établi sur le territoire d'un Etat 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 l'article 27.2 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 l'article 11 des BCR et en annexe 4 ;

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 à l'article 23.1 des BCR ;

i) les procédures de réclamation sont décrites à l'article 25 des BCR et en annexe 3 ;

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 l'article 22 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 l'article 29 des BCR ;

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 l'article 28 des BCR. 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 l'article 22.1 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 aux articles 24.4, 24.10 et 24.13 des BCR ;

n) enfin, l'article 21 et l'annexe 2.6 des BCR prévoient 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°24/2023 en date du 16 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 Nestlé, 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 Nestlé doivent être mises en conformité avec les Recommandations 01/2022 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 Nestlé 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 Nestlé qui sont approuvées par la présente décision couvrent le champ d'application suivant :

a. **Champ d'application :** ces BCR « responsable du traitement » s'appliquent lorsqu'une entité du groupe juridiquement liée par les BCR, et ayant mis en œuvre les engagements pris au titre des BCR agit en tant que responsable du traitement, de même que lorsque l'entité agit en tant que sous-traitant pour le compte du groupe Nestlé, ainsi qualifié de sous-traitant interne (article 1 des BCR).

b. **Etats membres de l'EEE depuis lesquels les transferts sont effectués :** Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Islande, Italie, Lettonie, Liechtenstein, Lituanie, Luxembourg, Malte, Norvège, Pays-Bas, Pologne, Portugal, République tchèque, Roumanie, Slovaquie, Slovénie et Suède.

c. **Pays tiers vers lesquels les transferts sont effectués :** Afrique du Sud, Algérie, Angola, Arabie saoudite, Argentine, Australie, Azerbaïdjan, Bahreïn, Bangladesh, Bolivie, Bosnie-Herzégovine, Burkina Faso, Cameroun, Canada, Chili, Chine continentale, Colombie, République démocratique du Congo, Corée, Costa Rica, Cuba, Égypte, Émirats arabes unis, Équateur, États-Unis, Éthiopie, Fidji, Gabon, Géorgie, Ghana, Guatemala, Honduras, Hong Kong, Inde, Indonésie, Iran, Irak, Israël, Jamaïque, Japon, Jordanie, Kazakhstan, Kenya, Koweït, Liban, Macédoine, Malaisie, Mali, Maroc, Maurice, Mexique, Moldavie, Monténégro, Mozambique, Myanmar, Nigéria, Nouvelle-Zélande, Pakistan, État de Palestine, Panama, Papouasie-Nouvelle-Guinée, Paraguay, Pérou, Philippines, Qatar, République arabe syrienne, République dominicaine, Russie, Salvador, Sénégal, Serbie, Singapour, Sri Lanka, Suisse, Taïwan, Tanzanie, Thaïlande, Trinité-et-Tobago, Turquie, Ukraine, Uruguay, Venezuela, Vietnam, Yémen, Zambie et Zimbabwe. Dans la pratique, les pays tiers de destination les plus courants sont la Suisse, l'Ukraine, le Brésil et les Philippines (annexe 2 des BCR).

d. **Les finalités des transferts :** les finalités sont détaillées en annexe 2 des BCR. Elles comprennent notamment les finalités suivantes :
   - **Administration de l'entreprise** (ex : la gestion des ressources humaines ; l'administration des systèmes informatiques de Nestlé ; la gestion économique, financière et administrative ; la planification et les rapports commerciaux) ;
   - **Bases de données du personnel** (ex : la communication interne et la facilitation des interactions au sein de l'entreprise) ;

- **Recrutement** (ex : fonctionnement et amélioration des objectifs de recrutement) ;
- **Gestion de la rémunération et des avantages sociaux** (ex : gestion de la paie, de la rémunération, des programmes incitatifs, des avantages sociaux et des pensions, remboursement des dépenses, planification et paiements de la rémunération, planification et conformité fiscale) ;
- **Services informatiques et sécurité de l'information** (ex : mise à disposition, maintenance, support et développement des systèmes informatiques de Nestlé ; mise en œuvre, maintien et amélioration des systèmes et mesures de sécurité de l'information ; enquête sur les incidents de sécurité informatique et violations de données à caractère personnel).

e. Catégories de personnes concernées : les catégories sont détaillées dans l'annexe 2 des BCR. Elles comprennent :

- le personnel de Nestlé ;
- les membres de la famille et autres bénéficiaires du Personnel de Nestlé ;
- les demandeurs d'emploi ;
- les consommateurs, visiteurs de tout site Internet de Nestlé et visiteurs des locaux de Nestlé ;
- le personnel des entreprises clientes ;
- le personnel des fournisseurs de l'entreprise ;
- les tiers (par exemple, les journalistes avec lesquels Nestlé interagit de temps à autre) ;
- les participants aux études de développement de produits et aux essais cliniques.

f. Catégories de données à caractère personnel transférées : les catégories sont détaillées, par finalité et par catégorie de personnes concernées dans l'annexe 2 des BCR.