



À LA RENCONTRE  
DES ACTEURS  
DE LA RECHERCHE

# **RGPD et collaborations internationales**

**mercredi 28 septembre 2022**





RÉPUBLIQUE  
FRANÇAISE

*Liberté  
Égalité  
Fraternité*

# 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, enregistrement, organisation, structuration, conservation, adaptation, modification, consultation...)

## Données personnelles

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



RÉPUBLIQUE  
FRANÇAISE

*Liberté  
Égalité  
Fraternité*

# Objectifs du RGPD

**anr** <sup>©</sup>  
agence nationale  
de la recherche  
AU SERVICE DE LA SCIENCE

## 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 sanctions en cas de manquement



RÉPUBLIQUE  
FRANÇAISE

*Liberté  
Égalité  
Fraternité*

**anr**®  
agence nationale  
de la recherche  
AU SERVICE DE LA SCIENCE

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

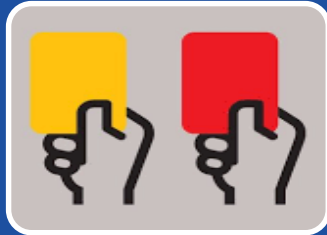
Non respect des règles  
en matières de transfert  
de données

# Les sanctions en cas de manquement\*



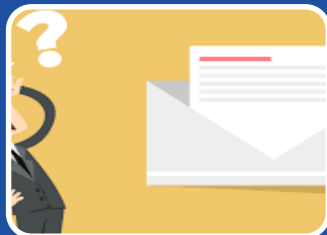
## Les contrôles en 2021

- 118 contrôles sur place
- 173 contrôles en ligne
- 65 contrôles sur pièce
- 28 contrôles sur audition



## 18 sanctions en 2021

- Cette année, les décisions ont concerné des secteurs d'activité et des acteurs très divers.
- Parmi les manquements les plus fréquents figurent le défaut d'information des personnes et des durées de conservation excessives.



## Les mises en demeure en 2021

- 133 non publiques
- 2 publiques

\*Rapport d'activité de la Cnil 2021

# 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





# 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





# Prévoir un encadrement des relations avec ses sous-traitants

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/reenvoi 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

# 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 :

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

# Le cadre des collaborations internationales

## Règles applicables

Applicable  
pour tout  
traitement

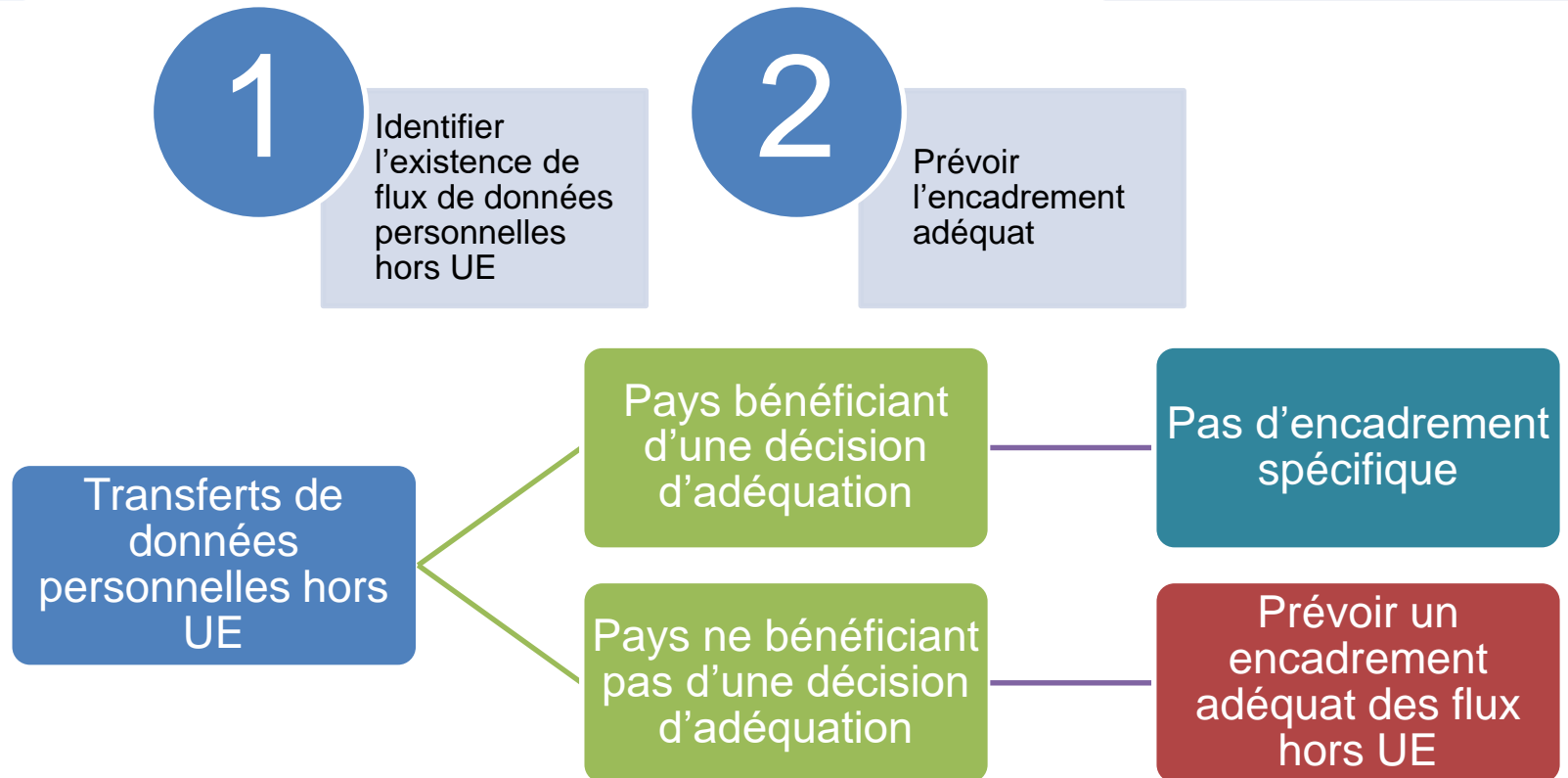
Dans le cas spécifique  
d'une collaboration  
internationale

