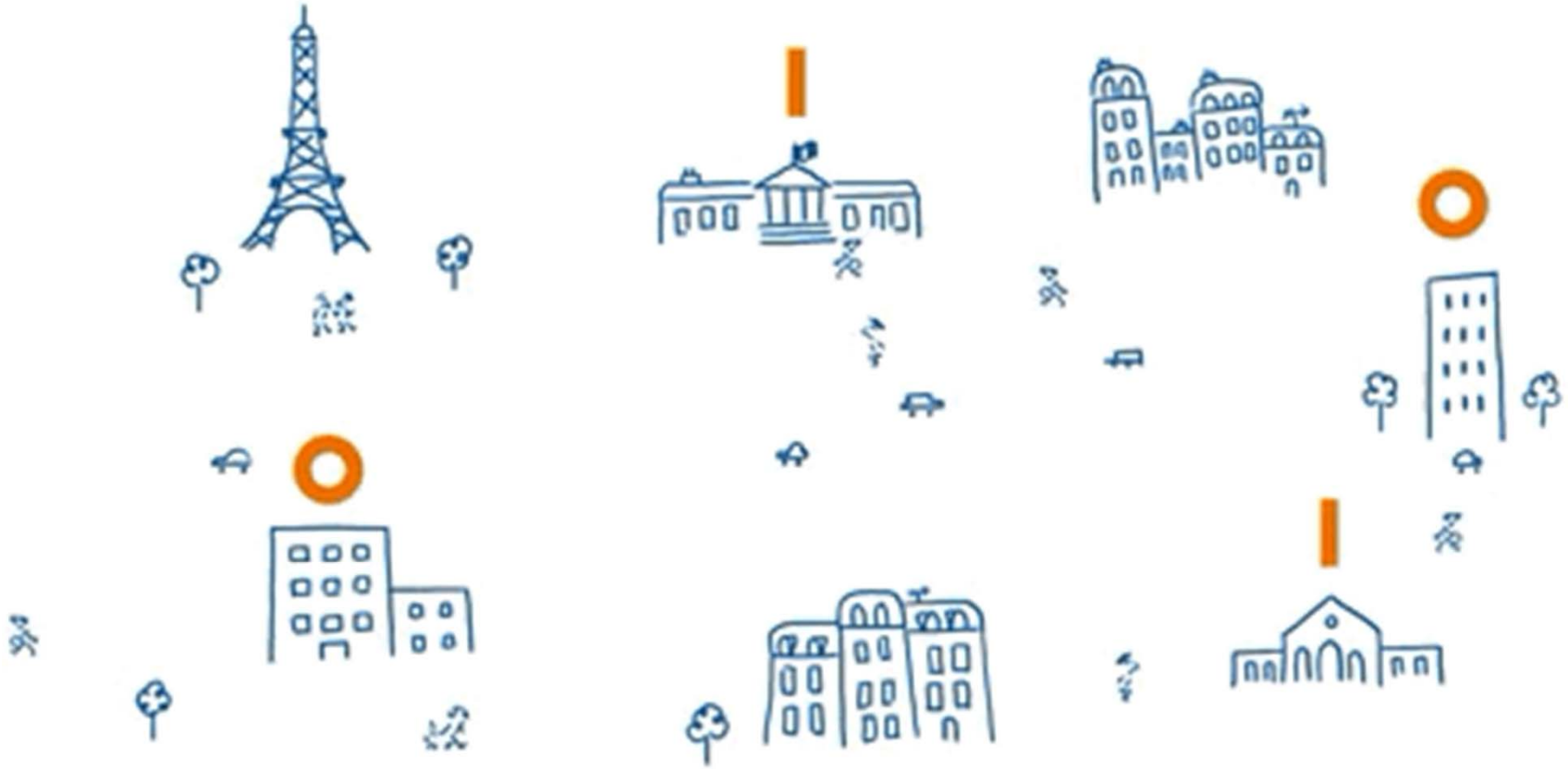


PROTECTION DES DONNÉES PERSONNELLES DES USAGERS ET DES AGENTS DES COLLECTIVITÉS TERRITORIALES : VERS UNE MUTUALISATION DÉPARTEMENTALE ?


