



**À la
rencontre
des acteurs
de la
recherche**

**Les
rendez-vous
anr[®]**

WEBINAIRE

**RGPD, Collaborations internationales et transfert de
données
2026-2027**

SOMMAIRE

Partie 1 : Maîtriser les notions RGPD et ses obligations

- ☐ Champ d'application et objectifs du RGPD
- ☐ Les principes fondamentaux à respecter
- ☐ Les acteurs d'un traitement
- ☐ Les obligations et devoirs du Responsable de traitement
- ☐ Les sanctions en cas de manquement

Partie 2 : les collaborations internationales et les obligations RGPD

- ☐ Le cadre des collaborations internationales
- ☐ Les transferts de données personnelles hors UE
- ☐ La responsabilité conjointe
- ☐ Désignation d'un DPD dans les collaborations internationales
- ☐ Résumé des actions en fonction des différents scénarios envisageables dans le cadre d'une relation internationale

Partie 3 : Transfert de données par une Administration

- ☐ Les documents/données non communicables
- ☐ Les documents/données communicables selon les destinataires
- ☐ Les documents/données à données restreintes



Partie 1 : Maîtriser les notions RGPD et ses obligations

- ❑ **Champ d'application du RGPD**
- ❑ **Objectifs du RGPD**
- ❑ **Les principes fondamentaux à respecter**
- ❑ **Les acteurs d'un traitement**
- ❑ **Les obligations et devoirs du Responsable de traitement**
- ❑ **Les sanctions en cas de manquement**



Champ d'application du RGPD

Le RGPD est un règlement de l'Union Européenne (UE) qui constitue le texte de référence en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données pour les personnes au sein de l'UE.

Qu'est ce qu'une donnée personnelle ?

Toute information permettant d'identifier directement (nom, prénom, adresse) ou indirectement (identifiant, IP...) une personne physique.

Exemples:

 Adresse email

 Numéro de téléphone

 Nom, prénom

Champ d'application du RGPD

Qu'est ce qu'un traitement ?

Toute opération ou ensemble d'opérations portant sur des données, quel que soit le procédé utilisé (collecte, modification, conservation, utilisation, transfert, destruction, consultation...)

Exemple:



Collecter

Formulaire d'inscription



Partager

Envoyer un email



Organiser

Base de données clients



Supprimer

Effacer un compte

💡 **En clair :**

Si on touche à une donnée personnelle, on la traite !

Objectifs du RGPD



Responsabiliser les acteurs du traitement

- Tenir un **registre** des traitements
- Désigner un **délégué à la protection des données (DPO)**
- Documenter la **conformité** (procédures internes)
- Prévoir un encadrement adéquat des **transferts de données** personnelles hors Union Européenne (UE)



Renforcer les droits des personnes

- **Information** des personnes avant toute collecte (mentions d'informations)
- **Politique** de protection des données
- **Droits individuels** : accès, rectification, effacement, opposition, limitation du traitement, portabilité des données



Sécuriser les données

- Mettre en place des **mesures techniques et organisationnelles** adaptées aux risques
- **Analyser l'impact** des traitements si nécessaire
- **Inform**er la Commission Nationale Informatique et Libertés (CNIL) en cas de faille de sécurité

Les principes fondamentaux à respecter



Licéité du traitement

Le traitement doit avoir pour fondement une base légale prévue par l'article 6 du RGPD.

→ Consentement, intérêt légitime, respect d'une obligation légale, exécution d'une mission de service public...)



Minimisation des données collectées

Les données collectées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard de la finalité.



Finalité(s) de la collecte

Les données collectées doivent être collectées pour des finalités déterminées, explicites et légitimes.



Durée de conservation

Les données personnelles doivent être conservées pendant une durée n'excédant pas la durée nécessaire au regard de la finalité du traitement.



Sécurité des données

Les données doivent être conservées de façon à garantir la sécurité des données à l'aide de mesures techniques et organisationnelles adéquates et éviter la perte, la destruction des données à l'aide de mesures techniques et organisationnelles appropriées.



Intégrité et confidentialité

Les données doivent être conservées de façon à garantir la sécurité des données et empêcher leur altération, perte, accès non autorisé ou divulgation.

Les acteurs d'un traitement

RESPONSABLE DE TRAITEMENT

Personne physique ou morale, autorité publique, service ou autre organisme qui détermine les finalités et les moyens du traitement

SOUS-TRAITANT

Personne physique ou morale, autorité publique, service ou tout autre organisme qui traite des données personnelles pour le compte du responsable du traitement (hébergement, maintenance...)

RESPONSABLES CONJOINTS

Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement

Prévoir un encadrement des relations avec ses sous-traitants

Art.28



Encadrement par un contrat liant le sous-traitant au responsable de traitement (objet, durée, finalité...).



Autorisation écrite préalable, spécifique ou générale, pour tout recours à un autre sous-traitant par le sous-traitant.



Traiter les données sur instruction documentée (on précise la finalité du traitement, le type de données, le moyen...).



Garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles adéquates.



Aide le responsable de traitement pour donner suite aux demandes d'exercice des droits des personnes concernées.



Obligation de confidentialité.



Mise à disposition du responsable de traitement de toutes les informations nécessaires au respect de ses obligations et permettre la réalisation d'audits.



Prévoir le sort des données (suppression ou retour des données).



Respecte les exigences de sécurité du règlement.

