BESLAY AVOCATS

RGPD: PROGRAMME DE CONFORMITÉ

Nathalie Beslay
AVOCAT
nathalie@beslay.net

MON PLAN POUR VOUS

Les points clés du RGPD

La mise en œuvre d'un programme de conformité

LE RÉFÉRENTIEL LÉGAL

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la **protection des personnes physiques** à l'égard du traitement des données à caractère personnel et à **la libre circulation de ces données**

- **Abrogation** de la Directive 95/46/CE

- Règlement général sur la protection des données = **RGPD**

- Entrée en vigueur le 24 mai 2016 et date limite de conformité au **25 mai 2018**

- Le RGPD est **d'application directe** dans tous les Etats de l'UE, la loi 78-17 du 6 janvier 1978 modifiée sera **adaptée.**

LE NOUVEAU CADRE DE CONFORMITÉ - RGPD

1. Les objectifs clés

2. Les acteurs

3. La classification des données

4. Les droits des personnes

5. Les obligations

6. Les instruments de la conformité

7. Les flux transfrontières de données

8. Les procédures

9. Les sanctions

1. LES OBJECTIFS CLÉS DU RGPD

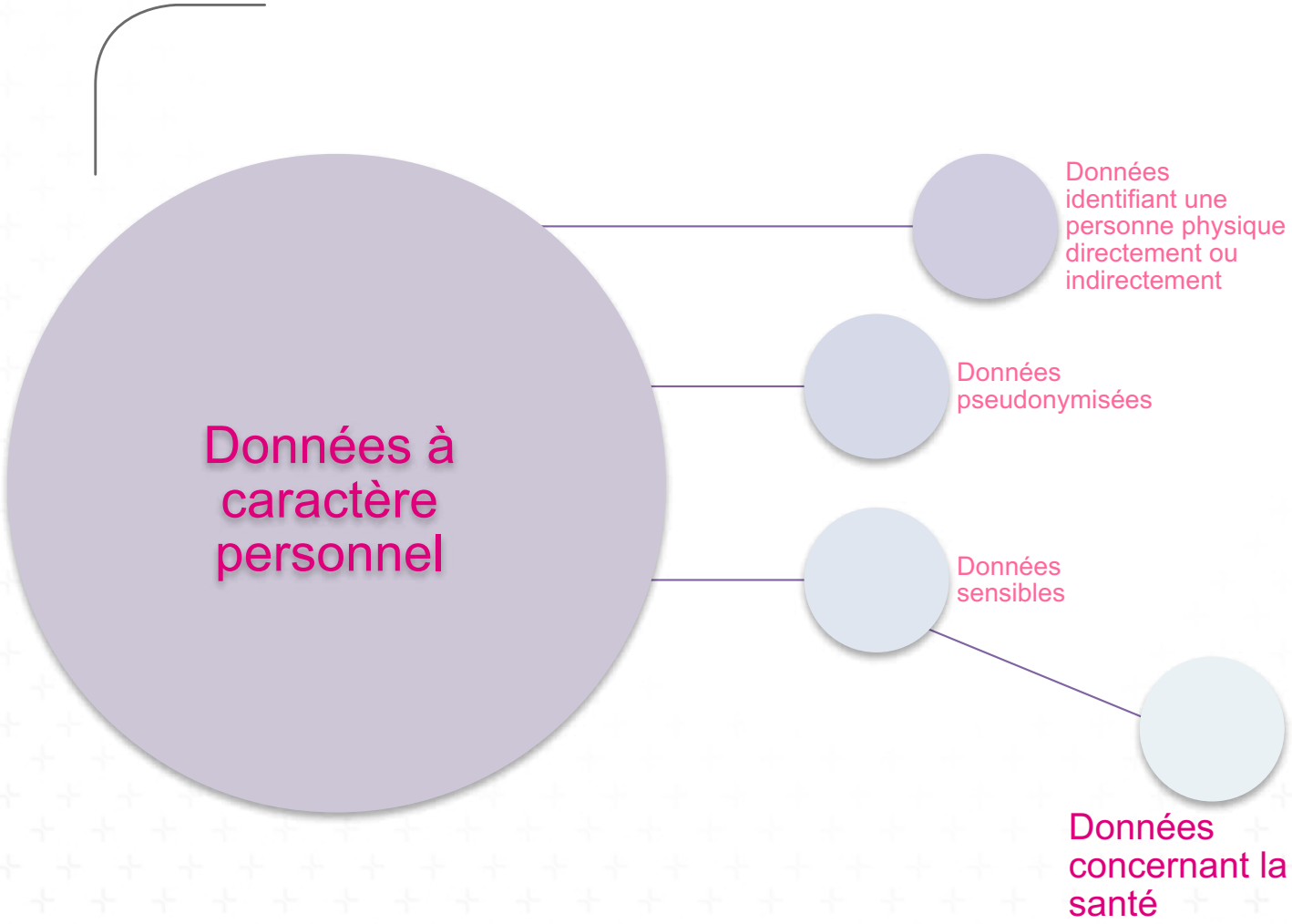
- Uniformiser les règles au niveau communautaire
- Renforcer les droits des personnes
- Clarifier des responsabilités opérationnelles
- Faciliter la libre circulation des données
- Transparence et responsabilisation du cadre de conformité
- Renforcer les sanctions