« Responsable de traitement » ?

2018 : « L'ANNÉE DES DONNÉES PERSONNELLES » ?

- **La loi « Informatique et Libertés »** (6 janvier 1978)

- **« Règlement Général pour la Protection des Données personnelles »** (en abrégé « RGPD ») du 27 avril 2016, **applicable au plus tard le 25 mai 2018** avec principalement trois objectifs :
  1. **Uniformiser** le droit européen,
  2. **Mieux protéger** les citoyens/usagers/clients/salariés,
  3. **Responsabiliser** ceux qui traitent les données (auto-contrôle), où qu'ils soient.

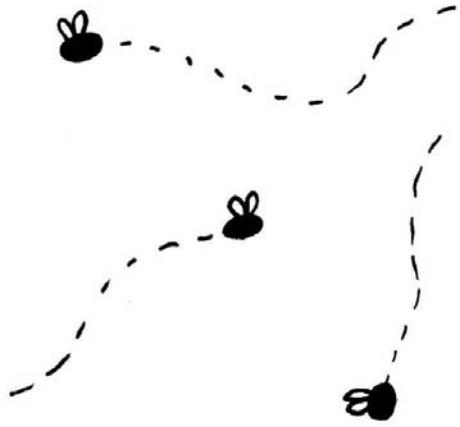
CE QUI NE CHANGE PAS (OU PEU)

- Cinq grands principes réaffirmés :
  - **Finalité/légitimité** (= pourquoi collecter/traiter ?)
  - **Pertinence et proportionnalité** (= le strict nécessaire)
  - **Durée de conservation limitée** (= tant que je peux en justifier le besoin)
  - **Sécurité, confidentialité** (= protéger les données de tout accès/divulgation)
  - **Respect des droits des personnes** (= information préalable, accès, rectification, etc.) → **obligations renforcées (cf. notamment la portabilité, le « consentement » explicite…)**
- Et aussi… **des sanctions (potentiellement financières) alourdies**

CE QUI S'EST PRATIQUÉ « AVANT » *(ET ENCORE MAINTENANT ?)*

aze

- Rappel de (mauvaises) pratiques *qui ont pu exister* :
  1. Je fais l'acquisition d'un nouveau logiciel,
  2. Je le déclare à la CNIL (avec éventuellement l'aide de mon fournisseur),
  3. Je suis tranquille pour « x » années…



CE QUI CHANGE RADICALEMENT « APRÈS » (LE 25 MAI 2018)

