

RGPD

Lancement marché
d'accompagnement
à la conformité « CDG79 »



**DATAVIGI
PROTECTION**
SÉCURITÉ ET CONFORMITÉ RGPD

Qui sommes nous ?



Une entreprise
à taille
humaine!



DATA VIGI PROTECTION

Qui sommes-nous ?

Créé en 2018, la SAS DATA VIGI PROTECTION travaille exclusivement dans le domaine de la mise en conformité RGPD

La satisfaction clientèle au cœur de la préoccupation



+1500
Clients pro et collectivités

10
Collaborateurs



De 26 à 62 ans ! Des équipes dynamiques, autonomes et performantes

Un CA en progression constante depuis 6 ans.



+10%
de CA en 2023

Focus sur

Data Vigi Protection

4

À ce jour plus de 1500 clients font confiance à notre entreprise, collectivités, associations, TPE, PME, dans tous les secteurs d'activités pour les accompagner dans leur processus de mise en conformité.

Data Vigi Protection est la première entreprise multi-secteur de France en terme de nombre de missions DPO déclarées auprès de la CNIL (+de 1200).



Echauffement...

.....

Maîtrisez vous
la base
du règlement ?



Echauffement

6

1 La nomination d'un DPO est obligatoire dans toutes les structures traitant de la donnée personnelle ?

NON

La désignation d'un DPO est obligatoire pour tous les organismes publics, mais uniquement dans certaines conditions au sein des structures de droits privés.

2 Le DPO est le responsable de la conformité de la structure à laquelle il est associé ?

NON

La responsabilité de la conformité pèse uniquement sur les épaules du RT.

3 Je dispose d'une base de données des entreprises de ma commune me permettant de les contacter pour diverses informations, est-ce une activité de traitement ?

CELA DEPEND

Si le fichier contient uniquement des coordonnées génériques (standard de l'entreprise, email générique) alors non. Si en revanche le fichier contient le nom d'un contact ou sa ligne directe par exemple, alors oui c'est une activité de traitement.

4 Le droit à l'oubli permet à un citoyen de demander la suppression de toutes les données qui le concernent ?

NON

Toutes les données d'un individu ne sont pas effaçables. En revanche, une pseudonymisation des données pourra être effectuée sur certaines données.

5 Une demande d'exercice de droits peut être formulée par email ?

VRAI

Le mail peut être utilisé pour exercer une demande de droit.

6 Le mot de passe : **Xcù78!%** est un bon mot de passe?

NON

12 caractères, des lettres, des chiffres, des symboles et surtout un mot de passe unique par service, voilà les bases d'un bon mot de passe.

7 Je collecte des données ne contenant ni nom, ni prénom, mon traitement n'est donc pas soumis au RGPD ?

CELA DEPEND

Si les autres informations collectées ne permettent pas de retrouver directement ou indirectement un citoyen, alors le RGPD ne s'applique pas. Dans le cas contraire, le RGPD s'applique.

8 Seul un accord explicite de la personne concernée peut me permettre de traiter ses données

NON

D'autres fondements légaux peuvent être utilisés pour traiter de la donnée sans le consentement explicite d'un citoyen, c'est le cas par exemple d'une obligation légale ou d'un intérêt vital ou contractuel.

9 Le RGPD concerne uniquement les données numériques ?

NON

Papier ou digitalisées, toutes les données personnelles sont soumises au RGPD.

10 Toutes les durées de conservation des données sont imposées par la loi ?

NON

Certaines durées de conservation sont légales (factures, paye...). En revanche, d'autres durées de conservation sont laissées à la libre appréciation du RT. En tout état de cause toutes les activités de traitements doivent avoir une durée de conservation définie, pertinente, et surtout raisonnable.

UN POINT sur le RGPD...

.....

Quoi, qui, quand ?

Principes et objectifs

Les données concernées

Les activités de traitements

RGPD
99 articles
à respecter !



RGPD : les infos clés...