Principes  
fondamentaux  
issus du  
RGPD

Responsabilité  
conjointe

Flux  
transfrontières  
hors UE

# Les transferts de données personnelles hors UE 1/6



Evènement important : invalidation du Privacy Shield qui encadrerait les transferts de données avec les USA – CJUE, 16 juil. 2020

# Les transferts de données personnelles hors UE 2/6

Art. 45

Décision  
d'adéquation

Pas  
d'encadrement  
spécifique  
(transferts libres)

Tous les pays membres de l'UE	Suisse	Uruguay	Chili	Japon	Nouvelle Zélande
Israël	Canada (traitements dans le cadre commercial)	Jersey	Andorre	Iles Féroé	Guernesey
Royaume-Uni	Ile de Man				

# Les transferts de données personnelles hors UE 3/6



Clauses contractuelles types	Règles internes d'entreprise (BCR)	Arrangement administratif	Code de conduite	Mécanisme de certification
<ul style="list-style-type: none"><li>• Adoptées par la Commission Européenne</li><li>• 4 modules : RT*/RT ; RT/ST* ; ST/ST ; ST/RT</li></ul>	<ul style="list-style-type: none"><li>• Article 47</li></ul>	<ul style="list-style-type: none"><li>• ou un texte juridiquement contraignant et exécutoire pour permettre la coopération entre les autorités publiques</li></ul>	<ul style="list-style-type: none"><li>• Adopté conformément à l'article 40</li><li>• Assortie de l'engagement contraignant et exécutoire d'appliquer les garanties appropriées</li></ul>	<ul style="list-style-type: none"><li>• Approuvé (comportant l'engagement contraignant et exécutoire pris par les destinataires hors UE d'appliquer les garanties appropriées)</li></ul>

\*RT : Responsable du traitement  
ST : Sous-traitant



# Les transferts de données personnelles hors UE 4/6



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.

