

Sensibilisation initiale au RGPD (profil RT)

MISSION RGPD





« Démystifions le RGPD »

RGPD : Règlement Général pour la
Protection des Données (GDPR :
General Data Protection Regulation)

Objectif de la sensibilisation



1. Nivelier les connaissances des participants pour servir de socle aux focus de perfectionnements .
2. Connaitre les principes fondamentaux et exigences en termes de protection des données personnelles.
3. Être capable d'engager sa mise en conformité et de sensibiliser les agents de l'Organisme.
4. Être informé des services et outils mis à disposition par « Mission RGPD » du Centre de Gestion.

Les limites de ce module : l'interface DLD, les sujets avancés (AIPD, exercice de droit, rédiger une mention... etc.) ne sont pas abordés dans ce module mais feront l'objet d'autres modules (présentiel, webinaire).

I. LES DEFINITIONS

- o Petit lexique
- o Les données à caractère personnel (DCP)
- o Les DCP dites de catégorie particulière
- o Regroupement des DCP en 8 catégories
- o Les traitements
- o Responsable de Traitement et Sous Traitant

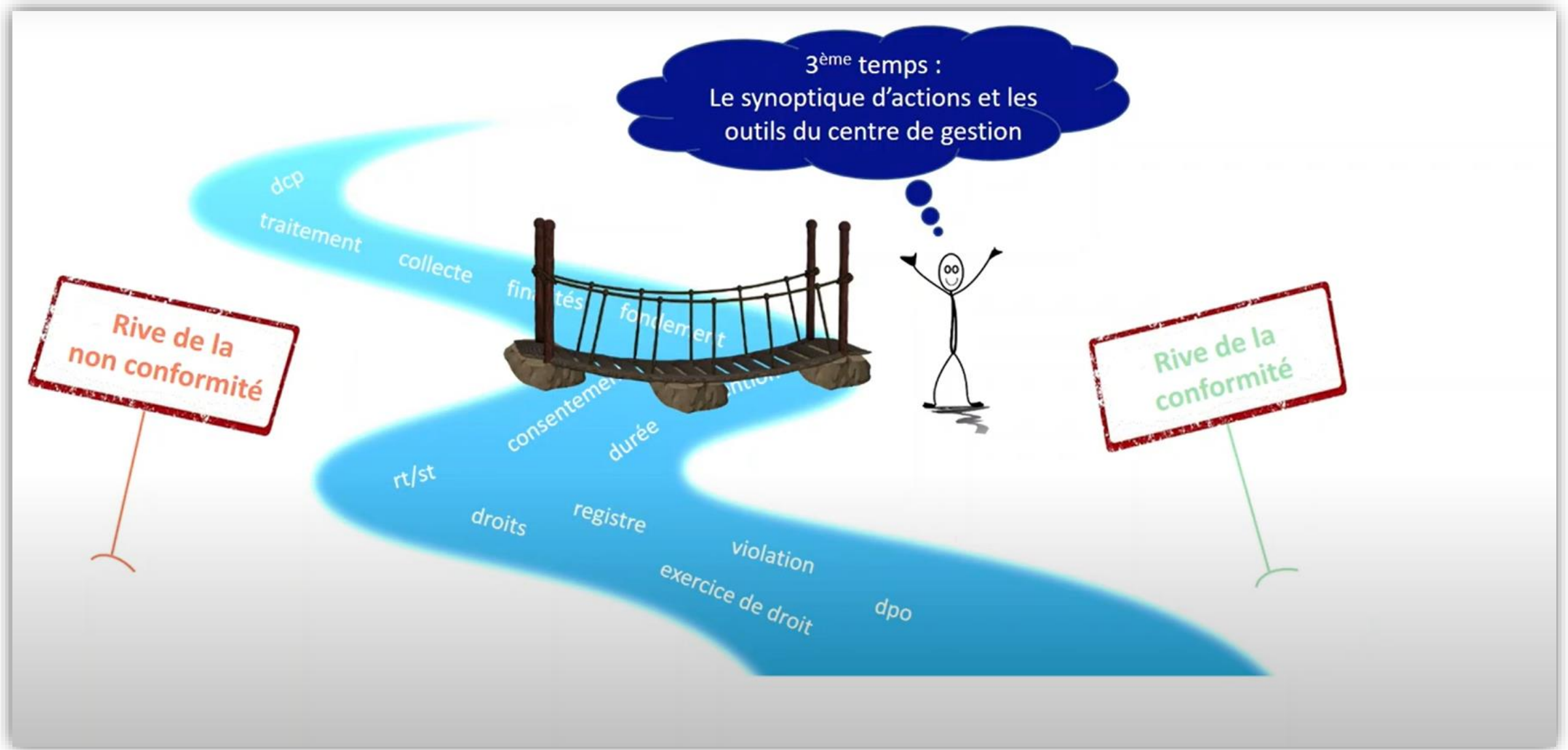
II. LES PRINCIPES FONDAMENTAUX

- o Les 8 règles d'or relatives aux traitements
- o Le fondement juridique
- o Le régime particulier du consentement
- o La suppression des DCP : un enjeu crucial
- o Les mentions d'information
- o La contractualisation des ST
- o Les droits des personnes
- o Résumons sous forme de cycle de vie de la DCP
- o La protection des DCP
- o Les risques et les sanctions