Le Règlement Général sur la Protection des Données

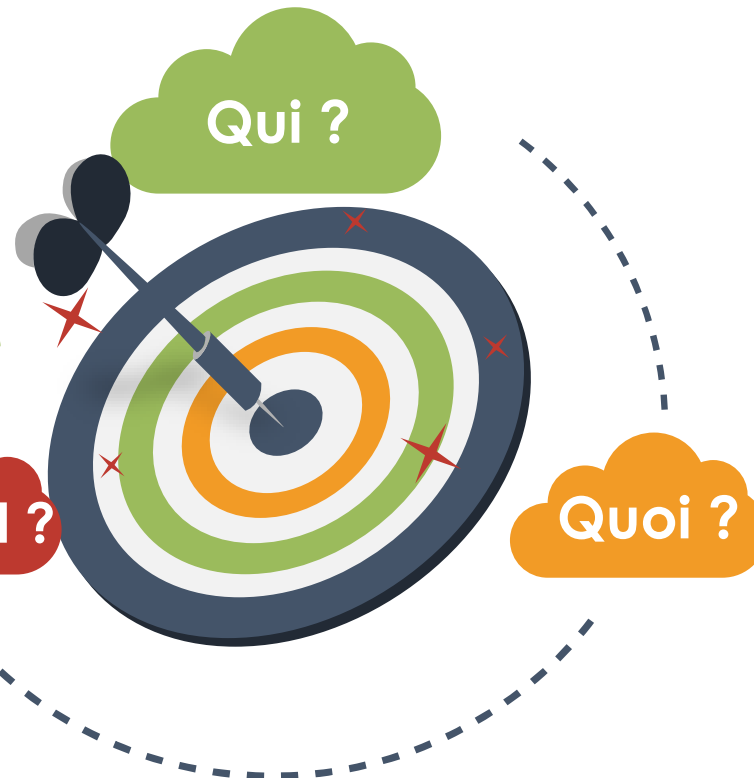
Qui ?

- Toute entreprise, organisme public, ou association qui traite des données personnelles concernant des citoyens européens
- Quelle que soit la taille de la structure
- Enjeux différents = actions à mettre en œuvre différentes

Quand ?

Quand ?

Depuis le 25 Mai 2018



Quoi ?

- Toutes données à caractère personnel collectées sont soumises au RGPD.
- Une donnée personnelle ce n'est pas seulement un nom ou un prénom !

Qu'est ce qu'une donnée personnelle ?

Au sens du RGPD

Constitue une donnée à caractère personnel (DCP), toute information permettant d'identifier directement, indirectement ou par recoupement une personne physique que ce soit par l'intermédiaire d'éléments informatisés ou pas.

- Nom
- Prénom
- Photo
- Adresse mail
- Numéro de téléphone
- CV

- Images de vidéosurveillance
- Numéro de sécurité sociale
- Plaque d'immatriculation
- Adresse IP
- RIB
- Situation familiale
- ...