Obligation d'informer les personnes concernées

Art. 13

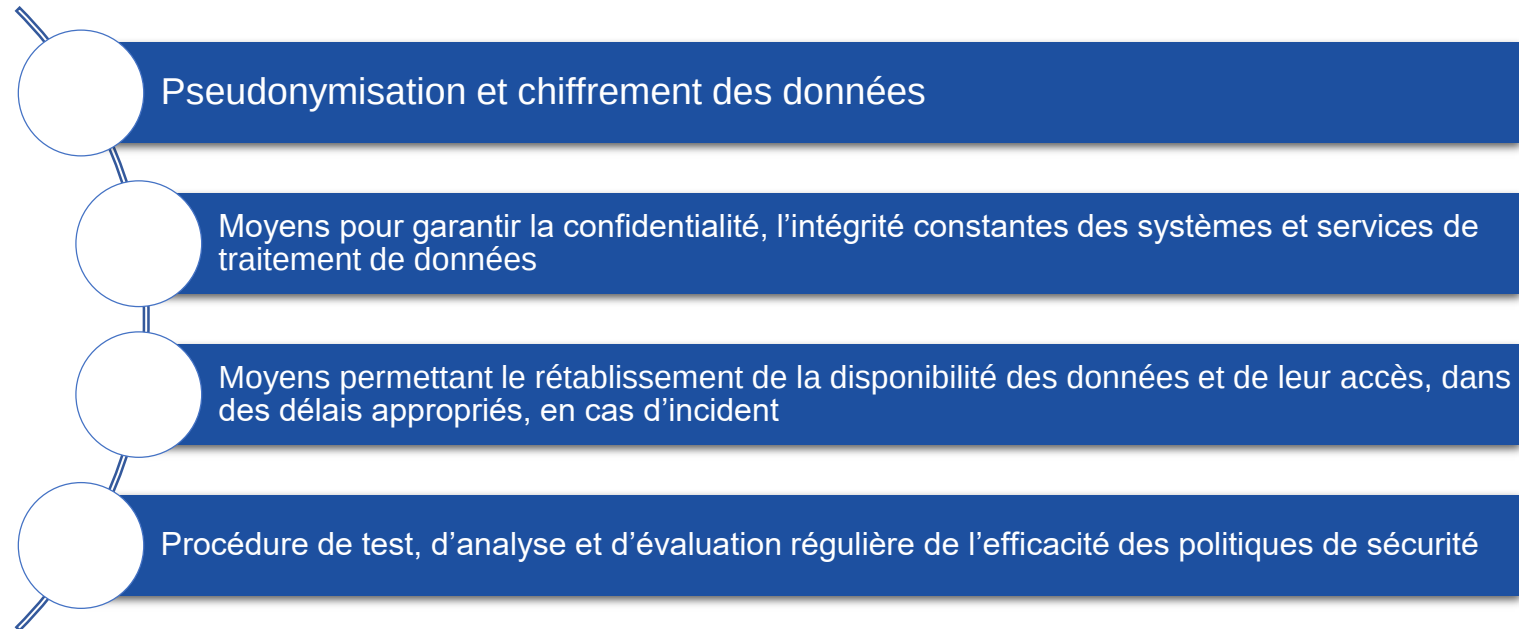
Conformément à l'article 13 du RGPD, les personnes concernées doivent être informées de manière transparente, compréhensible et aisément accessible; des éléments suivants:



A retenir: ces informations doivent être fournies **au moment de la collecte**, ou si elle ne sont pas obtenues auprès de la personne concernée, **dans un délai raisonnable**.

Assurer la sécurité des données personnelles

Obligation de mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, et notamment :



En cas de violation de données personnelles:

Destruction, perte, altération, divulgation non autorisée de données

Notification à la **CNIL** dans un délai de **72h**

Communication de la violation aux personnes concernées en cas de **risque élevé**

Les sanctions en cas de manquement

10M ou 2%
du CA

20M ou 4%
du CA

Absence de registre

Absence d'analyse
d'impact si nécessaire

Non respect de la
limitation de la
conservation des données

Non respect du droit des
personnes

Non respect des règles en
matières de transfert de
données

Quelques chiffres

323 contrôles et 83 sanctions (dont 78 amendes) en 2025



- 486 839 500€ d'amendes cumulées
- 259 mesures correctrices ont été prononcées par la CNIL
- Manquement les plus fréquents:
 - Défaut de coopération avec la CNIL;
 - Non-respect des droits des personnes;
 - Manquement en matière de sécurité des données;
 - Règles applicables aux cookies et à la prospection commerciale.



Les mises en demeure en 2025

- 143 mises en demeure
- 31 rappels aux obligations légales ont été adressées par la CNIL
- Principales thématiques:
 - Absence de réponse aux demandes d'exercice des droits;
 - Insuffisance des mesures de sécurité
 - Dispositifs de vidéosurveillance



Partie 2 : les collaborations internationales et les obligations RGPD

- ❑ Le cadre des collaborations internationales
- ❑ Les transferts de données personnelles hors UE
- ❑ La responsabilité conjointe
- ❑ Désignation d'un DPD dans les collaborations internationales
- ❑ Résumé des actions en fonction des différents scénarios envisageables dans le cadre d'une relation internationale