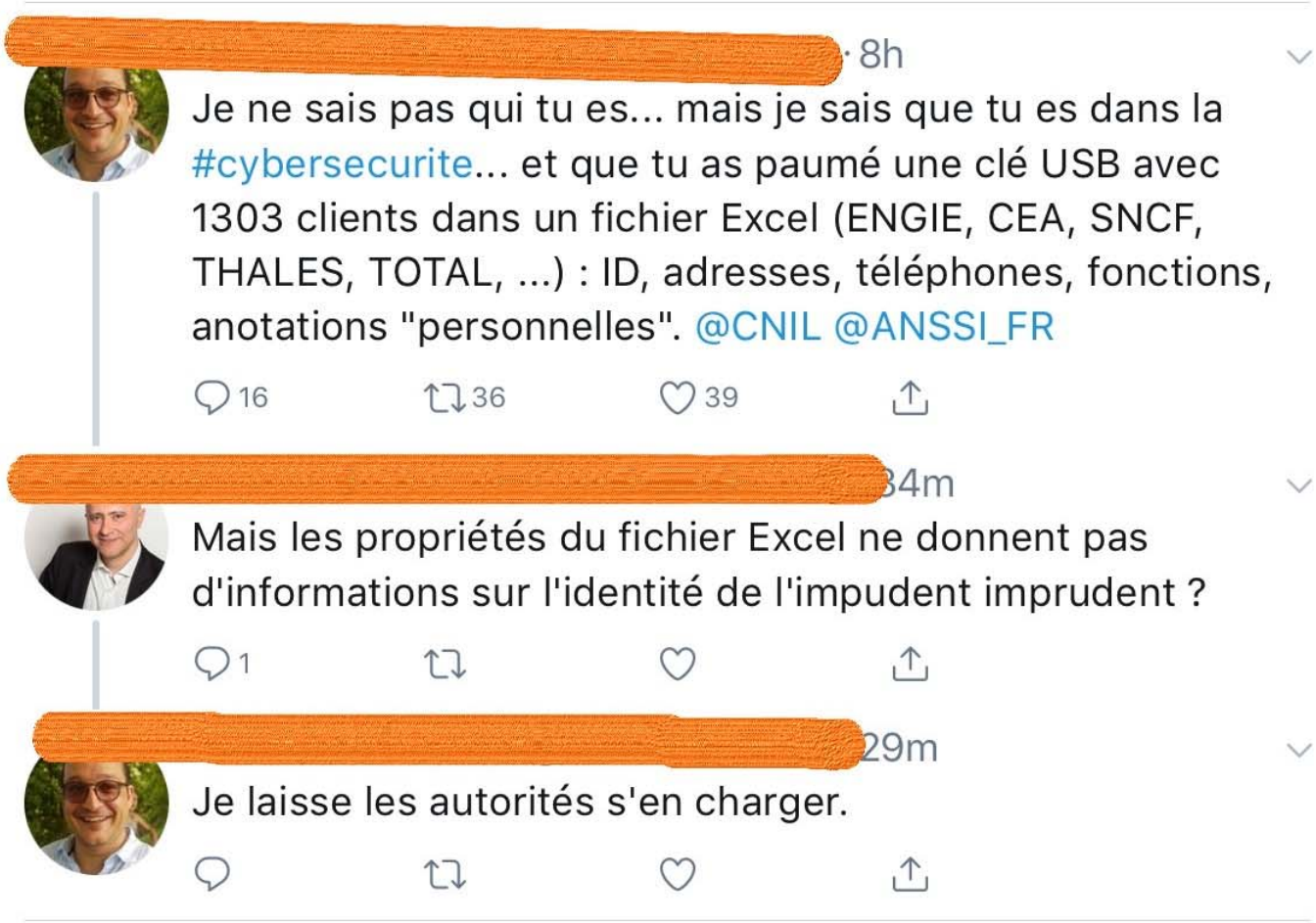
- Fin du régime déclaratif (quelques exceptions pourraient rester) ➔ logique de **responsabilisation / auto-contrôle permanent / gestion du risque**
- Protection des données personnelles **« dès la conception et par défaut »**
- Changement des pratiques et nouveaux « outils » :
  - Adopter **le point de vue des usagers** (nouveaux droits, consentement explicite…)
  - **Études d'impact formelles** pour les traitements les plus sensibles,
  - Tenue d'un « **registre** », traçabilité/documentation… → on doit pouvoir « rendre compte » des actions, des décisions, des analyses réalisées…
  - Contractualisation explicite à développer (fournisseurs, partenaires…)
  - Désignation d'un « **Délégué à la Protection des Données** » (obligatoire pour toutes les entités publiques)

ANALYSER LES RISQUES ET LES PALLIATIFS : EN PRATIQUE

Exemples de « risques »	Quelles solutions ?
Intrusion physique	et/ou protégés
Accès au poste de travail en l'absence	Protection pa e local fermé/sécurisé Chiffrage du post si les fichiers sont dessus…
Fichiers papier et/ou impressions a des tiers	te les dossiers » re les docum s
Vol/détournement d'une sauvegard	s sauv ous clé » hier
Données potentiellement accessibles ieur	[Fair ion du réseau et des droits d'accès (la règle pa un accès » !)
Conditions d'hébergement inconnues	lement les obligations (…)
Mais aussi… piratage, accès à des données sensibles	*vation non respectée, plainte/réclamation, etc. etc.*

Image, sanctions administratives et/ou financières, coût de « réparation », etc.