Activités de traitement

Les opérations portant sur les données personnelles

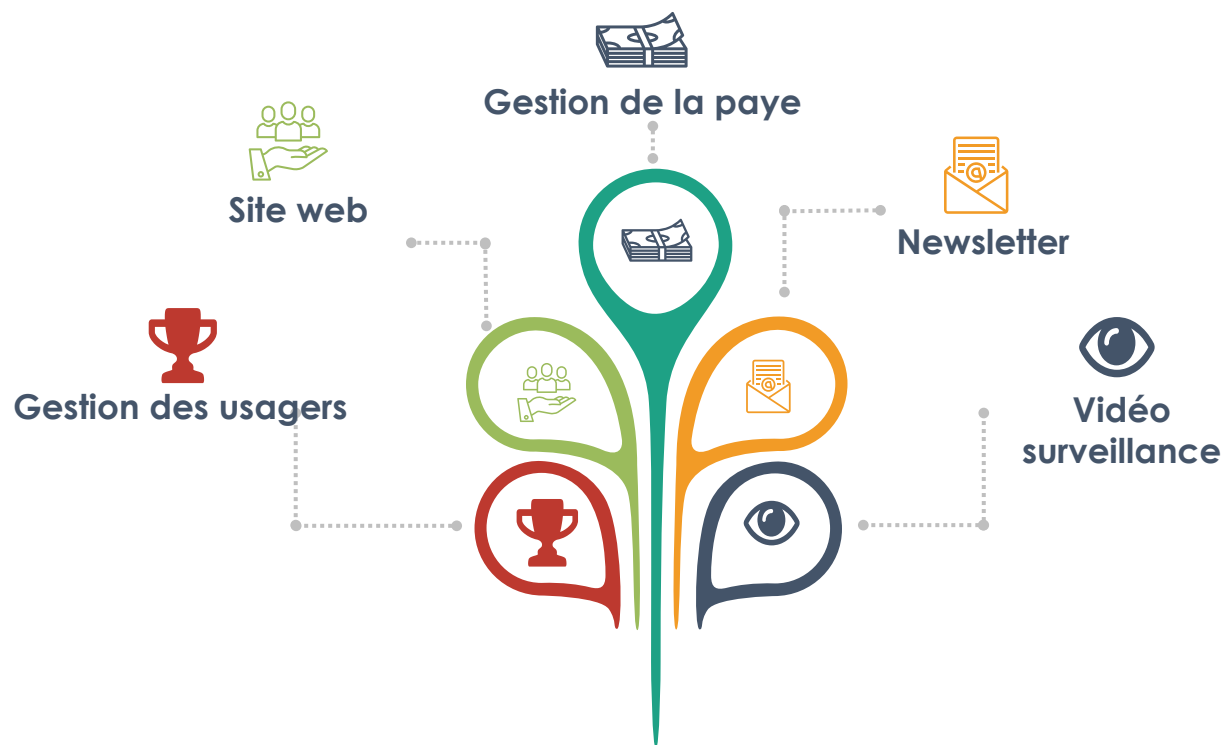
Toute opération ou ensemble d'opérations portant sur des données personnelles, quel que soit le procédé utilisé est considérée comme une activité de traitement.

OPERATIONS

- la collecte
- l'enregistrement
- l'organisation
- la structuration
- la conservation
- l'extraction
- la consultation
- l'utilisation
- la communication
- la diffusion
- le rapprochement
- l'effacement
- la destruction
- ...



ACTIVITES DE TRAITEMENTS



REGISTRE DES TRAITEMENTS

Fiche d'activités de traitement

La carte d'identité du traitement

Chaque activité de traitement doit faire l'objet d'une fiche. Cette fiche doit reprendre un certain nombre d'informations obligatoires. La CNIL met à disposition un modèle de fiche, mais n'impose pas de format particulier.

Doivent figurer à minima sur la fiche :

- La date de création
- La finalité du traitement
- Le fondement légal du traitement
- La durée de conservation des données
- La catégorie des données traitées
- La catégorie des personnes concernées par le traitement
- Si des données sensibles sont traitées
- Qui utilise ces données (les destinataires)
- Si des transferts de données ont lieu hors UE
- Les mesures de sécurité mise en œuvre pour garantir la protection des données du traitement

Le modèle de fiche d'activités de traitement de la CNIL est structuré comme suit :

