RGPD

Le Règlement sur la protection

des données personnelles

6 mars 2018

Le Règlement sur la protection des données personnelles

Hamdi KAZANCI

Expert - Droit des affaires

Introduction

RGPD

- 173 considérants
- 99 articles
- 11 Chapitres

Principe

- Toute collecte ou traitement de donnée permettant d'identifier une personne
- Traitement automatisé ou non
- Responsabilisation des acteurs

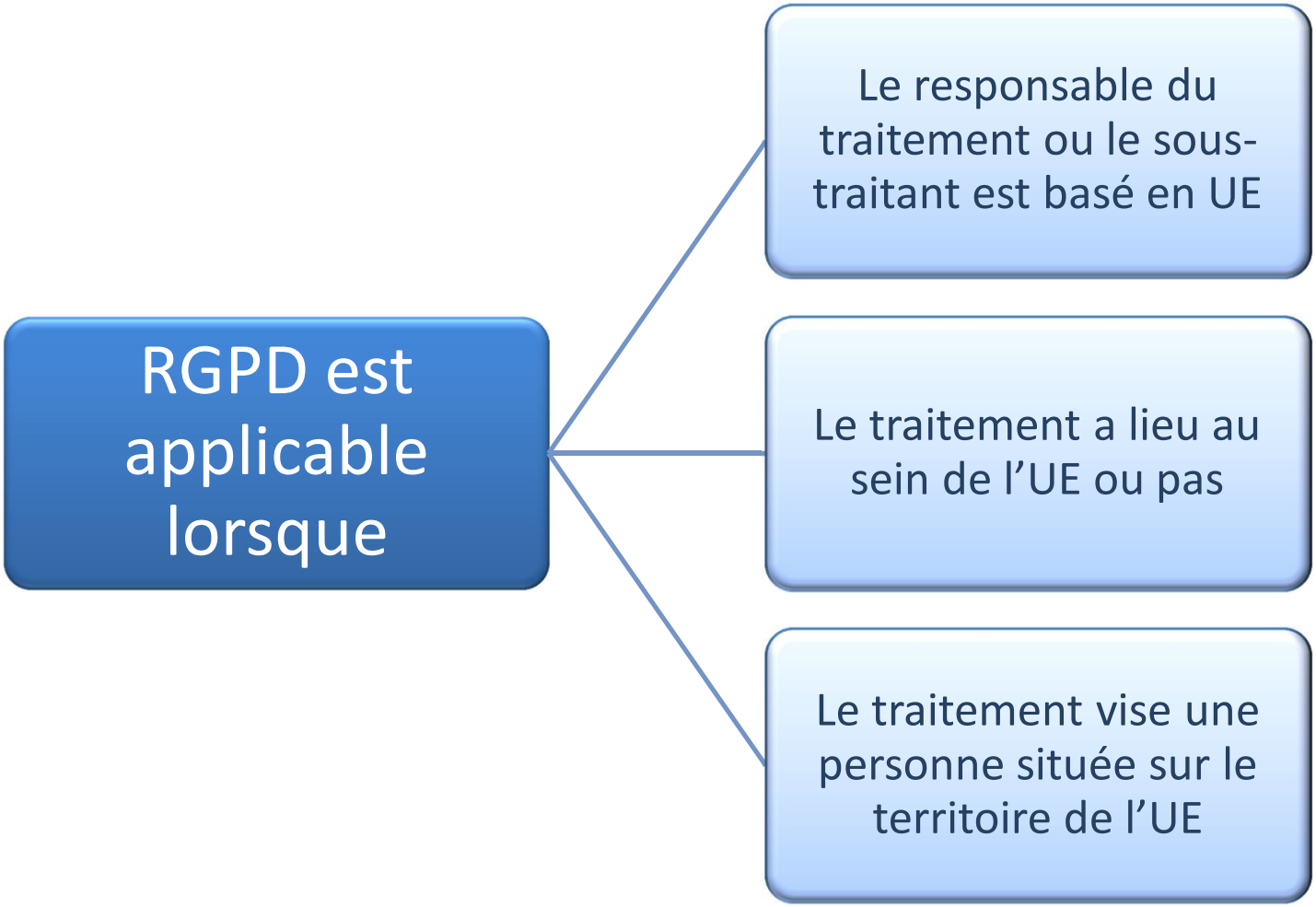
Date

- 25 mai 2018

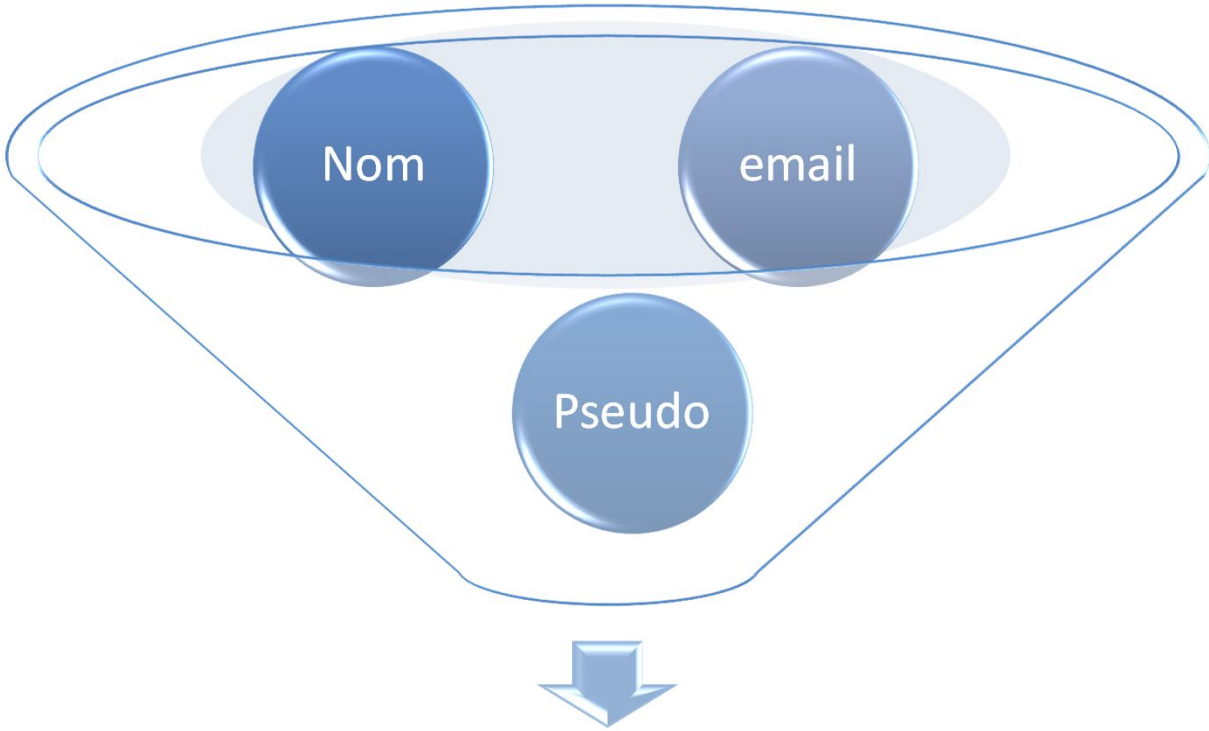
Sommaire

Sommaire

Applicable ou pas ?



Qu’est-ce qu’une donnée à caractère personnel ?



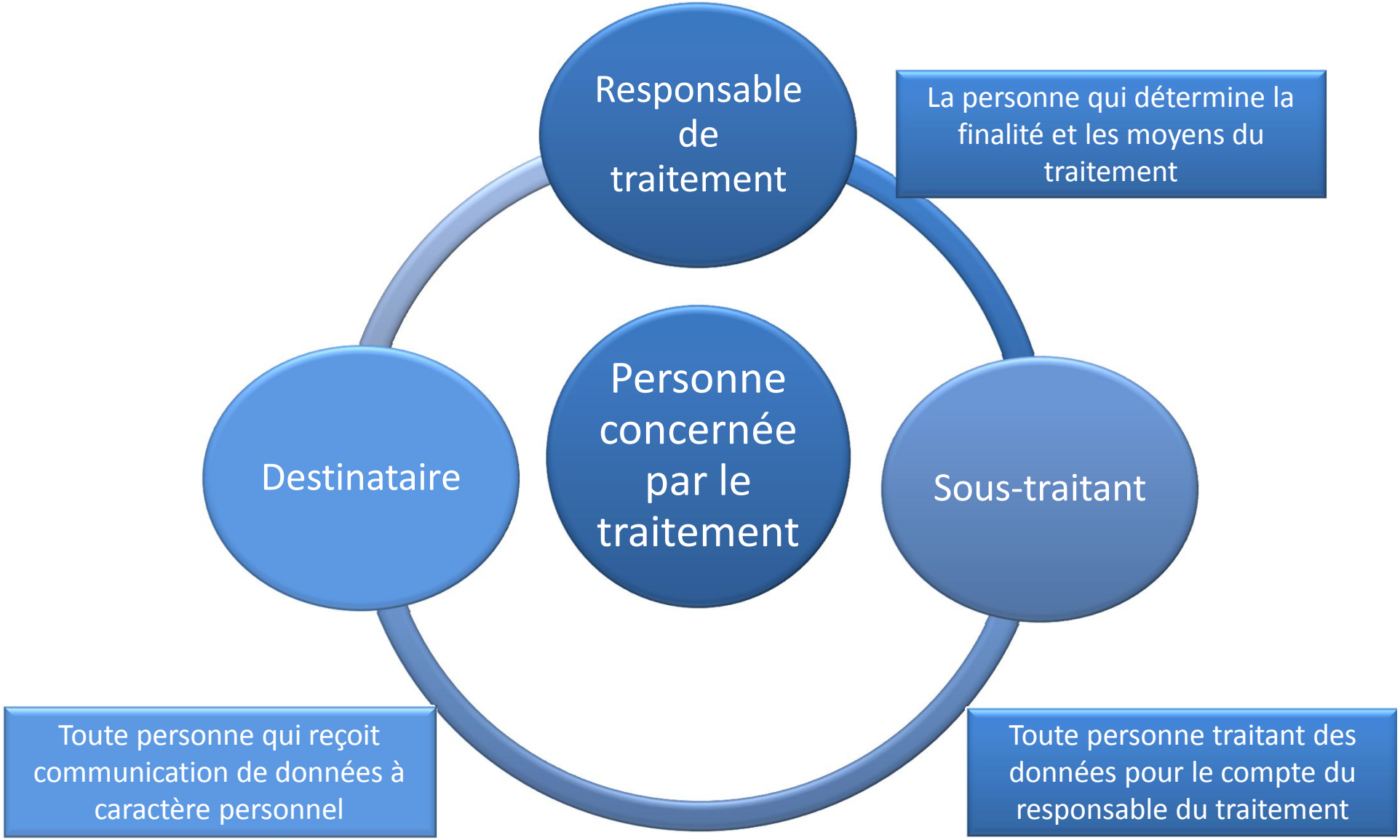
« ***toute information se rapportant à une personne physique identifiée ou identifiable*** » *Article 4*

