

JFTL 2020

Tester des SI sensibles en conformité avec le RGPD

RETOUR D'EXPÉRIENCE
Programme d'anonymisation
au SGMAS



SECRÉTARIAT
GÉNÉRAL
DES
MINISTÈRES SOCIAUX



open
YOUR DIGITAL WORLD



Intervenants



STÉPHANE NUDELMANN

Chargé de mission SSSI
et RGPD, au SGMAS

(Secrétariat Général des Ministères et des Affaires Sociales)



CHRISTOPHE BODEN

Directeur de mission, Open
Marché TRA SGMAS

(Tierce Recette Applicative)

SOMMAIRE

- #1 Contexte et objectifs
- #2 Démarche et résultats
- #3 Indicateurs / Métriques



1

CONTEXTE ET OBJECTIFS

Les SI des ministères sociaux sont sensibles



SECRÉTARIAT
GÉNÉRAL
DES
MINISTÈRES SOCIAUX



SANTE • SOCIAL • JEUNESSE...
...Une matière sensible



BAFA, Etablissement sportifs,
Manifestations sportives



Accueil des mineurs, Boussole
des jeunes, Service civique



SIAO 115, Comité d'éthique,
Déclaration publique d'intérêt



Mouvements de main d'œuvre,
Ruptures de contrat, Travailleurs
détachés, Contentieux administratifs



À maj CBO, sur les figures ministériels

La RGPD est à la genèse du projet



Le RGPD renforce la protection des données personnelles

Principes RGPD concernant les données

- ✓ PRINCIPE DE TRANSPARENCE
- ✓ PRINCIPE DE LIMITATION DES FINALITÉS
- ✓ PRINCIPE DE MINIMISATION DES DONNÉES
- ✓ PRINCIPE D'EXACTITUDE DES DONNÉES
- ✓ PRINCIPE DE LIMITATION DE LA CONSERVATION DES DONNÉES
- ✓ PRINCIPE DE SÉCURITÉ, D'INTÉGRITÉ ET DE CONFIDENTIALITÉ DES DONNÉES

**Utiliser des données sensibles (réelles) dans les tests
n'est pas conforme
car ne respecte pas les principes RGPD**



2018 : le SGMAS lance un programme transverse d'anonymisation

Se mettre en conformité avec le RGPD (mai 2018)

Garantir l'anonymat des données

Maîtriser l'ensemble des données du système d'information

Standardiser les bonnes pratiques de protection des données

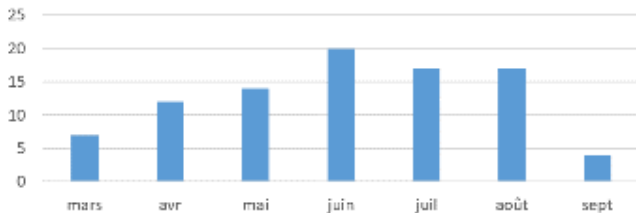


#1 Résorber la présence de données sensibles dans les environnements hors PRODUCTION

#2 Donner confiance aux Métiers en sécurisant les données

#3 Définir et mettre en œuvre l'offre de service d'anonymisation

► DEMANDE DE DUMP AUPRÈS DE L'INFOGÉRANT



Prérequis : Des solutions alternatives pour les besoins DSI (jeux de données anonymisés pour les tests et formations)

2

DÉMARCHE ET RÉSULTATS

- ▶ #1 L'étude de cadrage
- ▶ #2 La mise en place de la plateforme
- ▶ #3 La réalisation des pilotes
- ▶ #4 Le déploiement

#1 La démarche de l'étude de cadrage

Une étude de cadrage est menée sur 3 mois sous le sponsor de la sous-direction des projets SI et du chargé de mission SSI, articulée sur 4 chantiers, et impliquant l'ensemble des acteurs de la DSI

**Analyser les besoins en anonymisation,
des applications et projets**

Cas d'usage
Enquête CPI (chefs de projets)