2. LES ACTEURS

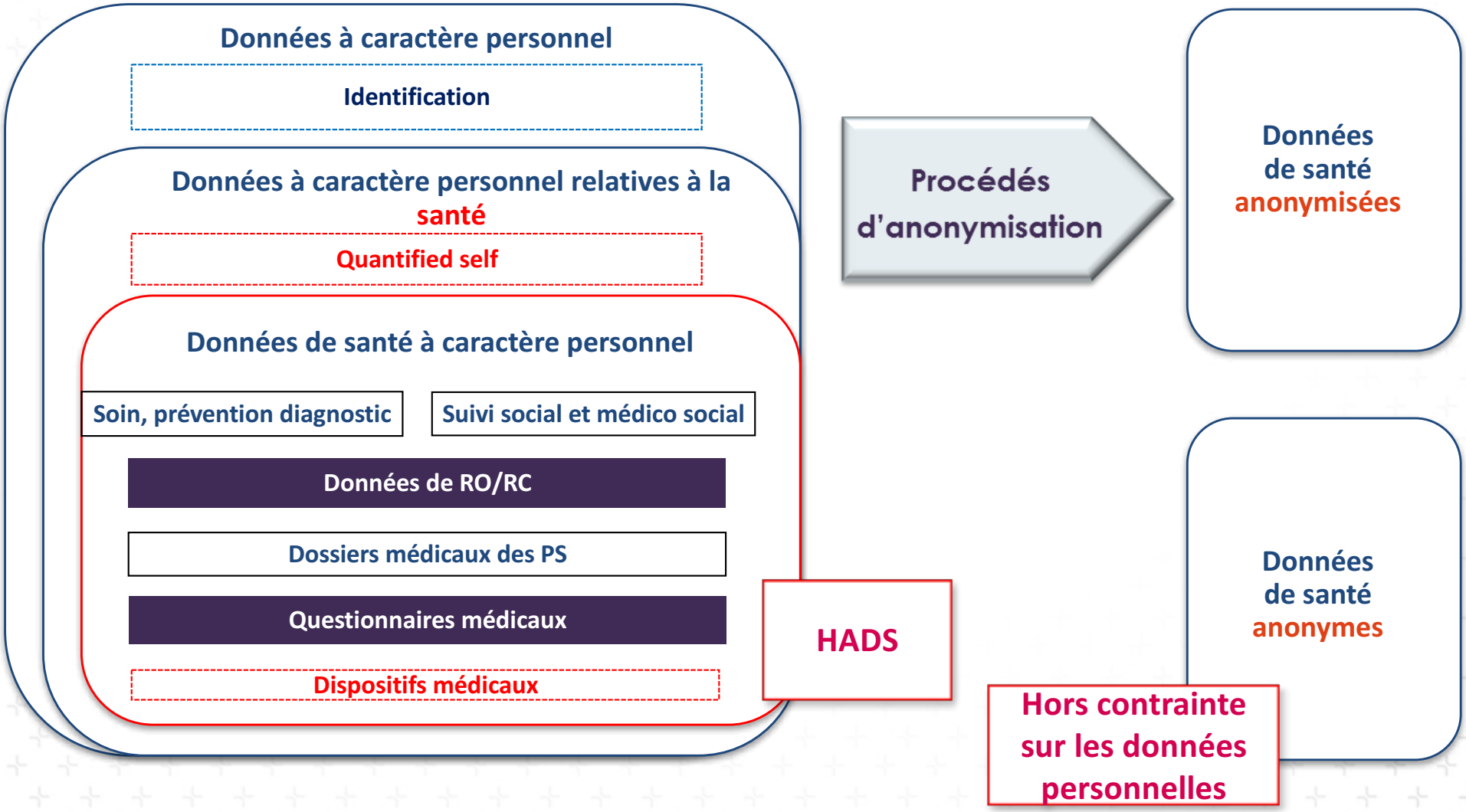
- Personne physique ou morale
- Autorité publique
- Service
- Tout autre organisme