Qu'est ce qu'un traitement?

Article 4

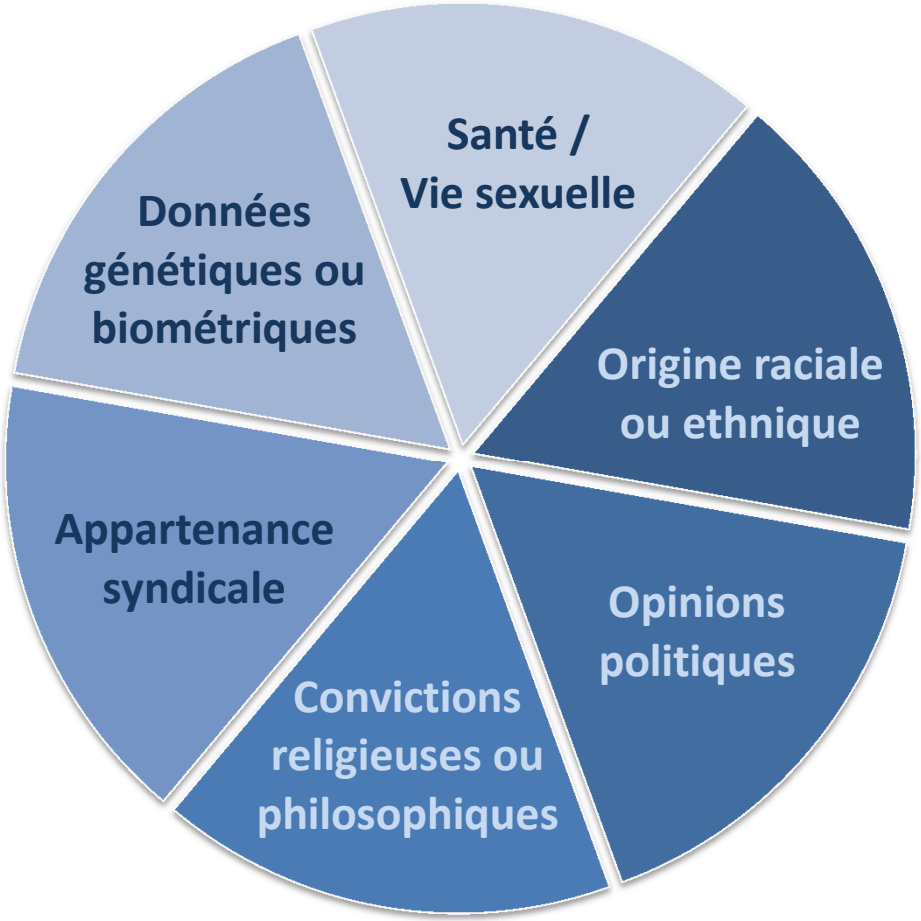
- *la collecte,*
- *l'enregistrement,*
- *l'organisation,*
- *la structuration,*
- *la conservation,*
- *l'adaptation ou la modification,*
- *l'extraction, la consultation,*
- *l'utilisation,*
- *la communication ou la diffusion,*
- *le rapprochement ou l'interconnexion,*
- *la limitation,*
- *l'effacement ou la destruction.*

Les acteurs (article 4)



Spécificité : les données sensibles

Principe : interdiction de collecter les données « sensibles »

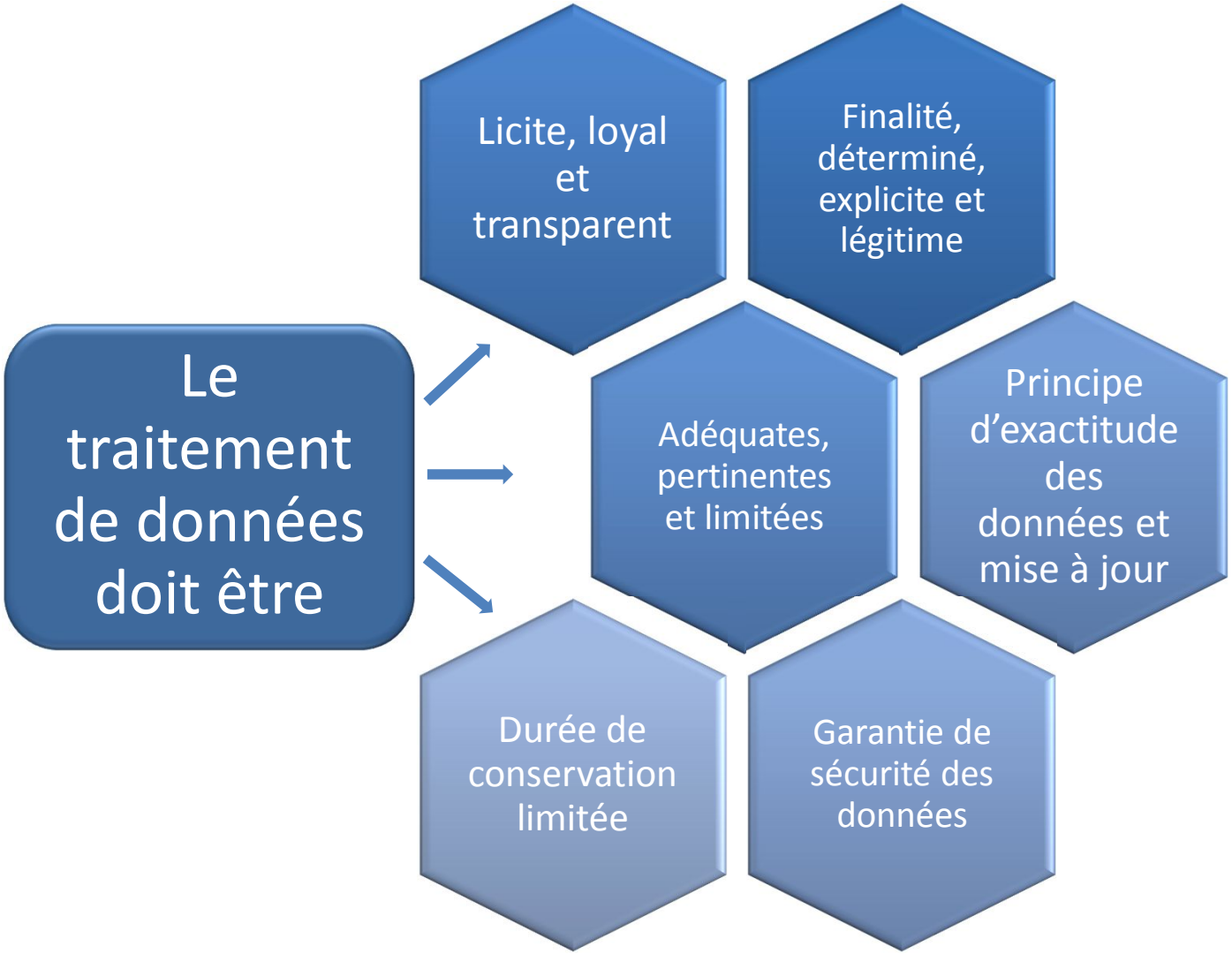


Exceptions (article 9)