Le cadre des collaborations internationales

Règles applicables

Applicable
pour tout
traitement

Dans le cadre spécifique
d'une collaboration
internationale

Principes
fondamentaux
issus du RGPD

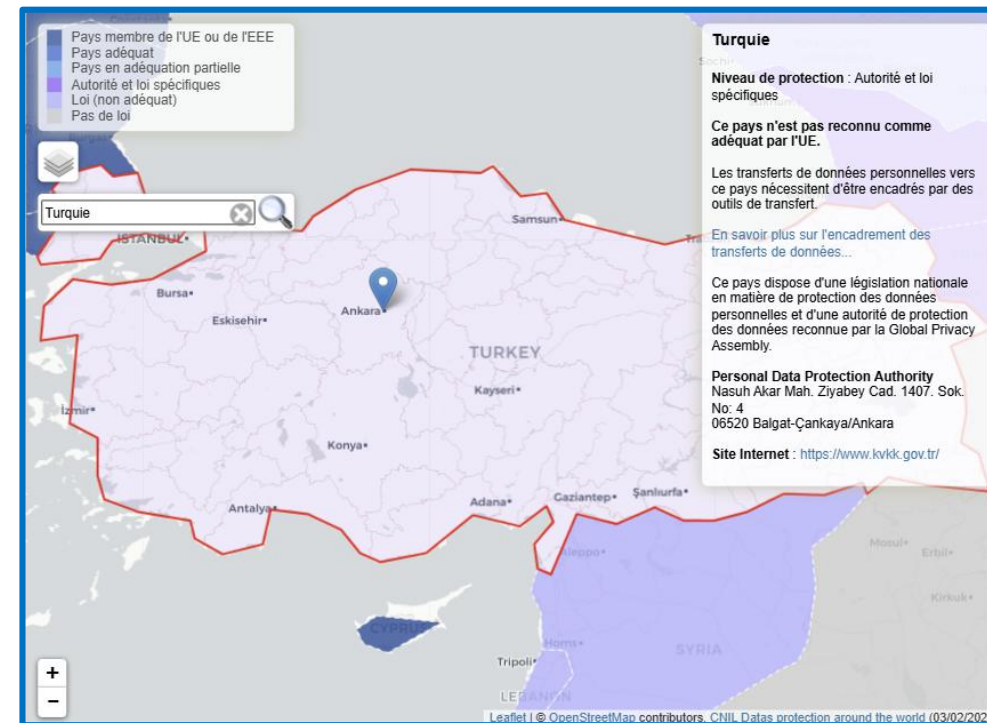
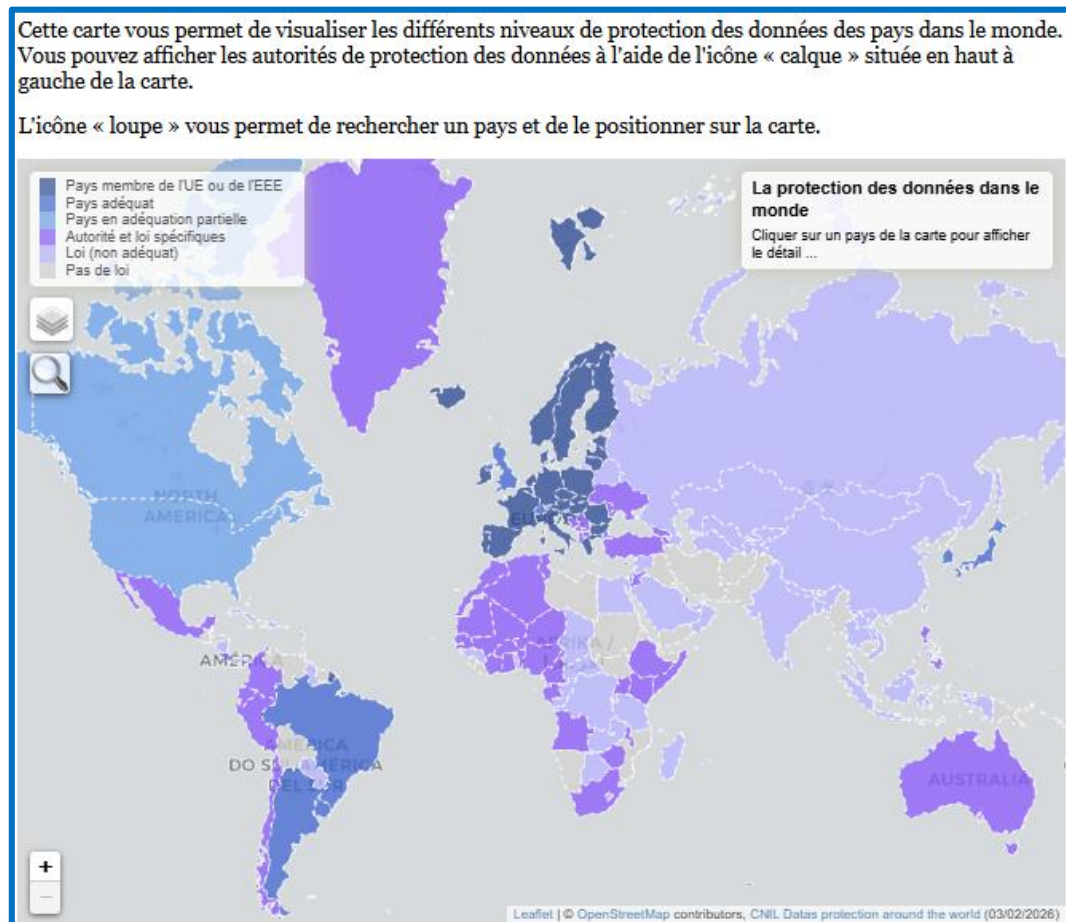
Responsabilité
conjointe