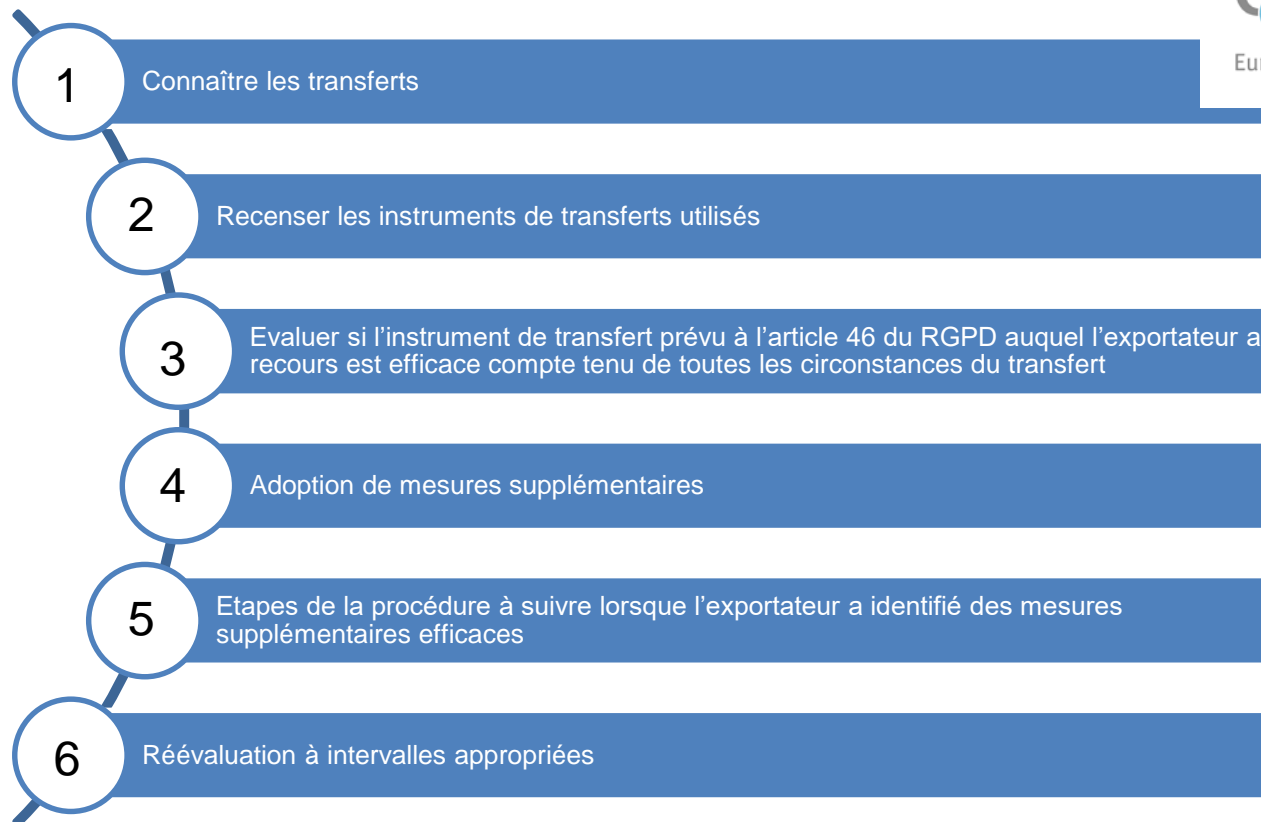
- **la personne concernée a donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle ;**
- le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à la mise en 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 5/6