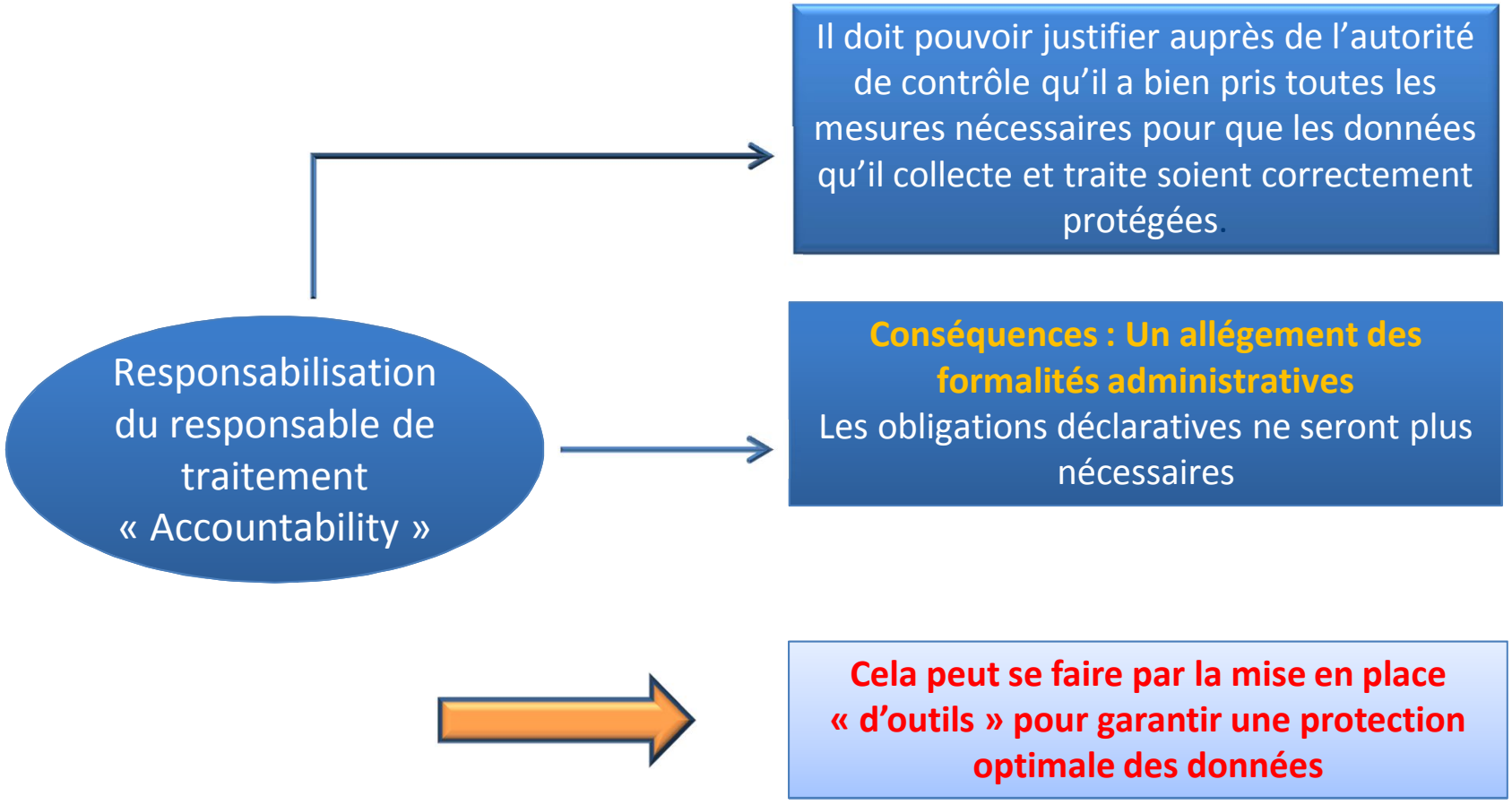
notamment :

- consentement exprès de la personne concernée ;
- traitements nécessaires à la sauvegarde des intérêts vitaux de la personne concernée ;
- traitements portant sur des données rendues publiques par la personne concernée ;
- traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ;
- traitements nécessaires pour des motifs d'intérêt public important.

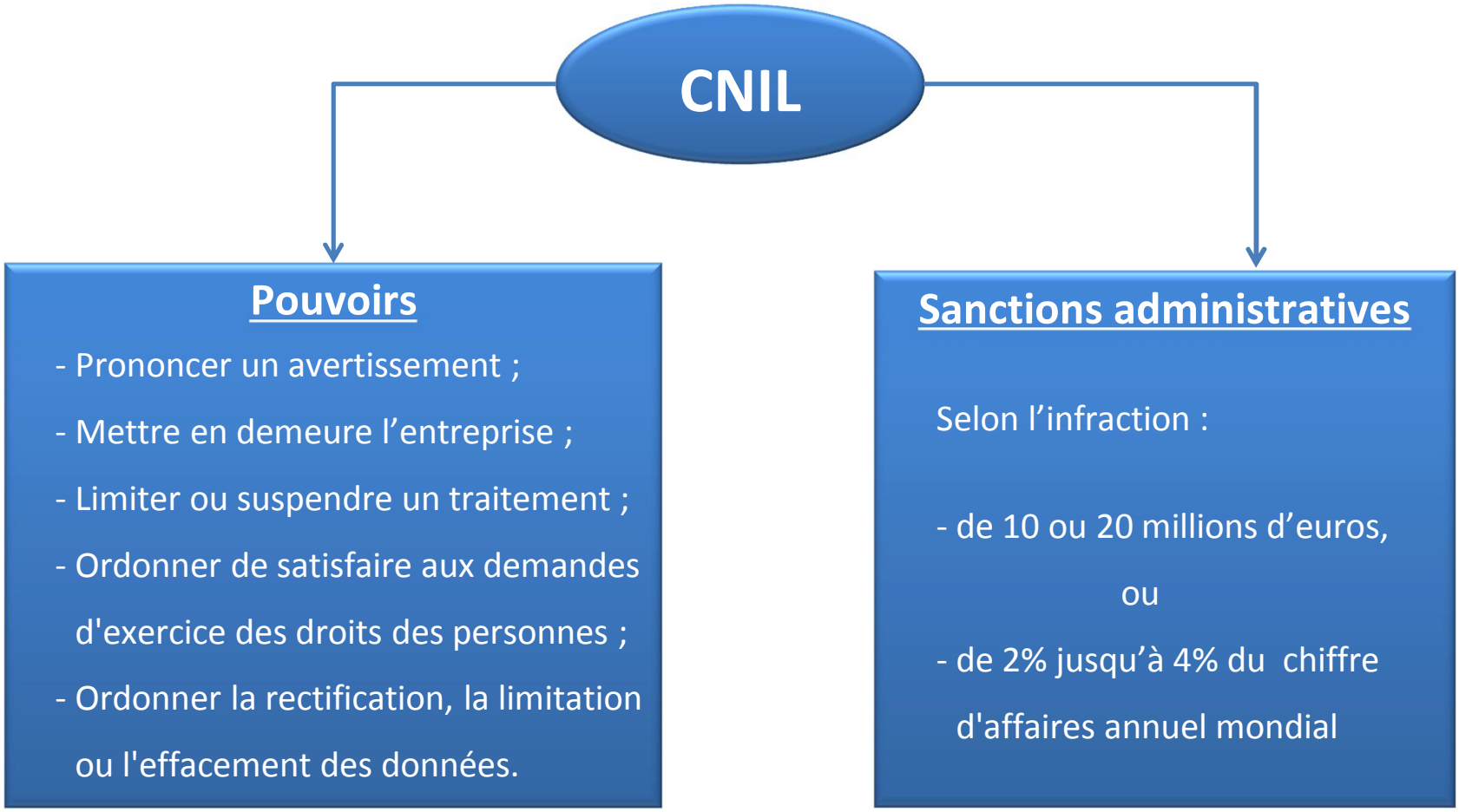
Les principes généraux du traitement



Responsabilisation : des données protégées !

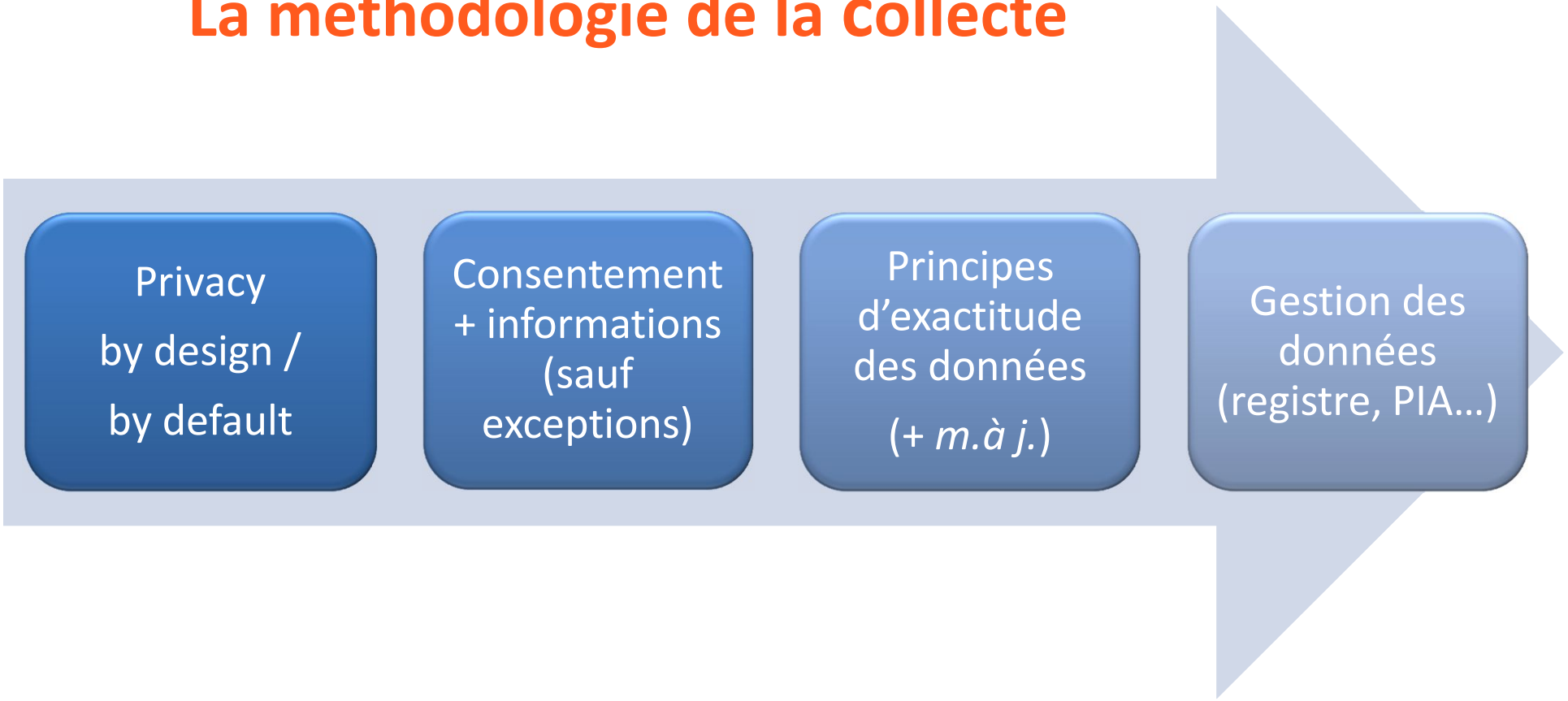


Sanctions


CNIL
Pouvoirs
- Prononcer un avertissement ;
- Mettre en demeure l'entreprise ;
- Limiter ou suspendre un traitement ;
- Ordonner de satisfaire aux demandes d'exercice des droits des personnes ;
- Ordonner la rectification, la limitation ou l'effacement des données.
Sanctions administratives
Selon l'infraction :
- de 10 ou 20 millions d'euros,
ou
- de 2% jusqu'à 4% du chiffre d'affaires annuel mondial

