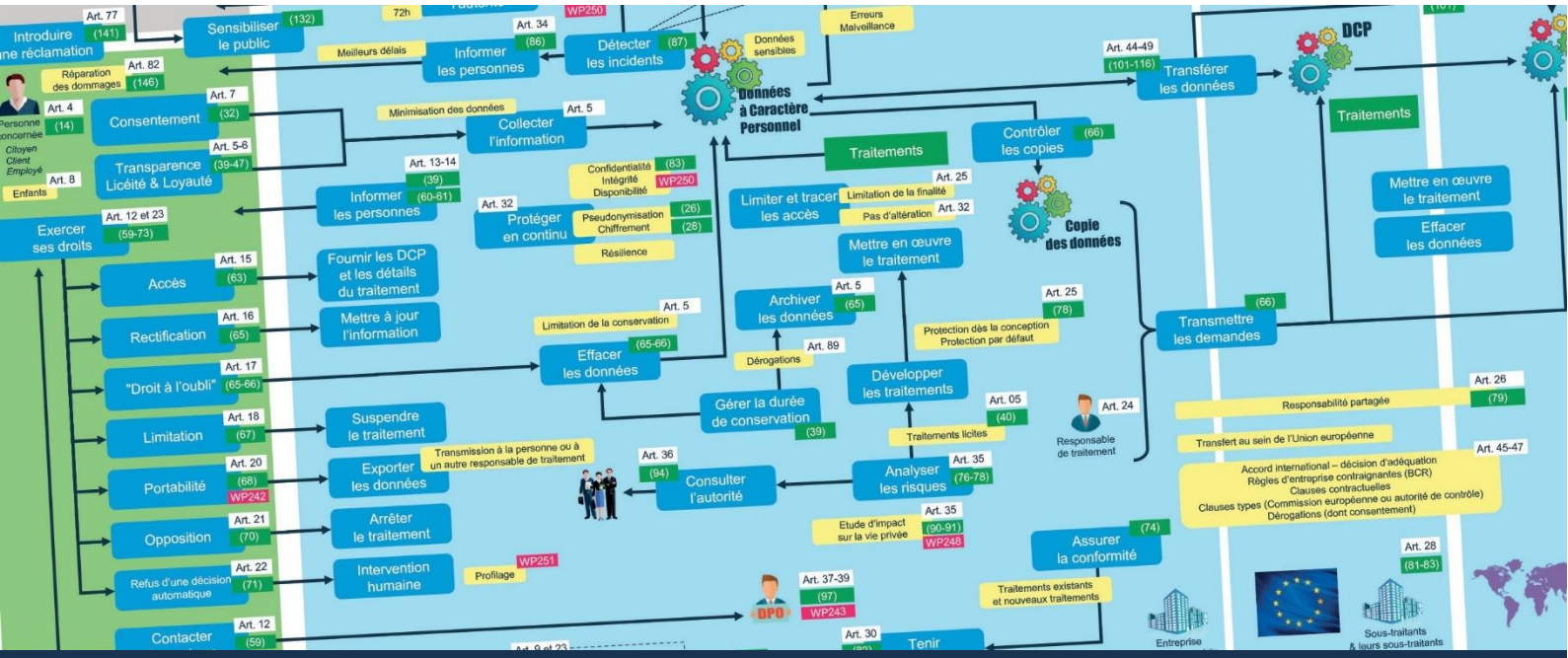
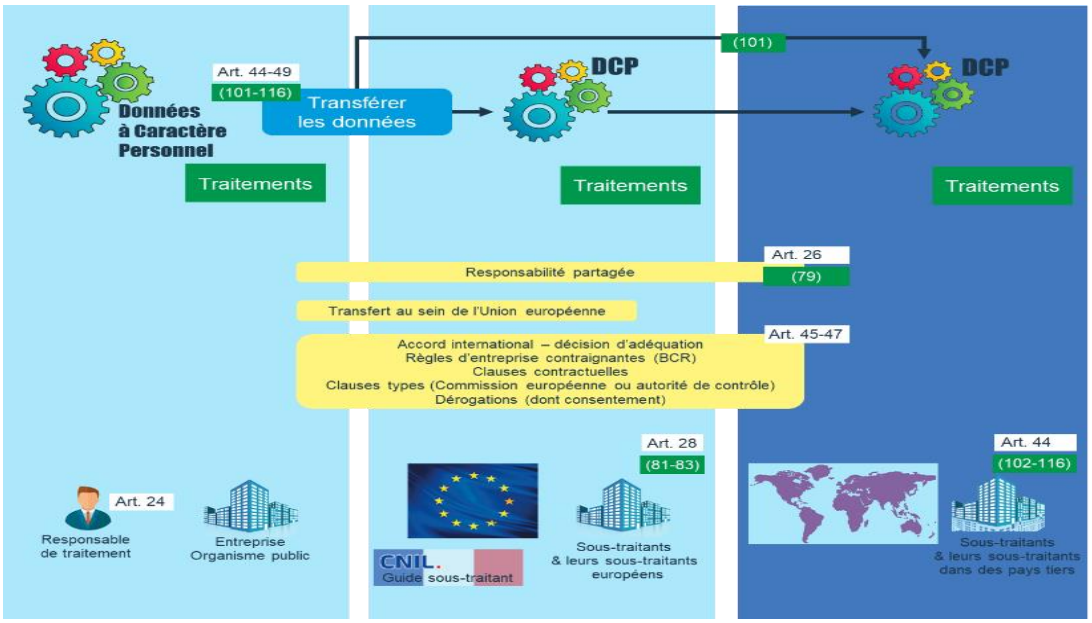
LES FICHES PRATIQUES du CLUSIF - RGPD



