



**PLATEFORME
DES DONNÉES
DE SANTÉ**
FRENCH HEALTH DATA HUB

**Plateforme des
données de santé**

**Présentation de la
checklist EDS**

Ordre du jour

1. Présentation du référentiel de la CNIL relatif aux entrepôts de données de santé et de la checklist associée
2. Montage et dépôt d'un dossier de demande d'autorisation d'entrepôt de données de santé auprès de la CNIL

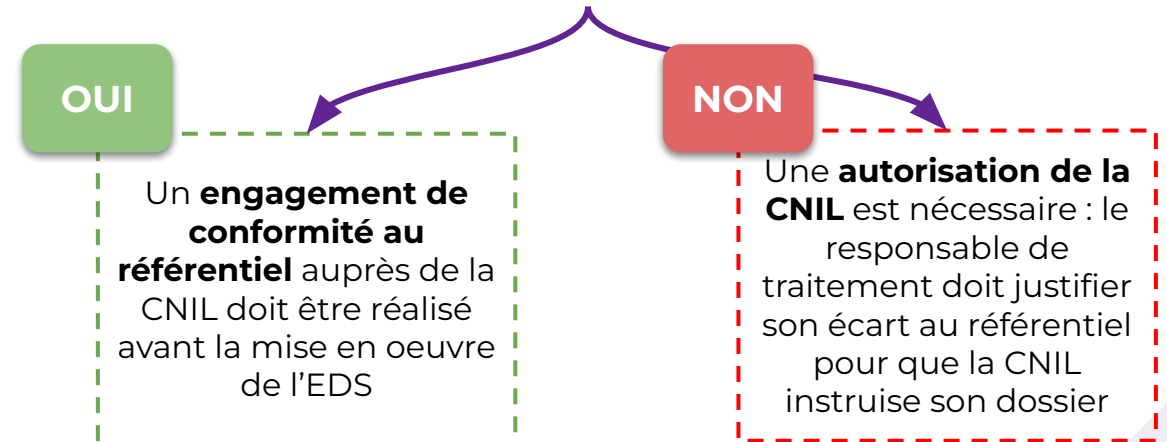
Objectif du référentiel relatif aux EDS

Le référentiel relatif aux entrepôts de données de santé (EDS) élaboré par la CNIL en concertation avec la PDS et les **organismes publics et privés représentatifs** des acteurs concernés est paru au Journal Officiel en **octobre 2021**

Le référentiel EDS un texte qui permet aux responsables de traitement dont le traitement est conforme aux exigences qu'il pose de **créer un EDS en adressant simplement un engagement de conformité au référentiel** à la CNIL sur son site internet.

Il n'est donc **pas nécessaire de demander une autorisation à la CNIL**.

L'EDS envisagé est-il conforme au référentiel EDS ?



Attention, si le responsable de traitement, c'est-à-dire de la personne, l'autorité publique ou l'organisme qui détermine les finalités, les objectifs et les moyens de l'EDS, **réalise un engagement de conformité au référentiel EDS sans en respecter les exigences**, il peut **engager sa responsabilité juridique**.
Il est donc important de **bien cadrer le projet pour ne pas se tromper !**

Présentation du référentiel de la CNIL relatif aux entrepôts de données de santé et de la checklist associée



Thématiques structurant le référentiel EDS

La **référentiel liste un certain nombre d'exigences** qui correspondent aux thématiques suivantes :

- | | |
|---|---|
| 1. Finalités de l'EDS <i>Zoom</i> | 7. Information des personnes <i>Zoom</i> |
| 2. Base juridique <i>Zoom</i> | 8. Droits des personnes |
| 3. Gouvernance <i>Zoom</i> | 9. Sécurité <i>Zoom</i> |
| 4. Données personnelles pouvant être versées dans l'EDS <i>Zoom</i> | 10. Sous-traitants |
| 5. Accès aux informations | 11. Transfert de données hors de l'Union européenne |
| 6. Durées de conservation | 12. Analyse d'impact sur la protection des données |

Zoom sur les finalités de l'EDS

L'EDS doit être constitué afin de **permettre la réutilisation des données qu'il contient** pour les finalités suivantes :

1. La **réalisation de recherche, d'étude ou d'évaluation** dans le domaine de la santé ;

La **finalité choisie conditionne les traitements que vous pourrez mettre en oeuvre** :

Ce traitement pourra être mis en œuvre **par tout responsable de traitement** ayant suivi les formalités applicables aux recherches (*MR ou autorisation CNIL*).