Sommaire

La méthodologie de la collecte



Privacy by default (art 25)

Mise en place d'une nouvelle organisation du traitement des données à caractère personnel avec un processus qui doit être appliqué systématiquement pour tout nouveau projet.
Avec des mesures techniques garantissant une confidentialité automatique.

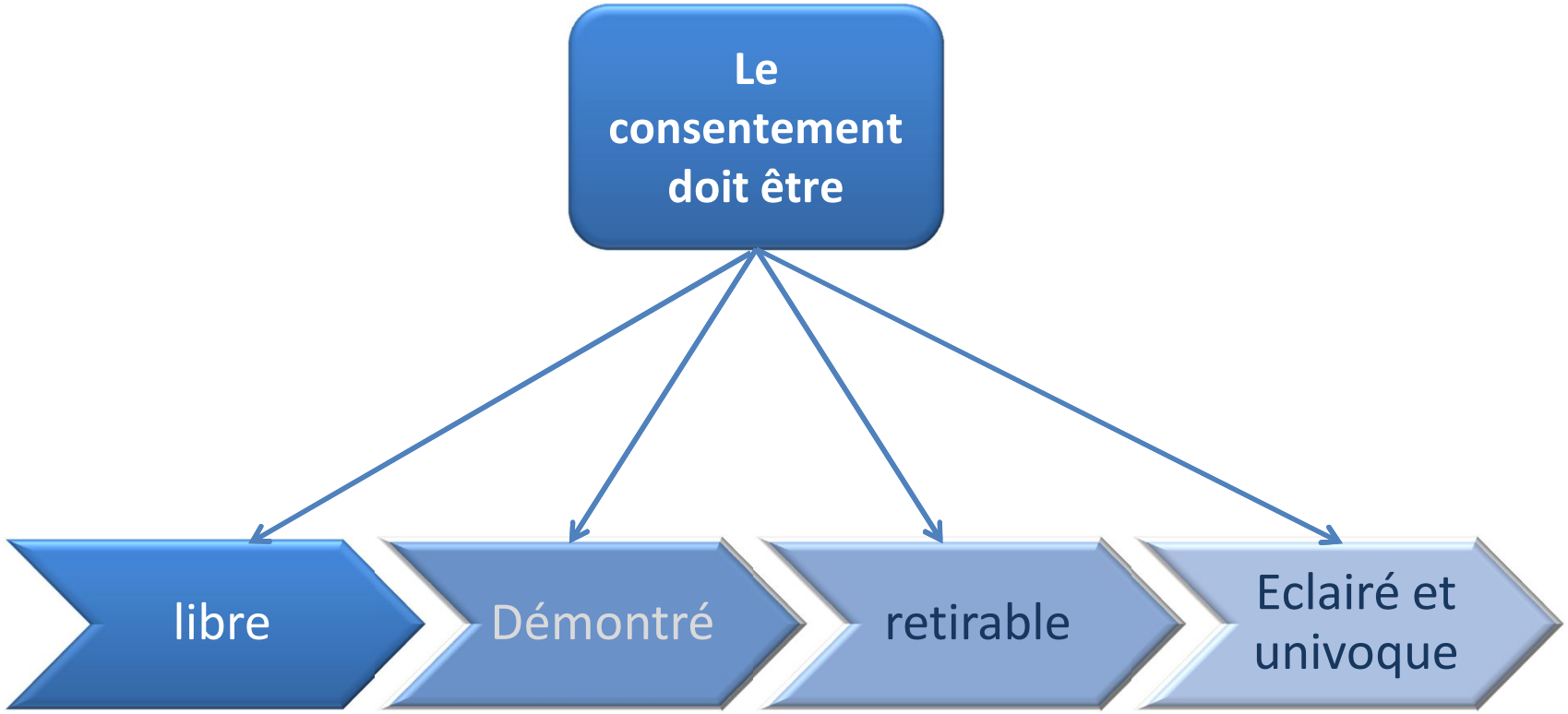
Privacy by design (art 25)

Dès le début de la conception, de veiller à ce que toute application, produit ou service traitant des données à caractère personnel offre le plus haut niveau possible de protection des données.

Privacy by default/design

- être proactif et non réactif,
- préventif,
- intégrée au système de traitement,
- chiffrement de bout en bout,
- transparence,
- pratique permettant de respecter la vie privée des utilisateurs (consentement, informations…).

Consentement (art 7)

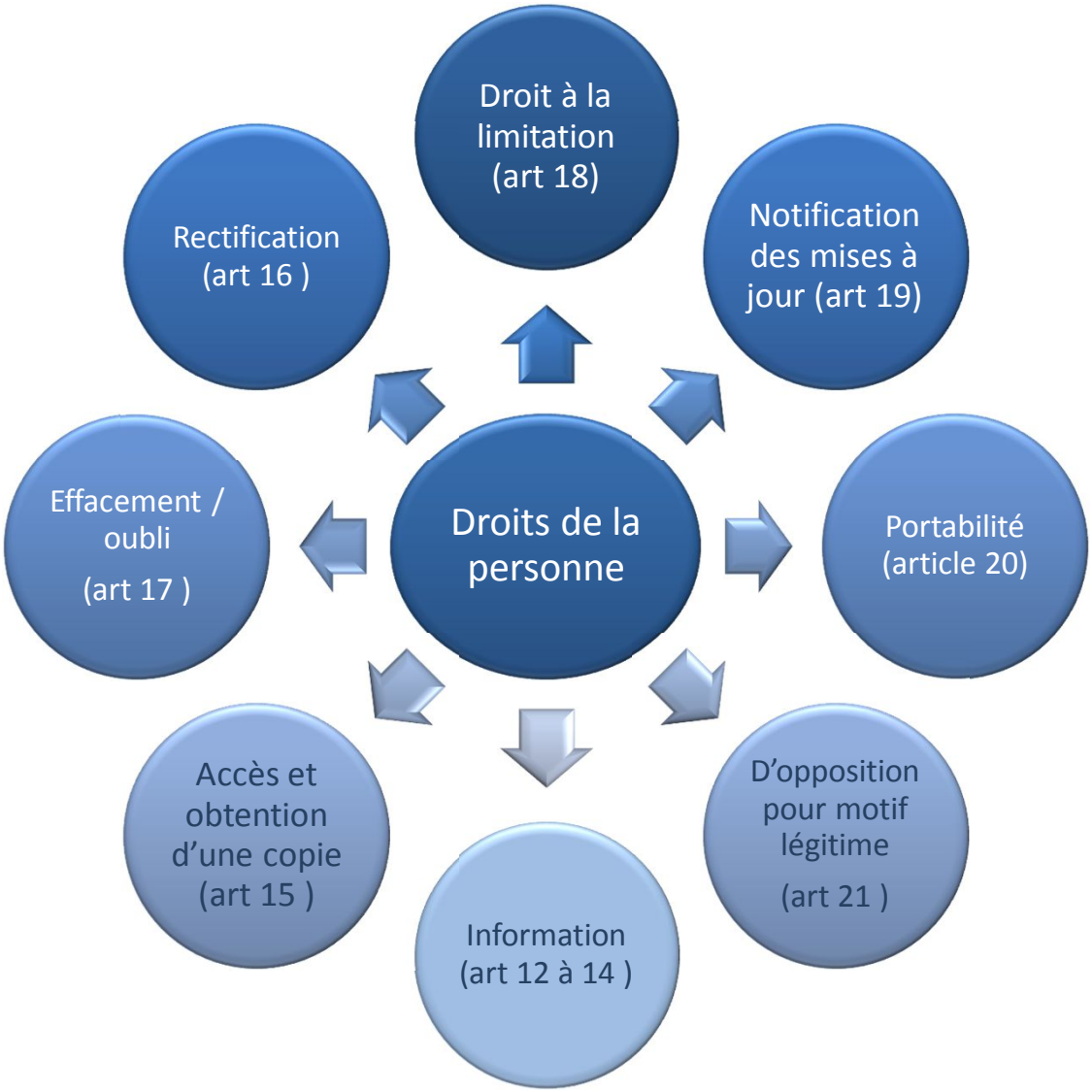


Exemples de consentements non valides : cases pré-cochées, tacite, silence, passif..