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



# Les transferts de données personnelles hors UE 6/6

- **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

Finalité du traitement décidé conjointement



Moyens du traitement choisis conjointement

Responsabilité conjointe

# 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)

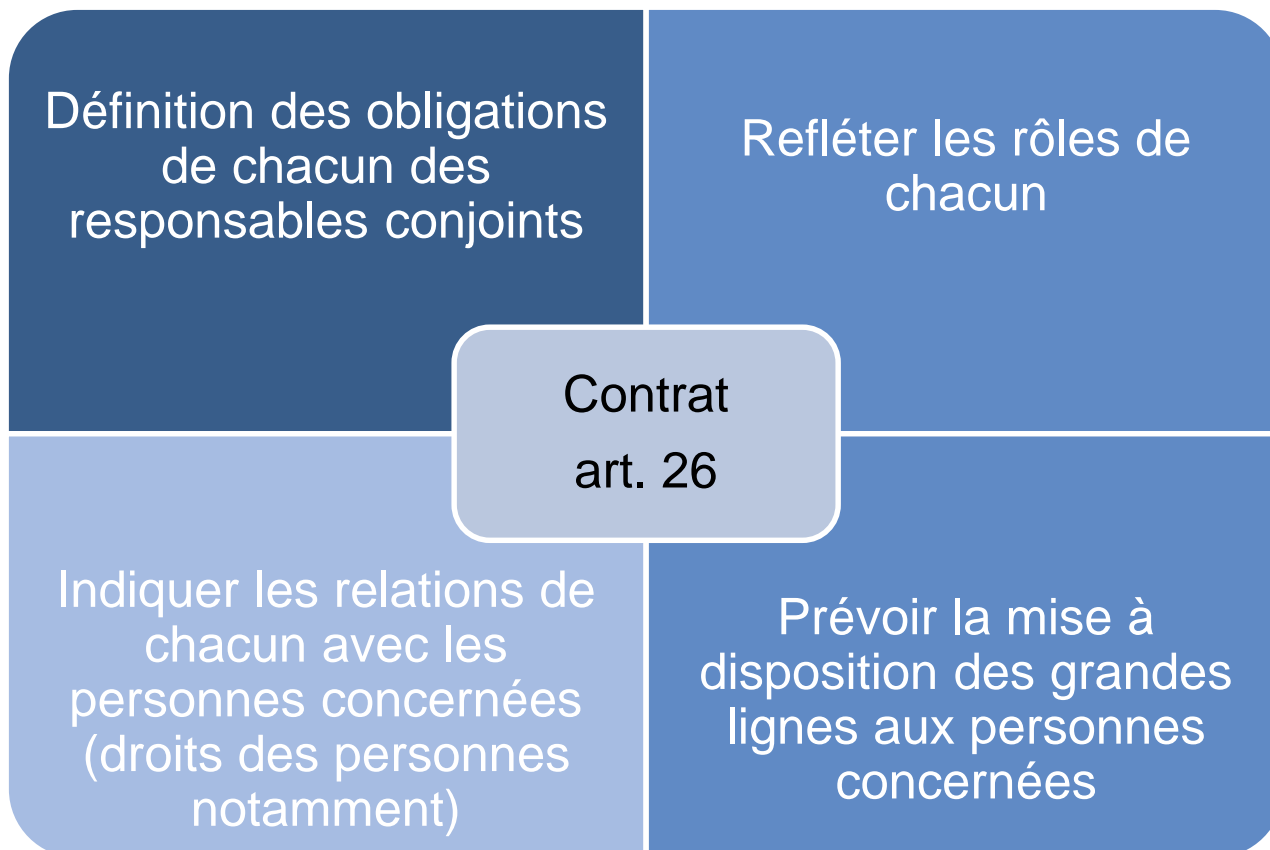
La participation conjointe doit englober, d'une part, la détermination des finalités et, de l'autre, la détermination des moyens (p. 22)

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

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

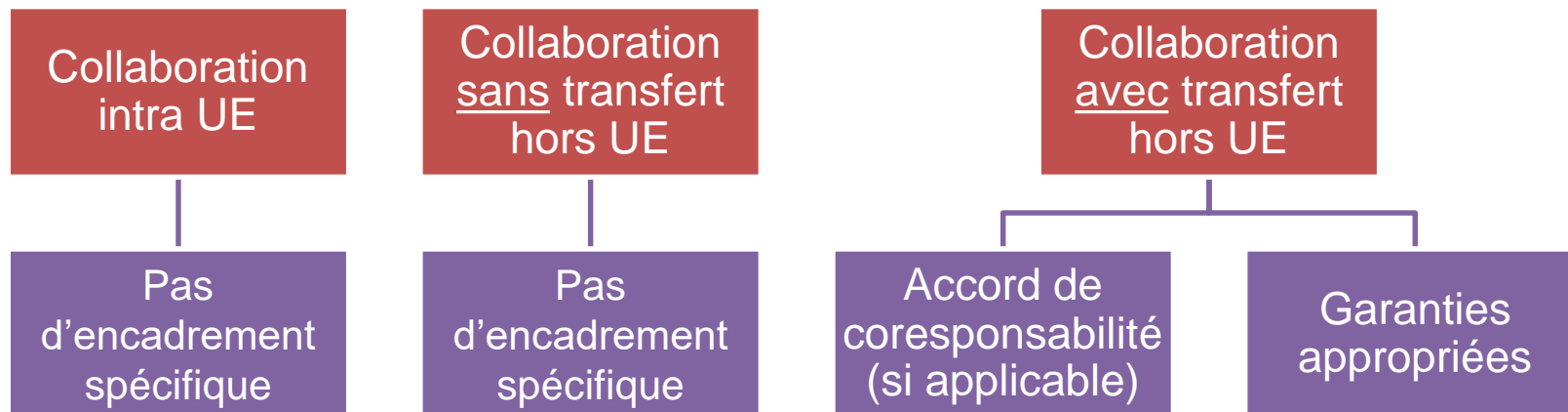
Il est possible de désigner un référent RGPD comme point de contact pour recenser les sujets sur la protection des données