1. La **production d'indicateurs et le pilotage stratégique de l'activité**, sous la responsabilité du médecin responsable de l'information médicale ;
2. L'**amélioration de la qualité de l'information médicale ou l'optimisation du codage** dans le cadre du programme de médicalisation des systèmes d'information (PMSI) ;
3. Le **fonctionnement d'outils d'aide au diagnostic médical ou à la prise en charge** ;
4. La **réalisation d'études de faisabilité** (pré-screening).

Ces traitements pourront être mis en œuvre **uniquement par les personnels habilités du responsable de traitement de l'EDS** et pour son usage exclusif.

Zoom sur la base juridique

Tout acteur ne peut pas être éligible au référentiel EDS. Ce dernier **restreint son champ d'application selon la base légale mobilisée par le responsable de traitement**, c'est-à-dire le fondement juridique qui autorise légalement la mise en œuvre de l'EDS :

La mission d'intérêt public

La création de l'EDS est nécessaire à l'exécution d'une mission d'intérêt public dont est investi le responsable de traitement



Consentement

La création de l'EDS est fondée sur le consentement des personnes concernées



L'intérêt légitime

La création de l'EDS est nécessaire à la poursuite des intérêts légitimes du responsable de traitement



Sont donc surtout concernés par le référentiel les acteurs publics (établissements de santé, fédérations hospitalières, instituts de recherche etc). Un EDS mis en œuvre sur la base du consentement des personnes concernées ou mis en œuvre par une société privée sur le fondement de son intérêt légitime sont exclus du référentiel (le premier peut être créé sans autorisation de la CNIL).

Zoom sur les données pouvant être versées

Pour être versées dans l'EDS, les données doivent (1) figurer dans le dossier médical du patient ou être issues de projets de recherche et (2) appartenir aux catégories suivantes :

Données directement identifiantes et administratives relatives aux patients

(conservées dans un espace distinct des autres données)

Ex : nom, prénoms, sexe, jour, mois, date, lieu de naissance, coordonnées, IEP, IPP, NIR

Autres données relatives aux patients dont les données sensibles

Ex : poids, taille, comptes rendus, résultats d'examens, données médico-administratives issues du PMSI local, antécédents, données génétiques, vie sexuelle, origine ethnique, niveau de formation, consommation de tabac, alcool, drogues, mode de vie, statut vital et cause du décès, échelle de qualité de vie, photographie, vidéo

Données relatives aux professionnels de santé

Ex : nom, prénom, titre, fonction, service et unité d'exercice, coordonnées professionnelles, numéro ADELI ou RPP

L'EDS ne peut pas contenir de données appariées **avec des données de la base principale du SNDS** dans le cadre du référentiel.

Zoom sur la gouvernance

Le référentiel impose la **création de deux instances de gouvernance** autour de l'EDS :

Détermine les orientations stratégiques et scientifiques de l'EDS : il tient une liste exhaustive des données de l'EDS et justifie de leur nécessité.



Comité
de
pilotage
ou équivalent

Comité
scientifique et
éthique ou
équivalent

Rend, de manière systématique, un avis préalable et motivé sur les propositions de projets nécessitant la réutilisation des données de l'EDS.

Zoom sur l'information des personnes

Le référentiel impose que les personnes concernées par les données de l'EDS **soient informées du versement des données dans l'EDS**. L'information doit être individuelle mais il peut y être dérogé dans deux situations :

- pour les patients dont les données de leurs dossiers médicaux ont été collectées antérieurement à la constitution de l'EDS et qui ne sont plus suivis ;
- pour les patients dont les données ont été collectées dans le cadre de recherches antérieures.

Les **arguments justifiant la dérogation doivent être documentés** dans l'analyse de risque relative à la protection des données (AIPD) ainsi que les **mesures compensatoires mises en œuvre**.

- Ex. la publication de la note d'information sur le site web du RT, une communication sur les réseaux sociaux, auprès d'associations de patients, la diffusion d'un communiqué de presse, etc.

