

RGPD : ce que les maisons sport-santé doivent savoir

Journées Nationales MSS
Juin 2025

Noémie BRIANTAIS-FOFANA
CNIL

LA CNIL : QUI SOMMES NOUS?

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

- › Autorité administrative indépendante
- › Créée en 1978



INFORMER LES PERSONNES ET PROTÉGER LEURS DROITS



ACCOMPAGNER LA CONFORMITÉ ET CONSEILLER



CONTRÔLER ET SANCTIONNER



ANTICIPER ET INNOVER

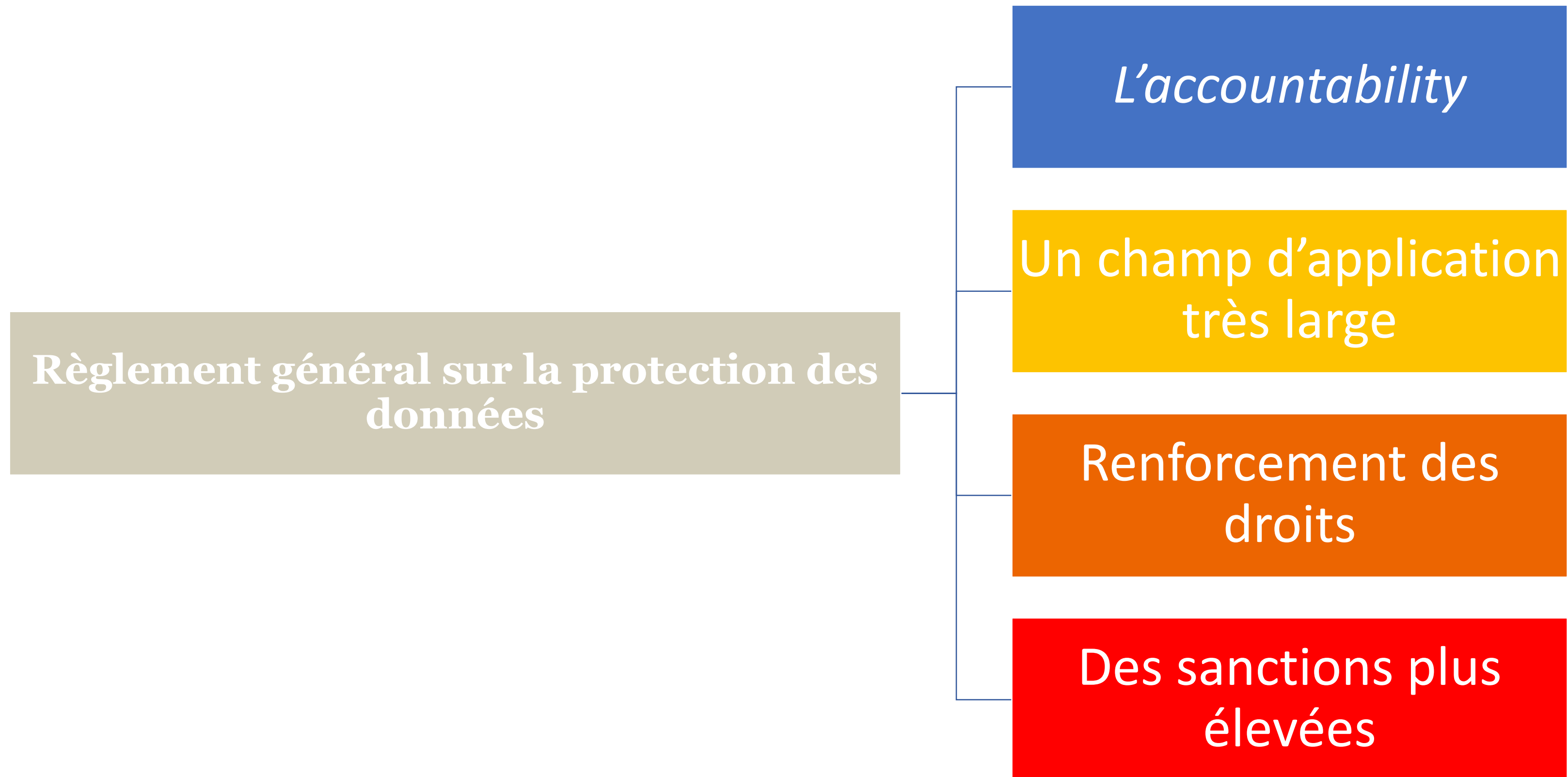
Plan de la présentation

1. Présentation du RGPD
2. Notions clés
3. Recours à un sous-traitant et désignation d'un DPO
4. Principes du RGPD
5. Régime particulier des données de santé
6. Information des personnes et exercice des droits
7. Mesures à mettre en œuvre et documentation obligatoire

