Délibération n° 2023-144 du 21 décembre 2023 portant approbation des règles d'entreprise contraignantes (BCR) « responsable du traitement » du groupe THALES

(demande d'approbation n° 20005721)

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

Saisie par la société Thales S.A. au nom et pour le compte du groupe Thales (ci-après « Thales ») 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 (article 3 des BCR, annexe 12 des BCR et article 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 10.2 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 ainsi qu'à l'annexe 8 des BCR ;

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 annexes 1 et 9 des BCR ;

c) la nature juridiquement contraignante, tant interne qu'externe, des BCR est reconnue à l'article 3 des BCR, en annexe 12 des BCR et à l'article 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 4, 5, 8 et 13 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 et, le cas échéant, une indemnisation pour

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).

violation des règles d'entreprise contraignantes, sont prévus aux articles 9, 10, 11 et 12 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 l'article 9 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 17.1 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 à l'article 20 des BCR et en annexes 2, 3, 5, 6 et 7 des BCR ;

i) les procédures de réclamation sont décrites aux articles 11 et 12 des BCR ainsi qu'aux annexes 2 et 3 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 l'article 19 des BCR et à l'annexe 5 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 21 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 16 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 19 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 l'article 8 des BCR ;

n) enfin, l'article 18 et l'annexe 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°31/2023 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 Thales, 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 Thales 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 Thales 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 Thales approuvées par la présente décision s'étendent au périmètre décrit ci-après :

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, ainsi qualifié de sous-traitant interne (article 2.2 des BCR). Les BCR couvrent plus particulièrement les transferts effectués par des entités liées situées en EEE vers des entités situées dans des pays tiers, ainsi qu'aux transferts ultérieurs effectués par des dernières (article 2.3 des BCR).

b. Etats membres de l'EEE depuis lesquels les transferts sont effectués.

Ces Etats membres sont visés à l'annexe 8.1 des BCR. Il s'agit des pays suivants : France, Autriche, Belgique, Danemark, Estonie, Finlande, Allemagne, Grèce, Hongrie, Italie, Lettonie, Pays-Bas, Norvège, Pologne, Portugal, Roumanie, Espagne et Suède.

c. Pays tiers vers lesquels les transferts sont effectués.

Ces pays tiers sont mentionnés en annexes 8.2 et 9 des BCR. Il s'agit des pays suivants : Afrique du Sud, Algérie, Arabie Saoudite, Argentine, Australie, Bahreïn, Bolivie, Brésil, Cameroun, Canada, Chili, Chine, Colombie, Corée du Sud, Côte d'Ivoire, Égypte, Emirats Arabes Unis, Etats-Unis d'Amérique, Gabon, Hong-Kong, Inde, Indonésie, Israël, Japon, Kazakhstan, Kenya, Liban, Malaisie, Maroc, Maurice, Mexique, Nigeria, Nouvelle-Zélande, Oman, Pakistan, Philippines, Qatar, Royaume-Uni, Sénégal, Singapour, Suisse, Taiwan, Thaïlande, Turquie et Venezuela.

d. Les finalités des transferts.

Ces finalités sont détaillées en annexe 1 des BCR, comme suit :

- Gestion du système informatique et du réseau téléphonique, contrôle des accès au système informatique ainsi qu'aux différents outils informatiques (logiciels, applications, imprimantes, etc.), gestion des autorisations ainsi que des nominations des Administrateurs IS/IT y afférentes, authentification des utilisateurs et gestion de leurs profils, suivi des actions réalisées par ceux-ci (ex., modification de base de données)
- Mise en œuvre d'un outil de messagerie électronique
- Suivi et audit des connections à certains outils et bases de données du système informatique afin de connaître le taux d'utilisation et calculer le coût des licences

