RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

anr agence nationale de la recherche
AU SERVICE DE LA SCIENCE

# RGPD et collaborations internationales

## Rendez-vous de l'ANR

# Sommaire

# 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.

## Traitement

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

## Données personnelles

- Toute information permettant d’identifier directement (nom, prénom, adresse) ou indirectement (identifiant, IP…) une personne physique

# 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)
- Prévoir un contrat avec les sous-traitants

**Renforcer les droits des personnes**

- Information des personnes avant toute collecte (mentions d'informations, politique de protection des données, politique sur les cookies)
- Davantage de droits individuels : accès, rectification, effacement des données, opposition et limitation du traitement, portabilité des données

**Sécuriser les données**

- Mettre en place des mesures techniques et organisationnelles
- Analyse d'impact des traitements si nécessaire
- Informer 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 telle que prévue par l'article 6 du RGPD (consentement des personnes, intérêt légitime, respect d'une obligation légale, exécution d'une mission d'intérêt public…). |
| Finalité(s) de la collecte | • Les données personnelles doivent être collectées pour des finalités déterminées, explicites et légitimes |
| Minimisation des données collectées | • Les données collectées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard de la finalité |
| Durée de conservation | • Les données 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 et éviter la perte, la destruction des données à l'aide de mesures techniques et organisationnelles adéquates |

# Les acteurs d'un traitement

## Responsable du 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

Article 28

- Garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles
- Autorisation écrite préalable, spécifique ou générale du responsable de traitement pour le recrutement d'un autre sous-traitant par le sous-traitant
- Encadrement par un contrat liant le sous-traitant au responsable de traitement (objet, durée, finalité…)
- Traiter les données sur instruction documentée
- Obligation de confidentialité
- Respecte les exigences de sécurité du règlement
- Aide le responsable de traitement pour donner suite aux demandes d'exercice des droits des personnes concernées
- Prévoir le sort des données (suppression/renvoi des données)
- Mise à disposition du responsable de traitement des informations nécessaires pour apporter la preuve du respect de ses obligations et permettre la réalisation d'audits

# Obligation d'informer les personnes


Article 13

# 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 :

Art. 32

- Pseudonymisation et chiffrement des données
- Moyens pour garantir la confidentialité, l'intégrité constantes des systèmes et services de traitement de données
- Moyens permettant le rétablissement de la disponibilité des données et de leur accès, dans des délais appropriés, en cas d'incident
- Procédure de test, d'analyse et d'évaluation régulière de l'efficacité des politiques de sécurité

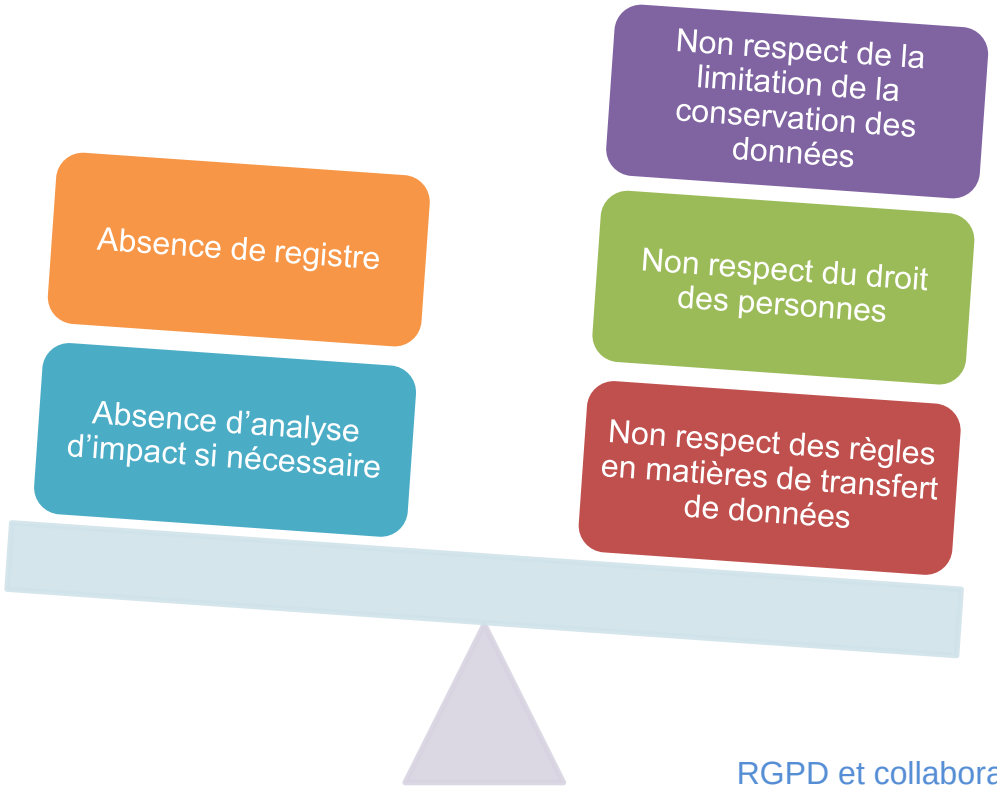
En cas de violation de données :