SDPSI, MIPIL, RSSI

**Etudier une solution d'anonymisation,
intégrée à l'organisation et à l'IT**

**Présentation de la solution progicielle
pressentie**
Définition de l'architecture (macro)



SDPSI, MIPIL, RSSI, MITECH, SDISU

**Elaborer une offre de service anonymisation
de la DSI**

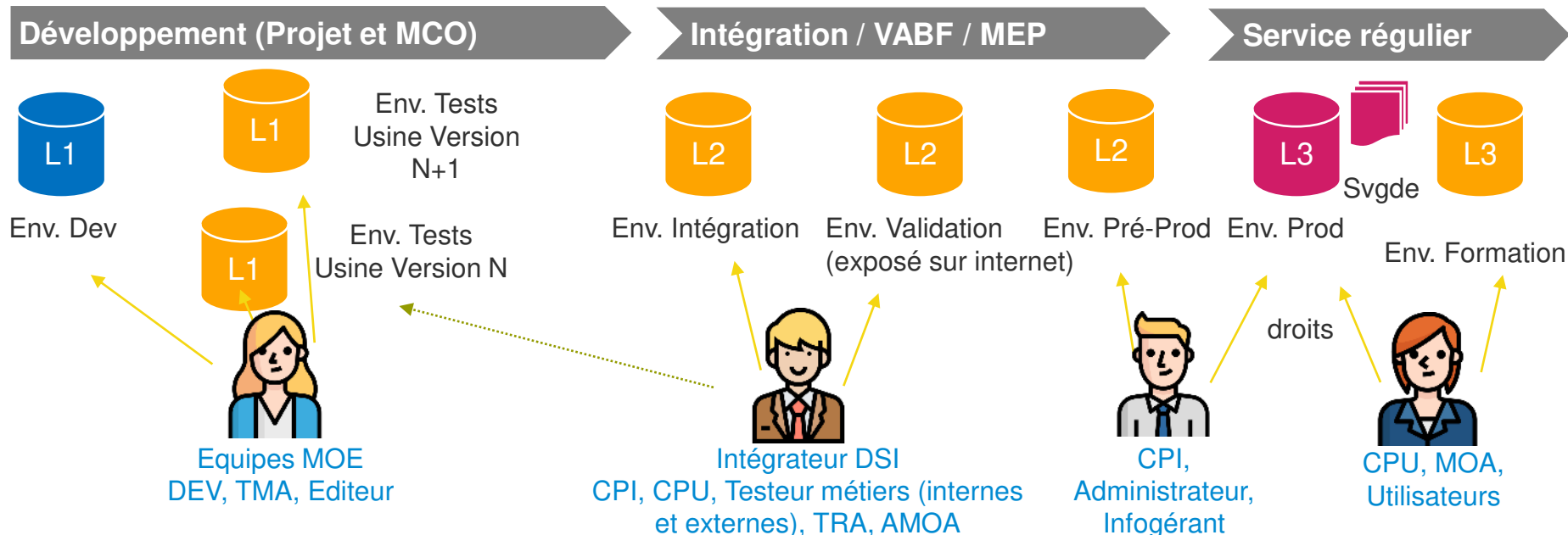
Stratégie de déploiement
Offre de services
Aide à la décision GO / NO GO

**Construire une feuille de route,
intégrant l'offre de service**



SDPSI

#1 Définir les cas d'usages de l'utilisation des jeux de données



#1 Faire un état des lieux

En mobilisant les chefs de projet informatiques (CPI)

► RÉSULTAT DE L'ENQUÊTE CPI SUR LES APPLICATIONS DE LA DSI SGMAS

Valeurs factices

Nombre d'application par complexité des données et niveaux de confidentialité :	1	2	3	4	(vide)	Total général
Complexe	12	29	5	4		50
Simple	36	43	7	4		90
Total général	48	72	12	8		140

Complexe : Données cohérentes et représentatives
Simple : mise à blanc ou remplacement des champs sensibles par un libellé unique