LES « RISQUES » DANS LA VIE RÉELLE… (APERÇU)



[source : échange de messages publics relevé sur Twitter, février 2018]

Petite suggestion : rejouer le même *dialogue* avec **« je sais que tu travailles dans une collectivité… tu as paumé une clé USB de sauvegarde de ton fichier des activités périscolaires, avec les coordonnées de 285 parents et de 168 enfants (…) »**

COMMENT FAIRE ?

- **Désigner un pilote,** à savoir le Délégué (mutualisé ou non)… sans oublier d'identifier un ou des agent(s) « relais »,
- **Recenser et qualifier les traitements** (« gestion de l'état-civil », « paie et ressources humaines », par exemple),
- **Prioriser les actions à réaliser** au regard de la sensibilité des données et de la gravité des « écarts » et des problèmes potentiels,
- **Gérer les risques critiques** (protection des données médico-sociales traitées par un CCAS, par exemple), en menant une analyse d'impact spécifique,
- **Organiser les processus** pour anticiper les sollicitations/problèmes susceptibles d'intervenir, et mettre en œuvre les améliorations/changements de pratiques
- **Documenter la conformité** pour attester des réflexions et de la démarche

(source : CNIL « se préparer en 6 étapes »)

UN « DÉLÉGUÉ » DANS, OU POUR CHAQUE COMMUNE ?

- La mutualisation du Délégué, recommandée par la CNIL, apparaît indispensable :
  1. Sauf exception, ce ne sera pas - loin s'en faut – un poste à plein temps,
  2. Il y faut des compétences spécifiques (techniques + juridiques),
  3. Le Délégué ne doit pas être juge et partie, il doit porter un regard neutre sur l'existant,
  4. Il y a matière à « industrialiser » *(pratiques, outils, capitalisation des connaissances sur les éditeurs, les configurations techniques, etc.)*,
  5. La mutualisation permet d'assurer une permanence et de faire bénéficier les adhérents de « l'effet du réseau ».

SARTHE ET MUTUALISATION NUMÉRIQUE…

- Le Département, un « opérateur de mutualisation numérique » de longue date :
  - Ingénierie (dont SATESE), via l'ATESART,
  - Plateformes et données numériques (marchés publics, contrôle de légalité [ACTES], numérisation cadastrale et données IGN, Web-SIG…) depuis une douzaine d'années,
  - *Et auparavant, pour mémoire…*

[Couverture en date du printemps 1990…]