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

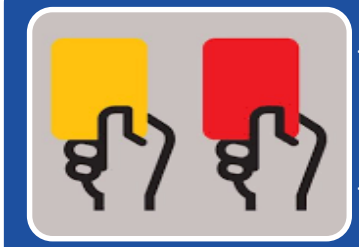
20M ou 4% du CA



# Les sanctions en cas de manquement*

Les contrôles en 2023

- 157 contrôles sur place
- 128 contrôles en ligne
- 38 contrôles sur pièce
- 17 contrôles sur audition



42 sanctions en 2023

- Accroissement du nombre de mesures adoptées : mise en œuvre de la procédure dite de « sanctions simplifiées », d'un accroissement des réclamations et de la coopération européenne.
- Les décisions de sanctions ont porté sur des thématiques variées et ont concerné des acteurs de taille et de secteurs divers.
- Une sanction sur trois comporte un manquement à la sécurité des données.
- 36 amendes pour un montant total de 89 179 500 euros.

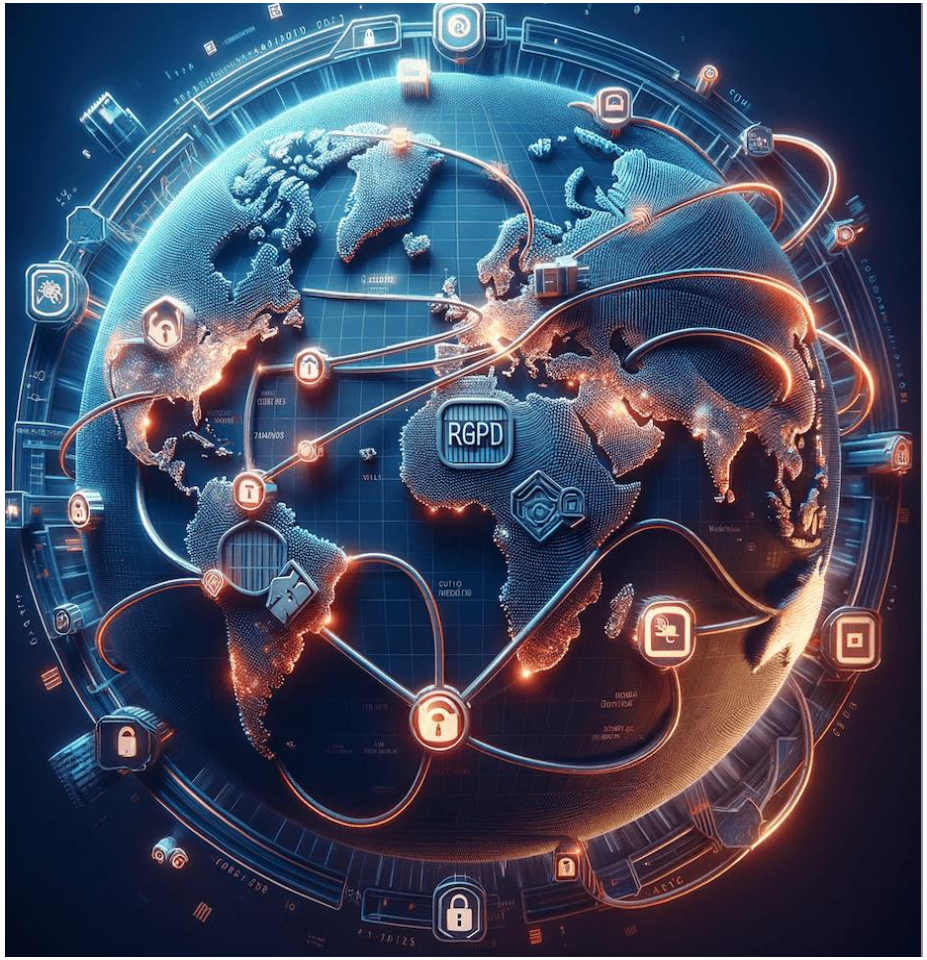
Les mises en demeure en 2023

- Nombre record de mises en demeures avec 168 décisions prononcées.
- Secteurs et problématiques variés : exercice des droits, défaut de coopération avec la CNIL et géolocalisation des procédures.
- Deux séries de décisions ont été adoptées sur des thématiques spécifiques.

*Rapport d'activité de la Cnil 2023

# 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

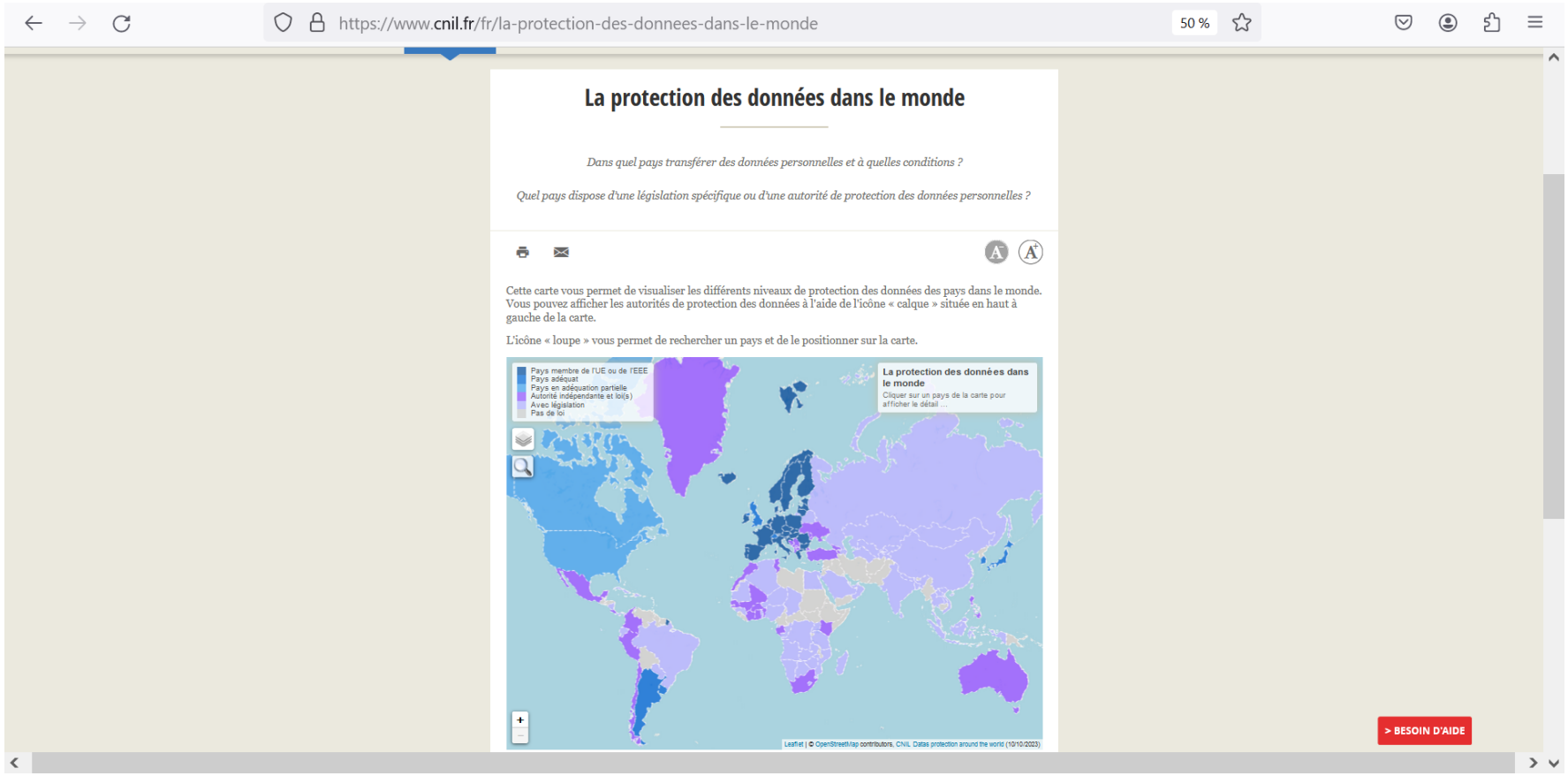
Dans le cas spécifique d'une collaboration internationale