Personne concernée	Personne physique identifiée ou identifiable
Responsable de traitement	Détermine seul ou conjointement les finalités et les moyens du traitement
Sous-traitant	Traite les données pour le compte du responsable de traitement
Destinataire	Reçoit communication des données; il peut être un tiers
Tiers	Personne non autorisée à traiter les données

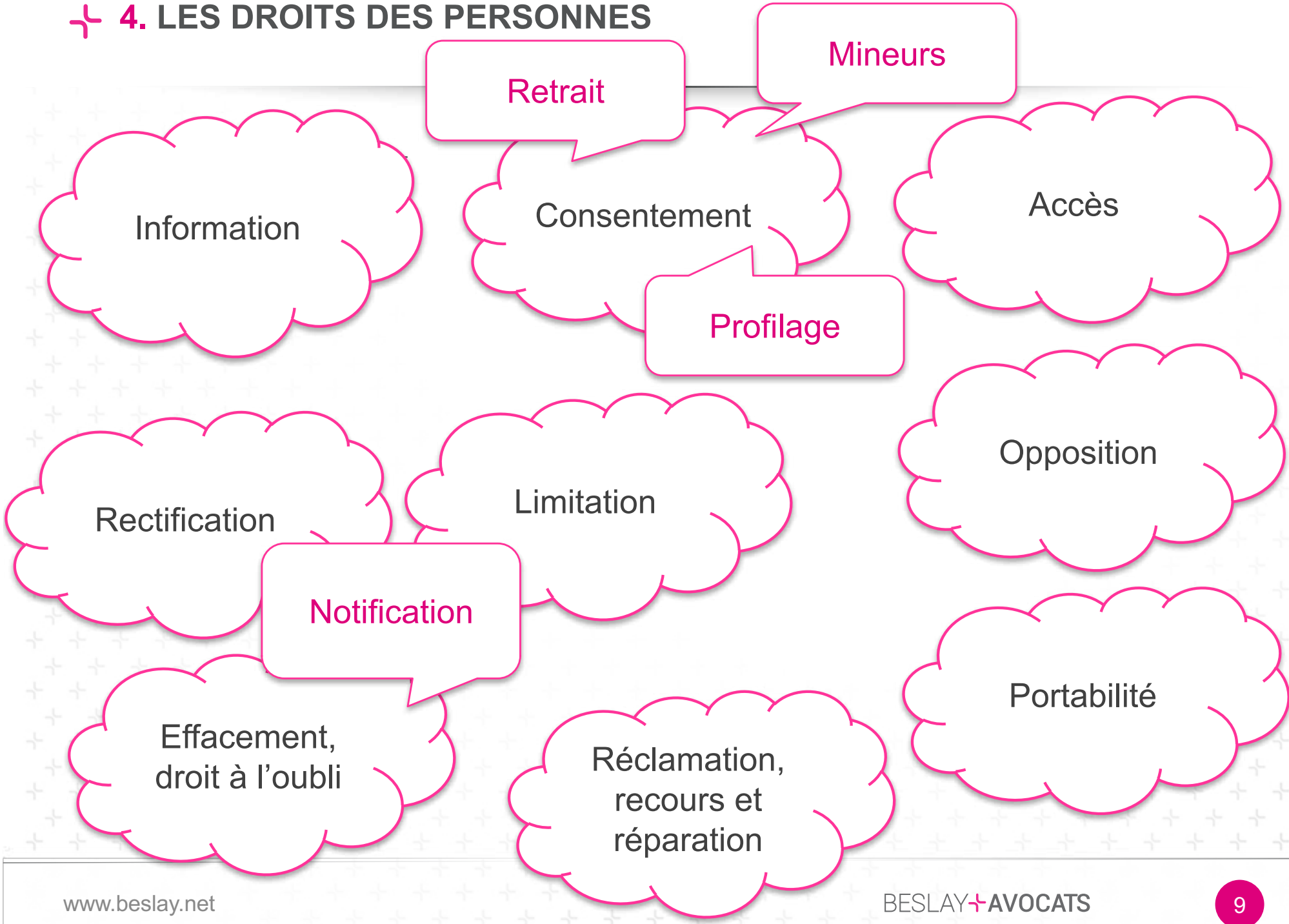
3. LA CLASSIFICATION DES DONNEES



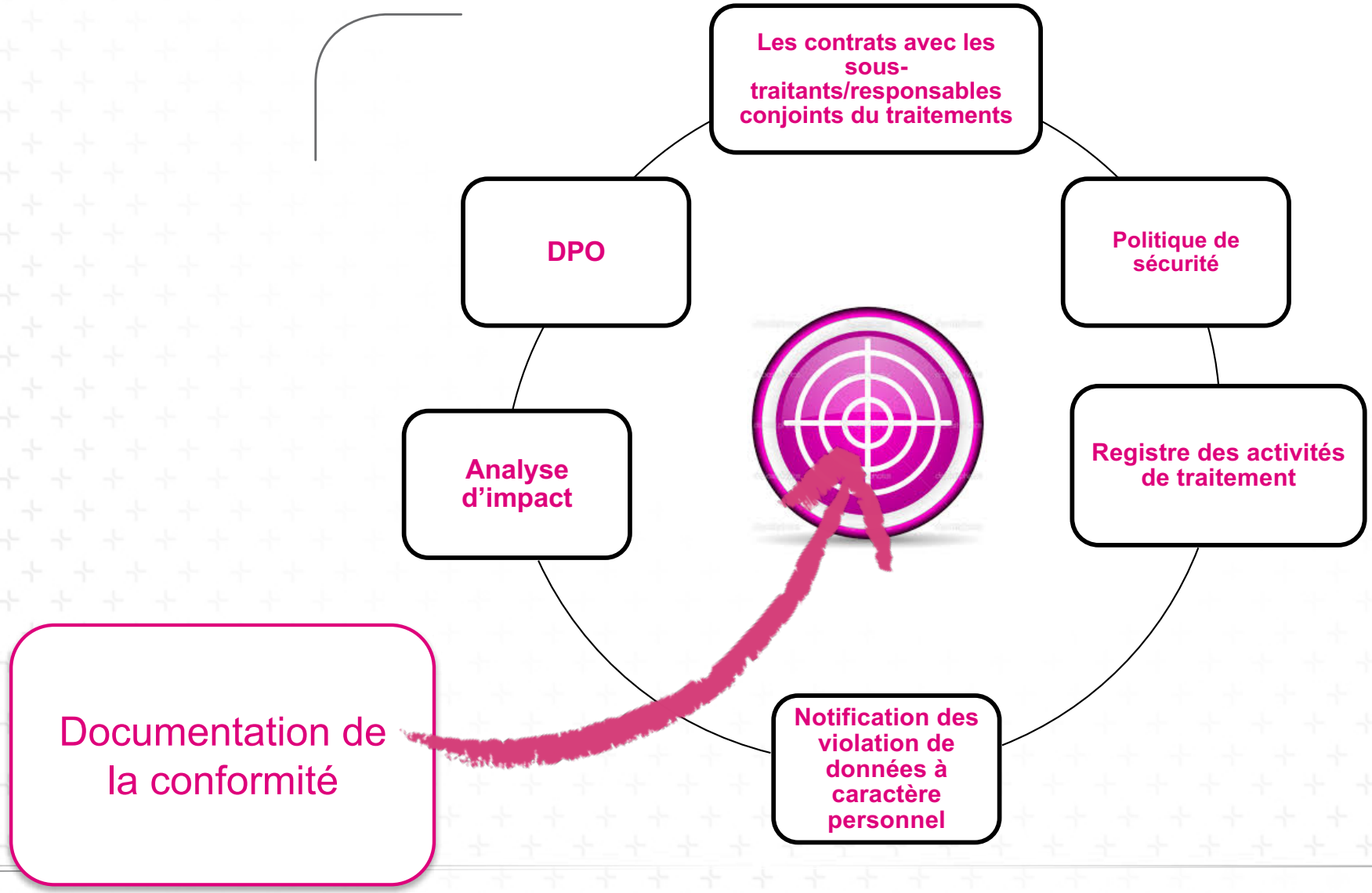
LES DONNÉES À CARACTÈRE PERSONNEL-SANTE



4. LES DROITS DES PERSONNES



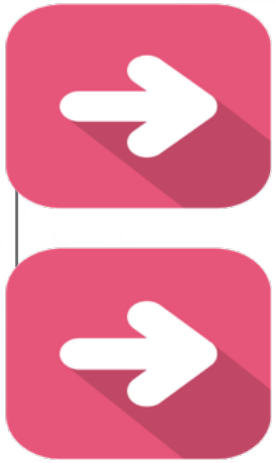
5. LES OBLIGATIONS NOUVELLES DE CONFORMITÉ



6. LES INSTRUMENTS DE LA CONFORMITÉ

- Code de conduite
- Certification, labels et marques