III. LE CHEMIN VERS LA CONFORMITE

IV. «MISSION RGPD »

- o Rôle du DPD ou DPO
- o Référent DPD interne et DPD (DPO) externe
- o Les services de « Mission RGPD »
- o Les outils de « Mission RGPD »



I] LES DEFINITIONS



LES DEFINITIONS

- **RGPD** Le Règlement Général pour la Protection des Données.
- **DCP** Données à caractère personnel (= DP : Données Personnelles).
- **RT** Responsable de traitement (au sens RGPD).
- **ST** Sous-traitant (au sens RGPD) qui répond aux instructions du RT.
- **DPO** Data Privacy Officer ou Délégué à la Protection des Données (DPD).
- **PERSONNE CONCERNEE** Personne physique propriétaire des DCP.
- **TRAITEMENT** Opération (manuelle ou automatique) qui manipule des DCP.
- **AIPD** Analyse d'Impact pour la Protection des Données ou PIA (Privacy Impact Assessment).
- **REGISTRE** Outil destiné à documenter et démontrer votre conformité (dans notre cas DLD).
- **Hors scope** Un traitement qui ne comporte pas de DCP n'est pas considéré par le RGPD.

Les données à caractère personnel (DCP)

DCP

Constitue une **DCP** toute information relative à une **personne physique identifiée** ou **identifiable**.

Une personne peut être identifiée :

- > **Directement** (nom, prénom).
- > **Indirectement** (par un identifiant « n° client », numéro de téléphone, une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image).



L'identification d'une personne peut être également réalisée à partir du **recoupement** d'un ensemble de données.



Historique
de navigation

Sites RS

Préférences
d'achat

Sondage

=> Le recoupement permet d'identifier la personne



**DONNEES
SENSIBLES**

Les DCP dites de « catégorie particulière »



DCP qui représentent un risque élevé pour les droits et libertés des personnes concernées
Données sensibles interdites à la collecte sauf exception dûment justifiée (art. 9) *

** Consentement exprès de la personne, informations rendues publiques par la personne, nécessité pour la sauvegarde de la vie humaine, intérêt public autorisé par la CNIL, membres ou adhérents d'une association ou d'une organisation politique, religieuse, philosophique, politique ou syndicale.*

Données de catégorie particulière (ex sensibles) au sens de l'art.9 du RGPD :

- Origine raciale ou ethnique ;
- Opinion politique ;
- Convictions philosophiques ou religieuses
- Appartenance syndicale ;
- Données de santé (physique ou mentale) ;
- Vie et orientation sexuelles ;
- Données génétiques ;
- Données biométriques aux fins d'identifier une personne physique de manière unique ;

Mais également une sensibilité particulière à considérer pour :

- > Numéro de sécurité sociale (ou NIR – Numéro d'Inscription au Répertoire) ;
- > Infractions, condamnations, mesures de sûreté, casier judiciaire ;
- > Données sur les mineurs.
- > Données de profilage (analyser et prédire le comportement d'une personne : performance au travail, situation financière, santé, préférences ou centres d'intérêt, habitudes de vie) ;



Regroupement des DCP en 8 catégories

1. Données d'état-civil ou d'identification

2. Données de connexion

3. Données de localisation

4. Vie personnelle

5. Vie professionnelle

6. Informations économiques privées et professionnelles

7. Données sensibles règlementées

8. Données bancaires



1.Nom, Prénom : Orange, LaCliente
1.Numéro client : 123456
1.Adresse : 112 avenue Faidherbe 75011, Paris

2.Dernière adresse IP : 192.168.1.1
2.Derniers sites consultés : Le Monde, Facebook

3. Dernière géolocalisation : Starbucks Saint Lazare

4.Statut Marital : Probablement Mariée
4.Née le : 05 Mai 1983

6.Profession : Cadre dans la banque, diplômée 2008 de LA FAC

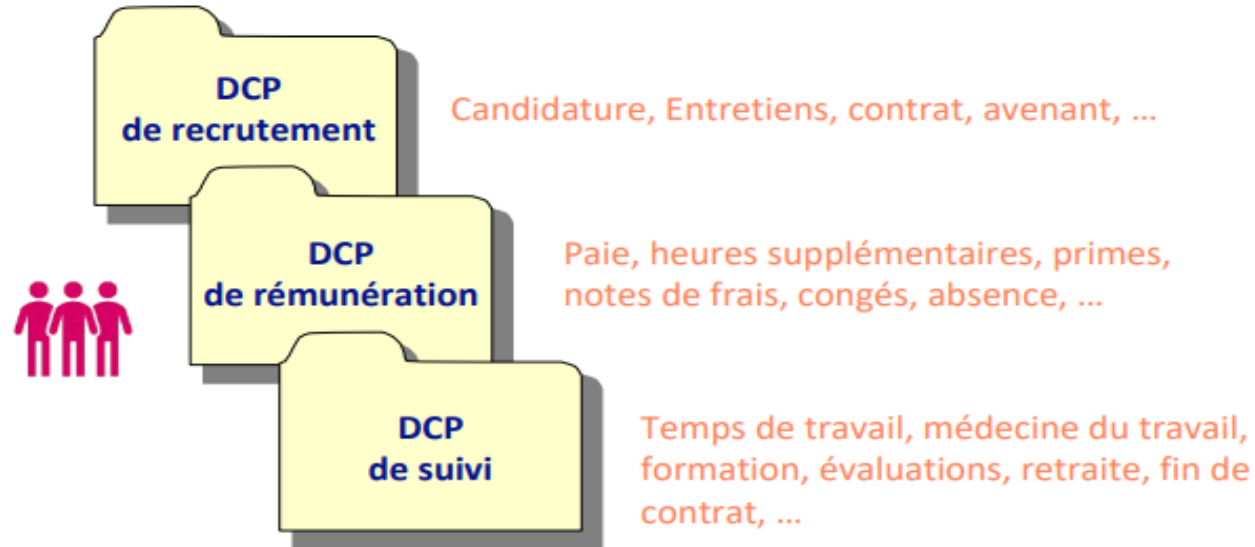
6.Salaire : entre 45 et 60K€
6.Impôts : éligible à la défiscalisation