Principes fondamentaux issus du RGPD

Responsabilité conjointe

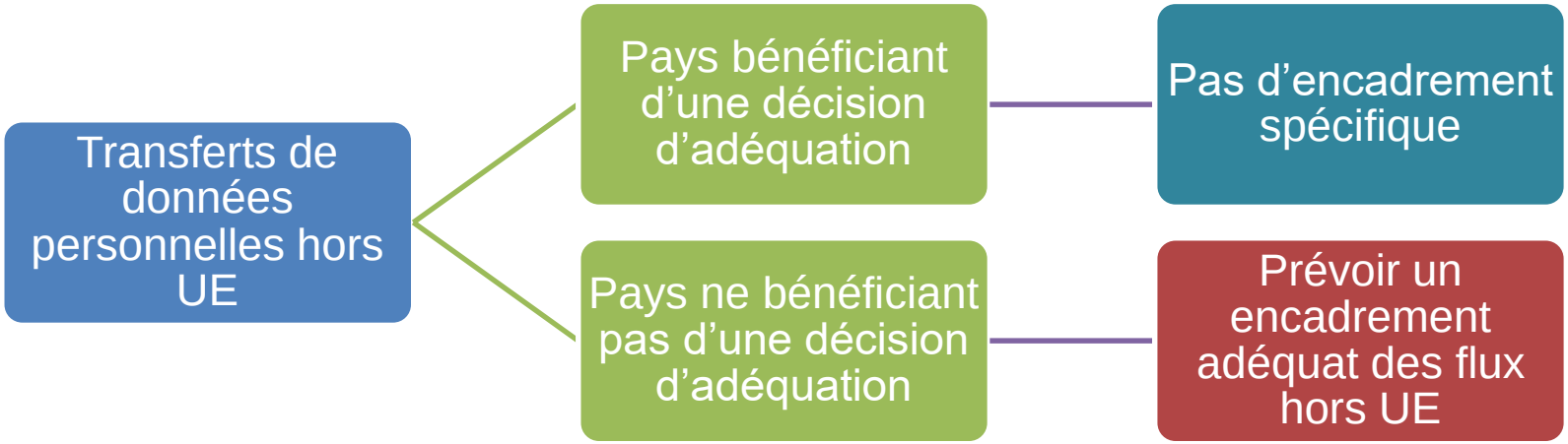
Flux transfrontières hors UE

# Les transferts de données personnelles hors UE 1/8



# Les transferts de données personnelles hors UE 2/8

1. Identifier l'existence de flux de données personnelles hors UE
2. Prévoir l'encadrement adéquat



RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

# Les transferts de données personnelles hors UE 3/8

anr agence nationale de la recherche
AU SERVICE DE LA SCIENCE

**<u>Evènements importants</u>** :

- CJUE, 16 juillet 2020 - arrêt Shrems II : invalidation du Privacy Shield qui encadrait les transferts de données avec les USA

- CJUE, 22 juin 2023 : les CCT ont été confirmées comme un mécanisme valide pour le transfert de données, à conditions que des garanties supplémentaires soient mises en place pour protéger les données transférées.