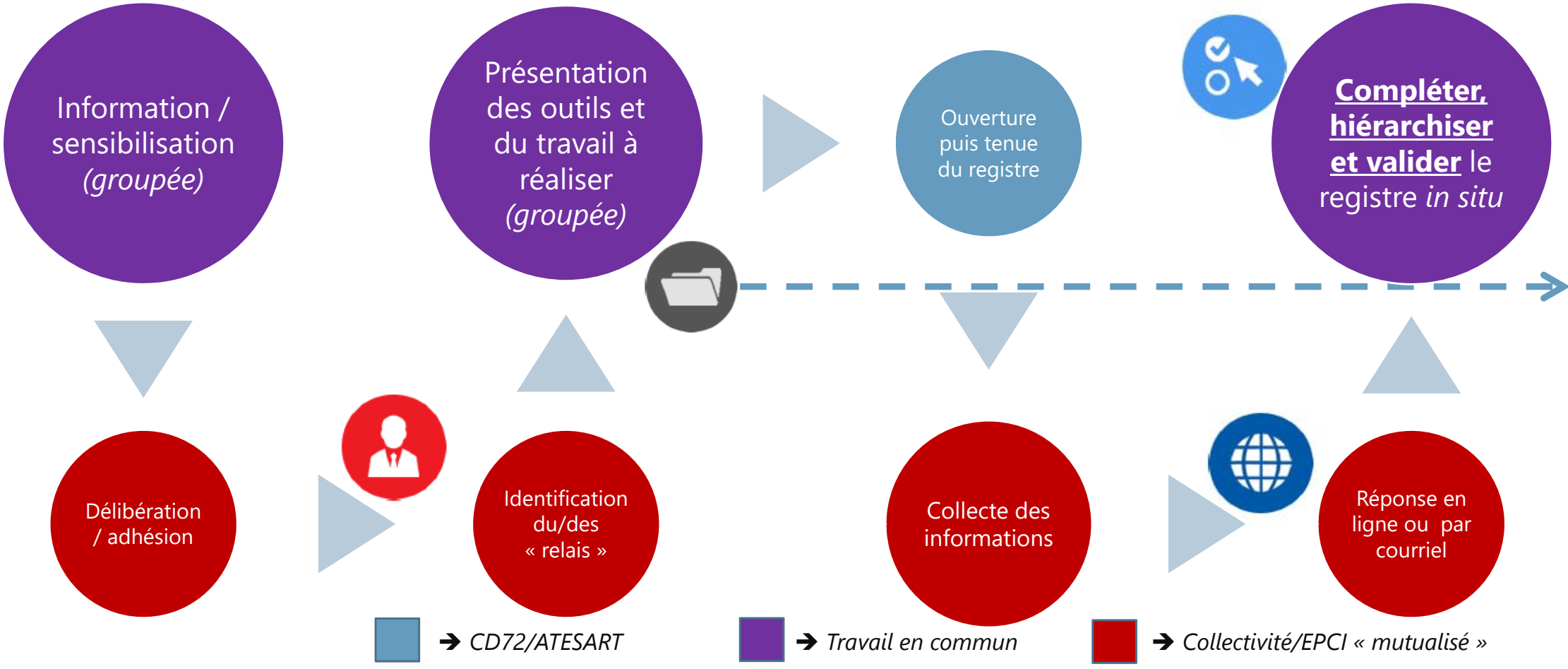
PARTAGER NOTRE/NOS FUTUR(S) DÉLÉGUÉ(S) ?

- Existe déjà dans une « petite » vingtaine de structures départementales et régionales,
- Portage envisagé : dans le prolongement et en cohérence avec **l'offre d'ingénierie départementale (ATESART)**,
- Aperçu des simulations financières :