Flux
transfrontières
hors UE

Le transfert de données personnelles hors UE

1/8

[La protection des données dans le monde](#) | [CNIL](#) : La CNIL met à disposition une carte qui permet de déterminer si le pays dispose d'une décision d'adéquation

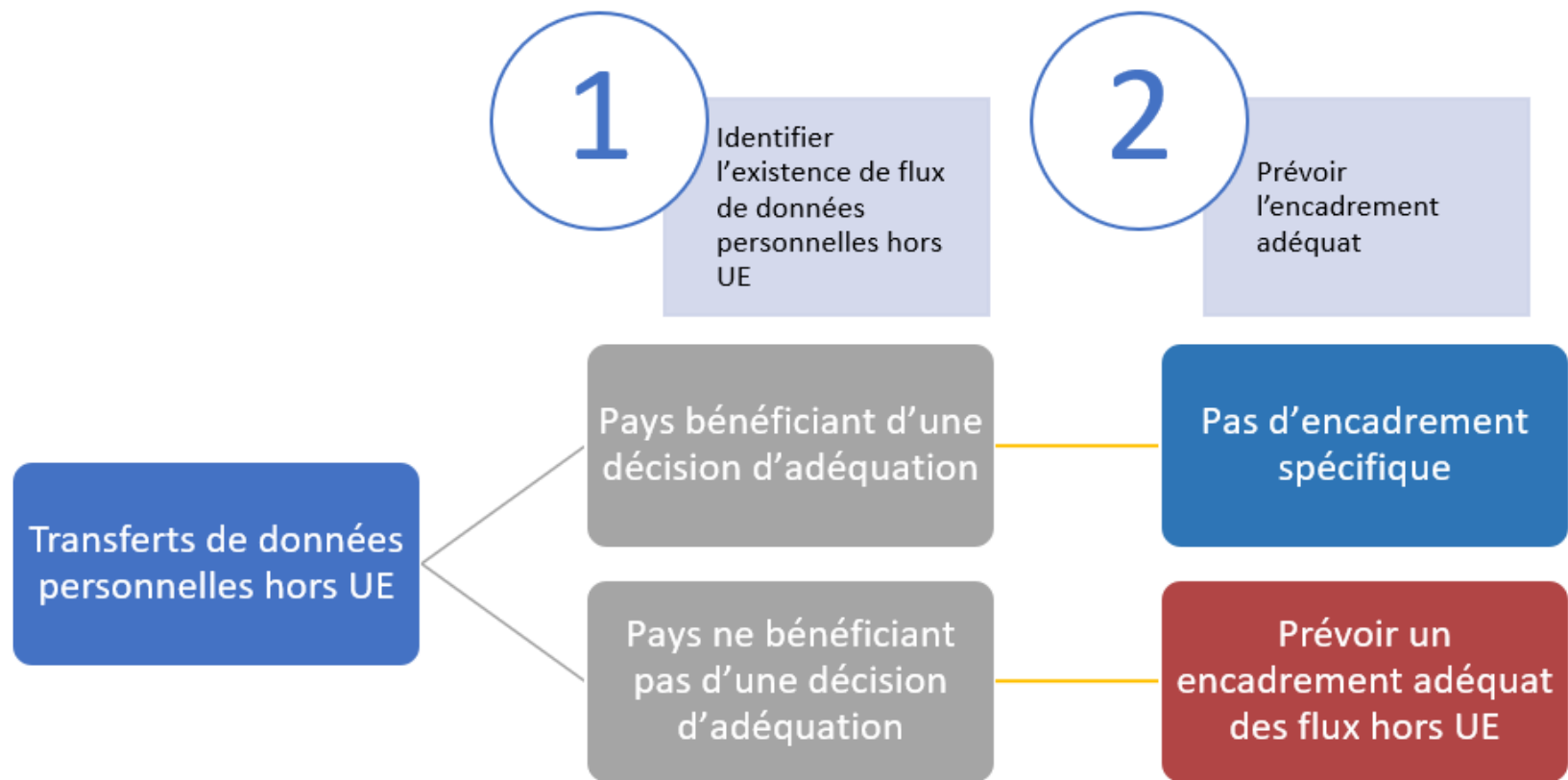


Si l'on est amené à transférer des données personnelles vers un pays ne bénéficiant pas d'une décision d'adéquation, il est alors obligatoire d'encadrer ce transfert.

Les rendez-vous
anr®

Le transfert de données personnelles hors UE

2/8



Le transfert de données personnelles hors UE

3/8

2020- SCHREMS II
(CJUE)

- Invalidation du **Privacy Shield**, qui encadrait les transferts de données entre l'UE et les États-Unis.
- Les **clauses contractuelles types (CCT)** demeurent valides, sous réserve de garanties complémentaires adaptées.

2022
Décisions Google
Analytics

- **DSB (Autriche), janvier 2022** : l'utilisation de Google Analytics entraîne un transfert illicite de données vers les États-Unis.
- **CNIL (France), février 2022** : même position ; les responsables de traitement doivent adapter leur utilisation ou cesser d'utiliser Google Analytics dans sa configuration concernée.

10 juillet 2023
DPF

- **Adoption du Data Privacy Framework (DPF)**: Nouveau cadre juridique permettant les transferts de données vers les organisations américaines certifiées.

26 septembre 2025t
TUE- DPF

- **Tribunal de l'Union européenne (Affaire *Latombe*, T-553/23)**: Confirmation de la validité de la décision d'adéquation relative au DPF.