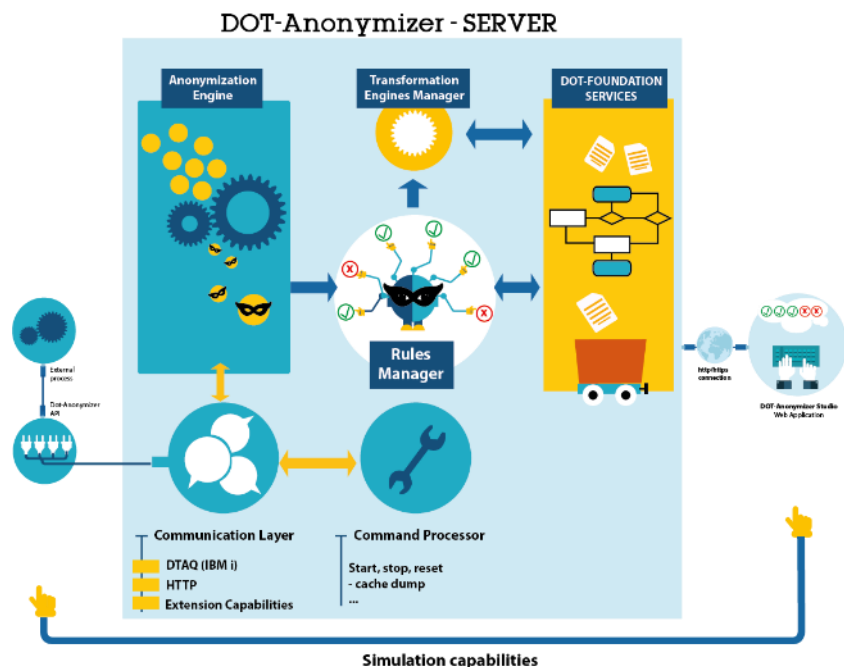
NIVEAUX DE SENSIBILITÉ

1. **NON SENSIBLE** : données publiques
2. **SENSIBILITÉ MOYENNE** : courante au sens CNIL
3. **SENSIBILITÉ FORTE** : perçu comme sensible au sens CNIL
4. **SENSIBILITÉ CRITIQUE** : déclaré sensible au regard de la loi

► **Enjeu** : collecter une information volumineuse
► **REX** : utiliser les outils DSI : cartographie du SI, espace collaboratif

#1 Présenter une solution

Une solution progicielle du marché pour couvrir les besoins de **constitution de jeux de données complexes, cohérents et représentatifs**, avec possibilité de **permanence des données**



► CARACTÉRISTIQUES :

- **Multi plate-formes**
- **Multi bases de données**
- **Fichiers structurés** (.csv, xml)
- **Statistiques** d'exécution
- Bibliothèques évolutives d'**algorithmes**
- **Lancement des exécutions & Planification**
- **Mécanisme d'exploration des données** à anonymiser
- **Modèle économique** : 1 licence Serveur + 1 licence par connecteur



- Enjeu : sécuriser le choix de la solution
- REX : une prez c'est bien, un POC c'est mieux ?

#1 Définir une feuille de route intégrée au processus et aux acteurs



Editeur

Installe la solution progicielle
Contribue aux projets pilote
Réalise le support technique