En cours…

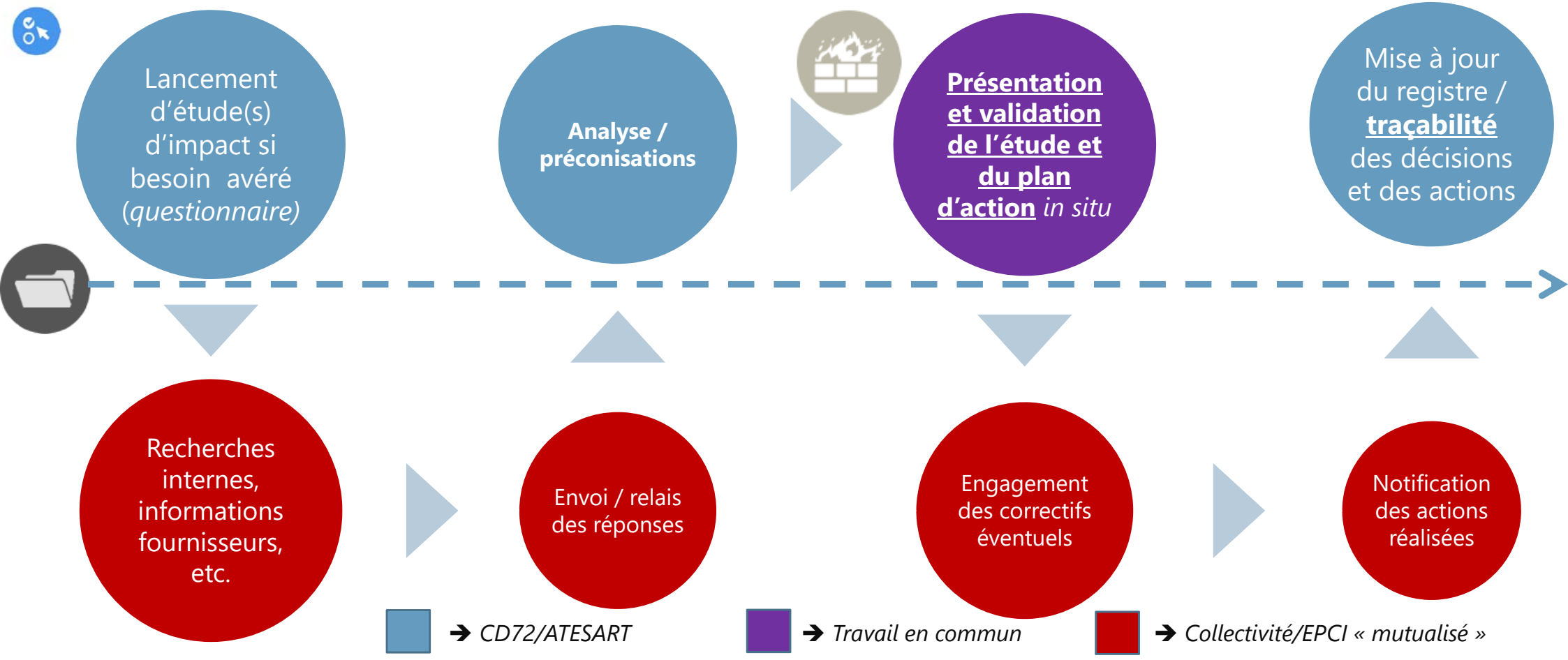
LE DÉLÉGUÉ MUTUALISÉ, EN PRATIQUE (#1)

Désignation du Délégué, et mise en place d'un registre des traitements avec hiérarchisation des principaux risques