7.Orientation politique : Adhérente du « Parti Politique »

8.Données bancaires : Paiement en Carte American Express 3749 XXXXXX XXXX0

Exemple : Dossier RH

Un dossier du personnel peut comporter jusqu'à 70 types de documents différents qui jalonnent le parcours de l'agent, de son embauche jusqu'à son départ.



Les Traitements



Responsable de traitement

Personne morale qui détermine :

Les finalités (objectifs, fonctionnalités, etc.)

Les moyens (financement, organisation, etc.)

Le RT ne doit faire **appel qu'à des sous-traitants qui présentent les garanties suffisantes** quant à la mise en œuvre des mesures techniques et organisationnelles appropriées pour respecter les exigences du RGPD.



Co-Responsable

Personne morale qui, avec un autre responsable de traitement, détermine conjointement :

Les finalités et/ou **les moyens**

La responsabilité conjointe doit faire l'objet d'un **éclaircissement** (contrat, convention) qui détaille les responsabilités uniques et conjointes (matrice de co-responsabilité*).

* Ca c'est **TOI**, ca c'est **MOI**, ca c'est **NOUS**



Sous-traitant au sens RGPD

Personne morale qui traite les données **pour le compte** du Responsable de Traitement.

Le ST répond sur **instructions** du RT.

Le ST ne doit faire appel qu'à des **sous-traitants ultérieur** (sous réserve de l'accord du responsable de traitement) **qui présentent les garanties suffisantes**.

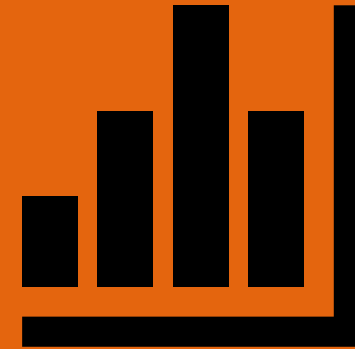


Clause, avenant ou annexe RGPD



Chaque traitement (au sens RGPD) doit avoir un RT identifié et identifiable.

II] LES PRINCIPES FONDAMENTAUX



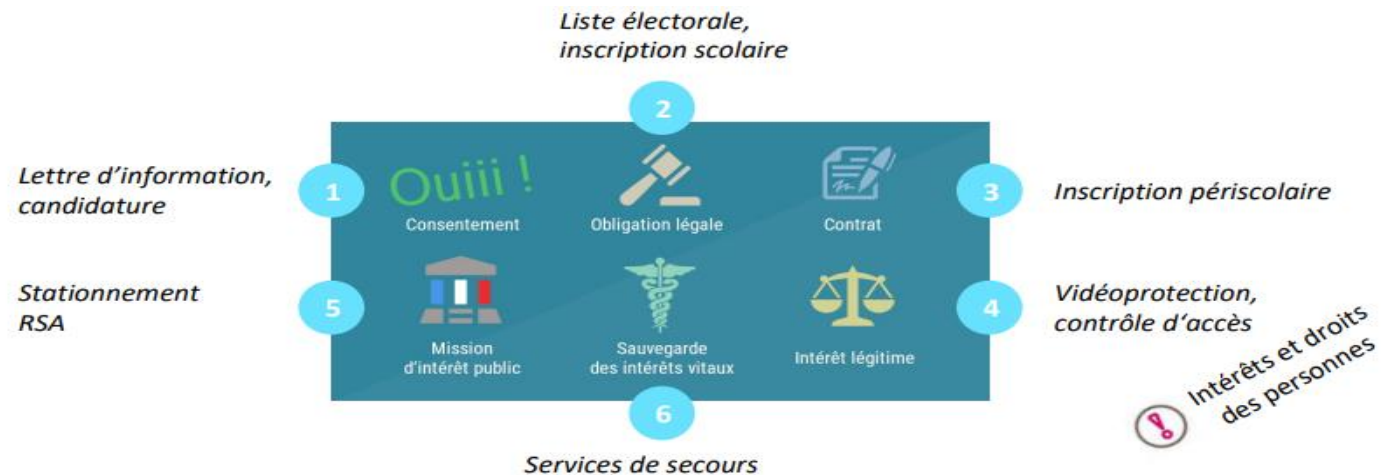
Les 8 règles d'or relatives aux traitements