Plan de la présentation

- 1. Présentation du RGPD**
- 2. Notions clés**
- 3. Recours à un sous-traitant et désignation d'un DPO**
- 4. Principes du RGPD**
- 5. Régime particulier des données de santé**
- 6. Information des personnes et exercice des droits**
- 7. Mesures à mettre en œuvre et documentation obligatoire**

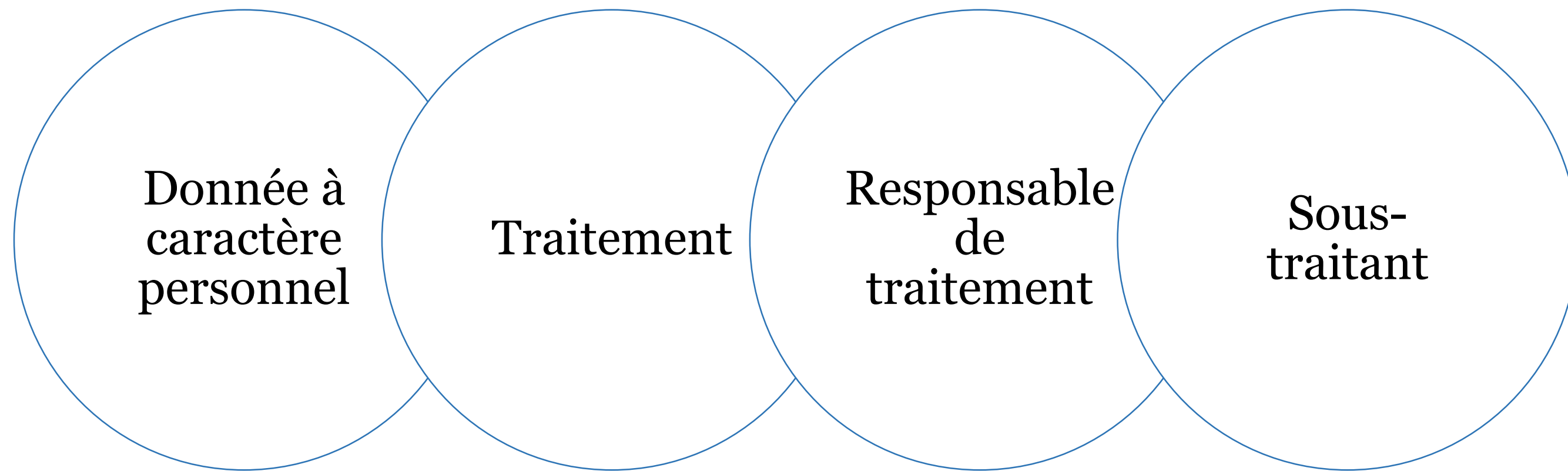
PRÉSENTATION DU RGPD



Plan de la présentation

1. Présentation du RGPD
2. **Notions clés**
3. Recours à un sous-traitant et désignation d'un DPO
4. Principes du RGPD
5. Régime particulier des données de santé
6. Information des personnes et exercice des droits
7. Mesures à mettre en œuvre et documentation obligatoire

NOTIONS CLÉS



Plan de la présentation

1. Présentation du RGPD
2. Notions clés
- 3. Recours à un sous-traitant et désignation d'un DPO**
4. Principes du RGPD
5. Régime particulier des données de santé
6. Information des personnes et exercice des droits
7. Mesures à mettre en œuvre et documentation obligatoire

RECOURS À UN SOUS-TRAITANT

Les **6 bonnes pratiques** à respecter dans le cadre d'une relation de sous-traitance :

- ✓ Déterminer le statut des acteurs impliqués
- ✓ Établir un contrat clair
- ✓ Documenter l'activité de sous-traitance
- ✓ Proposer des outils respectueux des données à caractère personnel
- ✓ Porter assistance pour répondre aux demandes d'exercices des droits des personnes
- ✓ Garantir la sécurité des données collectées

