RGPD et collaborations internationales

ANR TOUR

AGENCE NATIONALE DE LA RECHERCHE
ANR

Champ d’application du RGPD

Le RGPD est un règlement de l'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

AGENCE NATIONALE DE LA RECHERCHE
ANR

Objectifs du RGPD

Responsabiliser les acteurs du traitement

- Tenir un registre des traitements
- Désigner un DPO
- Documenter la conformité (procédures internes)
- Prévoir un encadrement adéquat des transferts de données personnelles hors 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

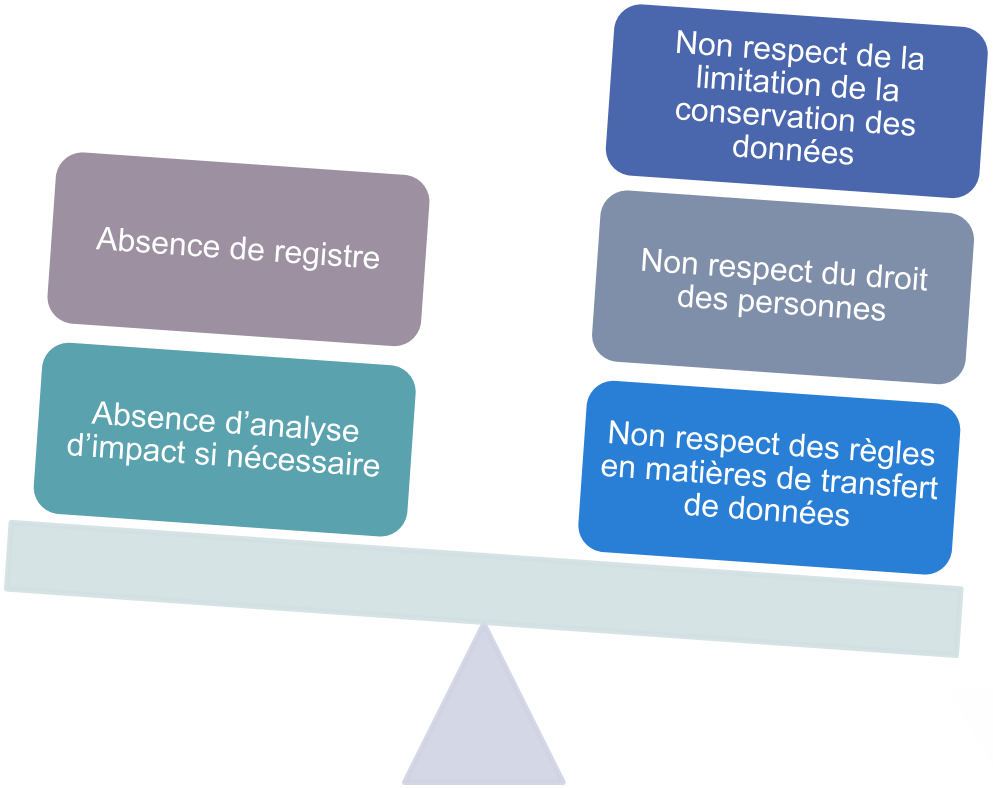
Sécuriser les données

- Mettre en place des mesures techniques et organisationnelles
- Analyse d'impact des traitements si nécessaire
- Informer la CNIL en cas de faille de sécurité

Les sanctions en cas de manquements

10M ou
2% du CA

20M ou
4% du CA



Les sanctions en cas de manquement

Les contrôles en 2019

- 169 contrôles sur place
- 53 contrôles en ligne
- 45 contrôles sur pièce
- 18 auditions

8 sanctions en 2019

- Ces sanctions concernaient principalement des atteintes à la sécurité des données personnelles, des manquements à l'obligation d'information des personnes, des manquements liés aux durées de conservations ds données et dans un cas, le non-respect du droit d'accès prévu par le RGPD.

Les mises en demeure en 2019

- 42 non publiques
- 2 publiques

Rapport d'activité de la Cnil 2019

Les acteurs d'un traitement

Responsable du traitement

- Personne physique ou morale, autorité publique, service ou autre organisme qui seul ou conjointement avec d'autres, 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