Licéité et Transparence	Le RT doit identifier le fondement juridique (base juridique légale) du traitement et informer les personnes concernées de façon concise, précise, transparente, compréhensible et aisément accessible .
Finalité	La collecte des données et leurs traitements doivent répondre à un but déterminé, légitime et explicite et limité .
Minimisation et Pertinence	Les données collectées doivent être adéquates, pertinentes, limitées au regard de la finalité pour laquelle elles sont traitées. Les données erronées doivent être corrigées ou effacées rapidement.
Données Sensibles	Les données sensibles et hautement personnelles doivent faire l'objet d'une attention particulière .
Durée de conservation	La conservation des données ne doit pas excéder la durée nécessaire au regard de la finalité visée. Le RT doit fixer les durées et la personne concernée doit en avoir connaissance (cf. Focus RGPD sur les durées de conservation).
Sécurité et Confidentialité	Le RT doit garantir la sécurité et la confidentialité des données personnelles .
Droit des personnes	Le RT doit garantir les droits des personnes pour qu'elles gardent la maîtrise de leurs données.
Responsabilité	Le RT doit s'assurer d'être en mesure de démontrer que les principes précédents sont bien respectés (Registre de traitement et documentation).



On peut
détailler ?

Le fondement juridique



Tout traitement de DCP doit être justifié par l'un des 6 fondements juridiques autorisés :

1. La personne **a consenti** au traitement de ses données personnelles
2. Le traitement est nécessaire au respect d'une **obligation légale**
3. Le traitement est nécessaire à l'exécution d'un **contrat** ou d'un **précontrat**
4. Le traitement est nécessaire aux fins des **intérêts légitimes** poursuivis par le responsable de traitement
5. Le traitement se fait sous couvert d'une **mission d'intérêt public**
6. Le traitement est nécessaire pour la **sauvegarde des intérêts vitaux**

Le régime d'exception du consentement

« Toute manifestation de volonté, libre, spécifique, éclairé et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement »

La personne ne subit pas de préjudice si elle refuse ou retire son consentement (ni contrainte, ni influencée)

Le consentement est recueilli pour une finalité déterminée et de manière distincte (pas d'acceptation groupée)

La personne doit être préalablement pleinement informée sur le traitement avant de consentir

Le consentement doit être déduit d'un acte positif clair de la personne (et non d'une inaction)

Le consentement est donné sans ambiguïté (pas de case pré cochée, d'acceptation au travers de CGU)

Le régime d'exception du consentement

/ Nous pouvons classer le consentement en 5 familles :

- Le consentement lié aux **cookies et traceurs** sur les sites Web (recommandation CNIL) ,
- Le consentement lié à la collecte de **données de santé** (spécifique et très sensible) ,
- Le consentement lié à la **prospection commerciale** (directive CNIL) ,
- Le consentement des **mineurs de moins de 15 ans** (consentement conjoint mineur + autorité parentale)
- Le consentement lié à une **finalité spécifique** (un consentement par finalité spécifique).

/ Il faut s'assurer de la bonne gestion du consentement (recueil, conservation, retrait)

- Assurer le **recueil** du consentement ,
- Assurer sa bonne conservation sur le temps défini du traitement (**traçabilité**) ,
- Assurer la prise en compte de son **retrait** par la personne concernée ou lorsque les finalités sont atteintes.

La CNIL suggère la tenue d'un registre des consentements qui documente les conditions de recueil du consentement.

Le régime de consentement est le plus compliqué à gérer (gestion de la preuve), il faut vérifier si une autre base légale ne répond pas au besoin quitte à légèrement ré orienter sa finalité.



La suppression des DCP : un enjeu crucial

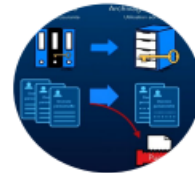
Les bonnes questions à se poser :

- / Jusqu'à quand ai-je vraiment besoin des DCP pour atteindre l'objectif fixé ?
- / Ai-je des obligations légales de conserver les DCP pendant un certain temps ?
- / Dois-je conserver certaines DCP en vue de me protéger contre un éventuel contentieux ? Lesquelles ?
- / Jusqu'à quand puis-je faire valoir ce recours en justice ?
- / Quelles DCP doivent être archivées ? Pendant combien de temps ? Selon quelles règles ?
- / Quelles sont les règles de suppression des DCP pour garantir le respect des durées de conservation fixées ?

La conservation doit être limitée dans le temps

Quand la finalité est atteinte...

... il n'y a plus lieu de conserver les DCP



Suppression* des DCP

*Suppression = Effacement numérique et destruction papier



Conserver des DCP sans délais ou au-delà des durées fixées est une infraction au RGPD.

**Sauf si obligation légale ou code du patrimoine
=> placement en archivage intermédiaire**

**Sauf si obligation du code du patrimoine
=> Placement en archivage définitif**

Exemple : dossier RH



Candidature, Entretiens, contrat, avenant, ...
Paie, heures supplémentaires, primes, notes de frais, congés, absence, ...
Temps de travail, médecine du travail, formation, évaluations, retraite, fin de contrat, ...

A finalités différentes = durées de conservation probablement différentes.