Avril 2026
un SCHREMS III?

- La **CJUE** accepte d'examiner le pourvoi dirigé contre le DPF.
- **À ce jour, le DPF reste pleinement applicable.**
- L'enjeu est de déterminer si les garanties américaines (EO 14086, Data Protection Review Court) assurent une protection **essentiellement équivalente** à celle exigée par le RGPD, notamment au regard des programmes de surveillance (**FISA 702** et **EO 12333**).

Le DPF est valable aujourd'hui, mais son avenir dépendra de la décision de la CJUE dans ce qui est déjà présenté comme un potentiel "Schrems III". Les organisations ont donc intérêt à anticiper d'éventuelles évolutions du cadre des transferts internationaux.

Le transfert de données personnelles hors UE

4/8



Suisse	Uruguay	Corée du Sud	Japon	Nouvelle Zélande	Israël
Canada (traitements dans le cadre commercial)	Jersey	Andorre	Iles Féroé	Guernesey	Ile de Man
	Royaume-Uni	Argentine	Etats-Unis (adéquation partielle)	Pays membres de l'EEE (Norvège, Islande, Liechtenstein)	

Le transfert de données personnelles hors UE

5/8

Absence de
décision
d'adéquation

Nécessité
d'encadrer les flux
par des garanties
appropriées

Clauses contractuelles types

- Modèles de contrats de transfert de données personnelles
- Adoptées par la Commission Européenne
- 4 modules : RT/RT ; RT/ST ; ST/ST ; ST/RT

Règles internes d'entreprise (BCR)

- Binding Corporate Rules
- Constituent un code de conduite, définissant la politique d'entreprise en matière de transferts de données personnelles
- Article 47

Arrangement administratif

- Doivent prévoir des droits opposables aux personnes concernées et être autorisés par la CNIL
- ou un texte juridiquement contraignant et exécutoire pour permettre la coopération entre les autorités publiques

Code de conduite

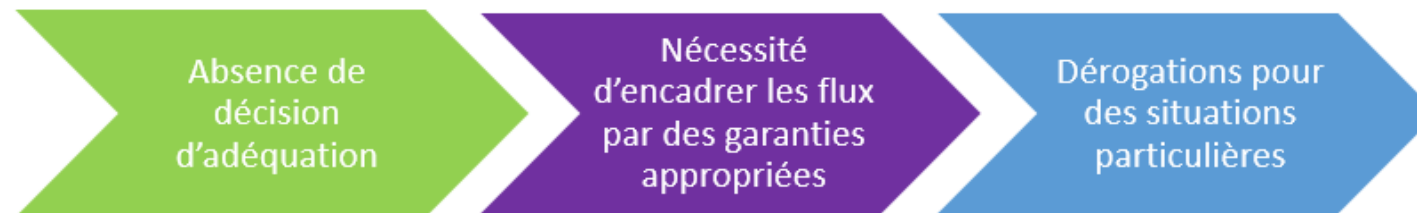
- Adopté conformément à l'article 40
- Assortie de l'engagement contraignant et exécutoire d'appliquer les garanties appropriées

Mécanisme de certification

- Approuvé (comportant l'engagement contraignant et exécutoire pris par les destinataires hors UE d'appliquer les garanties appropriées)