Contenu de l'information (article 13)

Identité du responsable du traitement / DPO	Finalité du traitement	Destinataires
Transfert hors UE	Durée de conservation	Droits de la personne
Prise de décision automatisée	Sources des données	Base juridique du traitement

Quels droits pour les personnes concernées ?



CONSERVATION

La durée doit être limitée au **strict minimum** c'est-à-dire que les données ne doivent pas être conservées plus longtemps que la **durée nécessaire à la réalisation des finalités** pour lesquelles elles ont été collectées

Droit à l'effacement

- Les données ne sont plus nécessaires pour le traitement
- Retrait du consentement
- Traitement illicite
- Obligation légale

Anomysation

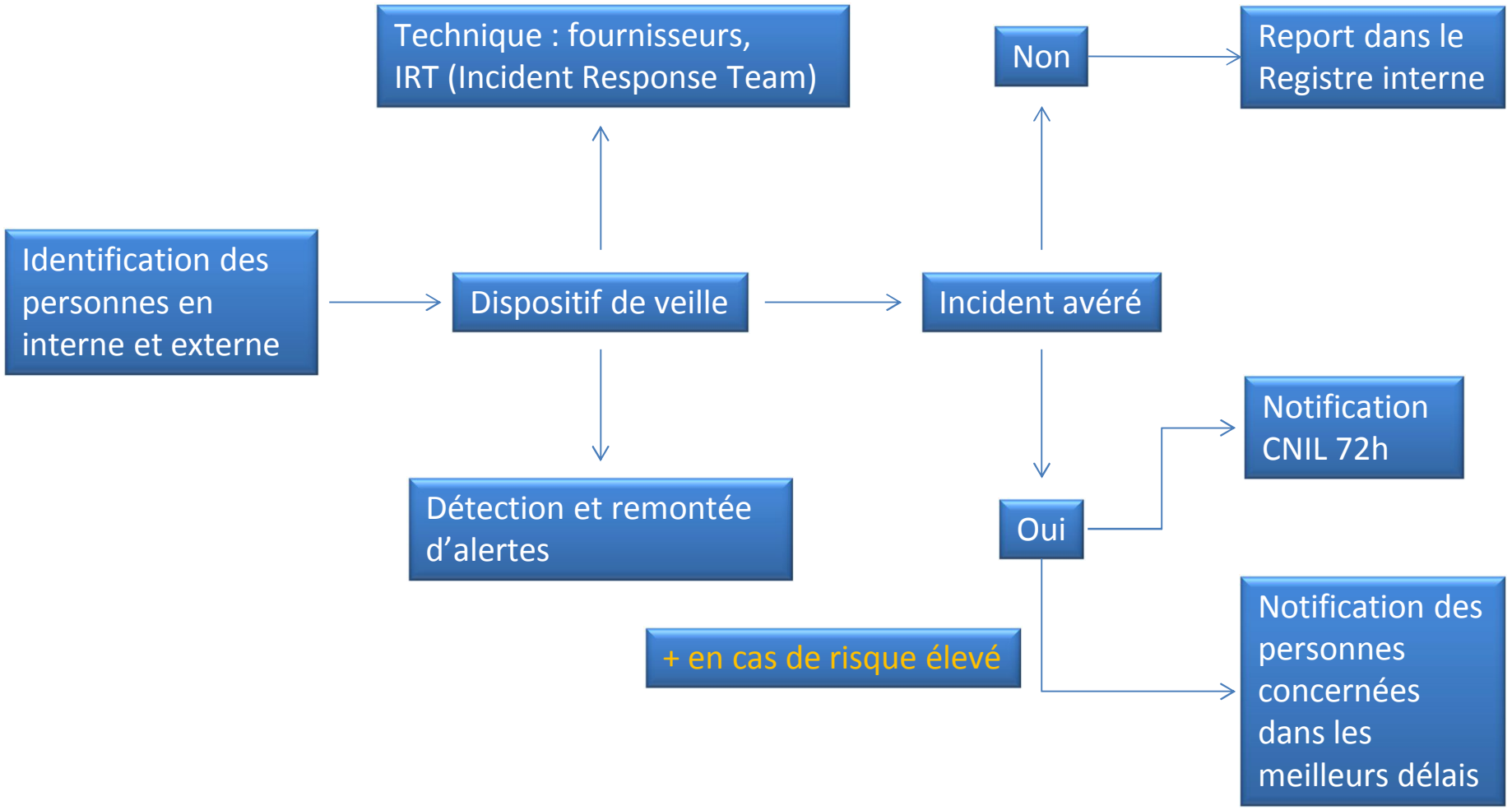
Cela à pour but d'empêcher toute identification d'une personne physique de manière définitive.
L'anonymisation doit avoir lieu :

- À la collecte
- Par un traitement spécifique **dans un bref délai** anonymisant les informations (une purge immédiate est nécessaire afin de rendre définitive l'anonymisation).

Pseudonymisation

La pseudonymisation permet de ne plus attribuer les informations collectées à une personne concernée sans un recours à des informations supplémentaires. Pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable..

Sécurité du traitement et déclaration des failles de sécurité



Transfert hors UE

Principe: interdiction

Exceptions

- Transferts vers un pays tiers ayant un niveau de protection adéquat (art. 45)
- Transferts effectués avec des garanties appropriées (art. 46)
  - L'existence d'un accord négocié dans le pays en question
  - La signature de clauses contractuelles
  - L'adoption de codes de bonne conduite (ou BCR)
- Autres dérogations pour des situations particulières
  - Si la personne à laquelle se rapportent les données a consenti expressément à leur transfert

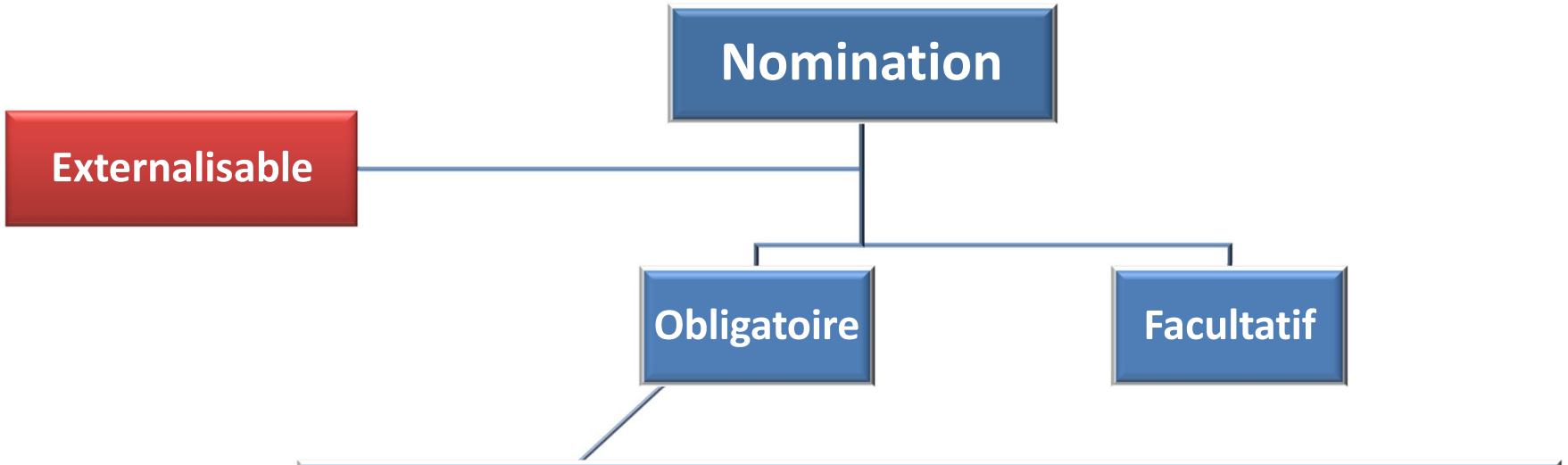
  OU
  - Si le transfert est nécessaire notamment à : la sauvegarde de la vie de cette personne ; l'intérêt public ; l'exercice ou la défense d'un droit en justice…