Exemple :  2 ans
5 ans
10 ans



Une mauvaise pratique serait d'absolument tout conserver sur l'agent pendant la durée la plus longue (ici 10 ans) ce qui serait jugé excessif.



Pour en savoir plus, vous dispos(er)ez d'un Focus RGPD sur les durées de conservation => Support pdf et tutovidéo dans DLD [ESPACE CDGx].

Les mentions d'information

Concises, transparentes, compréhensibles et aisément accessibles par les personnes concernées.



Support de collecte de DCP (collecte principal ou complémentaire) :

On collecte des DCP auprès de la personne (dossier de candidature, fiche RH, inscription scolaire)

- ▮ La mention d'information doit être adaptée et complète
- ▮ Les traitements facultatifs (non indispensables) doivent faire l'objet d'un consentement spécifique



Support d'autorisation de traitement :

Pour de nouvelles finalités basées sur les DCP déjà obtenues (droit à l'image)

- ▮ La mention d'information peut se concentrer sur le traitement (RT, finalité, fondement, destinataire, durée) et renvoyer vers un document d'information (deux niveaux)



Support de procédure contenant des DCP (visible ou non par la personne) :

Nécessaire pour réaliser le traitement légitime (planning, facture, ordre de service).

- ▮ Pas de mention



Support de droit à l'information :

CGV , règlement, site web

- ▮ Mention axée sur les droits, la procédure d'exercice de droit et la réclamation

La contractualisation des ST



Clause / Annexe / Avenant RGPD

Le **contrat** lie le RT au ST et doit préciser les responsabilités et les attendus respectifs concernant le RGPD notamment :

- la nature et la finalité du traitement,
- Les coordonnées du DPO,
- le type de DCP concernée,
- les catégories de personnes concernées,
- l'obtention de l'accord préalable du RT pour sous-traiter,
- le respect de la confidentialité,
- les mesures adaptées à la sécurité du traitement,
- la procédure lors d'un exercice de droit,
- la procédure de notification de violation de données.
- Les durées de conservation et le sort des données en fin de contrat

Les droits des personnes

	Droit à l'information	Disposer d'une information claire sur l'utilisation de ses données et sur ses droits
	Droit d'accès	Pouvoir obtenir et vérifier les données détenues par un organisme
	Droit à la rectification	Pouvoir faire rectifier des données inexactes ou incomplètes
	Droit d'effacement	Obtenir l'effacement des données (sous certaines conditions) et le droit à l'oubli (droit au déréférencement)
	Droit à l'opposition	Pouvoir s'opposer (pour motif légitime), à l'utilisation de ses données et pouvoir retirer un consentement
	Droit à la limitation	Pouvoir, sous certaines conditions , obtenir le gel de l'utilisation de ses données
	Droit à la portabilité	Disposer d'une copie des données liées à un contrat ou à un consentement dans un format aisément réutilisable par un tiers

Les droits des personnes

	Droit lié au profilage	Droit de ne pas faire l'objet d'une décision automatisée* (demande d'intervention humaine).
	Droit à la réclamation	Pouvoir déposer une réclamation (sous certaines conditions) en ligne auprès de la CNIL.
	Droit à réparation	Pouvoir obtenir réparation du préjudice subi, en cas de dommage matériel ou moral ou de violation de droit.

** Visant à évaluer certains aspects personnels (productivité au travail, état de santé, candidature, etc).*

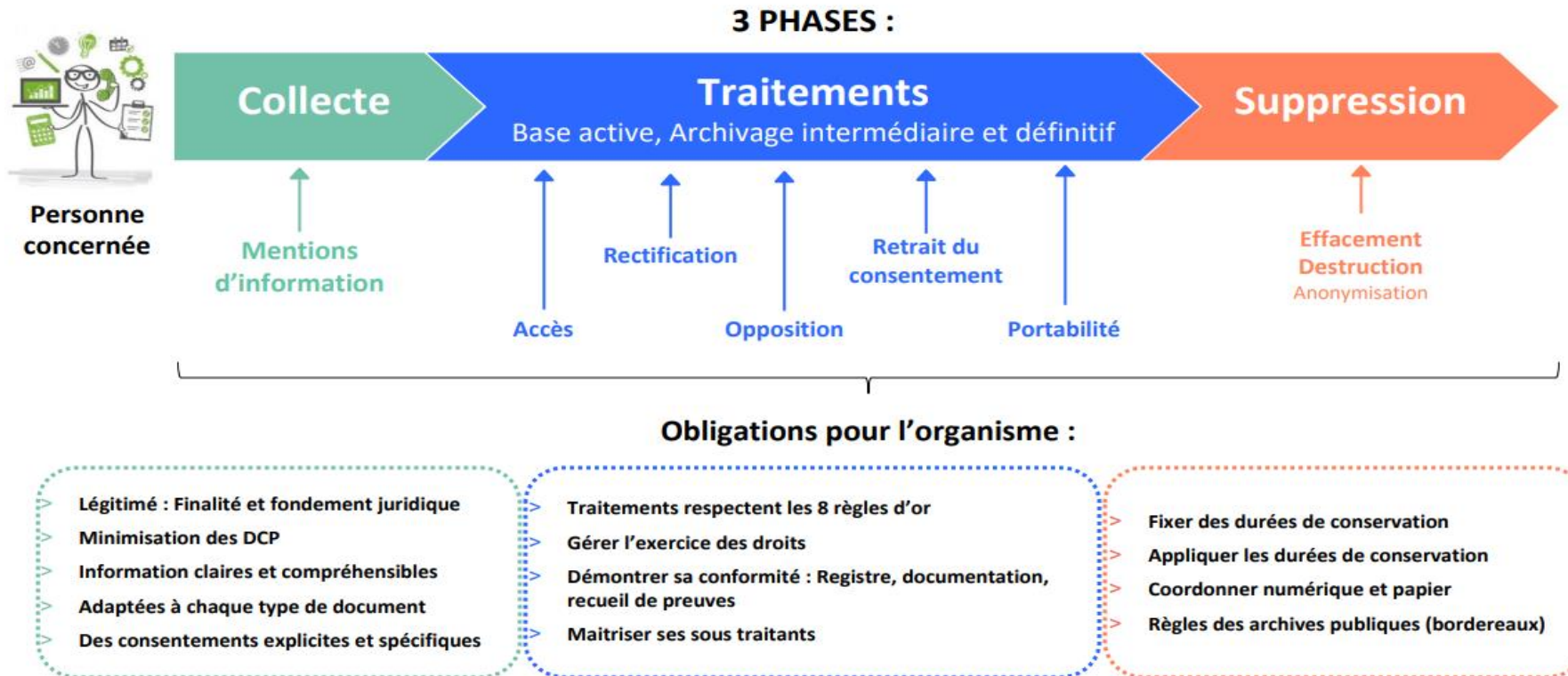
Exercice de droit :