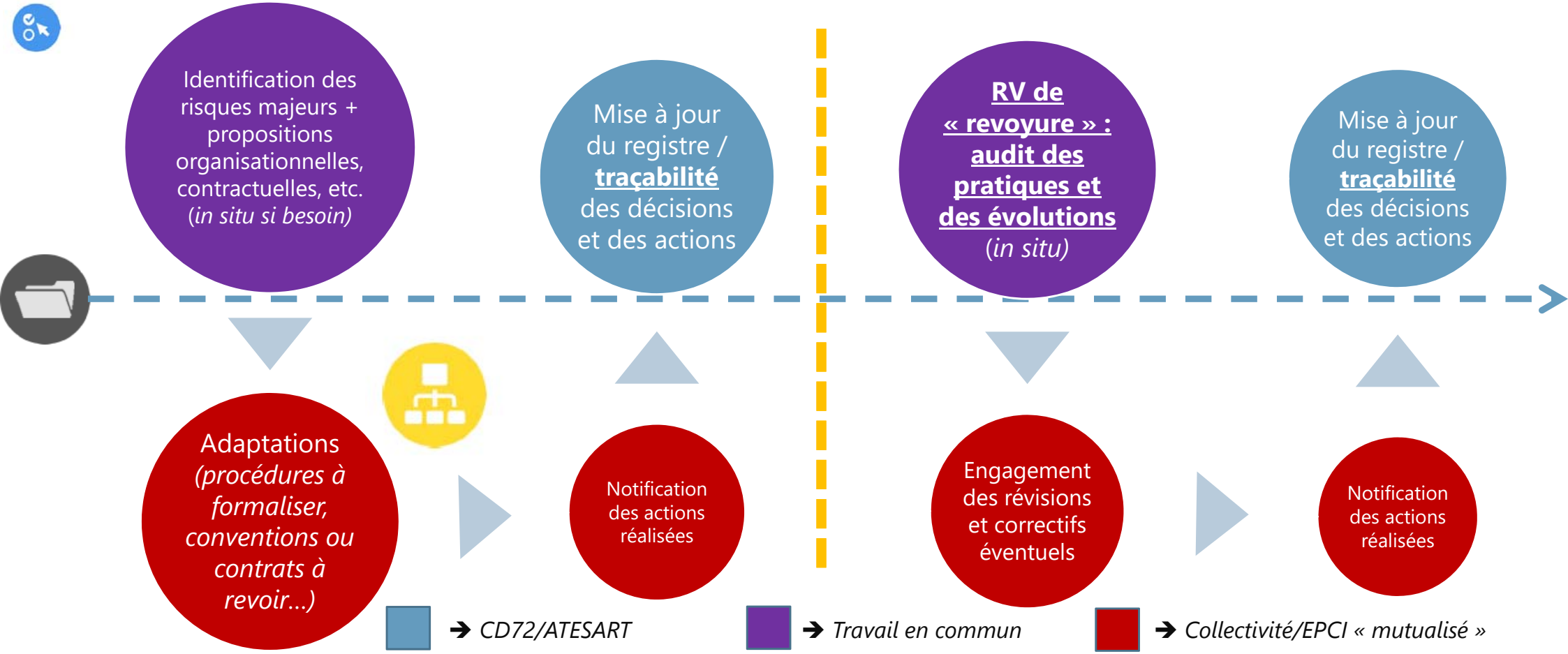
LE DPD MUTUALISÉ, EN PRATIQUE (#2 SI DONNÉES SENSIBLES)

S'il y a données « sensibles », il faudra mener une analyse d'impact dès que possible, au plus tard avant le 25 mai 2021



LE DÉLÉGUÉ MUTUALISÉ, EN PRATIQUE (#3)

Il faut s'organiser et documenter ce qui est fait pour mieux respecter les droits de l'usager + auditer régulièrement l'existant