- <u>Arrêts Google Analytics</u> :

→ Décision de la CNIL, février 2022 : l'utilisation de Google Analytics par un site web français entraîne un transfert illégal de données personnelles vers les États-Unis. La CNIL a ordonné au site web d'adapter son utilisation de Google Analytics ou de cesser son utilisation sous sa forme actuelle.

→ Décision de la DSB (autorité autrichienne de protection des données), janvier 2022

# Les transferts de données personnelles hors UE 4/8


| | | | | | |
|---|---|---|---|---|---|
| Tous les pays membres de l'UE | 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 | | | |

# Les transferts de données personnelles hors UE 5/8

Art. 46

RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

anr agence nationale de la recherche
AU SERVICE DE LA SCIENCE

Absence de décision d'adéquation

Nécessité d'encadrer les flux par des garanties appropriées

| Clauses contractuelles types | Règles internes d'entreprise (BCR) | Arrangement administratif | Code de conduite | Mécanisme de certification |
|---|---|---|---|---|
| • Modèles de contrats de transfert de données personnelles<br>• Adoptées par la Commission Européenne<br>• 4 modules : RT*/RT ; RT/ST* ; ST/ST ; ST/RT | • Binding Corporate Rules<br>• Constituent un code de conduite, définissant la politique d'entreprise en matière de transferts de données personnelles<br>• Article 47 | • Doivent prévoir des droits opposables aux personnes concernées et être autorisés par la CNIL<br>• ou un texte juridiquement contraignant et exécutoire pour permettre la coopération entre les autorités publiques | • Adopté conformément à l'article 40<br>• Assortie de l'engagement contraignant et exécutoire d'appliquer les garanties appropriées | • Approuvé (comportant l'engagement contraignant et exécutoire pris par les destinataires hors UE d'appliquer les garanties appropriées) |

*RT : Responsable du traitement
ST : Sous-traitant

# Les transferts de données personnelles hors UE 6/8

RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

anr agence nationale de la recherche
AU SERVICE DE LA SCIENCE

Art. 49

Absence de décision d'adéquation → Nécessité d'encadrer les flux par des garanties appropriées → Dérogations pour des situations particulières

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.

*RT : Responsable du traitement
ST : Sous-traitant

# Les transferts de données personnelles hors UE 7/8

RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

anr agence nationale de la recherche
LA SCIENCE

edpb European Data Protection Board

## Guidelines du CEDP* sur les transferts HUE de données.

1. Connaître les transferts
2. Recenser les instruments de transferts utilisés
3. Evaluer si l'instrument de transfert prévu à l'article 46 du RGPD auquel l'exportateur a recours est efficace compte tenu de toutes les circonstances du transfert
4. Adoption de mesures supplémentaires
5. Etapes de la procédure à suivre lorsque l'exportateur a identifié des mesures supplémentaires efficaces
6. Réévaluation à intervalles appropriées

* Recommandations 01/2020 version 2.0 adoptées le 18/06/2021

RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

# Les transferts de données personnelles hors UE 8/8

anr agence nationale de la recherche
AU SERVICE DE LA SCIENCE

- **Brexit : la Commission européenne adopte des décisions relatives à l'adéquation du niveau de protection des données concernant le Royaume-Uni.**

La Commission européenne a adopté le 28 juin 2021 deux décisions d'adéquation vis-à-vis du Royaume-Uni - l'une au titre du règlement général sur la protection des données (RGPD) et l'autre au titre de la directive en matière de protection des données dans le domaine répressif.