Demande faite par un requérant (agent, ex agent, administré, ex administré, etc.) auprès du Référent RGPD interne et/ou du DPO externe.

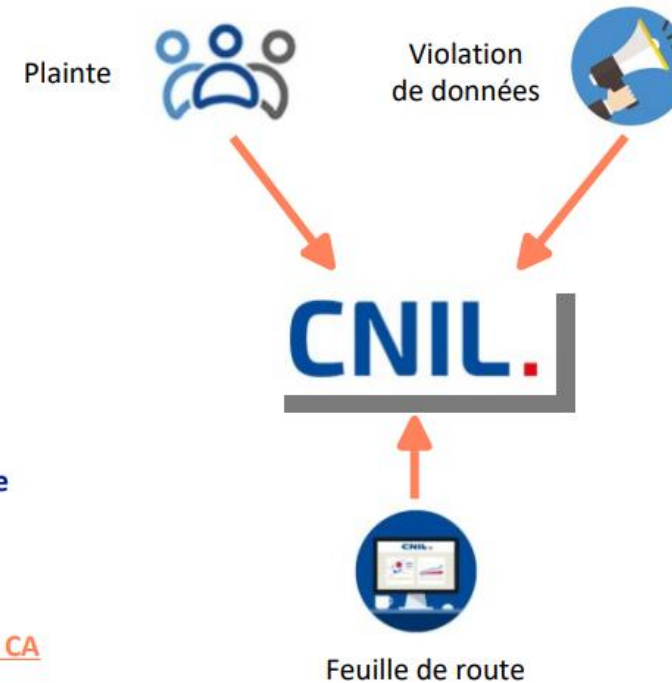
L'exercice déclenche une procédure formelle dont les étapes sont traçables dans le logiciel DLD.

=> Fera l'objet d'un Focus RGPD spécifique.