- En-tête :** Logo DATA VIGI PROTECTION, titre FICHE DE TRAITEMENT, sous-titre Organigramme accès locaux, date d'édition 25.11.2018.
- Informations générales :** Nom, adresse, téléphone, email, date de création, date de mise à jour, version, responsable du traitement, responsable de la sécurité.
- Finalité(s) :** Permet de déterminer quels individus ont accès aux locaux en fonction des badges ou clés en leur possession.
- Durée(s) de conservation :** pas de durée déterminée.
- Catégorie(s) de personnes concernées :** Collaborateurs, Associés.
- Catégorie(s) de données :**
 - Etat civil, identité, photos : Nom, Prénom, Photographie, Date de naissance, Lieu de naissance, Sexe.
 - Coordonnées : Adresse postale, Adresse électronique - email, Numéro(s) de téléphone.
 - Numéro de sécurité sociale.
 - Vie personnelle : Non concerné.
 - Vie professionnelle : Non concerné.
 - Informations économiques et financières : Non concerné.
 - Données de localisation : Non concerné.
 - Données de connexion : Non concerné.
 - Internet : Non concerné.
 - Autres(s) catégoriels :
- Impact sur la vie privée :** Faible.
- Données sensibles traitées :** Non.
- Destinataire(s) des données :**
 - Interne : Direction, service technique.
 - Sous-traitant(s) : Dany Fontaine.
 - Externe : sans objet.
- Transfert(s) des données hors UE :** Non.
- Si oui, pays destinataire(s) :** sans objet.
- Mesures de sécurité :**

Page 1/1

Le registre d'activités de traitement

La pièce maitresse de votre conformité

Le registre d'activités de traitement sera la première pièce demandée dans le cadre d'un contrôle de la CNIL.

Ce document qui va évoluer au gré de la création, de la modification ou de la suppression des activités de traitement doit au même titre que pour les fiches d'activités de traitement comprendre un certain nombre d'éléments :

- Le nom du responsable du traitement
- Eventuellement le nom du Délégué à la Protection des Données (DPO/DPD)
- La liste des activités des traitements ainsi que leur finalité.

Le registre est constitué d'une page de garde qui reprend les éléments précédemment cités. Cette page précède les fiches d'activités de traitement.


REGISTRE DES ACTIVITÉS DE TRAITEMENT
 Mainte de

Date d'édition : 12-09-2018

Informations du Responsable du Traitement		Nom et coordonnées du Délégué à la Protection des Données	
Nom :	XXX	Nom :	XXX
Prénom :		Société :	DATA VIGI PROTECTION
Adresse :		Adresse :	5 rue des Indes noires Arsens Est
Ville :	80440 BOVES	Ville :	80440 BOVES
Téléphone :		Téléphone :	03 22 44 22 30
Adresse de messagerie :		Adresse de messagerie :	xxxx@datavigiprotection.fr