DÉSIGNATION D'UN DPO



Informer et conseiller



Contrôler le respect du RGPD



Coopérer avec l'autorité
Etre le point de contact

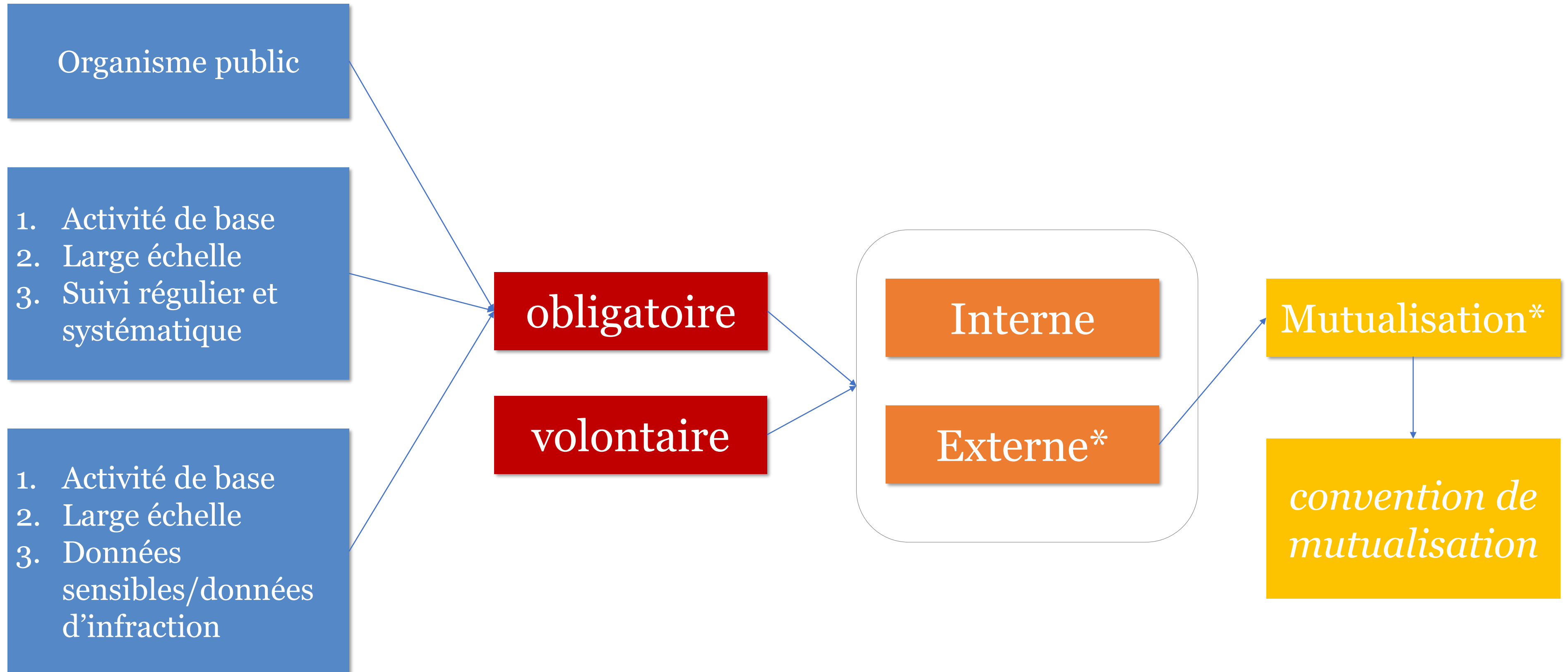


Conseils sur l'analyse d'impact
Vérifier son exécution



S'assurer de la bonne tenue
de la documentation

DÉSIGNATION D'UN DPO



Plan de la présentation

1. Présentation du RGPD
2. Notions clés
3. Recours à un sous-traitant et désignation d'un DPO
4. **Principes du RGPD**
5. Régime particulier des données de santé
6. Information des personnes et exercice des droits
7. Mesures à mettre en œuvre et documentation obligatoire

PRINCIPES DU RGPD

01



Base légale

Le traitement de données personnelles **doit être licite**, cad fondé sur **une base légale**

02



Finalité

Les données personnelles contenues dans un traitement ne sont recueillies et traitées que pour **un usage déterminé et légitime, préalablement défini**

03



Minimisation

Seules les données pertinentes et nécessaires au regard des objectifs poursuivis doivent être traitées