associées, analyse de la navigation des utilisateurs de sites internet afin de comprendre leurs usages et d'améliorer le(s) site(s) internet concerné(s)
- Réalisation d'audits de sécurité informatique, gestion et suivi des failles/incidents de sécurité, mise en place de procédures destinées à la sauvegarde des données et à la continuité d'activité en cas d'incidents affectant le système informatique
- Gestion et suivi des demandes d'assistance informatique soumises par les utilisateurs auprès du Helpdesk
- Gestion et administration des outils de téléphonie et des réseaux téléphoniques afférents mis à la disposition des employés
- Gestion d'outils collaboratifs
- Suivi des collaborateurs en déplacement professionnel aux fins d'assurer leur sécurité
- Recrutement de collaborateurs et suivi des candidatures
- Administration du personnel, gestion des profils des salariés, gestion des organisations, rapport et analyse de données RH
- Gestion de la performance, des rémunérations, avantages financiers ou non et du développement professionnel des salariés et des compétences
- Gestion de la paie, du dossier administratif des salariés (présence, absence, congés maladie, départs en retraite, transferts, etc.), et suivi du temps de travail
- Gestion de la formation professionnelle
- Gestion des salariés en situation de mobilité internationale (suivi de leur mission, des mesures d'accompagnement, situation familiale)
- Gestion des déplacements, réservation et paiement des titres de voyage, ainsi que le remboursement au personnel en déplacement des frais afférents, suivi et gestion des notes de frais soumises par les salariés, des cadeaux et invitations que les salariés pourraient envisager d'accepter ou offrir et des cartes bancaires professionnelles
- Mise en place de réseaux d'entreprise, notamment de réseaux sociaux d'entreprise
- Gestion de la charge de travail, organisation et suivi des projets et de l'activité
- Gestion des enquêtes auprès des salariés
- Gestion de la politique d'emploi des travailleurs handicapés
- Suivi des déclarations d'inventions dans le cadre des activités relatives à la propriété intellectuelle
- Création et gestion de listes d'initiés, des représentants d'intérêts, des déclarations anti-corruption, réalisation de due diligence des partenaires, gestion des procédures d'alerte, d'enquête interne et des conflits d'intérêts
- Suivi de la conformité en matière de contrôle des exportations
- Gestion des administrateurs en ce compris aux fins de se conformer avec des exigences légales
- Gestion documentaire
- Gestion des retours d'expérience fournis par les employés et de leur niveau de satisfaction, suivi des suggestions soumises par ceux-ci (ex. boîte à idées)
- Gestion des habilitations des employés et des prestataires aux fins d'obtenir les accréditations et/ou habilitations nécessaires (i) pour valider la conformité de

données, documents, produits ou services à des normes, standards ou réglementations ou (ii) pour procéder à des vérifications ou audits
- Gestion, suivi et inventaire du parc immobilier du groupe
- Gestion et suivi des plaintes ou demandes d'indemnisation d'employés, gestion de la relation avec les assureurs à cet égard
- Etude et résolution des plaintes de tiers, demandes d'indemnisation, des contentieux et des précontentieux, et pour la détermination des conseils assistant Thales dans les procédures contentieuses et précontentieuses
- Traitement de données à des fins d'organisation événementielle et de communication
- Gestion de la relation avec les clients, partenaires et prospects
- Gestion des opérations de fusions & acquisitions
- Gestion de la relation avec les fournisseurs et sous-traitants impliquant notamment la gestion des achats et le suivi des relations contractuelles
- Gestion des réservations, achats, évaluations et dispenses de formations par Thales au profit de ses clients internes et/ou externes
- Soumission de candidatures dans le cadre de processus d'appels d'offres initiés par de potentiels clients, impliquant dans certains cas des échanges de données avec des partenaires soumissionnaires
- Suivi et gestion de l'utilisation des plateformes interactives et réseaux mis à la disposition des clients finaux et des achats réalisés par ces derniers sur lesdites plateformes interactives et réseaux
- Traitements aux fins d'adaptation et de configuration des produits aux besoins des clients
- Gestion des incidents sur les produits et systèmes et rapports d'incidents établis par les salariés Thales
- Traitement destiné à assurer l'organisation, le suivi et la réalisation de formations dispensées par Thales pour ses clients
- Traitement de données résultant d'opérations de support technique et de maintenance réalisées pour les clients Thales
- Traitements aux fins de participation à et/ou de mise en œuvre de projets de recherche
- Traitement aux fins d'obtention de subventions
- Collecte et traitement de données personnelles à des fins de veille règlementaire, économique et d'intelligence stratégique
- Gestion comptable, fiscale générale et contrôle des opérations financières
- Réalisation d'audits internes au sein du groupe et suivi des actions en résultant

e. Catégories de personnes concernées.

Ces catégories sont indiquées dans l'article 2.2 et l'annexe 1 des BCR. Elles couvrent les :
- employés de Thales, y compris salariés, représentants et mandataires sociaux, ainsi que les anciens employés de Thales ;

- intérimaires et stagiaires de Thales ;
- candidats à l'emploi au sein de Thales ;
- employés et points de contact des clients existants et clients éventuels de Thales ;
- employés et points de contact des partenaires, prestataires, fournisseurs et sous-traitants de Thales ;
- employés, points de contact des clients des clients internes (un client interne désigne toute entité Thales agissant en qualité de responsable du traitement, pour le compte de laquelle une autre entité Thales traite des données à caractère personnel dans le cadre d'un contrat de prestations de services ou de fourniture de produits impliquant un traitement de données à caractère personnel).

f. Catégories de données à caractère personnel transférées.

Ces catégories sont reprises par l'article 2.2 des BCR et sont détaillés par finalité et par catégorie de personnes concernées dans l'annexe 1 des BCR. Il s'agit des :
- données d'identification ;
- données relatives à la vie professionnelle ;
- données de connexion ;
- données biométriques ;
- données relatives à la vie personnelle ;
- données économiques et financières ;
- données personnelles sensibles (telles que les données de santé) ;
- données de localisation ;
- permis de conduire ;
- toute information disponible publiquement ;
- des données relatives à l'utilisation de services interactifs.