Sommaire

Feuille de route

Source : www.cnil.fr

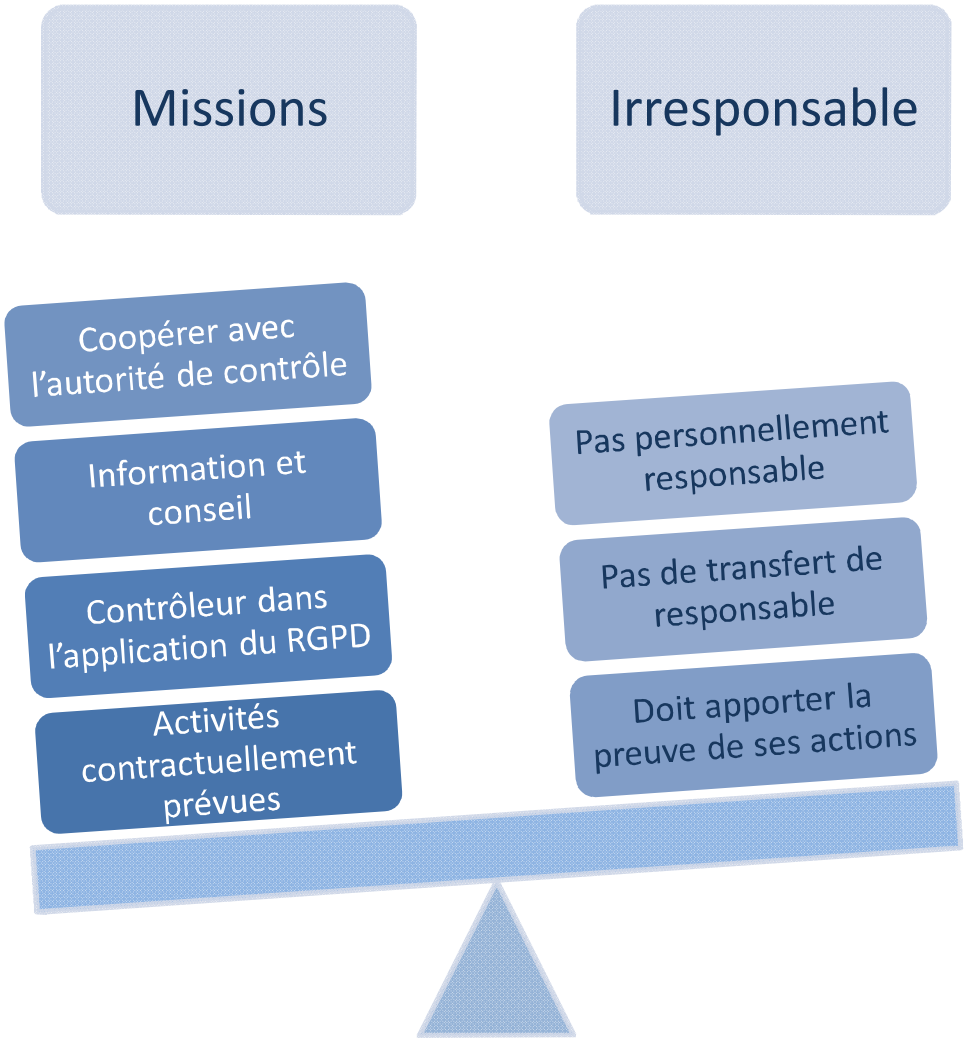
DPO / DPD



Article 37 :

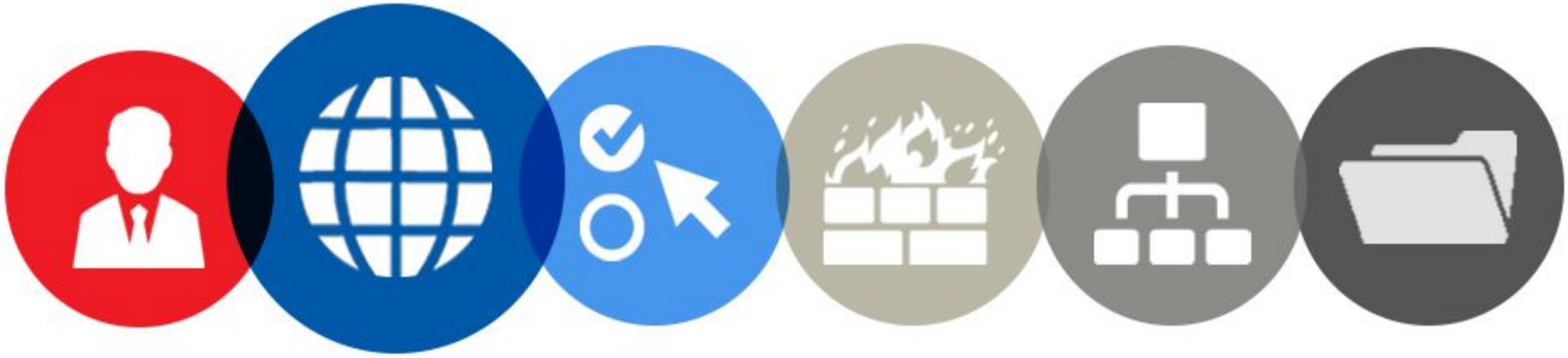
- Les autorités ou les organismes publics
- Les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle
- Les organismes dont les activités de base les amènent à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

DPO / DPD


Missions
Irresponsable
Coopérer avec l'autorité de contrôle
Information et conseil
Contrôleur dans l'application du RGPD
Activités contractuellement prévues
Pas personnellement responsable
Pas de transfert de responsable
Doit apporter la preuve de ses actions

Feuille de route

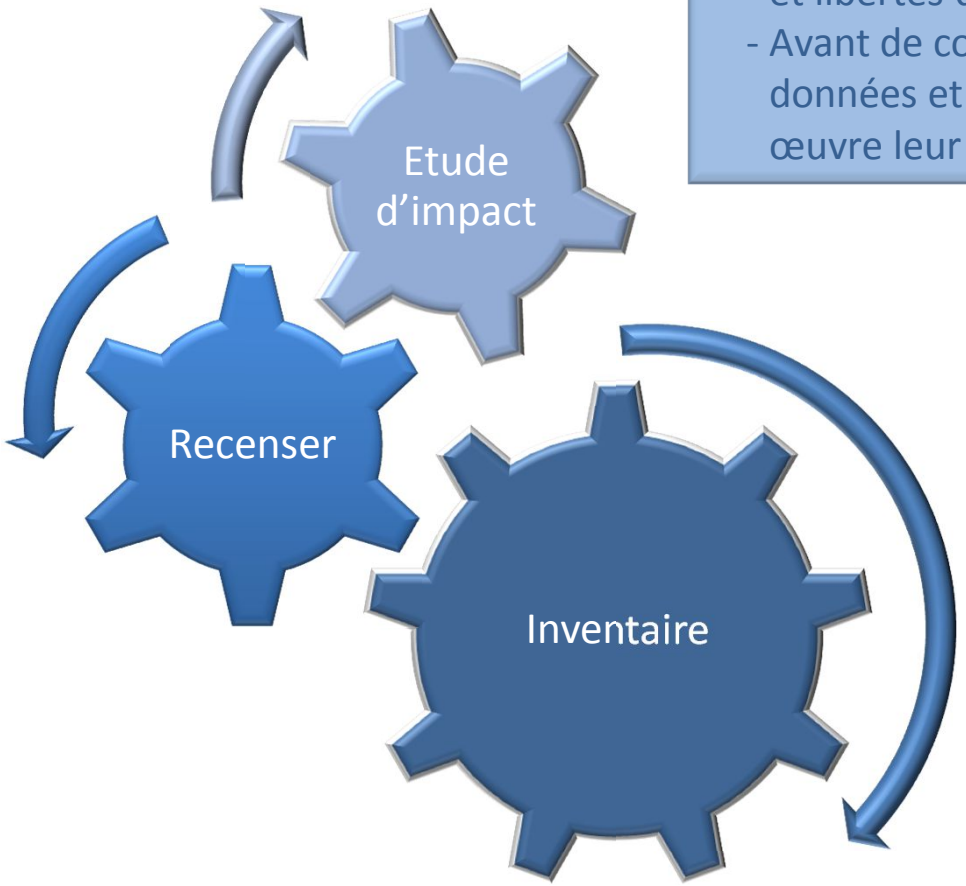
CARTOGRAPHIE



Source : www.cnil.fr

Cartographie

- Les traitements
- Les catégories de données traitées
- Les finalités
- Les acteurs du traitement
- Les transferts hors U.E

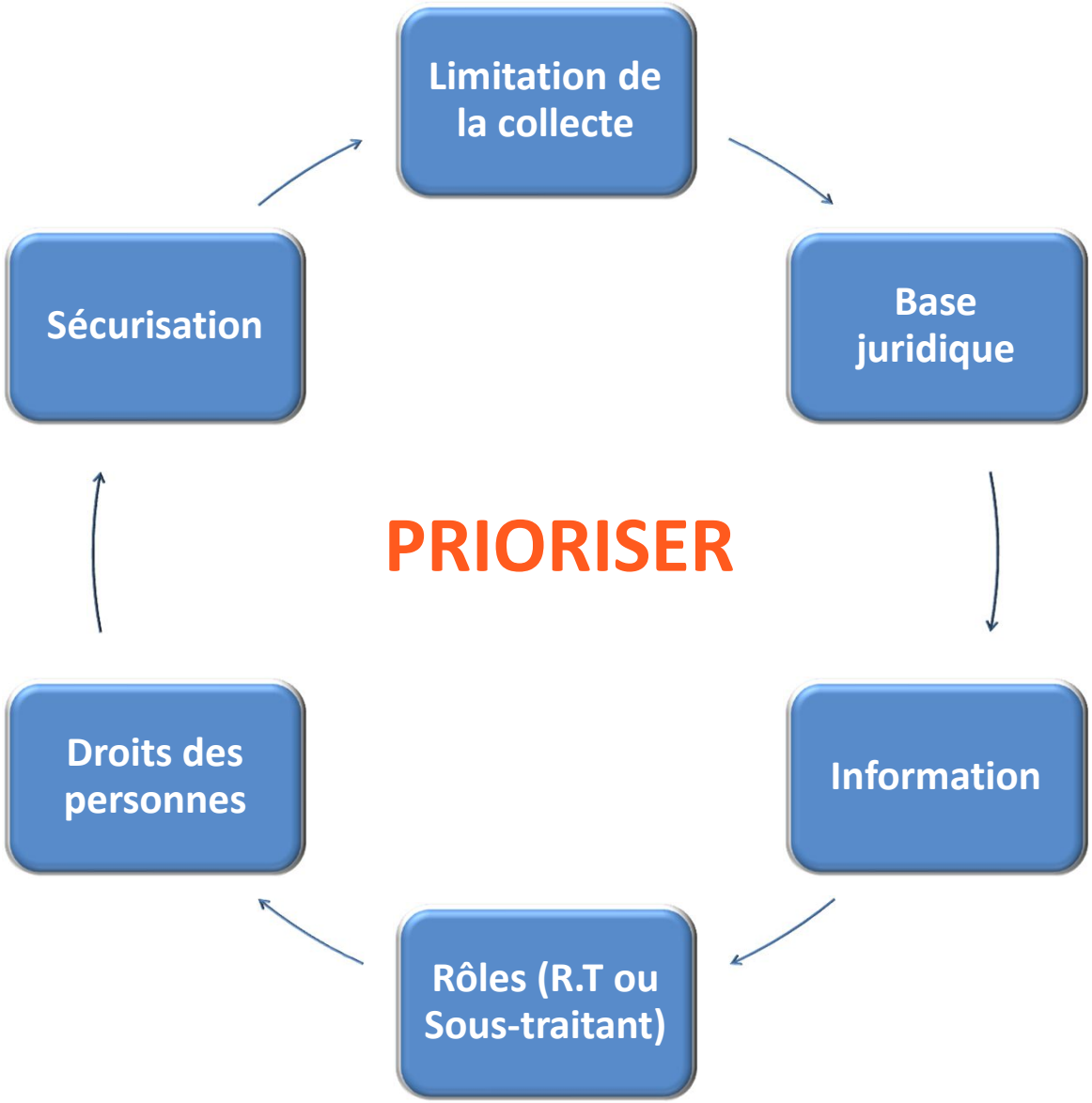


- Risque élevé pour les droits et libertés des personnes
- Avant de collecter les données et de mettre en œuvre leur traitement