AGENCE NATIONALE DE LA RECHERCHE
ANR

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

AGENCE NATIONALE DE LA RECHERCHE
ANR

Obligation d'informer les personnes

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

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

Le cadre des collaborations internationales

Règles applicables

Applicable pour tout traitement

Dans le cas spécifique d'une collaboration internationale

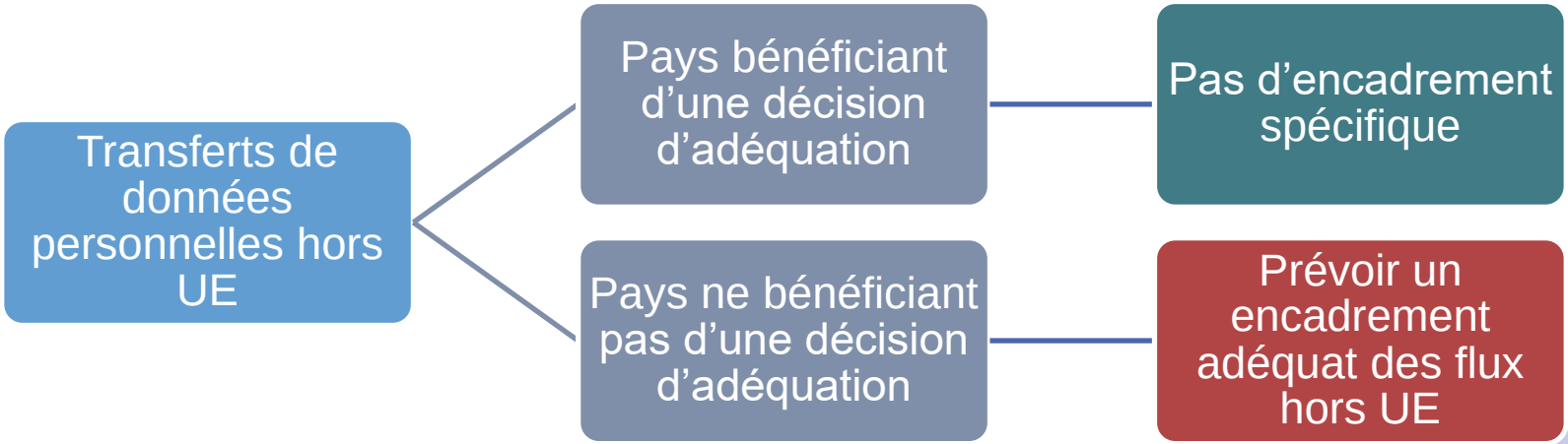
Principes fondamentaux issus du RGPD

Responsabilité conjointe

Flux transfrontières hors UE

Les transferts de données personnelles hors UE 1/3

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



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

Les transferts de données personnelles hors UE 2/3

Décision d'adéquation

Pas d'encadrement spécifique (transferts libres)

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

Les transferts de données personnelles hors UE 3/3

Absence de décision d'adéquation → **Nécessité d'encadrer les flux**

Clauses contractuelles types

- Adoptées par la Commission Européenne
- Deux versions : RT/RT et RT/ST

Consentement des personnes concernées

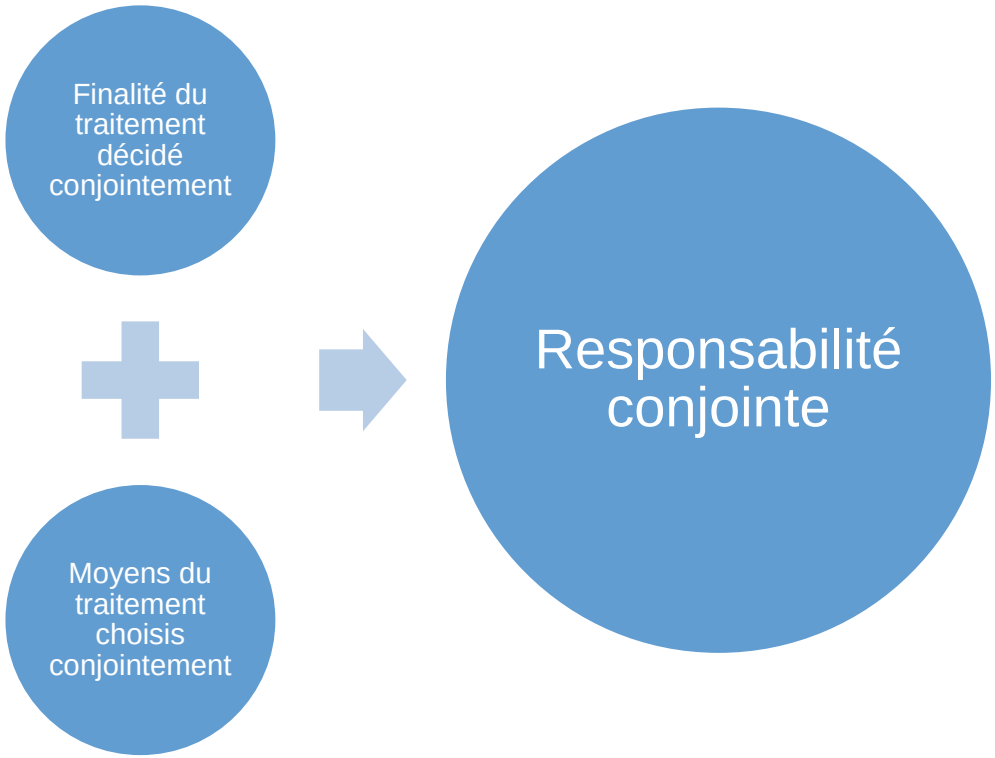
- Exception prévue à l'article 29 RGPD
- Prévoir une case à cocher au moment de la collecte des données personnelles concernées par le transfert hors UE

AGENCE NATIONALE DE LA RECHERCHE
ANR

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 en cours de rédaction.