04



Durée limitée de conservation

Tant qu'elles présentent un caractère identifiant, **les données ne peuvent être conservées de façon indéfinie dans les fichiers**

05



Sécurité

Le responsable du traitement doit **prendre les mesures nécessaires pour garantir l'intégrité et la confidentialité des données**

06



Droits des personnes

Toute personne dont les données sont utilisées dans un traitement disposent d'un **droit d'accès, de rectification et, selon la base légale, d'un droit d'opposition**

LA BASE LÉGALE

- 01  Le consentement
- 02  L'exécution du contrat
- 03  L'obligation légale
- 04  La sauvegarde des intérêts vitaux
- 05  La mission d'intérêt public
- 06  L'intérêt légitime

Plan de la présentation

1. Présentation du RGPD
2. Notions clés
3. Recours à un sous-traitant et désignation d'un DPO
4. Principes du RGPD
- 5. Régime particulier des données de santé**
6. Information des personnes et exercice des droits
7. Mesures à mettre en œuvre et documentation obligatoire

RÉGIME PARTICULIER DES DONNÉES DE SANTÉ

▪ Qu'est-ce qu'une donnée de santé ?

- Données relatives à la **santé physique** (ex : conditions physiques, pathologies, antécédents médicaux, etc.) ou **mentale** (ex. : troubles cognitifs, psychiatriques, etc.) passée, présente ou future d'une personne qui **révèlent des informations sur son état de santé**.

RÉGIME PARTICULIER DES DONNÉES DE SANTÉ

■ Comment reconnaît-on une donnée de santé ?

TROIS CATÉGORIES DE DONNÉES DE SANTÉ

```
graph TD; A[TROIS CATÉGORIES DE DONNÉES DE SANTÉ] --> B[Données de santé par nature]; A --> C[Données de santé du fait d'un croisement avec d'autres données]; A --> D[Données de santé du fait de l'utilisation des données];
```

Données de santé par nature

Ex : scanner, mesure de glycémie, tension artérielle, diagnostic de cancer, etc.

Données de santé du fait d'un
croisement avec d'autres
données

Ex : l'association de la mesure de la tension artérielle avec l'âge du patient

Données de santé du fait de
l'utilisation des données

Ex : la photographie d'une personne intégrée à son dossier médical en vue de la réalisation d'un acte de chirurgie réparatrice

RÉGIME PARTICULIER DES DONNÉES DE SANTÉ

- **À quelles conditions peut-on utiliser les données de santé ?**
 - Les **données de santé** sont des **données sensibles** : leur utilisation est strictement encadrée par le RGPD et la loi « Informatique et Libertés ».
 - **Principe** : le **traitement de cette donnée** (collecte, enregistrement, transmission, utilisation, accès, etc.) est **interdit**.

RÉGIME PARTICULIER DES DONNÉES DE SANTÉ

○ **Exception** : à titre dérogatoire, la **donnée de santé** peut être **collectée, enregistrée, transmise**, etc. **dans des cas précis et listés par le RGPD**, notamment :

1. **en cas de consentement explicite de la personne concernée**
2. pour permettre l'exécution d'obligations ou l'exercice des droits du responsable de traitement ou de la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale
3. parce qu'elle est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée
4. parce qu'elle est manifestement rendue publique par la personne concernée
5. parce qu'elle est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou pour que la juridiction fonctionne dans son cadre juridictionnel
6. **pour des motifs d'intérêt public important**
7. **parce qu'elle est nécessaire à la prise en charge médicale ou à la protection sociale**
8. **pour des motifs d'intérêt public dans le domaine de la santé publique**
9. **parce qu'elle est utilisée à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historiques ou à des fins statistiques**

Plan de la présentation

1. Présentation du RGPD
2. Notions clés
3. Recours à un sous-traitant et désignation d'un DPO
4. Principes du RGPD
5. Régime particulier des données de santé
- 6. Information des personnes et exercice des droits**
7. Mesures à mettre en œuvre et documentation obligatoire

INFORMATION DES PERSONNES

La personne concernée par un traitement de données à caractère personnel doit recevoir une **information** délivrée de **façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples.**

INFORMATION DES PERSONNES

A quel moment le responsable de traitement est tenu d'informer les personnes concernées ?

Les personnes concernées par le traitement de leurs données à caractère personnel doivent être informées, selon les cas :

➤ Collecte directe des données à caractère personnel

Dès que possible, soit **préalablement à la collecte** des données, soit **au moment de la collecte** des données personnelles **au plus tard**.