LE TRANSFERT DE DONNÉES À CARACTÈRE PERSONNEL

Le règlement européen et la loi Informatique et Libertés posent le **principe de la libre circulation des données à caractère personnel au sein de l'Union européenne (UE)**. Les États membres de l'UE sont en effet tous soumis à la réglementation européenne en vigueur qui prévoit les mêmes principes et garanties pour le traitement de données à caractère personnel.

Ils encadrent précisément les transferts internationaux de données. Les responsables de traitement et les sous-traitants peuvent transférer des données à caractère personnel en dehors de l'Union européenne et de l'Espace Economique Européen (EEE) à condition d'assurer un **niveau de protection des données suffisant et approprié** *"de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet"* (*LIL, Art 68*). Ils doivent encadrer ces transferts en utilisant les différents outils juridiques définis aux articles 44 à 50 du règlement, qui répondent aux différentes situations rencontrées par les responsables de traitement de données et leurs sous-traitants.



Les outils de transfert proposés par le règlement européen sont complémentaires et répondent chacun à un besoin spécifique tant pour le secteur privé que pour le secteur public. Ils permettent aux organisations d'offrir une meilleure conformité et une protection plus efficace pour les individus.

1. DÉFINITION DU TRANSFERT DE DONNÉES À CARACTÈRE PERSONNEL

La notion de transfert de données en dehors de l'Union Européenne n'est pas définie dans le RGPD. Toutefois, elle doit être interprétée de façon large, comme l'est d'ailleurs la notion de traitement. Ainsi, selon le guide de la CNIL[1] publié en 2012, *« Le transfert peut s'effectuer par communication, copie ou déplacement de données, par l'intermédiaire d'un réseau (ex. accès à distance à une base de données) ou d'un support à un autre, quel que soit le type de support (ex. d'un disque dur d'ordinateur à un serveur) »*, ou encore *via* un support papier. Le transfert peut donc avoir lieu en cas de consultation par un tiers des données dans le système de traitement.

La qualification de transfert a été écartée par la Cour de justice de l'Union européenne (CJUE) dans le cas suivant : lorsqu'une personne qui se trouve dans un État membre, poste un contenu avec des données personnelles sur un site internet hébergé dans un État membre, rendant ainsi ces données accessibles à toute personne connectée à internet, y compris depuis un pays tiers (*CJUE C-101-01, 6 novembre 2003, Bodil Lindqvist*[2]).

Pour rappel, le règlement est également applicable lorsque les personnes concernées par un traitement de données se voient offrir des biens ou services au sein de l'Union Européenne, alors même que le responsable de traitement ou le sous-traitant seraient hors de l'Union. En pratique, la réglementation, qui instaure un socle minimum de protection des données, est donc opposable à de nombreuses entreprises situées en dehors de l'Union Européenne.

[1] https://www.cnil.fr/sites/default/files/typo/document/GUIDE-transferts-integral.pdf

[2] http://curia.europa.eu/juris/document/document.jsf?docid=48382&doclang=FR

2. MÉCANISMES À METTRE EN PLACE EN CAS DE TRANSFERT DE DONNÉES

L'article 44 du règlement pose le principe selon lequel un transfert de données par un responsable de traitement ou un sous-traitant hors d'un pays de l'Union Européenne, ne peut se faire que si le niveau de protection des données mis en place par le règlement est garanti *via* différents mécanismes. Le caractère suffisant du niveau de protection assuré par un État s'apprécie en fonction notamment *"des dispositions en vigueur dans cet État, des mesures de sécurité qui y sont appliquées, des caractéristiques propres du traitement (finalités, durée de conservation) ainsi que de la nature, de l'origine et de la destination des données traitées"* (*LIL, Art 68*).