Zoom sur la sécurité

Pour être conforme au référentiel, l'entrepôt doit **respecter des mesures techniques et organisationnelles de sécurité**. Ces mesures sont regroupées en 13 thématiques :

1. Cloisonnement réseau
2. Cloisonnement logique et cryptographique
3. Constitution et alimentation de l'entrepôt
4. Pseudonymisation des données
5. Accès physique aux données
6. Gestion des habilitations et accès logique aux données
7. Authentification pour la consultation et l'administration de l'entrepôt
8. Espace de travail
9. Exportation de données hors de l'entrepôt et hors des espaces de travail
10. Sensibilisation des utilisateurs et sécurité des postes de travail
11. Journalisation
12. Procédures de ré-identification
13. Gestion des incidents de sécurité et des violations de données personnelles

Les mesures de sécurité listées par le référentiel **sont exigeantes**. Il est important d'y travailler au plus tôt **en associant le RSSI de votre organisation**.

Checklist de la CNIL : évaluer la conformité d'un projet d'EDS au référentiel

Cette [checklist](#) permet à tout responsable de traitement souhaitant constituer un EDS **de vérifier facilement sa conformité** au référentiel EDS de la CNIL.

La checklist **reprend l'ensemble des exigences du référentiel** sous forme d'affirmations auxquelles le responsable de traitement répond par vrai/faux, le cas échéant « non applicable ». C'est pourquoi il est nécessaire de connaître **l'ensemble des caractéristiques** de son projet d'EDS (finalités, données traitées, information des personnes, sécurité etc) avant de se lancer dans la complétion de la checklist.

Suis-je conforme au référentiel EDS ?

Je réponds "Vrai" ou "Non applicable" pour chaque affirmation de la checklist

OUI

J'ai répondu par "Faux" à au moins une affirmation de la checklist

NON

Attention, si votre projet d'EDS est conforme au référentiel, il est important de bien documenter cette conformité en interne, pour le prouver en cas de contrôle de la CNIL.

Checklist de la CNIL : que faire en cas de non conformité ?

J'ai répondu par "Faux" à au moins une affirmation de la checklist

NON

Je demande une autorisation à la CNIL



Comment ?

Le référentiel est un outil pédagogique qui pose un cadre de bonnes pratiques auxquelles le RT doit se référer. La checklist peut ainsi être utilisée comme un **outil que le RT peut intégrer dans son dossier de demande d'autorisation**. La colonne « Raison de la non conformité » permet à la CNIL d'identifier plus facilement les points sur lesquels elle doit cibler son instruction.

La CNIL s'attend à ce que la non conformité soit bien justifiée et que des mesures compensatoires soient prévues !

Point du référentiel	Critères	Réponse	Raison de la non-conformité
1. À qui s'adresse ce référentiel			
1.3	L'entrepôt envisagé entre dans le champ d'application du référentiel (voir les quatre situations dans lesquelles le référentiel ne s'applique pas en page précédente).	<input type="checkbox"/> Vrai <input type="checkbox"/> Faux Si « faux » : non-conformité au référentiel	
3.1. Finalités			
3.1.1	L'entrepôt est mis en œuvre afin de permettre la réutilisation des données qu'il contient (recherche, évaluations, calcul d'indicateurs, etc.).	<input type="checkbox"/> Vrai <input type="checkbox"/> Faux	
3.1.2	Toute utilisation uniquement des données de l'entrepôt par le responsable de traitement et pour son usage exclusif, l'est à des fins de : <ul style="list-style-type: none">production d'indicateurs et le pilotage stratégique de l'activité, sous la responsabilité du médecin responsable de l'information médicale ;amélioration de la qualité de l'information médicale ou l'optimisation du codage dans le cadre du programme de médicalisation des systèmes d'information (PMSI) ;fonctionnement d'outils d'aide au diagnostic médical ou à la prise en charge ;réalisation d'études de faisabilité (pré-screening) ;réalisation de recherches, études et évaluations dans le domaine de la santé.	<input type="checkbox"/> Vrai <input type="checkbox"/> Faux	
3.1.4	En dehors des utilisations mentionnées ci-dessus, le responsable de traitement doit s'interroger sur la nécessité ou non de réaliser des formalités spécifiques auprès de la CNIL pour toute réutilisation des données. Les données ne sont et ne seront pas exploitées : <ul style="list-style-type: none">à des fins de promotion des produits mentionnés au II de l'article L. 5311-1 CSP en direction de professionnels de santé ou d'établissements de santé ;à des fins d'exclusion de garanties des contrats d'assurance, ni de modification de cotisations ou de primes d'assurance d'un individu ou d'un groupe d'individus présentant un même risque	<input type="checkbox"/> Vrai <input type="checkbox"/> Faux	

CNIL

3

Montage et dépôt d'un dossier de demande d'autorisation auprès de la CNIL en cas de non conformité au référentiel EDS



Dans quels cas déposer une demande d'autorisation ?