Feuille de route

Source : www.cnil.fr

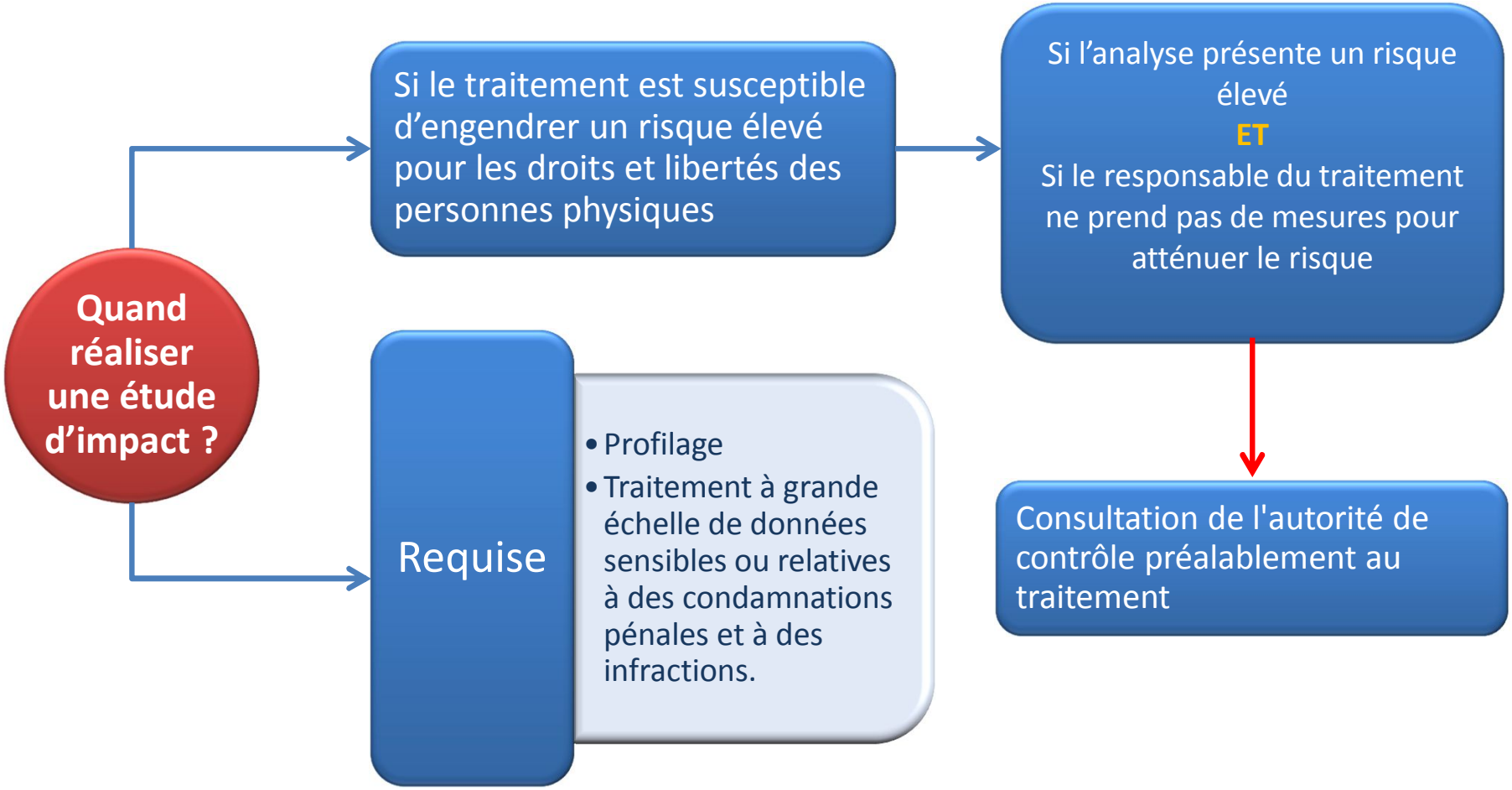
Le Règlement sur la protection des données personnelles



Feuille de route

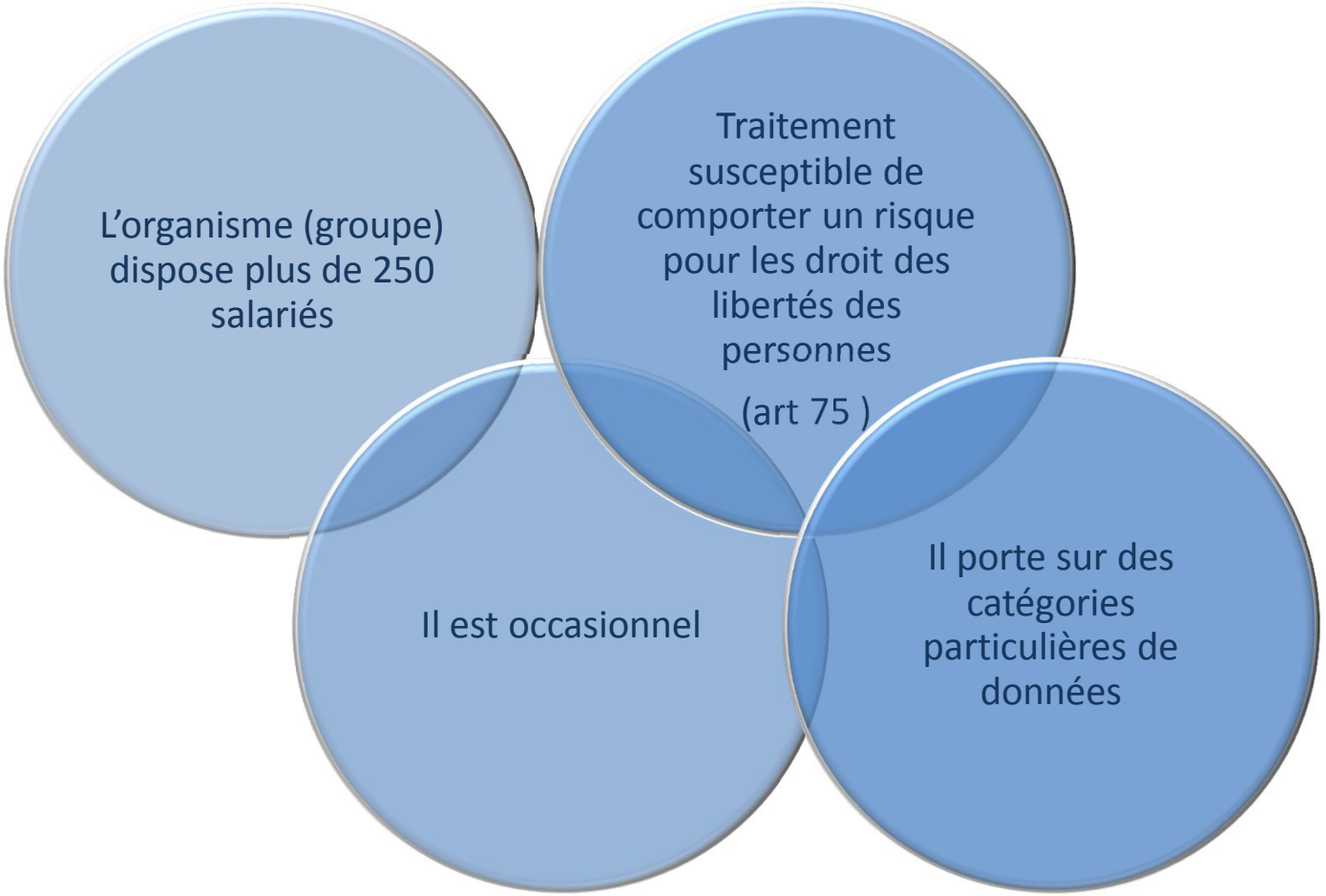
Source : www.cnil.fr

Les analyses d'impact sur la vie privée (AIVP/PIA)