Le transfert de données personnelles hors UE

6/8



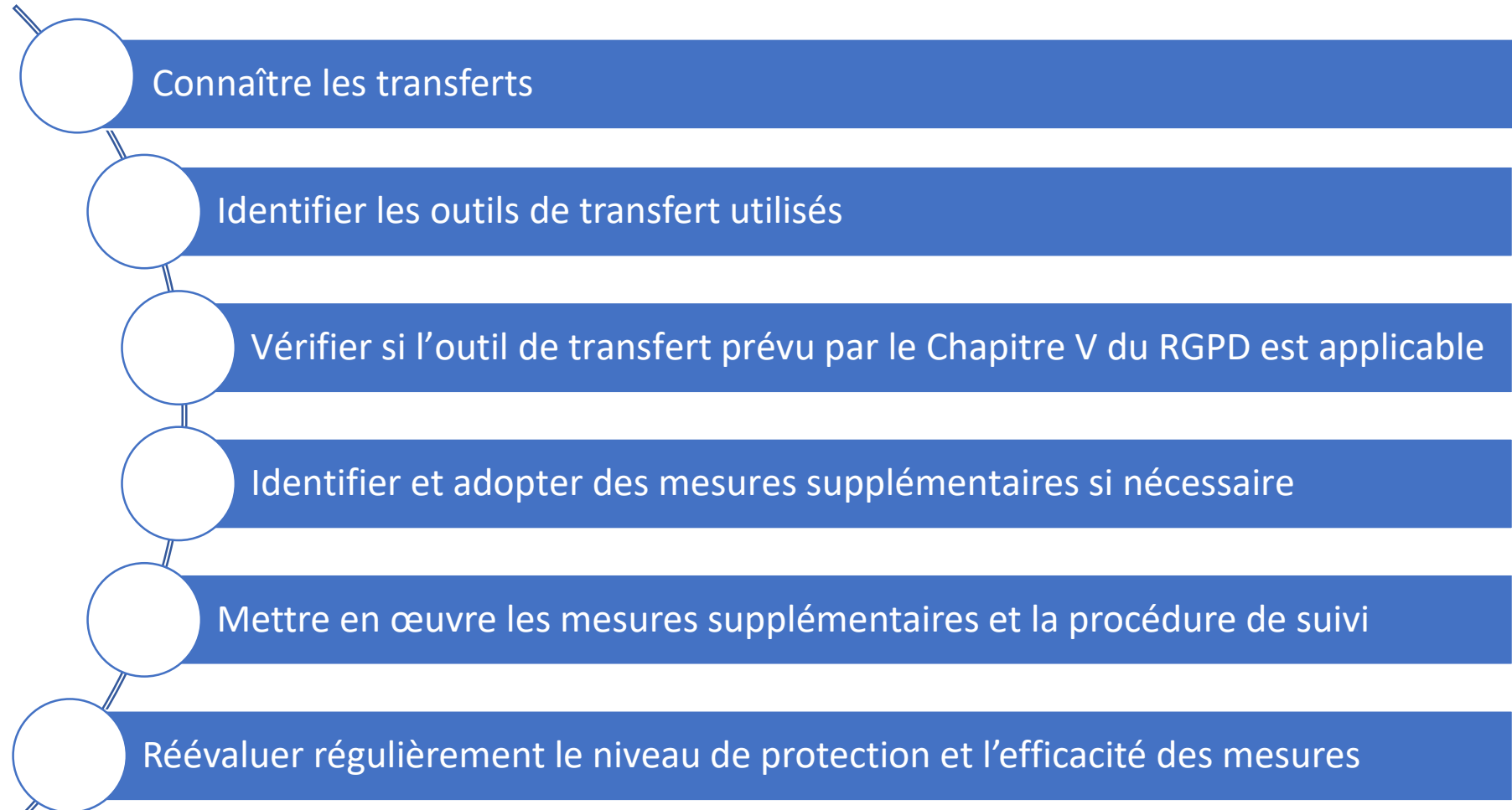
Lorsqu'un Etat tiers n'est pas reconnu comme offrant un niveau de protection adéquat et en l'absence de garanties appropriées encadrant ce transfert, le transfert peut néanmoins, par exception, être opéré. **Ces dérogations ne peuvent être utilisées que dans des situations particulières** : les responsables de traitement doivent s'efforcer de mettre en place des garanties appropriées et ne doivent recourir à ces exceptions qu'en l'absence de telles garanties. **L'article 49 du RGPD fait l'objet d'une interprétation stricte par les autorités de protection des données**, afin que l'exception ne devienne pas la règle.

- **la personne concernée a donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle ;**
- le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à la mise en œuvre de mesures précontractuelles prises à sa demande ;
- le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et une autre personne physique ou morale ;
- le transfert est nécessaire pour des motifs importants d'intérêt public ;
- le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice ;
- le transfert est nécessaire à la 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;
- le transfert a lieu au départ d'un registre qui est légalement destiné à fournir des informations au public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime.

Le transfert de données personnelles vers des pays tiers

7/8

Guidelines CEDP- recommandations



Le transfert de données personnelles hors UE

8/8

A la suite du Brexit, le Royaume-Uni est devenu un pays tiers au sens du RGPD. Toutefois, la Commission Européenne a adopté une décision d'adéquation, **reconnaissant que le niveau de protection des données personnelles offert par le Royaume-Uni est substantiellement équivalent à celui garanti au sein de l'UE.**

Conséquences pratiques: Les transferts de données personnelles depuis l'UE vers le Royaume-Uni peuvent être réalisés sans mise en place de garanties additionnelles de transfert.

Les organismes européens peuvent ainsi transférer des données personnelles vers le Royaume-Uni dans les mêmes conditions que vers tout autre pays bénéficiant d'une décision d'adéquation.



La responsabilité conjointe 1/3

1

Identifier une
responsabilité
conjointe entre
les partenaires

2

Prévoir un
contrat conforme
à l'article 26
RGPD

Finalité du
traitement
décidé
conjointement



Responsabilité
conjointe

Moyens du
traitement
choisis
conjointement

La responsabilité conjointe 2/3

Guidelines du CEDP* sur la notion de responsable du traitement.



Tous les traitements impliquant plusieurs entités ne donnent pas lieu à une responsabilité conjointe de traitement (p. 22)