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





RÉPUBLIQUE  
FRANÇAISE

*Liberté  
Égalité  
Fraternité*

**anr**®  
agence nationale  
de la recherche  
AU SERVICE DE LA SCIENCE

# Transfert de données non personnelles

## ANR TOUR



# Demandeurs

---

Chercheurs impliqués ou non dans un projet financé par l'ANR

Etat, agences de l'Etat,

Collectivités territoriales

Agences homologues étrangères

Institutions FR/UE

## DES DOCUMENTS/DONNÉES NON COMMUNICABLES :

- ✓ 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 (CR réunions Comex ou direction/ interdirection/ dépt/... qui ne seraient pas décisionnelles)
- ✓ sur lesquels **les tiers détiennent des DPI** (docs scientifiques, certains résumés dès lors qu'il y a risque de divulgation pour brevet => info à faire aux bénéficiaires)
- ✓ qui se rattachent à une **activité non administrative** (juridictionnelle, judiciaire, de contrôle ou d'enquête ou à une activité privée)
- ✓ **à caractère personnel** (fiches de paye des agents ANR, adresse mail d'un agent ou ligne directe, infos nominatives sur les déposants sauf consentement)
- ✓ 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)



- ✓ **contenu « sensible »** = la divulgation porterait atteinte aux secrets protégés par la loi, au secret de la 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 (n° SS, RIB...)
- ✓ relevant du **secret industriel et commercial** (s'applique aux déposants/partenaires quel que soit leur statut) :
  - 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)

Par ex:

- doc scientifique (sc) /compte-rendu scientifique, intermédiaire ou final
- annexes sc des conventions/rapport sc si la communication de ces docs et les occultations faites pour protéger les données dénaturent ces documents/privent d'intérêt la communication
- production/travaux/publication des chercheurs (relèvent de l'exercice de leurs droits propres).



**DES DOCUMENTS/ DONNÉES COMMUNICABLES À CERTAINES PERSONNES uniquement :**



Intéressé(e)	Tiers
<p>Documents <b>comportant mentions:</b></p> <ul style="list-style-type: none"> <li>Avec <b>appréciation sur une personne physique</b></li> <li><b>protégées par le législateur</b> (par ex : <u>secret</u> en matière industrielle et commerciale, secret des dossiers médicaux, protection de <u>la vie privée</u>)</li> </ul> <p><b>ET</b> qu'il n'est <b>pas possible de disjoindre/occulter du document</b> sans en altérer la compréhension.</p> <p><b>Les Informations à caractère médical.</b></p> <p><u>Par ex:</u></p> <ul style="list-style-type: none"> <li>-EAE des agents, dossier administratif de l'agent</li> <li>-Motifs de rejet de l'offre à un marché public</li> <li>-Nom des évaluateurs</li> <li>-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</li> </ul>	<p>Documents administratifs <b>à caractère personnel/informations nominatives</b> contenus dans un fichier informatique, un traitement automatisé, <b>conditions :</b></p> <ul style="list-style-type: none"> <li>- non mise en cause d'une personne</li> <li>- communication partielle possible (occultation données sensibles/ à caractère personnel)</li> </ul> <p><u>Par ex:</u></p> <ul style="list-style-type: none"> <li>- Liste de projets avec nom des responsables scientifiques des projets sélectionnés</li> <li>- Données sur les projets/ portefeuilles de projets, qui nécessitent des requêtes informatiques complexes /non habituelles si convention avec le demandeur</li> </ul>

## DES DOCUMENTS/ DONNÉES À TRANSMISSION RESTREINTE :

- 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)
- Plans nus d'architecture du plateau de l'ANR (pas d'infos pour la localisation des serveurs, onduleurs etc pour raisons de sécurité)
- Convention et compte-rendu financier final de la subvention (=relevé des dépenses justificatif) communicables d'après la CADA (occulter les données sensibles).