Tenue d'un registre des activités du traitement

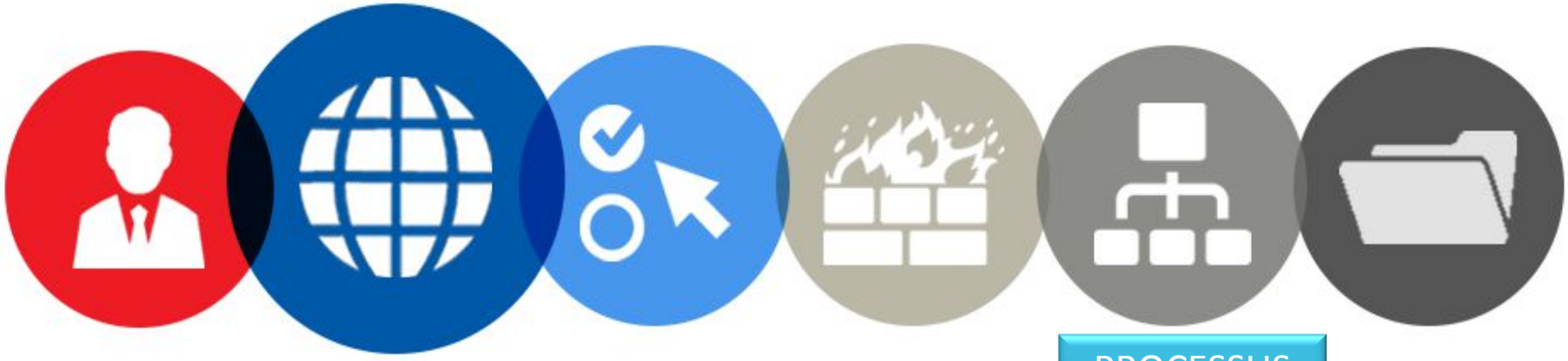
Le registre n'est pas obligatoire sauf si :



Le registre doit obligatoirement contenir :

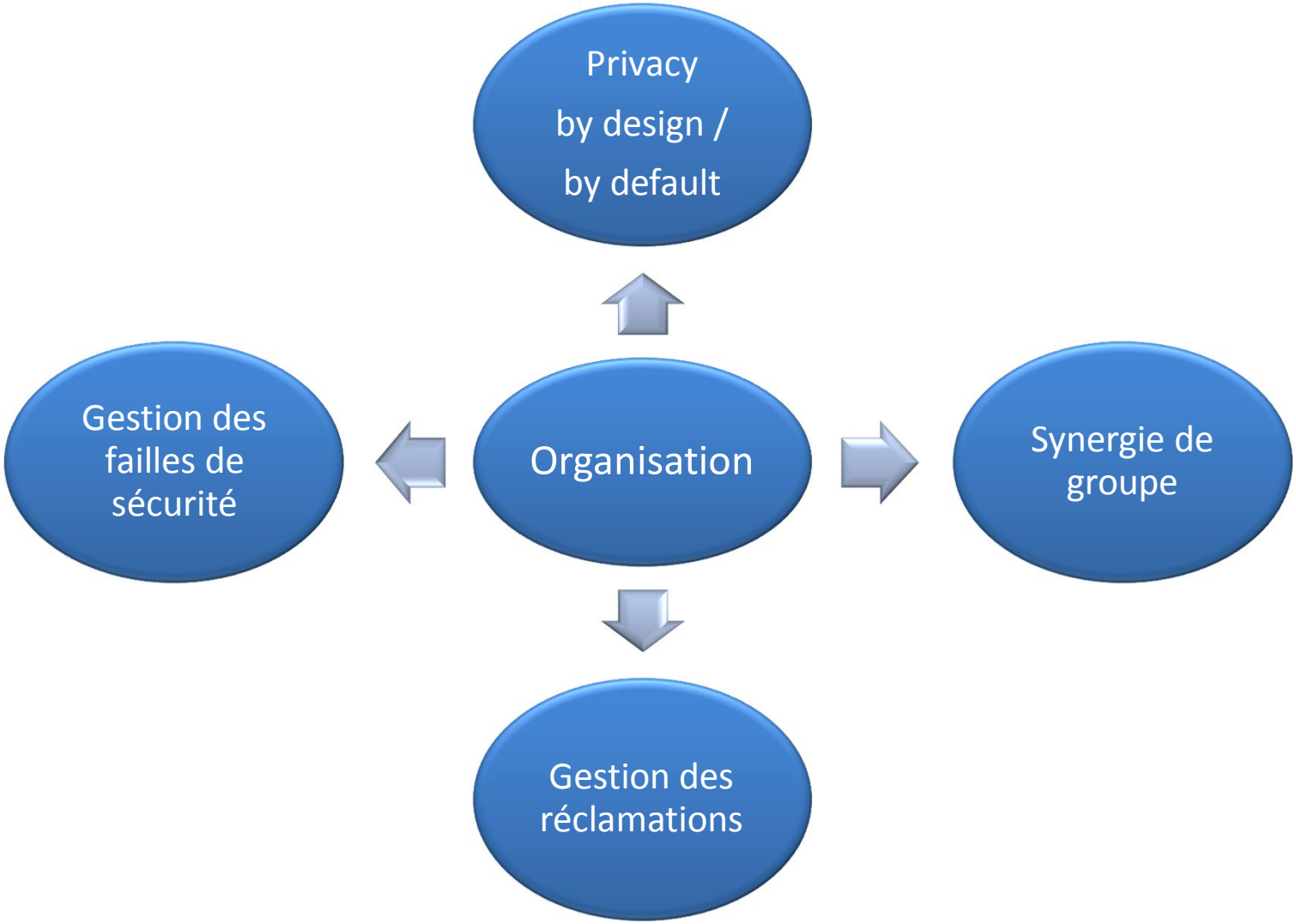
Responsable du traitement		Sous-traitant
✖	Le nom, les coordonnées des sous-traitants et des responsables du traitement	✖
✖	Les finalités et catégories du traitement	✖
✖	Une description des catégories de personnes concernées et des catégories de données à caractère personnel	
✖	Les destinataires	
✖	Les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale	✖
✖	Les délais prévus pour l'effacement	
✖	Une description générale des mesures de sécurité techniques et organisationnelles	

Feuille de route



Source : www.cnil.fr

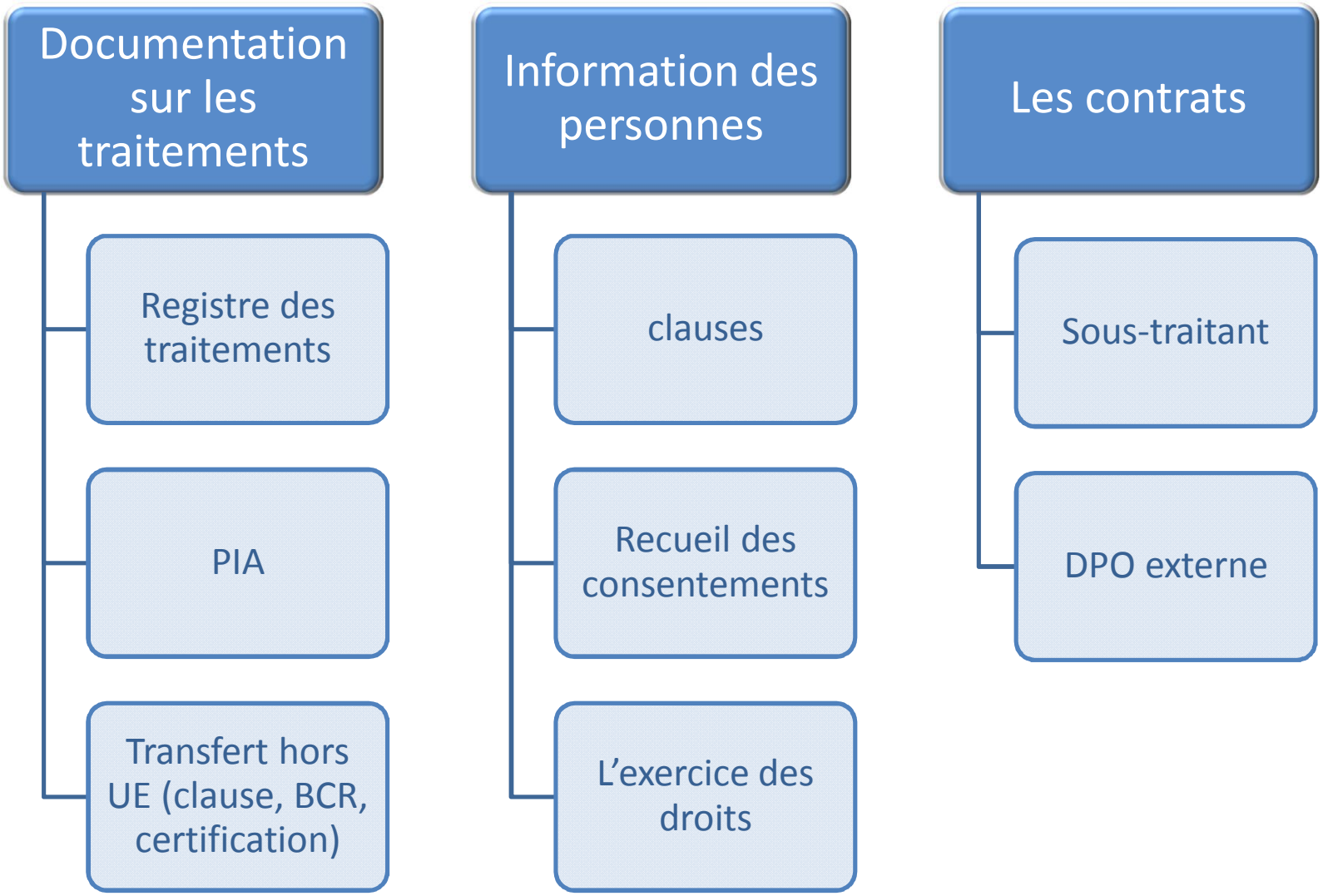
Processus Interne



Feuille de route

Source : www.cnil.fr

Documentation interne



Merci de votre attention

Vos questions…