Afin d'assurer ce haut niveau de protection des données mentionné par le règlement, les organismes souhaitant transférer des données vers un pays tiers peuvent recourir aux outils suivants, le mécanisme étant construit en cascade :

Décision d'adéquation (*RGPD, Art 45*)	**1er outil juridique d'encadrement**. Examen global de la législation en vigueur : • Dans un État ; • Sur un territoire applicable ; • À un ou plusieurs secteurs déterminés au sein de cet État.	• ***Décision de la Commission européenne*** *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.* • ***Privacy Shield*** *Repose sur le principe d'auto-certification des organismes (renouvelable tous les ans). Le transfert doit obligatoirement faire l'objet d'un contrat.* *La liste des organismes auto-certifiés est tenue par le Department of Commerce, USA.*	Aucune formalité CNIL
Garanties appropriées (*RGPD, Art 42, 46 et suivants*)	**En l'absence de décision d'adéquation** Pour la majorité, constituées par des décisions des autorités de contrôle et qui sont prises à la lumière des engagements des organismes concernés.	• ***Clauses contractuelles types*** *CCT adoptées par la CNIL ou la CE qui pourront être reprises telles quelles par l'entreprise, par le responsable de traitement, ou le sous-traitant et l'entreprise située hors UE.* *(RGPD, Art 46.2(c) et (d))* • ***BCR - Binding Corporate Rules*** *Transfert entre filiales d'un même groupe : Règles d'entreprises contraignantes au sein d'un groupe qui seront approuvées par une autorité de contrôle européenne.* *(RGPD, Art 47)* • ***Code de conduite approuvé*** *Élaboré par une association représentant des catégories de responsables de traitement ou de sous-traitants.* *Approuvé (comportant l'engagement contraignant et exécutoire pris par les destinataires hors UE d'appliquer les garanties appropriées).* • ***Mécanisme de certification approuvé*** *Comportant l'engagement contraignant et exécutoire pris par les destinataires hors UE d'appliquer les garanties appropriées.* *Approuvé par un organisme de certification ou une autorité de contrôle européenne.* *(RGPD, Art 42 et 46.2 (e))*	Aucune formalité CNIL

		• ***Instruments juridiques contraignants et exécutoires entre autorités et organismes publics*** *(RGPD, Art 46.2 (a))*	
		• ***Arrangement administratif ou un texte juridiquement contraignant et exécutoire*** *pris pour permettre la coopération entre autorités publiques* *(MOU - Mémorandum of Understanding dit MOU ou convention internationale…).* *(RGPD, Art 46.3 (b)* • ***Clauses contractuelles ad hoc*** *Clauses contractuelles spécifiques qui devront être autorisées par une autorité de contrôle européenne (et alors considérées comme équivalentes aux modèles de clauses de la CE).* *(RGPD, Art 46.3)*	Accord CNIL
Dérogations (*RGPD, Art 49*)	En l'absence de telles garanties appropriées, le transfert peut enfin être réalisé par **dérogation** à ces outils globaux d'encadrement, dans des situations particulières et des conditions spécifiques. Le CEPD a précisé les dispositions de l'article 49 dans ses lignes directrices 2/2018 adoptées le 25 mai 2018.	• ***Consentement exprès 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 ») ;* • ***Transfert nécessaire*** *(liste limitative) :* *1.* ***Sauvegarde de la vie humaine*** *;* *2. Sauvegarde de* ***l'intérêt public*** *;* *Exemple en cas d'échange entre autorités de la concurrence, administrations fiscales ou douanières, entre autorités de surveillance financières, entre services chargés des questions de sécurité sociale ou relatives à la santé publique,* *3. Respect des obligations permettant d'assurer la constatation, l'exercice ou la défense d'un* ***droit en justice*** *;* *4. Consultation d'un* ***registre public destiné à l'information*** *et ouvert à la consultation du public ;* *5.* ***Exécution d'un contrat*** *entre le responsable de traitement et la personne concernée ;* *6.* ***Contrat dans l'intérêt de la personne concernée*** *conclu entre le responsable de traitement et un tiers.*	Aucune formalité CNIL
		• ***RGPD, Art 49 - situations particulières*** *:* *Il est possible de transférer les données si les conditions (cumulatives) sont réunies :* • *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.*	Info CNIL

3. MAINTIEN DES AUTORISATIONS ACCORDÉES

Les **autorisations de transfert** accordées avant le 25 mai 2018 restent valables jusqu'à leur modification, remplacement ou abrogation par l'autorité de contrôle. Concrètement, les entreprises pourront se prévaloir de ces autorisations tant que les garanties et les décisions sur lesquelles sont fondées leurs transferts sont toujours valables, par exemple, tant que les Clauses contractuelles type adoptées par la Commission européenne n'ont pas été modifiées, remplacées ou abrogées.

Si tel est le cas, à défaut de dispositions spécifiques contraires, il sera nécessaire de signer de nouvelles clauses ou de prévoir de nouvelles garanties appropriées pour encadrer les flux de données hors du territoire européen.

Les décisions d'approbation des BCR restent également valables. Toutefois les groupes ayant des BCR déjà approuvées doivent adapter leurs BCR aux exigences du règlement européen et aux lignes directrices du CEPD.

Les responsables de traitement et sous-traitants devront donc être alertes, pour détecter les différents cas de transfert les concernant, et choisir le ou les mécanismes de garantie qui leur conviennent le mieux. Les grands groupes opteront plus facilement pour les BCR, alors que les clauses contractuelles types pourraient s'avérer plus accessibles aux PME.

LES FICHES PRATIQUES

L'intégralité de la FAQ RGPD (version 2018) et la liste des membres qui ont contribué à son élaboration sont consultables sur le site du CLUSIF : **www.clusif.fr/publications**

CLUSIF