Résumons sous forme de cycle de vie de la DCP

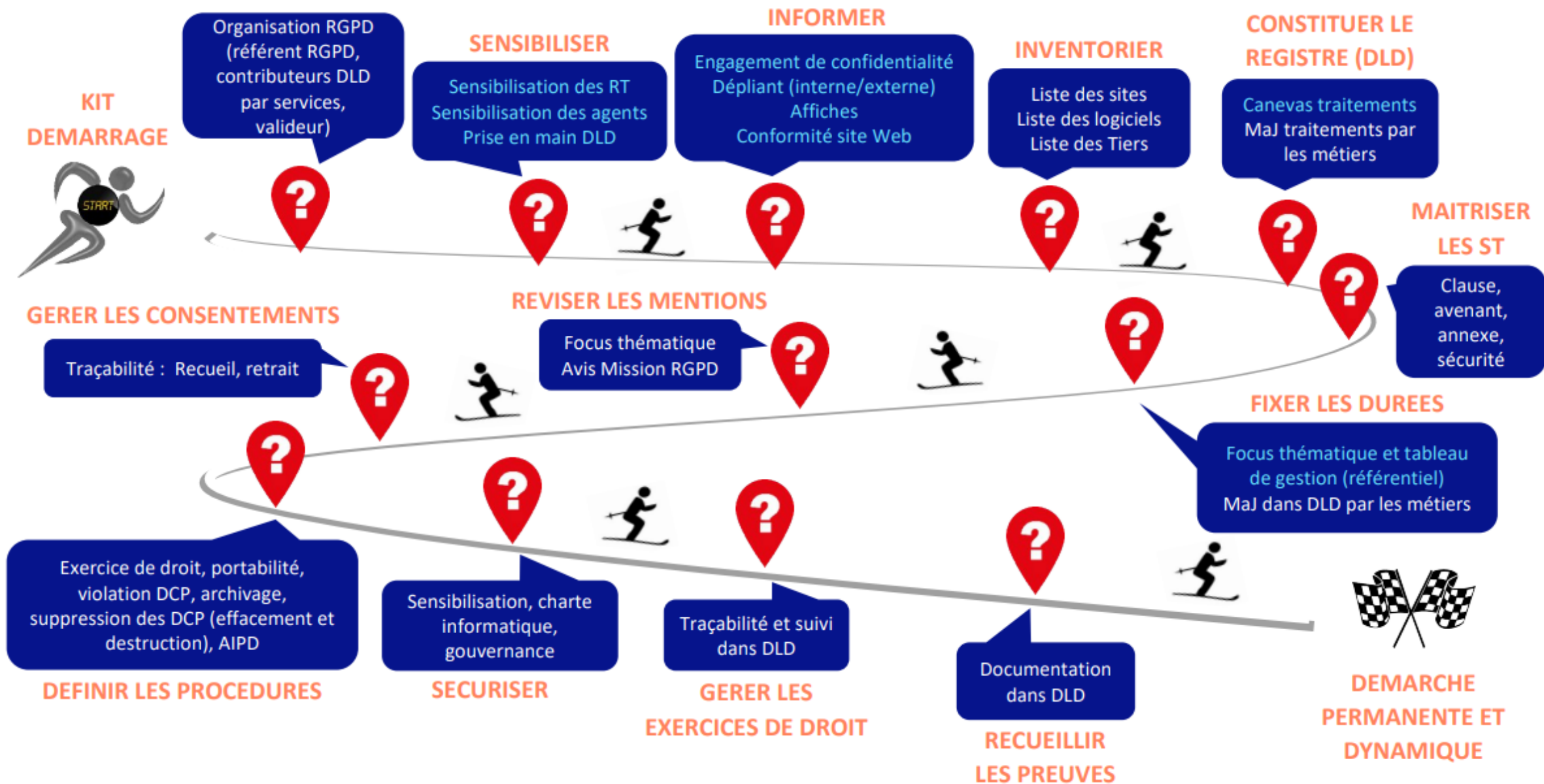


Les risques et les sanctions



III] LE CHEMIN VERS LA CONFORMITE

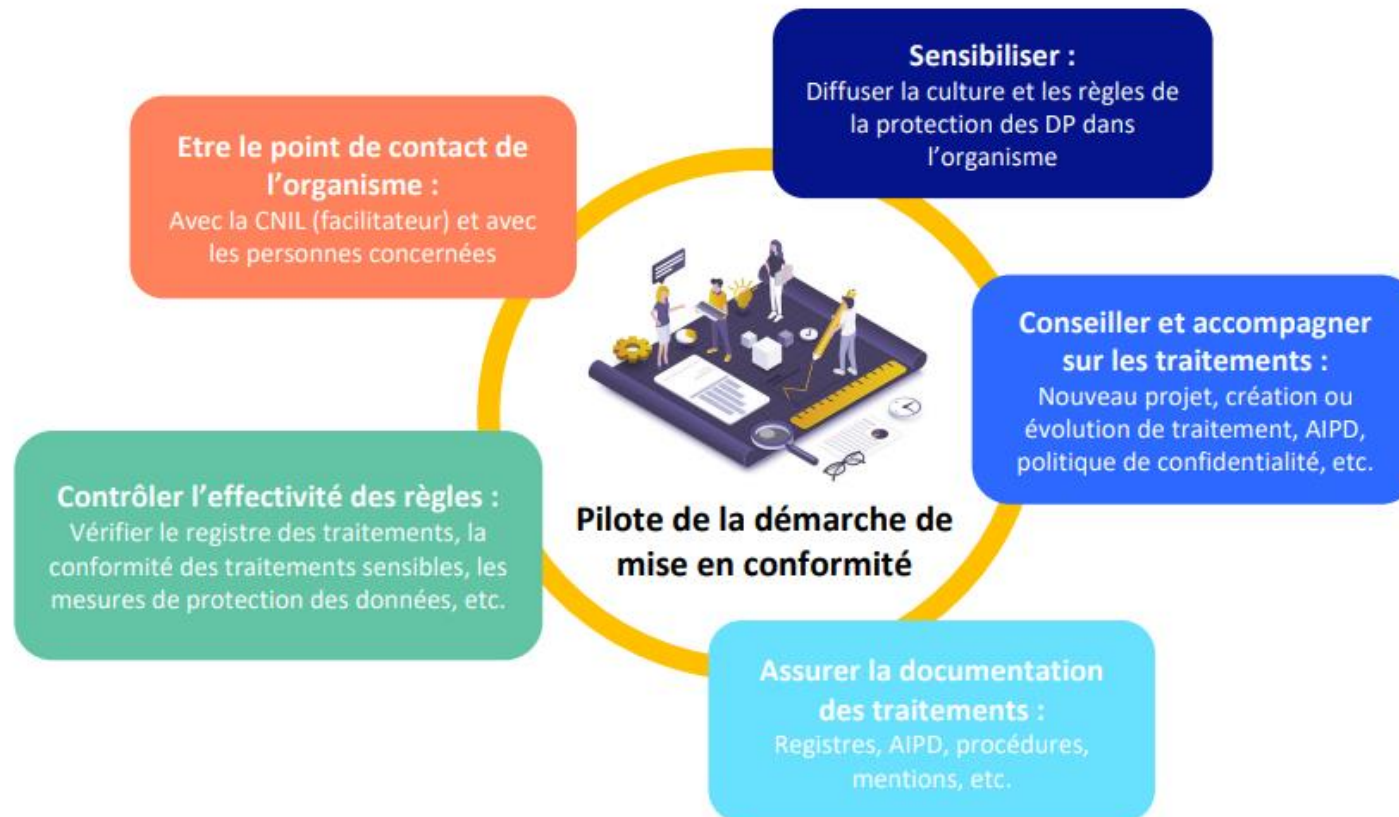




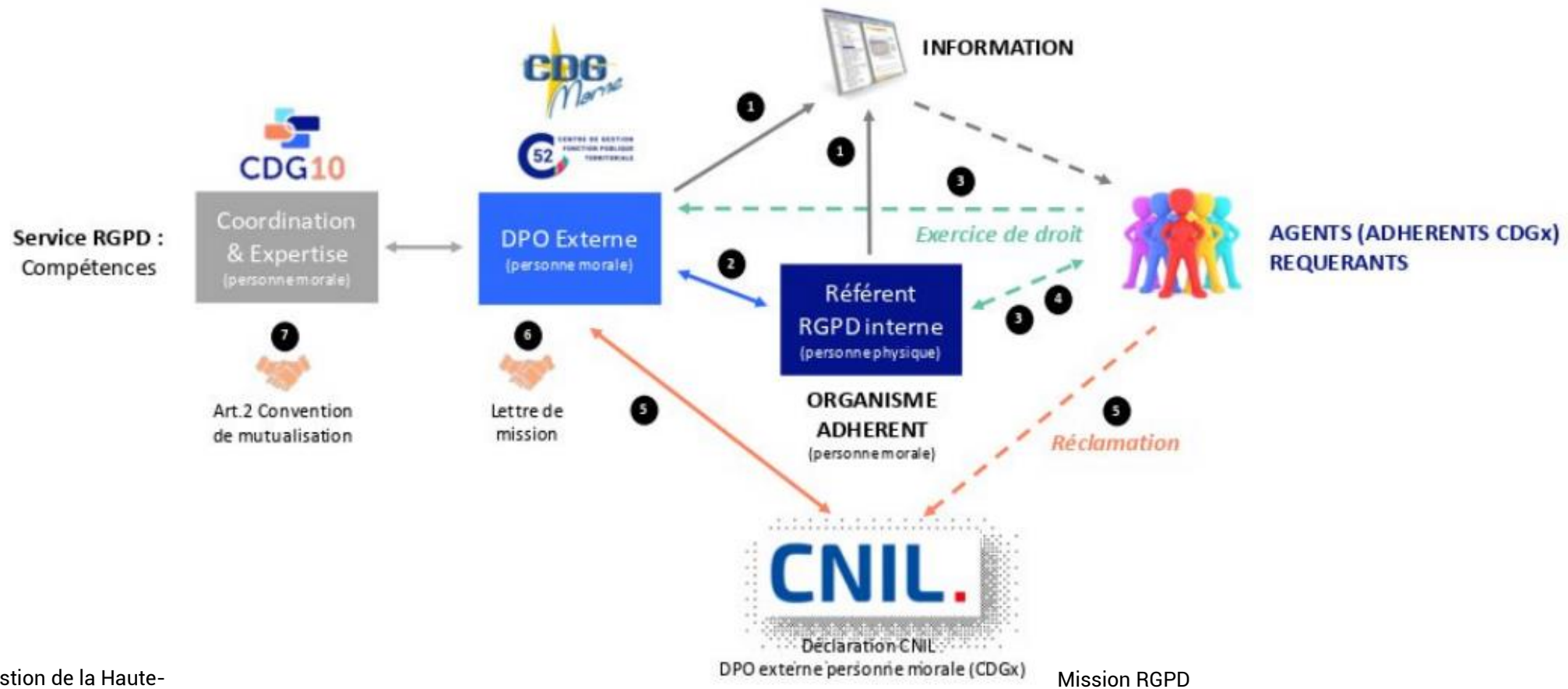
IV] Mission RGPD



Rôle du DPD ou DPO



Référent DPD interne et DPD (DPO) externe



Les services de « Mission RGPD »



Les outils de « Mission RGPD »»»

RGPD ▾ ESPACE CDG52 ▾ Rechercher

RGPD / Accountability

ACCOUNTABILITY

Rechercher un document

Documents juridiques

Doc. techniques & organisationnels

Sensibilisations initiales au RGPD 2

Initiation à Data Legal Drive 2

Sensibilisations initiales au RGPD

MODIFIER SUPPRIMER

Sensibilisation_RGPD_initiale_1.pdf

Sensibilisation_RGPD_initiale_2.pdf

Des livraisons => Information par courriel

MERCI



Léa KOSSURA,
archiviste itinérante et
référente RGPD



dpo@cdg52.fr



03.25.35.33.20