2. Collecte indirecte des données à caractère personnel

Dès que possible et **au plus tard dans un délai d'un mois**.

Il y a **deux exceptions** au délai d'un mois :

- Si les données sont utilisées pour **communiquer avec la personne concernée** : les informations doivent être délivrées **au plus tard lors de la première communication** avec celle-ci ;
- Si les informations sont **communiquées à un autre destinataire** : les informations doivent être délivrées au plus tard lorsque les données sont communiquées pour la première fois.

Quelles informations fournir aux personnes concernées ?

➤ Dans tous les cas :

- L'identité et coordonnées du **responsable du traitement** des données ;
- Les **finalités** du traitement ;
- La **base légale** du traitement de données ;
- Le **caractère obligatoire ou facultatif du recueil des données** et **les conséquences** pour la personne en cas de non-fourniture des données ;
- Les **destinataires** ou catégories de destinataires des données ;
- La **durée de conservation** des données (ou les critères permettant de la déterminer) ;
- Les **droits des personnes** concernées ;
- Les **coordonnées du délégué à la protection** des données de l'organisme, s'il a été désigné, ou d'un **point de contact** sur les questions de protection des données personnelles ;
- Le **droit d'introduire une réclamation auprès de la CNIL**.

INFORMATION DES PERSONNES

➤ Selon les cas :

- les intérêts légitimes poursuivis par le responsable du traitement si le traitement est fondé sur la base légale de l'intérêt légitime ;
- **le fait que les données sont requises par la réglementation**, par un contrat ou en vue de la conclusion d'un contrat ;
- l'existence d'un transfert des données vers un pays hors Union européenne (ou vers une organisation internationale), les garanties associées à ce transfert et la faculté d'accéder aux documents autorisant ce transfert ;
- l'existence d'une prise de décision automatisée ou d'un profilage, les informations utiles à la compréhension de l'algorithme et de sa logique, ainsi que les conséquences pour la personne concernée ;
- **le droit au retrait du consentement à tout moment**, si le base légale du traitement est le consentement des personnes ;
- les autres droits applicables au traitement, en fonction de sa base légale : droit d'opposition et droit à la portabilité.

➤ Informations supplémentaires à donner en cas de collecte indirecte :

- **Catégories de données** recueillies ;
- **Source des données** (en indiquant notamment si elles sont issues de sources accessibles au public).

DROITS DES PERSONNES



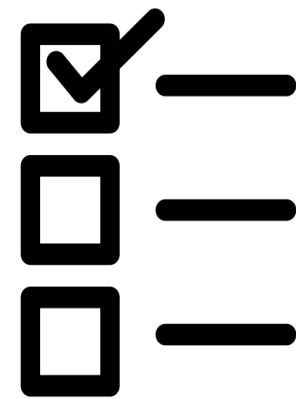
1. Information
2. Accès
3. Rectification
4. Effacement
5. Opposition
6. Limitation
7. Portabilité des données
8. Décision individuelle automatisée

Plan de la présentation

1. Présentation du RGPD
2. Notions clés
3. Recours à un sous-traitant et désignation d'un DPO
4. Principes du RGPD
5. Régime particulier des données de santé
6. Information des personnes et exercice des droits
- 7. Mesures à mettre en œuvre et documentation obligatoire**