Pour la mise en oeuvre de l'EDS

Une demande d'autorisation auprès de la CNIL doit être déposée dans le cas où un **écart au référentiel EDS est constaté** pour le projet d'EDS.

C'est pourquoi il est important de **mener l'analyse de la conformité au plus tôt** pour anticiper le délai d'obtention de l'autorisation de la CNIL : il varie de **2 à 4 mois** et il faut compter le délai pour constituer le dossier **(au moins 2 mois) !**

Pour l'utilisation des données de l'EDS

Une demande d'autorisation CNIL sera nécessaire dans deux autres cas :

- Pour les projets qui réutiliseront les **données contenues dans l'EDS** (sauf conformité à une méthodologie de référence) ;
- Plus largement, pour les projets qui réutiliseront les **données de la base mise au catalogue**.

La **mise au catalogue n'implique pas de réaliser une demande d'autorisation** auprès de la CNIL car elle est encadrée par un arrêté pris après avis de la CNIL. Néanmoins, il est **important de l'anticiper**, notamment en informant les personnes sur ce point dans le cadre de la mise en œuvre de l'EDS.

Quelles pièces pour mon dossier ?



Mon dossier doit comprendre

- ❖ Un argumentaire (équivalent d'un protocole scientifique pour un projet de recherche) ;
- ❖ Des annexes à l'argumentaire:
 - Calendrier de mise en oeuvre de l'EDS ;
 - Convention de coresponsabilité le cas échéant ;
 - Expression de besoin en données SNDS le cas échéant ;
 - Liste des financeurs de l'EDS ;
 - Note d'information aux personnes concernées ;
- ❖ Une AIPD ;
- ❖ La checklist de la CNIL.

Le dépôt de mon dossier s'effectue sur une plateforme en ligne, via la complétion du [formulaire de demande d'autorisation CNIL](#). L'ensemble de la procédure est dématérialisée. Mon dossier ne sera instruit que s'il est complet.

Zoom sur l'argumentaire

Partie	Contenu
1. Rôles et responsabilités	1.1 Parties prenantes 1.2 Sous-traitants 1.3 Destinataires ou catégories de destinataires 1.4 Gouvernance
2. Objectifs et finalités	2.1 Contexte, objectifs et justification de l'EDS 2.2 Base légale et justification de l'intérêt public
3. Données traitées	3.1 Sources de données 3.2 Population(s) concernée(s) 3.3 Catégories de données et variables
4. Cycle de vie de la donnée	4.1 Schéma de circulation de la donnée 4.2 Traitement des données 4.3 Circuit de pseudonymisation 4.4 Modalités techniques de transfert 4.4.1 Transfert et appariement des données 4.4.2 Modalités d'accès aux données 4.4.3 Conservation des tables de correspondance
5. Protection de la vie privée, sécurité et confidentialité des données	5.1 Respect des droits des personnes concernées 5.1.1 Information des personnes concernées 5.1.2 Modalités d'exercice des droits 5.2 Confidentialité et sécurité des données 5.2.1 Mesures techniques et organisationnelles de sécurité 5.2.2 Conservation des données 5.2.3 Modalités et garanties de transferts hors Union Européenne

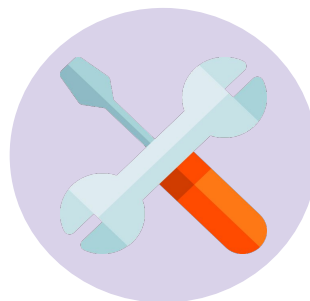
Zoom sur l'analyse d'impact relative à la protection des données (AIPD)

L'AIPD est un outil important pour la **responsabilisation des organismes** : elle les aide à construire des traitements de données respectueux de la vie privée, et à démontrer leur conformité au RGPD.

Elle concerne tous les traitements de données qui sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes (art. 35 du RGPD) tels que les **traitements de données sensibles**.



Terme retenu dans le RGPD.
AIPD est synonyme de PIA
(Privacy Impact Assessment)



Permet de construire un traitement conforme au RGPD et respectueux de la vie privée



4 parties :

- Le contexte ;
- La conformité juridique aux principes de protection des données ;
- L'évaluation des risques (de sécurité) .
- Validation.