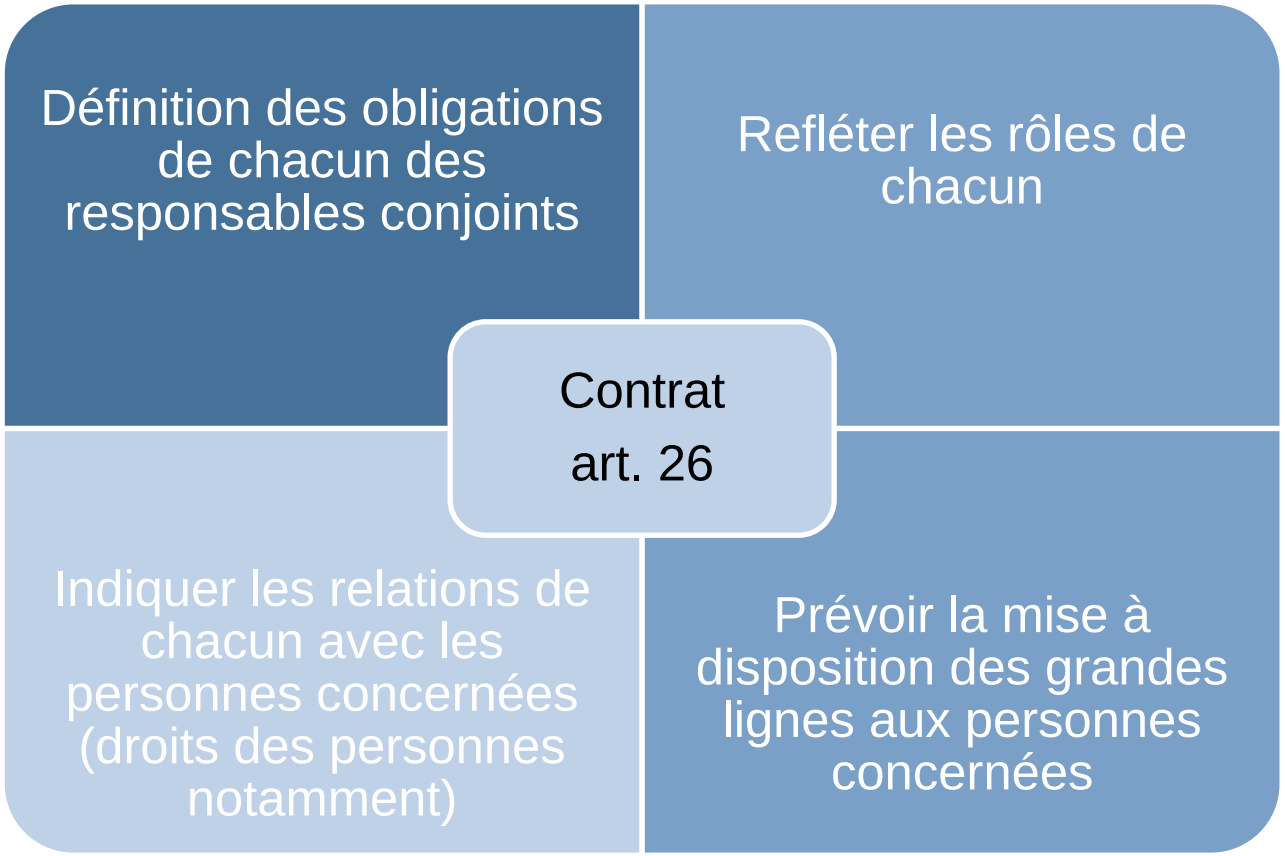
- Une version de travail a été publiée et détaille la notion de responsabilité conjointe

edpb
European Data Protection Board

- Une collaboration n'entraîne pas automatiquement une responsabilité conjointe (p.17)
- Il faut que les responsables participent ensemble à la détermination de la finalité et des moyens du traitement (p.17)
- 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 (p.18)
- La responsabilité conjointe n'implique pas un même niveau de responsabilité des acteurs (p.19)

AGENCE NATIONALE DE LA RECHERCHE
ANR

La responsabilité conjointe 3/3



Désigner un référent pour les questions relatives à la protection des données

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

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