CPI

Exprime le besoin

Rédige le plan d'anonymisation

Teste et Valide le projet
d'anonymisation

Demande de
Dump

Fournit le Dump
anonymisé



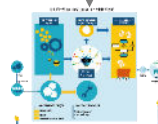
Infogérant

► **Enjeu : contractualiser l'offre**
► **REX : peut prendre 6 mois !**



Consultant

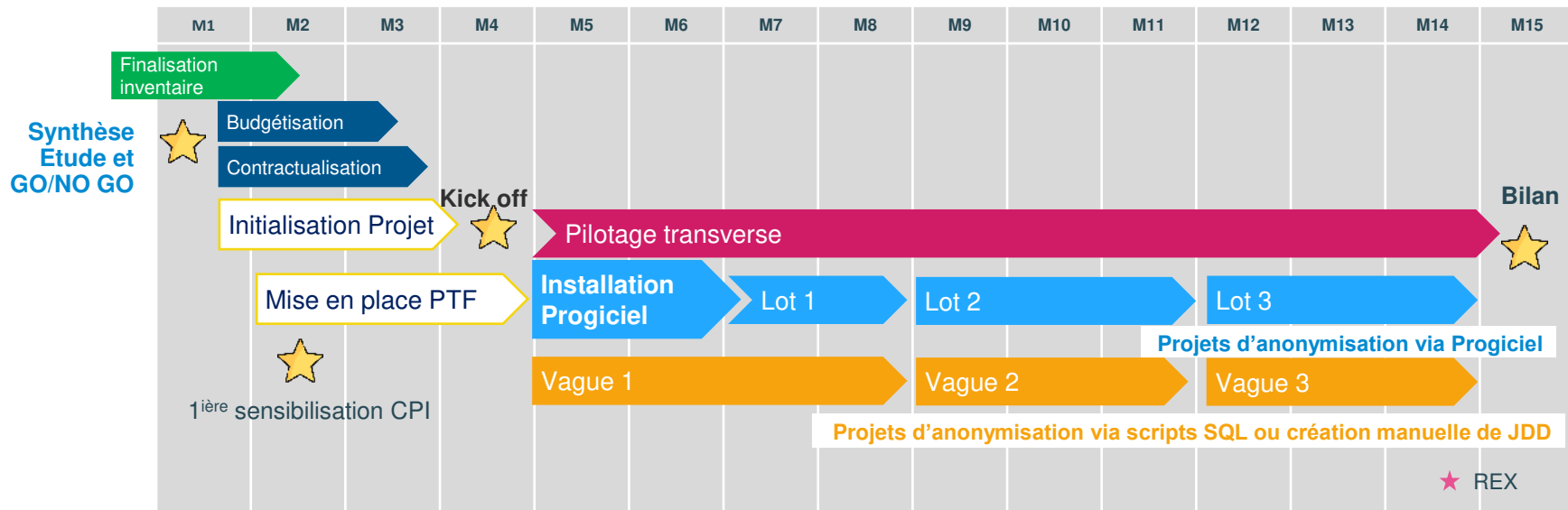
Paramètre l'anonymisation de l'appli



Lance l'exécution des traitements avant la fourniture d'un Dump

#1 Projeter une feuille de route

Arbitrer parmi des scénarios et faciliter la budgétisation



LES SCÉNARIOS

Scénario 1 (nominal) : Solutions ajustées aux besoins

Scénario 2 (exhaustif) : Solution progicielle pour tous

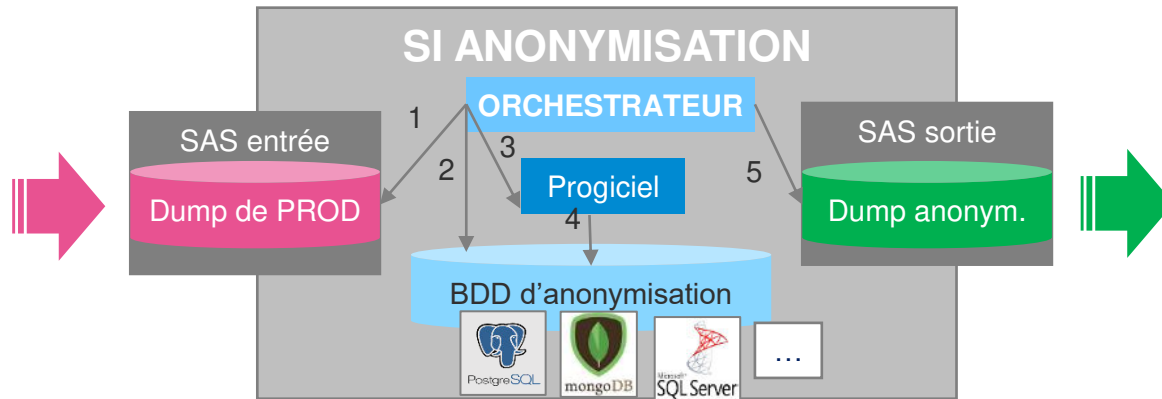
Scénario 3 (dégradé) : Solutions maison pour tous

