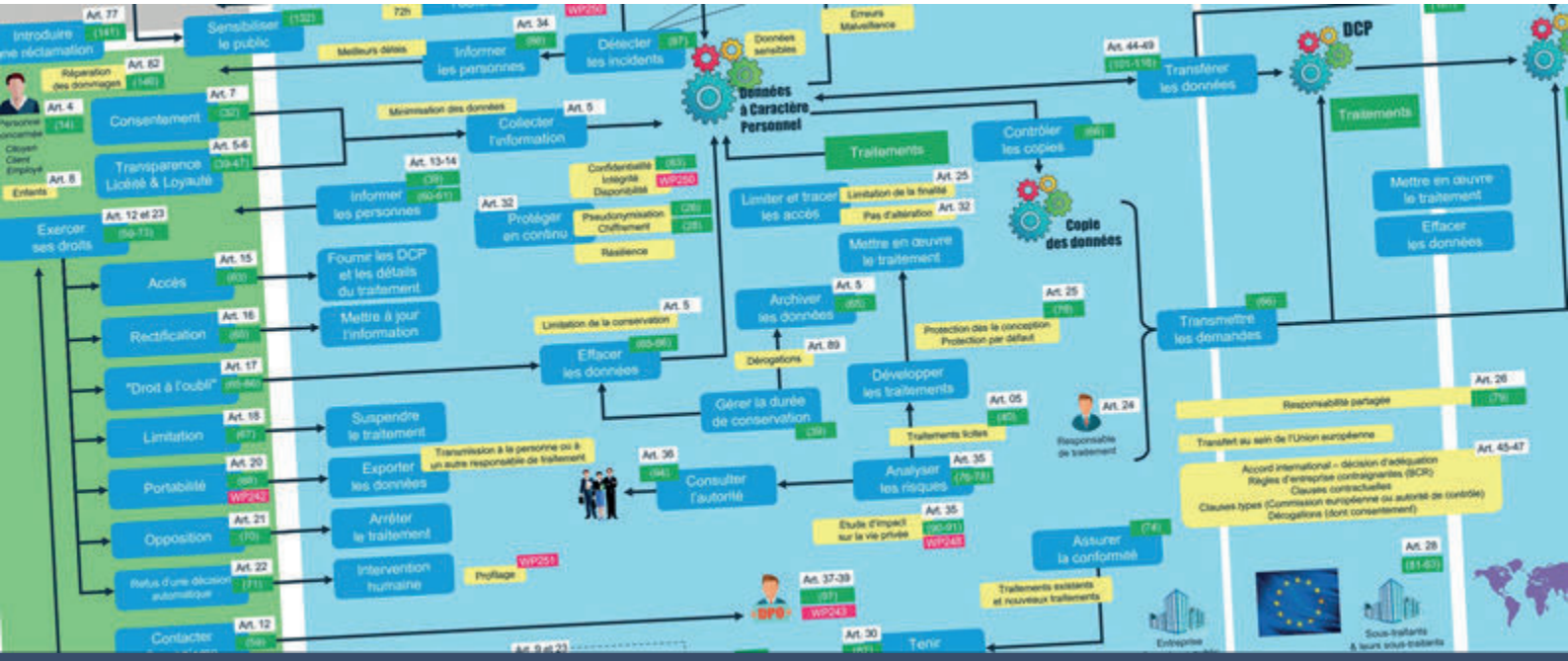
CLUSIF

LES GUIDES PRATIQUES DU CLUSIF - RGPD




# LES AUTRES OUTILS POUR LES TRANSFERTS DE DONNÉES (BCR...)

## 1. EN L'ABSENCE D'ADÉQUATION ET DE CCT

Au-delà du cas des transferts vers un Etat membre de l'Union européenne ou vers le Royaume-Uni, ces transferts peuvent s'effectuer sans formalité lorsqu'ils s'effectuent vers un pays ayant fait l'objet d'une décision d'adéquation par la Commission Européenne. La décision d'adéquation reconnaît le niveau de protection suffisant de la vie privée, des droits fondamentaux et des libertés des personnes à l'égard du traitement dont ces données font l'objet.

La décision d'adéquation peut être générale (Andorre, Argentine, Îles Féroé, Guernesey, Israël, Île de Man, Japon, Jersey, Nouvelle-Zélande, République de Corée, Suisse, Royaume-Uni, Uruguay), limitée aux seules entreprises commerciales (Canada) ou limitées aux entreprises qui ont accompli la démarche d'auto-certification (États-Unis).

Les transferts peuvent également s'effectuer après adoption de clauses contractuelles types selon le modèle proposé par la Commission européenne.