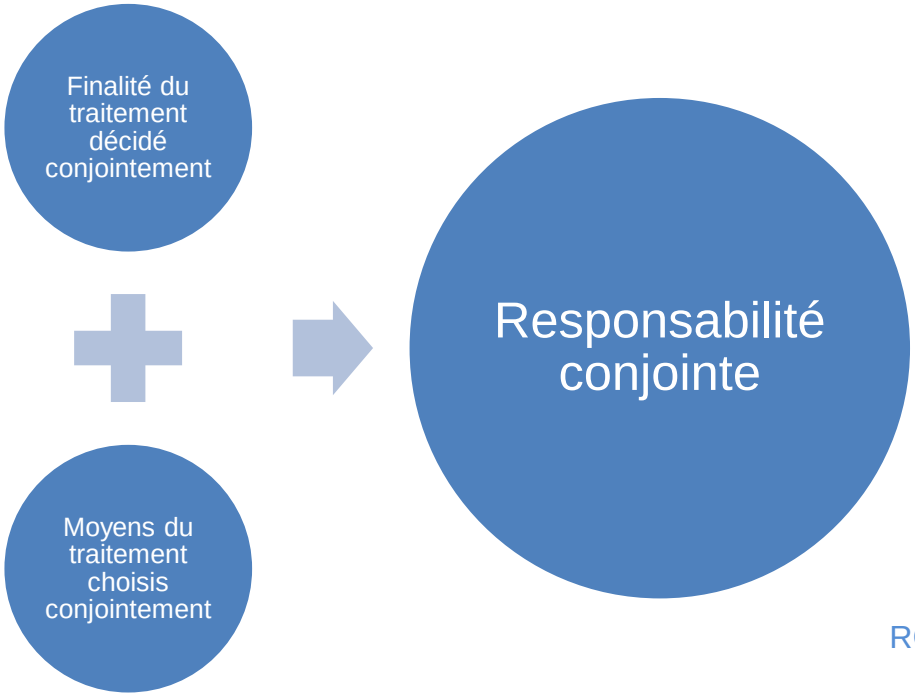
**Les transferts de données personnelles depuis l'Union européenne vers le Royaume-Uni peuvent donc s'effectuer sans encadrement spécifique**, dans la mesure où la Commission européenne constate par ses décisions que ces données bénéficient d'un niveau de protection substantiellement équivalent à celui garanti en vertu de la législation de l'Union.

En pratique, les flux de données personnelles depuis l'UE vers le Royaume-Uni sont bien considérés comme des transferts vers un pays tiers, mais **les responsables du traitement et sous-traitants pourront librement mettre en œuvre ces traitements, sans garanties ou conditions supplémentaires.**