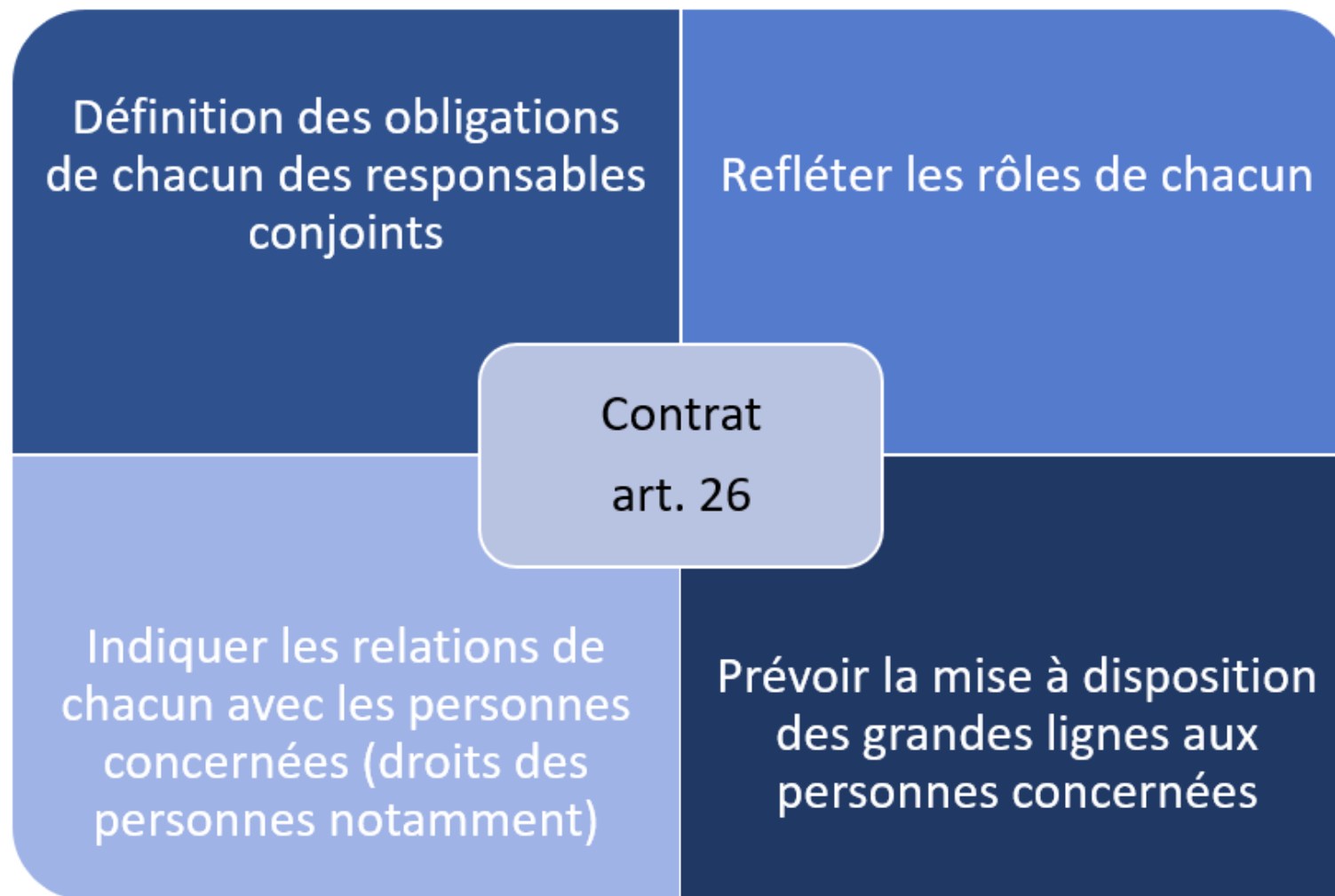
La participation conjointe doit englober, d'une part, la détermination des finalités et, de l'autre, la détermination des moyens (p. 22)

Une analyse du traitement au cas par cas est nécessaire (p.22)

Un critère est soulevé : celui de l'impossibilité de réaliser le traitement sans la participation conjointe des responsables du traitement à la détermination des finalités et des moyens (p. 22)

La responsabilité conjointe n'implique pas un même niveau de responsabilité des acteurs (p.23)

La responsabilité conjointe 3/3



Désignation d'un DPD* dans les collaborations internationales

Il est possible de désigner un référent RGPD comme point de contact pour recenser les sujets sur la protection des données

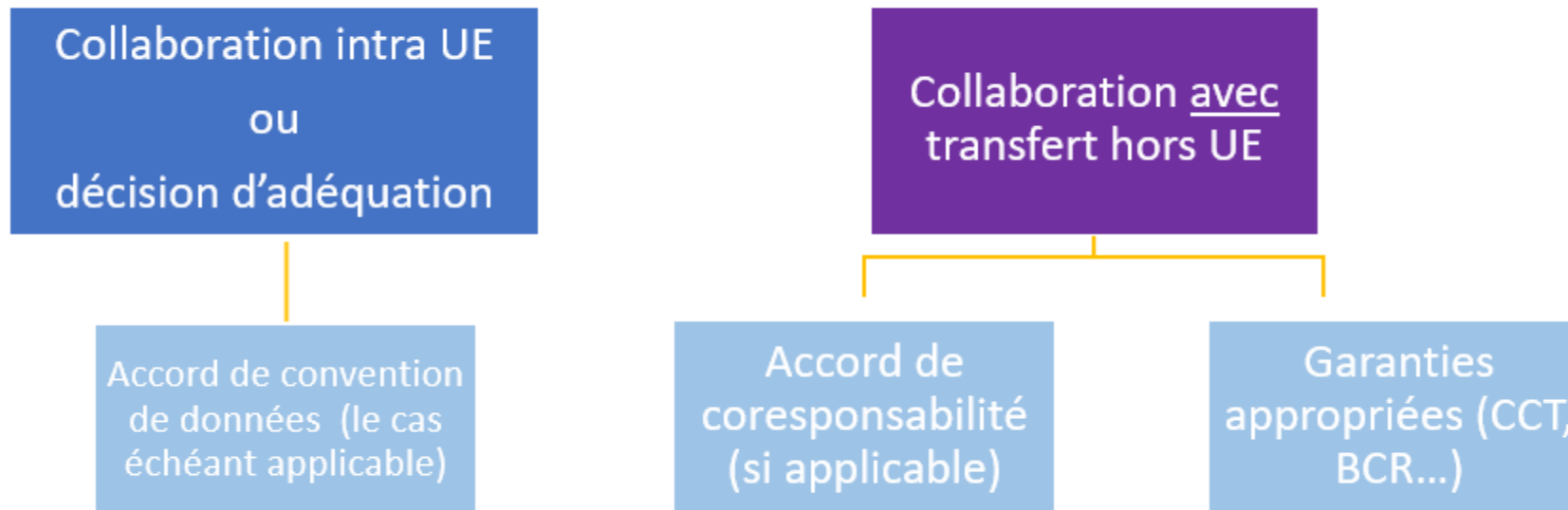
Ce référent peut permettre d'aider les partenaires qui n'auraient pas de DPO ou de référent interne pour les questions RGPD