Décision :
industrialiser,
penser transverse

#2 La mise en place d'une plateforme

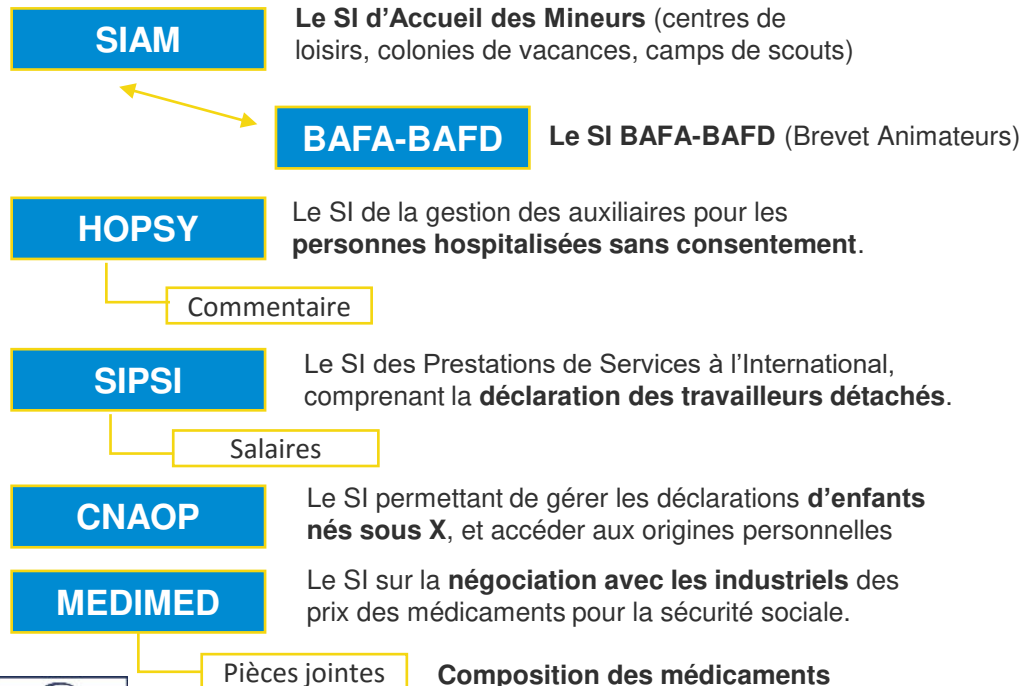
Répondre à une double exigence de sécurité et de fluidité

Les choix : limiter les gestes manuels, limiter le nombre d'utilisateurs et les droits, limiter la durée de conservation au minima (temporaire, voir éphémère)



- Enjeu : les infrastructures sur le chemin critique
- REX : anticiper la commande des serveurs / VM !

#3 La réalisation de projets pilotes sur un panel représentatif et des besoins urgents



► **Enjeu : la cohérence des données partagées par des SI en interaction**
► **REX : Lier les projets pour maintenir la cohérence**

► **Enjeu : anonymiser les commentaires**
► **REX : traquer les données non structurées**

► **Enjeu : cohérence entre les montants**
► **REX : anonymiser les organisation et les noms, plutôt que transformer les montants**

► **Enjeu : les documents sensibles**
► **REX : peu d'intérêt pour les tests**
=> remplacer par une PJ générique