Pour les autres situations, d'autres outils peuvent être employés pour assurer la conformité des transferts de données personnelles :

- Les règles d'entreprise contraignantes (Binding Corporate Rules ou BCR) ;
- Les codes de conduite ;
- Des mécanismes de certification approuvé par l'autorité de contrôle ;
- Des instruments juridiques contraignants ;
- Et dans certains cas, des dérogations.

# 2. LES BCR – RÈGLES D'ENTREPRISE CONTRAIGNANTES (BINDING CORPORATE RULES)

Connues sous l'acronyme BCR, pour « Binding Corporate Rules », le Règles d'entreprise contraignantes sont un outil qui permet d'assurer la conformité de transferts de données personnelles entre filiales d'un même groupe, après avoir été approuvées par une autorité de contrôle européenne. Les BCR sont définies par l'article 47 du RGPD qui indique que des règles d'entreprise contraignantes peuvent être approuvée par une autorité de contrôle, dans le cadre du mécanisme de contrôle de la cohérence entre les autorités de contrôle européennes, prévu par l'article 63. Pour être valide, les BCR doivent être juridiquement contraignantes, et appliquées par toutes les entités concernées de l'entreprise y compris leurs employés. Elles doivent conférer expressément aux personnes concernées des droits opposables en ce qui concerne le traitement de leurs données à caractère personnel et comporter au minimum une série de 14 dispositions énumérées au paragraphe 2 de l'article 47.

Les BCR doivent préciser en particulier :

- l'identification du groupe d'entreprises et de ses entités ;
- la description des transferts de données prévus, notamment les catégories de données à caractère personnel, les finalités du traitement et les destinataires des données ;
- le caractère juridiquement contraignantes pour toutes les entités du groupe d'entreprises ;
- les modalités de garantie du respect des principes généraux du RGPD, tels que la limitation de la finalité, la minimisation des données et la protection des données dès la conception ;
- les modalités de garantie des droits des personnes concernées, tels que le droit d'accès, de rectification et d'effacement ;
- la responsabilité du responsable du traitement en cas de violation des BCR ;
- les modalités d'Information des personnes concernées sur les BCR ;
- les mécanismes de supervision mis en œuvre pour garantir leur respect ;
- les modalités de mise à jour régulière pour tenir compte des évolutions législatives et technologiques.

Les BCR doivent, pour être valides, être approuvées par les autorités de contrôle compétentes. L'EDPB publie la liste des BCR approuvées (https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en).

# 3. LE CODE DE CONDUITE APPROUVÉ

Le code de conduite est un outil élaboré par une entité représentative d'une catégorie de responsables de traitement ou de sous-traitants, comportant l'engagement contraignant d'appliquer les garanties appropriées pour assurer la conformité de transferts de données. Prévu par les articles 40 et 41 du RGPD, un code de conduite est un ensemble de règles juridiques qui définissent les bonnes pratiques en matière de protection des données personnelles dans un secteur d'activité donné. Il est élaboré par une organisation représentative du secteur et est juridiquement contraignant pour les professionnels qui y adhèrent.

Un code de conduite présente certains avantages : il permet de construire un socle commun de bonnes pratiques en matière de protection des données, de démontrer sa conformité au RGPD, d'harmoniser les pratiques d'un secteur d'activité, de répondre aux besoins des micros, petites et moyennes entreprises, et d'envoyer un signal positif aux clients et aux professionnels.

Le code de conduite ne doit pas être confondu avec une charte (document non contraignant qui énonce les valeurs et les principes d'une organisation), un guide pratique (document qui fournit des conseils et des recommandations) ou à un code de déontologie (document qui définit les règles de conduite à respecter par les membres d'une profession),

Pour être valable, le code de conduite doit être approuvé par une autorité de contrôle, qui vérifie en particulier le respect de certaines conditions : mise en place par une organisation représentative du secteur, conformité aux exigences du RGPD, accessibilité au public, existence de mécanismes de contrôle et de sanction.

Conformément à l'article 40.11 du RGPD, le comité européen de la protection des données (CEPD/EDPB) qui regroupe les autorités de contrôle, tient à jour un registre des codes conduite approuvés. Cinq ans après l'entrée en application

du RGPD, une dizaine de codes de conduite seulement ont été approuvés en Europe[1], dont celui des fournisseurs de services d'infrastructures *cloud*, approuvé par la CNIL.

Le CEDP/EDPB a adopté le 22 février 2022 ses *« lignes directrices 04/2021 sur les codes de conduite en tant qu'outils pour les transferts »*[2] qui précisent comment les codes de conduite peuvent assurer la conformité des transferts.

Pour que ces codes soient valides, ils doivent aborder les principes, droits et obligations essentiels découlant du RGPD pour les responsables du traitement et les sous-traitants, ainsi que les garanties spécifiques au contexte des transferts.