Ce référent ne sera jamais responsable de la mise en conformité des partenaires

Chaque partenaire devra toujours se conformer par ses propres moyens aux exigences du RGPD

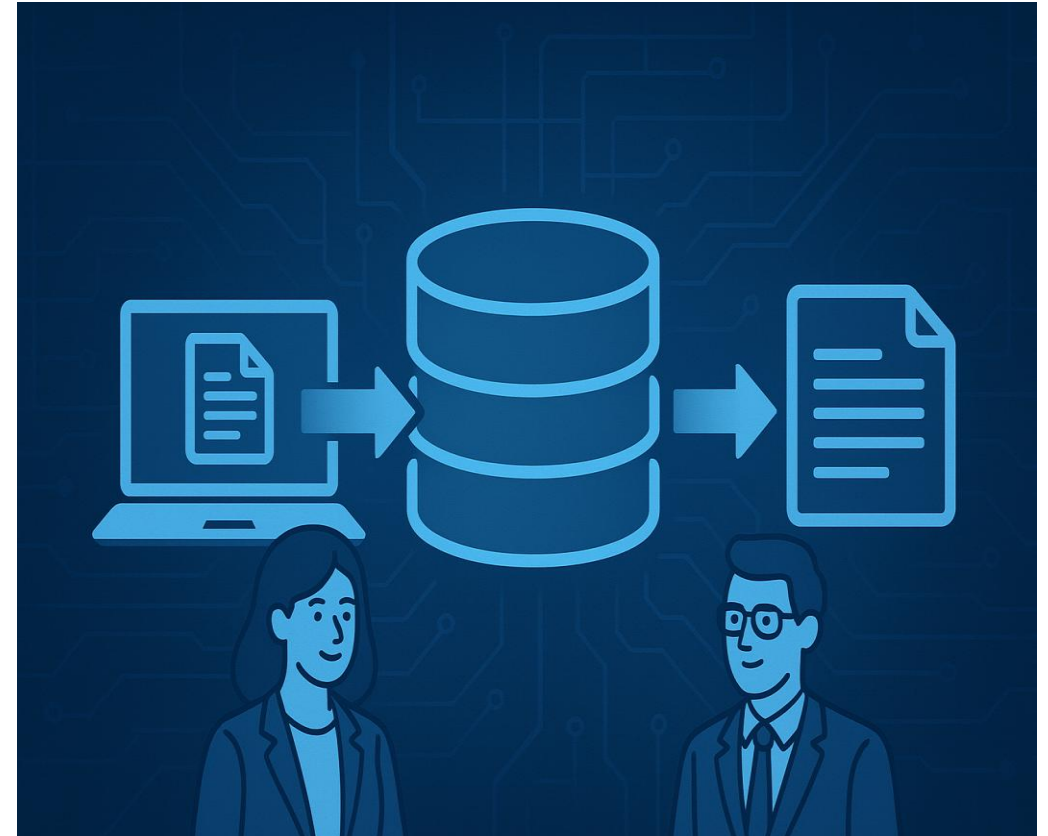


Résumé des actions en fonction des différents scénarios envisageables dans le cadre d'une relation internationale



Partie 3 : Transfert de données par une Administration

- ☐ documents/données non communicables
- ☐ documents/données communicables selon les destinataires
- ☐ documents communicables moyennant retraitement du doc



Les documents/données non communicables

Couverts par un secret spécifique = la divulgation porterait atteinte à :

- des enquêtes policières
- des mesures d'instructions par les juridictions,
- la sécurité publique
- des opérations militaires, la sûreté de l'Etat, la sécurité intérieure, la défense nationale



Les demandes irrecevables

Une autre série d'exceptions, non liée au contenu ou à la nature de la donnée, prévoit que la communication peut être refusée dans d'autres cas, notamment :

- documents faisant déjà l'objet d'une diffusion publique (librement accessibles)
- documents que l'administration ne possède pas ou qui n'existent pas
- documents préparatoires à une décision (tant que la décision n'a pas été prise)
- demandes abusives



Les documents/données à communication restreinte

Ne sont en principe communicables qu'aux personnes concernées les documents :

- portant une appréciation ou un jugement de valeur sur une personne physique
- qui font apparaître le comportement d'une personne, dès lors que la divulgation pourrait lui porter préjudice
- qui dévoilent la vie privée
- qui relèvent du secret médical
- qui relèvent du secret des affaires



Communication sous réserve de retraitement du doc

Le(s) document(s) = mentions non librement communicables à un tiers (exemple secret des affaires, secret vie privée...)

MAIS qu'il est possible d'occulter ou de disjoindre du document.

Droit à communication moyennant occultation (anonymisation, occultation) ou séparation des informations litigieuses :

Par ex:

Rapports scientifiques/rapport de choix des offres pour les marchés publics/PV de « jurys » si les occultations à opérer ne dénaturent pas les docs/ne les rendent pas illisibles



Merci de votre attention

**Contact :
secretariatdaj@anr.fr**