#4 Le déploiement

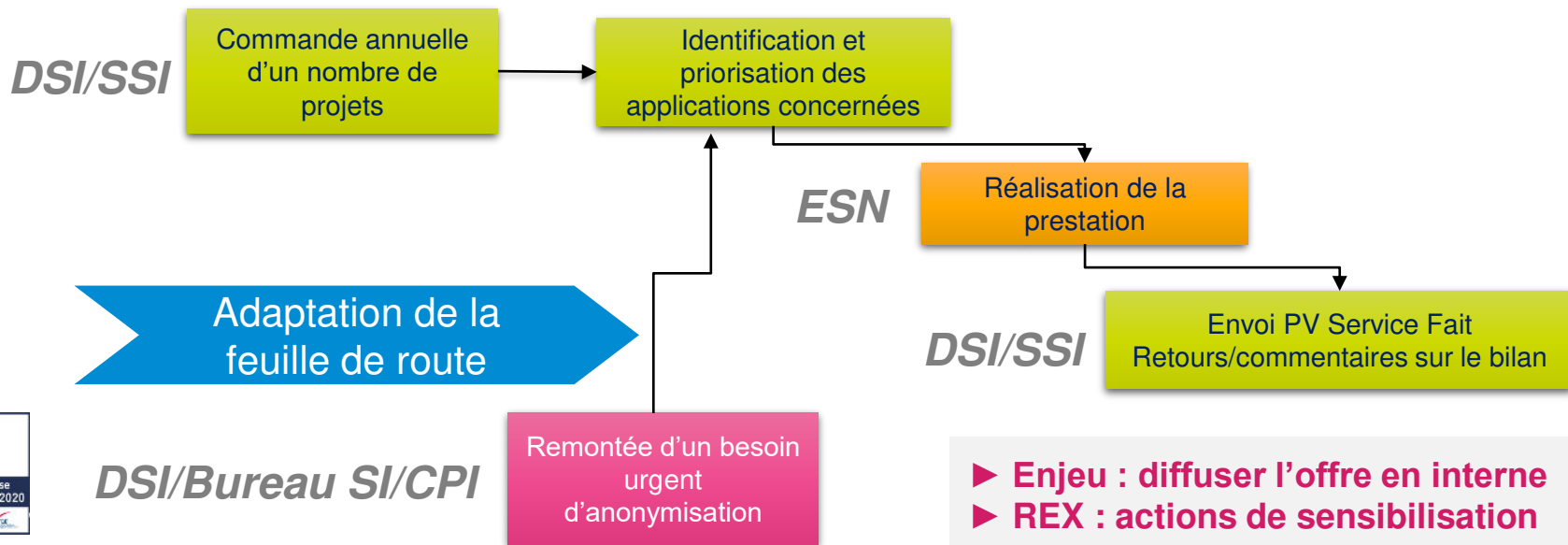
Un pilotage transverse, une feuille de route annuelle et adaptable

Pilotage transverse du programme par SSI

(coordination, suivi, et reporting : indicateurs de pilotage)

Feuille de route annuelle des projets d'anonymisation

(cible : applications en production avec données personnelles / sensibles)

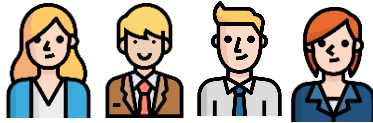


#4 Le déploiement

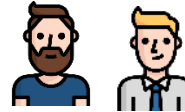
La conduite du changement

Séminaire organisée par l'équipe programme avec l'appui de la DPD ministérielle
(Déléguée à la protection des données)

RGPD un changement culturel à s'approprier



CHEFS DE PROJET INFORMATIQUE



INFOGÉRANTS

**Sensibiliser à la protection des données et
aux enjeux de l'anonymisation.**

3

INDICATEURS ET MÉTRIQUES



Métriques sur quelques projets

Volumétries



SIPSI



MEDIMED



BAFA-BAFD

Nb Attributs anonymisé	Nb de dossiers	Nb d'ocurrences	Temps de traitement
80	4 millions	300 millions	2 h 30
20	0,3 millions	6 millions	0 h 20
70	3 millions	200 millions	8 h 30

80%

Générique : nom, prénom, date de naissance, adresse, tél

20%

Spécifique : anonymisation conditionnelle, vieillissement...