7. LES FLUX TRANSFRONTALIERS DE DONNÉES HORS UE



Pays bénéficiant d'une décision d'adéquation

Garanties appropriées prises par le responsable de traitement ou le sous-traitant

Privacy Shield Framework

Décision/Convention entre les autorités

Code de bonne conduite

Clauses contractuelles types Commission Européenne/CNIL

Certification

Règles d'entreprises contraignantes

8. LES PROCÉDURES

› Suppression de l'obligation générale de « notification » d'un traitement de données à caractère personnel après de l'autorité compétente

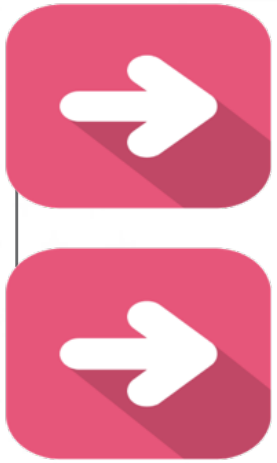
› Principe de responsabilisation du responsable de traitement par une documentation de la conformité comprenant pour les traitements les plus à risques une analyse d'impact

› Obligation de consultation préalable de l'autorité de contrôle uniquement pour les traitements présentant une analyse d'impact/risques élevés pour les droits et libertés

› Le droit des Etats membres peut décider qu'une consultation préalable est obligatoire lorsque le traitement est effectué dans le cadre d'une mission d'intérêt public, y compris la protection sociale et la santé publique.

Attente du texte d'adaptation du RGPD par la France/CNIL

9. LES SANCTIONS



Amendes administratives

Pouvoirs

- Enquêtes, contrôles, audits, accès aux locaux, aux informations et aux données
- Notification d'une violation du RGPD
- Avertissement
- Mise en demeure/injonction
- Suspension des flux/certification