# La responsabilité conjointe 1/3

1. Identifier une responsabilité conjointe entre les partenaires

2. Prévoir un contrat conforme à l'article 26 RGPD



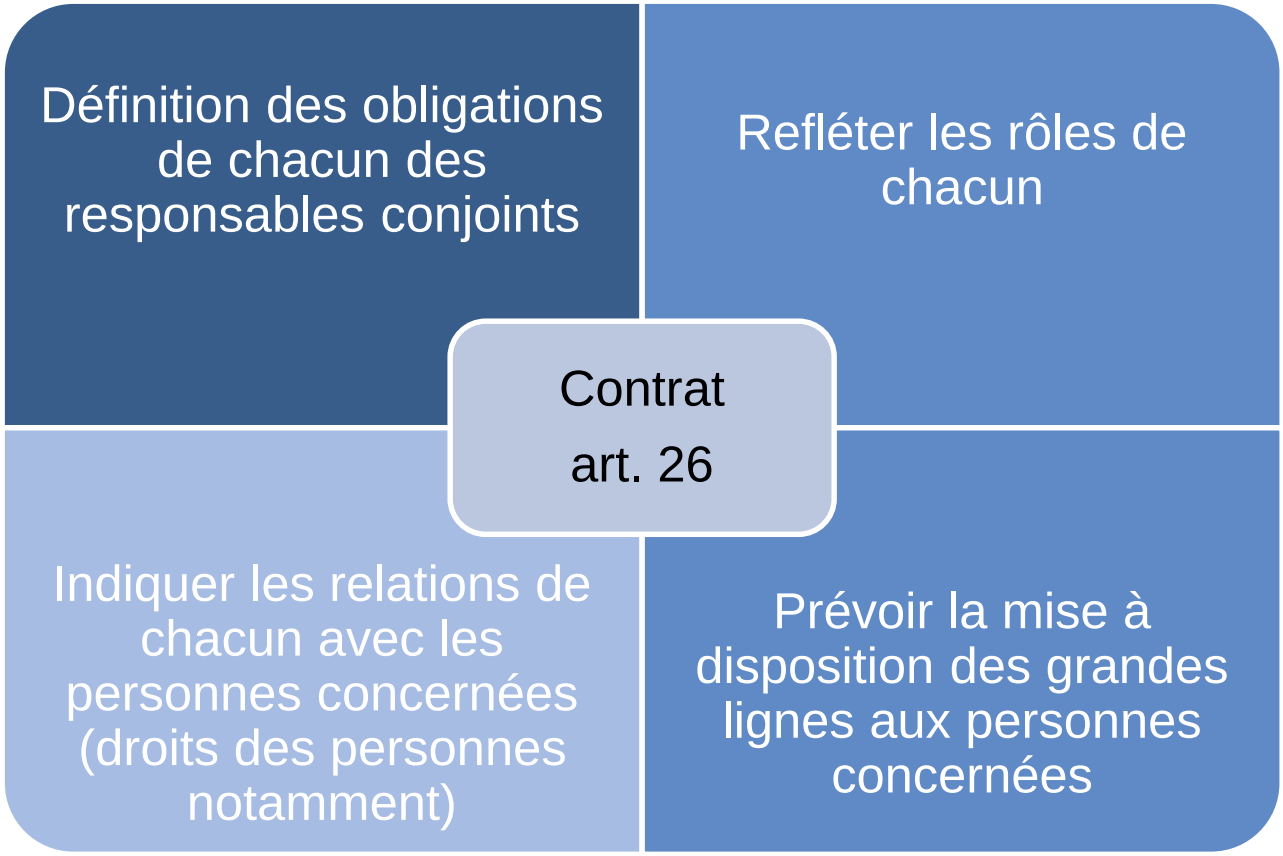
# La responsabilité conjointe 2/3

## 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)

* Lignes directrices 07/2020 version 2.0 adoptées le 07/07/2021

# La responsabilité conjointe 3/3



# Désignation d'un DPD* dans les collaborations internationales

Parfois dans le cadre de certaines collaborations internationales, il est demandé de mettre en place un référent RGPD

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 RGDP

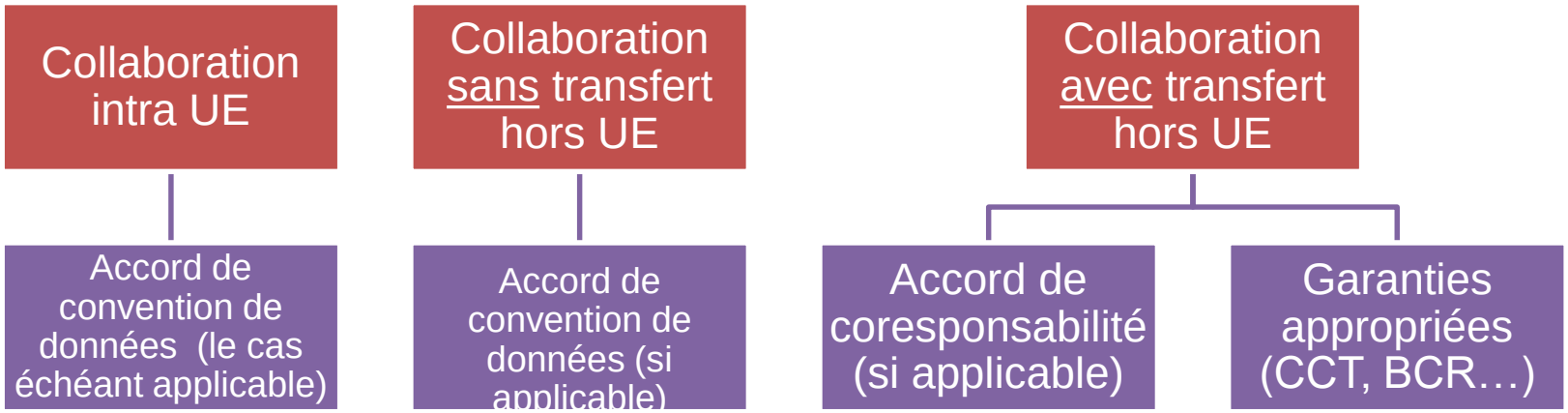
Ce référent ne sera jamais responsable de la mise en conformité des partenaires