MESURES ET DOCUMENTATION À METTRE EN ŒUVRE

Fiche registre



Analyse d'impact
relative à la protection
des données



FOCUS SUR LE REGISTRE DE TRAITEMENT

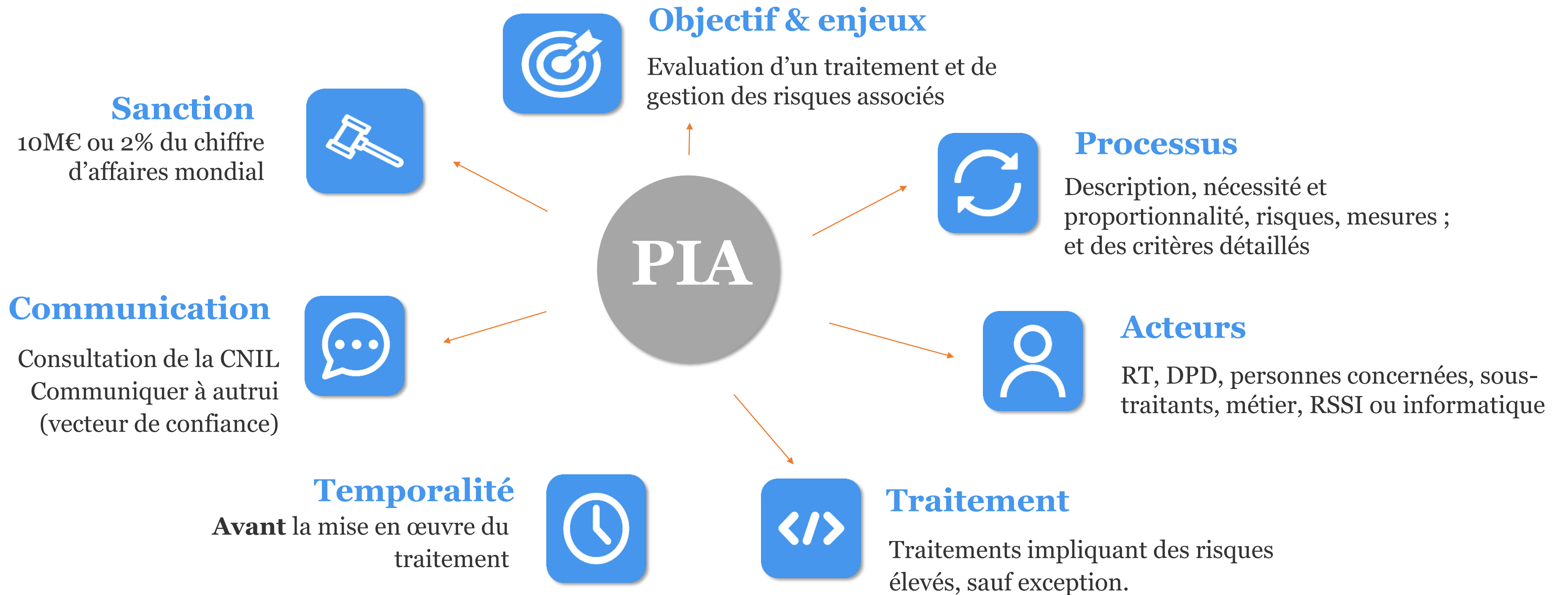
La tenue d'un registre est obligatoire :

- pour les organismes ayant plus de 250 employés ;
- si le traitement des données est susceptible de comporter un risque pour les droits et libertés des personnes concernées ;
- si le traitement des données n'est pas occasionnel ;
- si le traitement des données porte notamment sur les catégories particulières de données (santé, religion etc.) ou sur des condamnations pénales et des infractions.

Contenu du registre du responsable de traitement de données à caractère personnel

- nom et coordonnées du responsable de traitement et du délégué à la protection des données ;
- finalités du traitement ;
- catégories de personnes concernées et catégories de données ;
- catégories de destinataires ;
- transferts de données vers un pays tiers ou à une organisation internationale ;
- les délais prévus pour l'effacement des données.

ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES (AIPD)



DANS QUELS CAS RÉALISER UNE AIPD

Obligatoire

- **Risques élevés: 9 critères à considérer**
 - *Évaluation/scoring*
 - *Décision automatique avec effet légal*
 - *Surveillance systématique*
 - *Données sensibles/hautement personnel*
 - *Large échelle*
 - *Croisement de données*
 - *Personnes vulnérables*
 - *Usage innovant*
 - *Blocage d'un droit/contrat*
- **Liste publiée par la CNIL**

Pas obligatoire

- **Pas susceptible d'engendrer des risques élevés**
- AIPD existant sur traitement similaire
- Traitement ayant fait l'objet d'une formalité avant le 25 mai et si aucune modification
- Base légale UE/nationale + AIPD
- **Liste de traitements dispensés**
- Démonstration que les risques ne sont pas élevés



Vous avez une question ?

1/ Le responsable de traitement est défini comme :

- la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.
- la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers.

Bonne réponse : selon l'article 4.7 du RGPD, le responsable de traitement est défini comme, la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

Est responsable de traitement l'organisme qui détermine le « pourquoi » (objectifs poursuivis) et le « comment » (moyens techniques, matériel et organisationnel) du traitement.

Par ailleurs, des organismes peuvent être co-responsables de traitement s'ils déterminent conjointement les finalités et moyens de traitement.