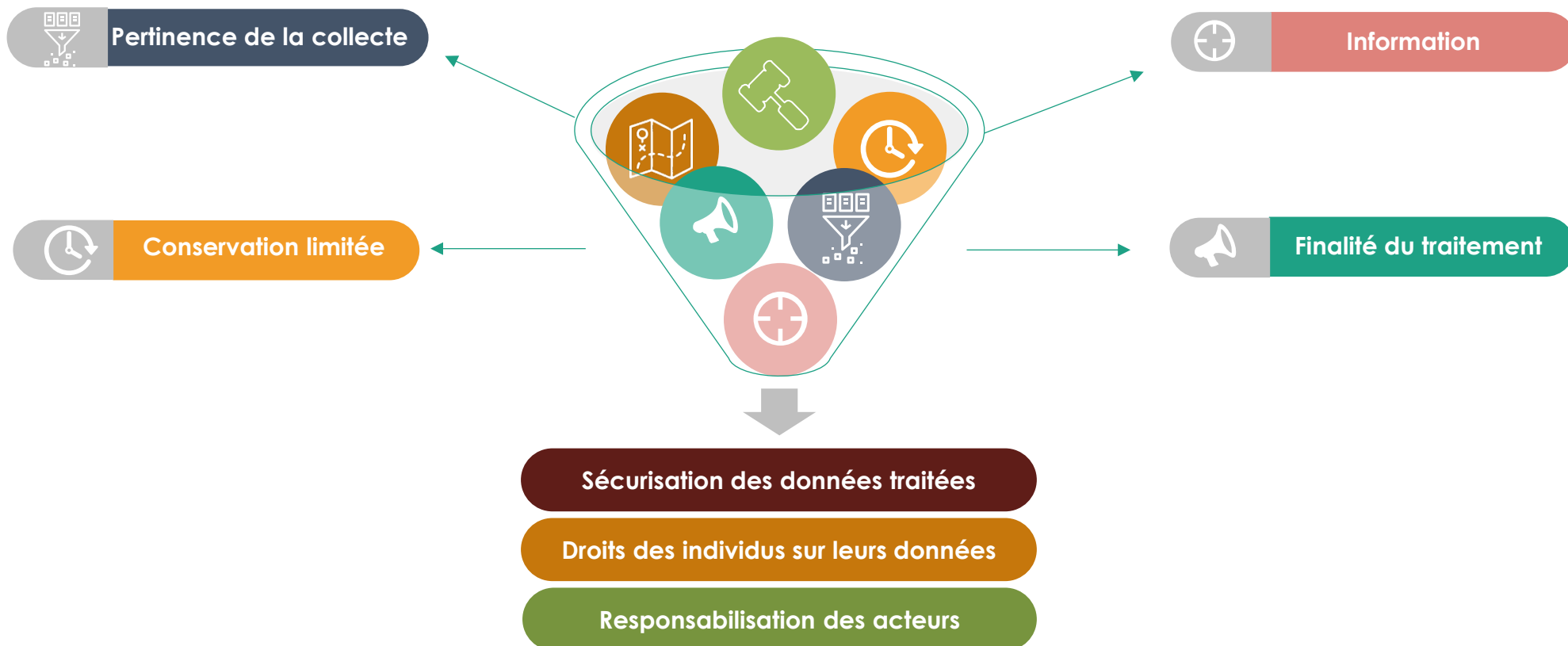
Activités impliquant le traitement de données à caractère personnel

Nom	Finalité(s)	Base légale	Actif ?
Gestion aide sociale d'urgence	Permet la gestion et le suivi des bénéficiaires des aides sociales d'urgence délivrées par le CCAS de la commune	Loi	Oui
Situations sociales à risques	Permet d'assurer un suivi resserré des foyers fragiles socialement (seuil, aides sociales, orientation...)	Consentement	Oui
Gestion des demandes de logements	Permet d'assurer le suivi des demandes de logements sociaux sur la commune (création de dossier logement, présentation des dossiers en CAL, attribution)	Contrat	Oui
Gestion du service portage de repas	Permet d'assurer la gestion du service de portage des repas aux seniors (inscriptions, suivi des demandes, facturation)	Consentement	Oui
Gestion service baby-sitting	Permet d'assurer le suivi d'un service de mise en relation de parents avec des baby-sitters (inscriptions parents et baby-sitters, mise en relation, suivi des demandes, enquête satisfaction)	Consentement	Oui
Liste des médailles du travail	Permet de suivre les médailles du travail délivrées aux agents de la collectivité	Loi	Oui
Suivi des activités seniors	Permet de recenser l'ensemble des personnes inscrites aux différentes activités proposées aux seniors afin d'établir des statistiques	Consentement	Oui
Suivi RSA	Permet d'assurer le suivi des personnes bénéficiaires du RSA (convocation, orientation, formation, déblocage de l'aide...)	Loi	Oui
Elus du Conseil municipal	Permet de contacter les élus en cas de besoin (convocation, invitation...)	Loi	Oui
Gestion de l'école de musique	Permet le suivi de la gestion de l'école de musique (inscriptions des élèves, horaires de présence, facturation, relances, invitations concert, convocations examen)	Consentement	Oui
Demandes RSA	Permet la gestion et le suivi des demandes des RSA auprès du public	Loi	Oui
Liste invitations événements communaux	Permet l'envoi d'informations relatives aux événements organisés par la commune (mail, téléphone, sms, voie postale)	Consentement	Oui
Liste des enseignants école de musique	Permet de contacter les enseignants de l'école de musique en cas de besoin	Loi	Oui
Liste des jurys potentiels concours école de musique	Permet de contacter les personnes pouvant faire office de jury en cas de besoin	Consentement	Oui
Liste des naissances de l'année	Permet d'inviter les parents à un pot de l'année suite à la naissance d'un enfant l'année précédente	Consentement	Oui
Liste une naissance un autre	Permet d'inviter les parents inscrits à la célébration une naissance un autre suite à la naissance d'un enfant l'année précédente	Consentement	Oui