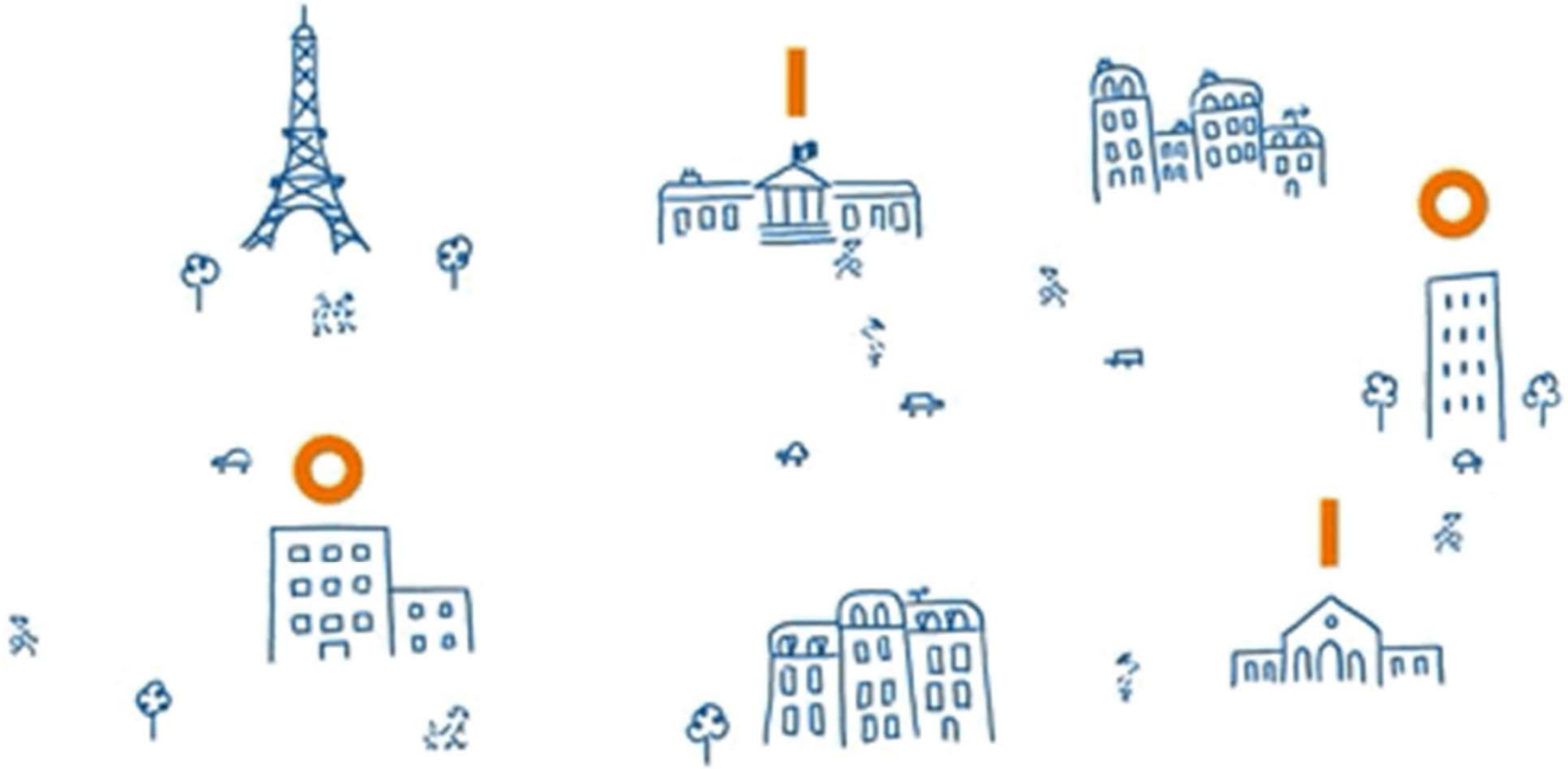


UN REGISTRE ? COMMENT CELA SE PRÉSENTE-T-IL ?

➔ Voir un exemple…

LE RGPD… UN « BIEN » OU UN « MAL » ?

- Des charges nouvelles et des difficultés à surmonter…
  - Travail « en plus » à réaliser ensemble : le Délégué « chef d'orchestre » ne peut pas *faire à la place de…*
  - Difficile de se responsabiliser et de « s'auto-contrôler » *(le « risque zéro » n'existe pas…)*,
  - Difficile d'apprendre du passé, terrain non (encore) balisé → quels risques ? quelles sollicitations/plaintes ? quels moyens effectivement nécessaires ?
  - △ « effet de rattrapage » : pas de délai de grâce ni d'indulgence pour l'antériorité !
- Mais aussi des avantages indirects :
  - Responsabiliser = faire appel à l'intelligence plutôt qu'imposer un modèle unique,
  - Exploiter le délai d'adaptation/régularisation consenti par la CNIL (3 ans),
  - Mieux connaître et mieux contrôler de ses « actifs numériques » (sécurité, etc.),
  - Confiance, transparence, lutte contre la cybercriminalité : une démarche valorisante et valorisable (usagers, agents…).



MERCI DE VOTRE ÉCOUTE