Les lignes directrices 04/2021 fournissent une liste de contrôle des éléments à inclure dans un code de conduite destiné aux transferts.

Le code de conduite est un outil à portée collective et n'est donc pas une solution adaptée pour les transferts réalisé par une entité individuelle.

# 4. LE MÉCANISME DE CERTIFICATION APPROUVÉ

Conformément à l'article 46.2.f du RGPD, la conformité des transferts de données hors Union européenne peut être assurée par des engagements garantis par un mécanisme de certification, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.

Le processus de certification est défini par les articles 42 et 43 du RGPD.

La certification permet d'établir qu'un produit, un service, un processus ou un système de données a été évalué conforme aux critères d'un référentiel, préalablement approuvés par une autorité de contrôle ou par le Comité européen de la protection des données (CPED/EDPB). L'évaluation est effectuée par un tiers certificateur qui doit lui-même être agréé.

Selon le site de la CNIL[3], *« la certification est donc un outil de responsabilisation (accountability ou redevabilité) car elle permet aux entreprises, administrations, associations, etc., de disposer d'éléments qui leur permettront de démontrer le respect du RGPD en justifiant de leur conformité à des critères précis. Ces critères prennent en compte les obligations qui incombent aux responsables du traitement et aux sous-traitants et peuvent également intégrer des exigences dont le but est de : valoriser certaines pratiques plus protectrices des données ; guider les professionnels dans leur mise en conformité au RGPD ; assurer la cohérence entre les évaluations réalisées par différents organismes certificateurs et ; apporter davantage de transparence auprès des personnes dont les données font l'objet d'un traitement. »*

Le CEPD/EDPB a adopté le 14 janvier 2023 ses « lignes directrices 07/2022 sur la certification en tant qu'outil au service des transferts »[4] qui précisent comment un mécanisme de certification peut assurer la conformité des transferts.

Ces lignes directrices fournissent un cadre complet pour l'utilisation de la certification comme mécanisme de transfert de données à caractère personnel vers des pays tiers, et traitent des points suivants :

- Les exigences en matière d'agrément des organismes de certification ;
- Les critères de certification spécifiques applicables aux transferts vers des pays tiers ;
- Les engagements contraignants et exécutoires que les importateurs et exportateurs de données doivent prendre ;
- Des exemples de mesures supplémentaires qui peuvent être prises pour compléter les garanties fournies par la certification.

# 5. LES DÉROGATIONS

Enfin, l'article 49 du RGPD prévoit qu'en l'absence des situations d'adéquation ou d'encadrement précédentes, les transferts de données peuvent s'effectuer dans le cadre de dérogations pour des situations particulières et des conditions spécifiques.

1 https://edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_fr
2 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_fr
3 https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-la-certification
4 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072022-certification-tool-transfers_fr

Le CEPD/EDPB a précisé ces cas de dérogation dans ses Lignes directrices 2/2018 relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679 adoptées le 25 mai 2018[5]. Ces dérogations sont les suivantes :

**1. Consentement explicite de la personne**, après avoir été informée des risques que pouvaient représenter ce transfert (par exemple via une case à cocher « j'accepte le transfert ») ;

**2. Transfert nécessaire à l'une des situations** suivantes (liste limitative) :

- **Exécution d'un contrat entre la personne concernée et le responsable du traitement** ou mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée ;
- **Conclusion ou exécution d'un contrat conclu dans l'intérêt de la personne concernée** entre le responsable du traitement et une autre personne physique ou morale ;
- **Motifs importants d'intérêt public** ;
- Constatation, exercice ou défense de **droits en justice** ;
- **Sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes**, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;
- Transfert effectué au départ d'un **registre public** ;
- **Intérêts légitimes impérieux**, sous réserve de respecter les conditions (cumulatives) suivantes :
  - Le transfert n'est pas répétitif,
  - Il ne touche qu'un nombre limité de personnes,
  - Il est nécessaire aux fins des intérêts impérieux poursuivis par le responsable de traitement (mais ne prévalent pas sur les droits des personnes),
  - Le responsable de traitement a évalué toutes les circonstances du transfert et offre des garanties appropriées,
  - La CNIL est informée du transfert.
  - La personne concernée est informée du transfert et des intérêts légitimes impérieux poursuivis.

5 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_fr.pdf

Campus Cyber
Tour Eria
5 rue Bellini
92821 Puteaux cedex
Tel : +33 1 53 25 08 80
clusif@clusif.fr
https://clusif.fr

L'intégralité de la FAQ RGPD et la liste des membres qui y ont contribué sont consultables sur le site du Clusif
https://clusif.fr/les-publications