9. LES SANCTIONS

Amendes administratives

Jusqu'à 20 000 000 d'euros ou 4% du CA annuel mondial de l'exercice précédent

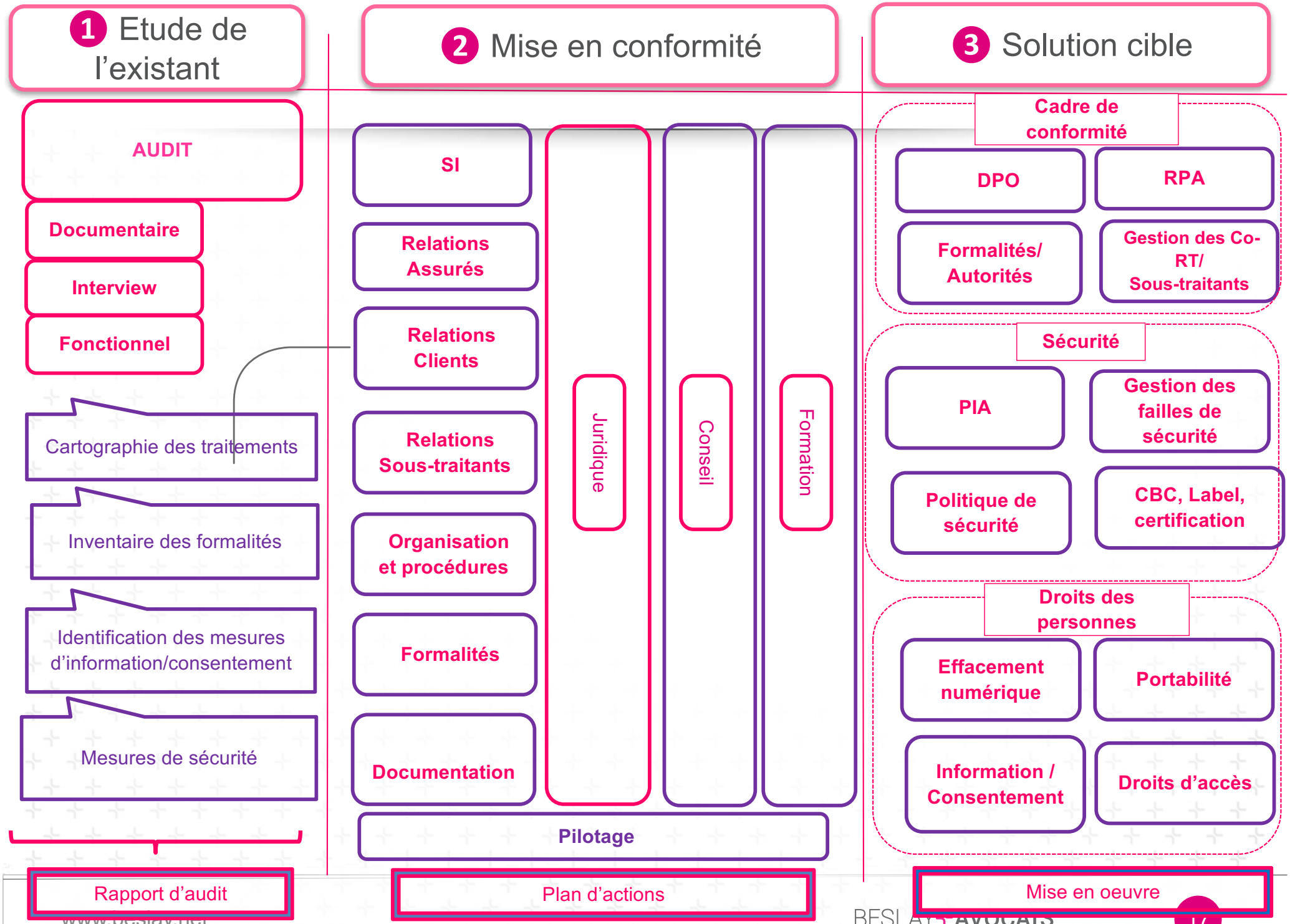
Montant le plus élevé

Principe de graduation, de proportionnalité et de dissuasion en fonction de la nature des violations

Analyse au cas par cas/ Circonstances

Garanties procédurales appropriées – Recours juridictionnel

La mise en œuvre d'un programme de conformité


1 Etude de l'existant
2 Mise en conformité
3 Solution cible
AUDIT
Documentaire
Interview
Fonctionnel
Cartographie des traitements
Inventaire des formalités
Identification des mesures d'information/consentement
Mesures de sécurité
SI
Relations Assurés
Relations Clients
Relations Sous-traitants
Organisation et procédures
Formalités
Documentation
Juridique
Conseil
Formation
Pilotage
Cadre de conformité
DPO
RPA
Formalités/ Autorités
Gestion des Co-RT/ Sous-traitants
Sécurité
PIA
Gestion des failles de sécurité
Politique de sécurité
CBC, Label, certification
Droits des personnes
Effacement numérique
Portabilité
Information / Consentement
Droits d'accès
Rapport d'audit
Plan d'actions
Mise en oeuvre