Contenu de l'AIPD

Le porteur de projet en lien avec le RSSI et le DPD doivent intégrer dans leur AIPD :

❖ Description du contexte

- Vue d'ensemble (*traitement, responsabilités, référentiels applicables*) ;
- Données, processus et supports (*données traitées, cycle de vie des données, supports des données*).

❖ Respect des principes fondamentaux

- Proportionnalité et nécessité du traitement (*base légale, respect des principes de minimisation, de proportionnalité et d'exactitude, durée de conservation*) ;
- Mesures protectrices des droits (*information des personnes, consentement (si applicable), modalités d'exercice des droits*).

❖ Etude des risques liés à la sécurité des données

- Mesures existantes ou prévues (*mesures organisationnelles, mesures sur les données, mesures générales de sécurité du système*) ;
- Accès illégitime à des données, modifications non désirées de données et disparition de données (*impacts et menaces potentiels sur les personnes, sources, mesures pour traiter le risque, gravité et vraisemblance du risque*).

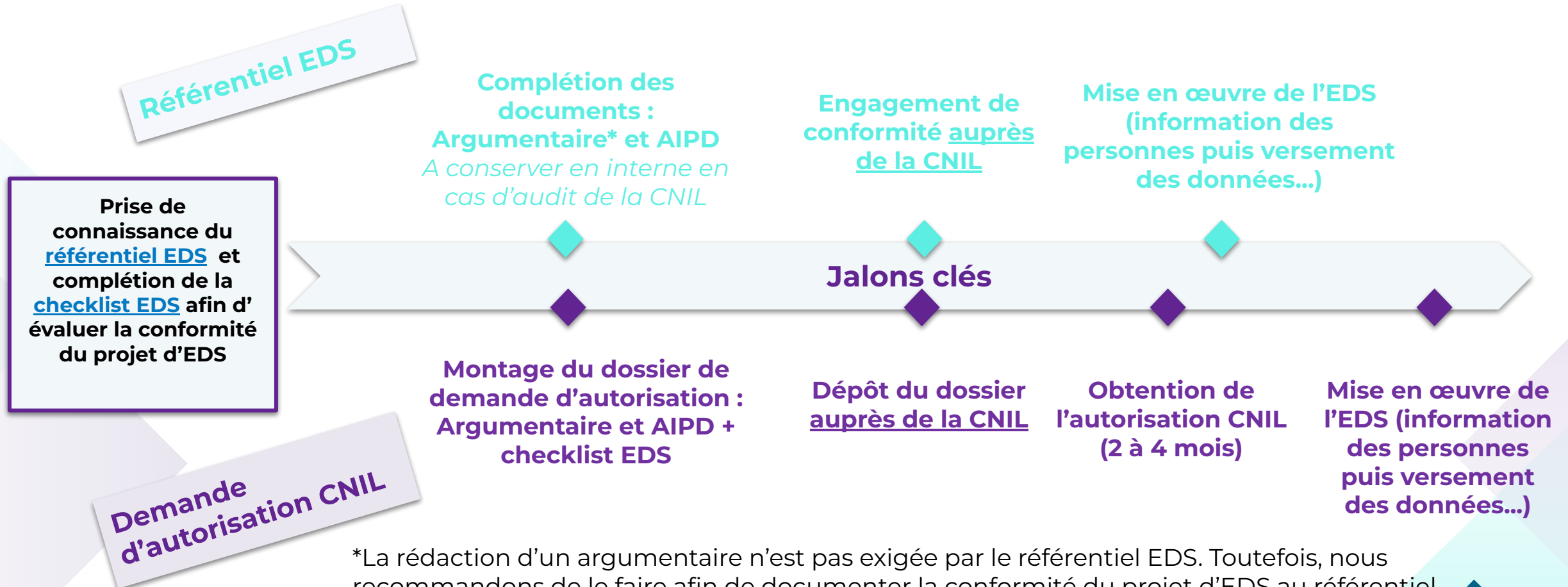
❖ Validation

- Cartographie des risques (*avant et après application du plan d'action*) ;
- Plan d'action ;
- Avis et signature du DPD.



Pour aider le porteur de projet, la PDS met à disposition un template d'AIPD avec des paragraphes types.

Différences entre demande d'autorisation et conformité au référentiel EDS





Suivez-nous sur les réseaux sociaux !