© Copyright 2018 DATA VIGI PROTECTION. Confidential, tous droits réservés. Registre des activités de traitement - version 1.0

Grands principes et objectifs

4 grands principes visant 3 objectifs majeurs



Grands principes et objectifs

Principe d'information : la collecte loyale



- Exigence de collecte des données de manière loyale et transparente
- Interdiction de collecter des DCP à l'insu des individus
- Explication sur l'objet de la collecte
- Renforcement du consentement

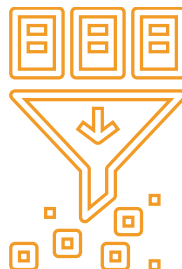


J'autorise le responsable de traitement à traiter les informations personnelles présentes sur ce formulaire, en vue de l'inscription au service qu'il propose.



Grands principes et objectifs

Pertinence de la collecte et du traitement



- La quantité de données détenues est adaptée aux finalités pour lesquelles elles sont traitées
- Les champs de données traitées sont ceux strictement utiles au traitement

Grands principes et objectifs

Finalité du traitement



- Le RT ne peut collecter et utiliser des informations sur des personnes physiques que dans un but bien précis et explicite. On peut imaginer une finalité de traitement principale et des finalités secondaires ou sous finalités.
- Utiliser des DCP pour faire autre chose que ce qui avait été prévu au moment de la collecte est INTERDIT.