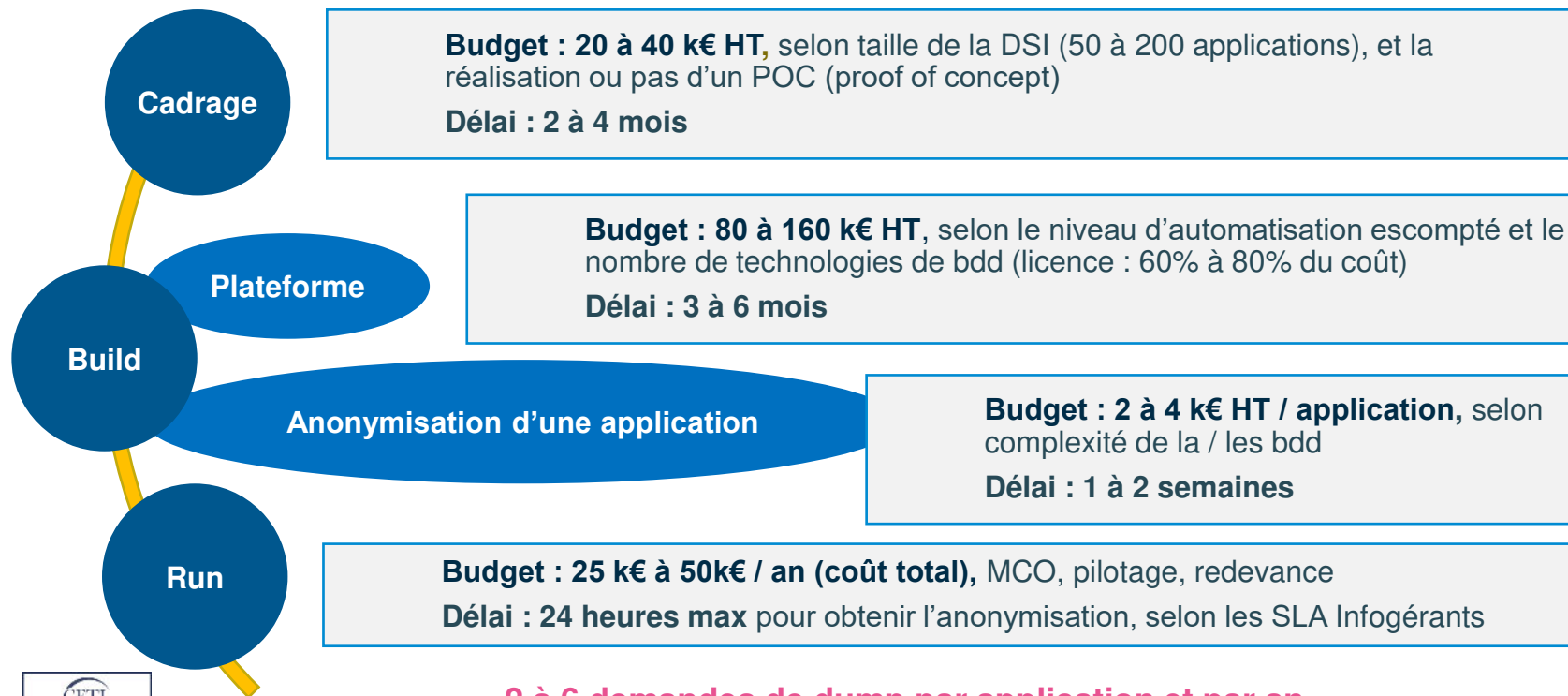
Indicateurs de pilotage

Un suivi au niveau de chaque projet, consolidé à l'échelle du programme

Indicateurs		Objectifs / commentaire
IP1 : Non-conformité RGPD	Date de MEP :	Date de mise en service du traitement d'automatisation
	Nb incident :	Objectif : 0 incident (données personnelles dévoilées)
IP2 : Demande dérogatoire de Dump non anonymisé*	Nb Dump / période :	Permet de mesurer les dérogations réalisées par les CPI, nécessite un REX pour améliorer l'offre de service Objectif : 0
IP3 : Respect délais Dépôt Dump sur SAS d'Entrée	Nb Dump dans les délais / période :	Objectif : à définir avec l'infogérant
IP4 : Respect délais Accès Dump désensibilisés sur SAS de Sortie (RUN)	Nb Dump dans les délais / période :	Objectif : 90% des dumps fournis en moins de 24 heures
	Nb Dump / période :	Permet de mesurer l'activité du service rendu final (mode à la demande)
IP6 : Respect délais Projet d'anonymisation (BUILD)	SFD :	Objectif : 90% des SFD fournis 3 jours au plus tard après l'atelier de recueil de besoin
	Dump désensibilisé :	Objectif : 90% des projets terminés 2 semaines au plus tard après l'atelier de recueil de besoin
QualiPREST :	Compétence du dispositif :	Compétence du dispositif, Respect des engagements, à remplir par le biais d'un formulaire

- **Enjeu : limiter à l'essentiel**
- **REX : collecte des valeurs à partir des outils DSI**

Métriques d'un programme d'anonymisation, Définis sur la base du constaté à date et/ou des objectifs définis



2 à 6 demandes de dump par application et par an

**MERCI
DE VOTRE ATTENTION !**