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

anr©

* Délégué à la protection des données

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



# Partie 3 : Transfert de données

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

# Les documents/données non communicables 1/2

- faisant **déjà l'objet d'une diffusion publique**
- que l'établissement **ne possède pas**
- qui ont **disparu**, qui n'existent pas
- faisant **l'objet de demandes abusives** (par leur nombre, caractère répétitif…)
- **inachevés** ou en cours d'élaboration jusqu'à prise de décision
- **préparatoires à une décision** en cours d'élaboration
- sur lesquels **les tiers détiennent des DPI** qui se rattachent à une **activité non administrative** ( juridictionnelle, judiciaire, de contrôle ou d'enquête ou à une activité privée)
- **à caractère personnel** dont **l'accès implique la mise en œuvre de requêtes informatiques complexes** ou d'une succession de requêtes particulières qui diffèrent de l'usage courant pour lequel ce fichier a été créé (càd hors données brutes, ou agrégées par thématique, régions, genre, public/privé etc., données de caractérisation des projets)

# Les documents/données non communicables 2/2

**Couvert par le secret** = la divulgation porterait atteinte aux secrets protégés :

- défense nationale,
- à la mise en œuvre de la politique extérieure de la France,
- à la sûreté de l'Etat,
- à la sécurité publique,
- à la sécurité des systèmes d'information des administrations,
- des personnes,
- le secret des affaires :
  - secret des procédés ( techniques de fabrication/travaux de recherche, moyens humains techniques mobilisés, matériels utilisés, nb/qualif° du personnel, secret des brevets, de fabrique)
  - secret des informations économiques et financières (CA, volumes de production, capacités d'exploitation et montant des investissements, bases d'imposition)
  - Le secret des stratégies commerciales (prix/remises, liste des fournisseurs, politique de développement à l'exportation)

# Les documents/données communicables selon l'interlocuteur

| L'intéressé | Tiers |
|---|---|
| Documents **comportant mentions**:<br>▪ Avec **appréciation sur une personne physique**<br>▪ **protégées par le législateur** (par ex : secret en matière industrielle et commerciale, secret des dossiers médicaux, protection de la vie privée)<br>**ET** qu'il n'est **pas possible de disjoindre/occulter du document** sans en altérer la compréhension.<br>Les **Informations à caractère médical.**<br><br>Par ex:<br>- Dossier administratif d'un agent<br>-Motifs de rejet de l'offre à un marché public<br>-Nom des évaluateurs à l'issue de la procédure de sélection<br>-Evaluation/expertise/avis/ recommandations relatifs à l'évaluation d'un projet après prise de décision : transmission à tout membre de l'équipe/à l'intéressé | Documents administratifs **à caractère personnel/informations nominatives** contenus dans un fichier informatique, un traitement automatisé, **conditions :**<br>- non mise en cause d'une personne<br>- communication partielle possible (occultation données sensibles/ à caractère personnel)<br><br>Par ex:<br>- Liste de projets avec nom des responsables scientifiques des projets sélectionnés<br>- Données sur les projets/ portefeuilles de projets, qui nécessitent des requêtes informatiques complexes /non habituelles si convention avec le demandeur<br>- Rapport d'enquête sur présence d'amiante au sein d'un HLM, anonymisation des noms des résidents (données personnelles / respect vie privée) |

# Les documents/données à données restreintes

- Mentions non communicables
- Mentions protégées par le législateur
- Mentions qui mettent en cause une personne

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

**Droit à communication s'exerce seulement si occultation (anonymisation, marqueur) ou séparation des informations litigieuses** :

- est possible matériellement (document divisible)
- ne dénature pas le sens du document, ni prive d'intérêt la communication.

Par ex:

- Rapports scientifiques/rapport de choix des offres pour les marchés publics/PV de « jurys » si les occultations des données sensibles ne dénaturent pas les docs/privent d'intérêt la communication sinon : NON communicables

-Documents relatifs aux marchés (après notification du marché) communicables avec occultation des données sensibles (Cf. fiches DAJ sur les données essentielles des MP)

-Convention et compte-rendu financier final de la subvention (=relevé des dépenses justificatif) communicables d'après la CADA (occulter les données sensibles).

# Des questions ?