Grands principes et objectifs

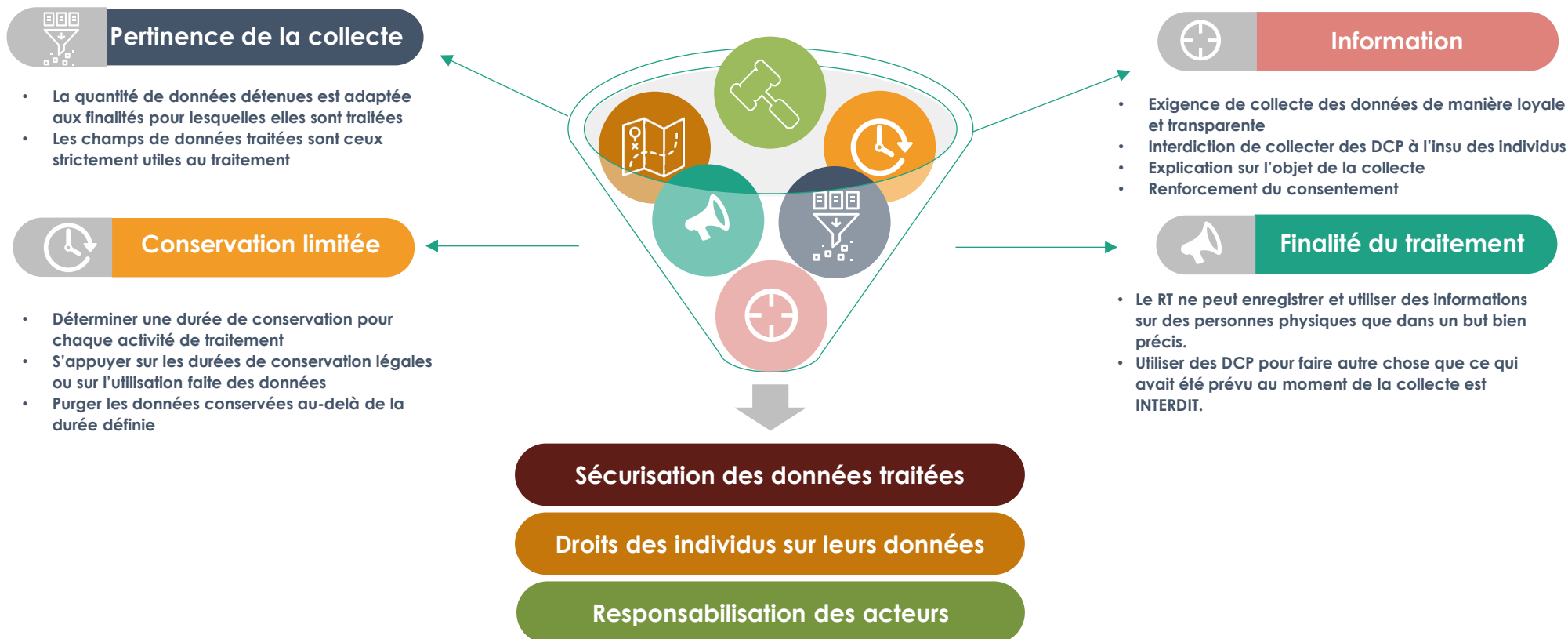
Conservation des données



- Déterminer une durée de conservation pour chaque activité de traitement
- S'appuyer sur les durées de conservation légales ou sur l'utilisation faite des données
- Purger les données conservées au-delà de la durée définie

Grands principes et objectifs

4 grands principes visant **3 objectifs majeurs**



Grands principes et objectifs

3 Objectifs majeurs

Sécurisation des données traitées

- Sécurité physique
- Sécurité logique
- Sécurité contractuelle

Droits des individus sur leurs données

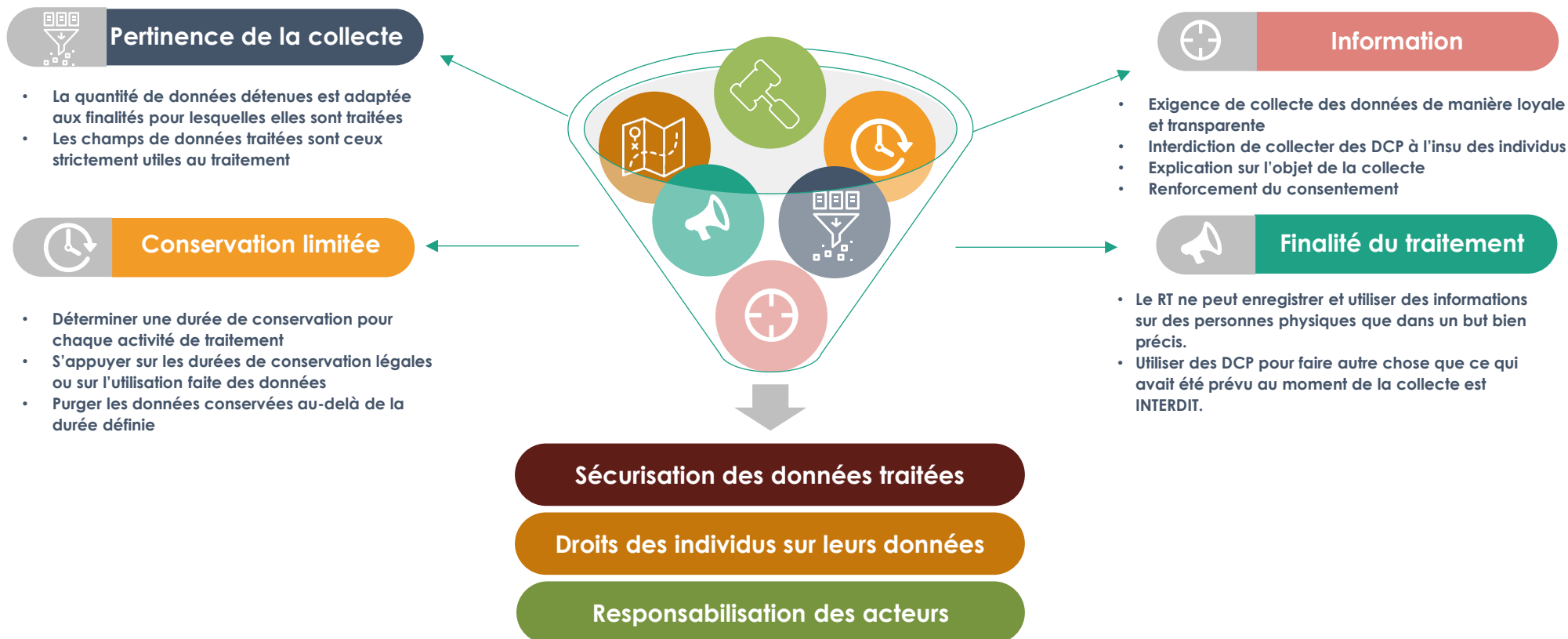
- Respecter les droits des individus, notamment d'accès ou d'effacement
- S'assurer de la capacité à répondre dans les délais impartis