2/ Dans le cadre de l'évaluation de l'impact des maisons sport-santé (MSS), celles-ci doivent transmettre des informations sur leur activité et leurs bénéficiaires. Les nom et prénom des bénéficiaires ne sont pas transmis. S'agit-il d'un traitement de données à caractère personnel ?

- OUI
- NON

Bonne réponse : oui.

Une donnée personnelle peut être définie comme toute information se rapportant à une personne physique identifiée ou identifiable.

Ce n'est pas parce que les organismes ne traitent pas le nom et le prénom qu'il n'y a pas de données personnelles, dès lors qu'il est possible à partir des autres données d'identifier la personne concernée.

3/ Il est possible de traiter des données à caractère personnel au cas où le responsable de traitement en aurait besoin à l'avenir :

- VRAI
- FAUX

Bonne réponse : faux.

La finalité doit être déterminée, explicite et légitime.

Pour être déterminée, il ne doit pas y avoir de buts cachés ni de collectes de données « au cas où » car elles pourraient être utiles à des objectifs non encore définis. La finalité doit être déterminée avant toute mise en œuvre du traitement.

4/ Une donnée à caractère personnel peut être conservée pour une durée illimitée :

- VRAI
- FAUX

Bonne réponse : faux.

Les données ne peuvent être conservées durant une durée indéfinie.

La durée de conservation des données est strictement limitée et cohérente avec l'objectif poursuivi.

5/ Dans le cadre de la prise en charge d'un bénéficiaire d'une pratique sportive adaptée, son poids, sa taille, sa tension artérielle et son âge sont collectés. S'agit-il de données de santé ?

- OUI
- NON

Bonne réponse : oui.

Il s'agit des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée.

Cela comprend :

- des données de santé par nature ;
- des données de santé par croisement ;
- des données de santé du fait de l'utilisation de celles-ci.

6/ Il est en principe interdit de collecter des données de santé.

- VRAI
- FAUX

Bonne réponse : vrai.

Selon l'article 9.1 du RGPD, le traitement de données sensibles est par principe interdit. L'article 9.2 prévoit cependant certaines exceptions pour lesquelles il est possible de traiter des données sensibles :

- a) lorsque la personne concernée a donné son consentement explicite ;
- b) le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits en matière de droit du travail, de la sécurité sociale et de la protection sociale (ex de la déclaration des accidents de travail) ;
- c) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée dans le cas où elle se trouve dans l'incapacité physique ou juridique de donner son consentement ;
- d) le traitement est effectué pour la gestion des membres d'un organisme à but non lucratif (politique, philosophique, religieuse ou syndicale) ;
- e) le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée ;
- f) le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ;
- g) le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un 'État membre ;
- h) le traitement est nécessaire à des fins médicales (médecine préventive ou de la médecine du travail, diagnostics médicaux, gestion des systèmes de santé ou de protection sociale) ;
- i) le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, sur la base du droit de l'Union ou du droit de l'État membre ;

j) le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, sous réserve d'être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

7/ Une MSS recourt à un prestataire pour héberger les données de ses bénéficiaires, qu'elle traite sur son système d'information. L'hébergeur est le sous-traitant de la MSS.

- VRAI
- FAUX

Bonne réponse : vrai.

Selon l'article 4.8 du RGPD, le sous-traitant est entendu comme la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

Les catégories de sous-traitant sont multiples et peuvent notamment comprendre les prestataires de services informatiques (hébergement, maintenance).

Les 6 bonnes pratiques à respecter dans le cadre d'une relation de sous-traitance :

- ✓ Déterminer le statut des acteurs impliqués ;
- ✓ Établir un contrat clair ;
- ✓ Documenter l'activité de sous-traitance ;
- ✓ Proposer des outils respectueux des données à caractère personnel ;
- ✓ Porter assistance pour répondre aux demandes d'exercices des droits des personnes ;
- ✓ Garantir la sécurité des données collectées.

8/ Lors de l'accueil d'un bénéficiaire, une MSS collecte auprès de ce dernier des données personnelles pour l'orienter vers la bonne structure. Peut-elle informer le bénéficiaire du traitement de ses données une fois sa prise en charge par la structure compétente confirmée ?

- OUI
- NON

Bonne réponse : non.

En cas de collecte directe des données à caractère personnel, l'information doit être apportée aux personnes concernées dès que possible, soit préalablement à la collecte des données, soit au moment de la collecte des données personnelles, au plus tard.