Responsabilisation des acteurs

- Le RT doit s'assurer de sa conformité et la documenter
- Il doit être proactif et anticiper la conformité de ses activités de traitements
- Il doit veiller à ce que l'ensemble des personnes traitant des données dans sa structure maîtrise bien les ressorts du RGPD

Grands principes et objectifs

4 grands principes visant **3 objectifs majeurs**



Les sanctions et les risques

A ne pas sous estimer...



SANCTIONS

De 10 millions en cas d'absence de DPO ou de registre de données à jour, à 20 millions d'euros pour les organismes publics qui ne respectent pas les droits des personnes; et jusqu'à 4% du CA des entreprises, les sanctions financières encourues sont colossales.



RISQUES

Le risque contentieux est à prendre au sérieux. Quelques semaines après la mise en application du RGPD, plusieurs milliers de plaintes avaient déjà été déposées auprès de la CNIL.

Un administré mécontent ou un collaborateur ou un adhérent en froid avec sa commune, son entreprise ou son association pourra se retourner contre cette dernière et demander réparation en cas de non-respect du caractère personnel des données le concernant.



IMAGE

Au-delà du risque financier pesant sur les collectivités qui ne seraient pas en règle avec le RGPD, la dégradation de son image pourrait également être très préjudiciable pour les responsables de la collectivité en cas de sanction, de non-conformité ou de contentieux. L'effet boule de neige pourrait vite devenir incontrôlable et ouvrir la voie à d'autres sanctions ou d'autres contentieux.

La CNIL fait office de gendarme en matière de RGPD. Ses pouvoirs sont étendus tout comme son périmètre d'action.

La CNIL peut ainsi perquisitionner sans demande préalable le siège d'une collectivité entre 6h du matin et 21h.

Et vous, où en êtes-vous ?



Checklist des éléments incontournables

Votre
situation



CHECKLIST DES ELEMENTS INCONTOURNABLES

Votre situation

24



Ont dû être réalisées a minima :

- ✓ Sensibilisation des agents de la collectivité manipulant de la donnée
- ✓ Création du registre d'activités de traitement avec mises à jour régulières
- ✓ Mise en place de procédures internes (violation de données, demande d'exercice de droits...)
- ✓ Réalisation des analyses d'impact sur la vie privée (AIVP) sur les traitements le nécessitant.
- ✓ Existence d'un plan d'action de conformité
- ✓ Registre des sous-traitants avec analyses contractuelles
- ✓ Mise en conformité des sites web, si existants (cookies, politique de confidentialité, formulaires...)
- ✓ Insertion des mentions d'informations sur les formulaires de collecte de données

NOTRE ACCOMPAGNEMENT



Une approche globale, mais adaptable

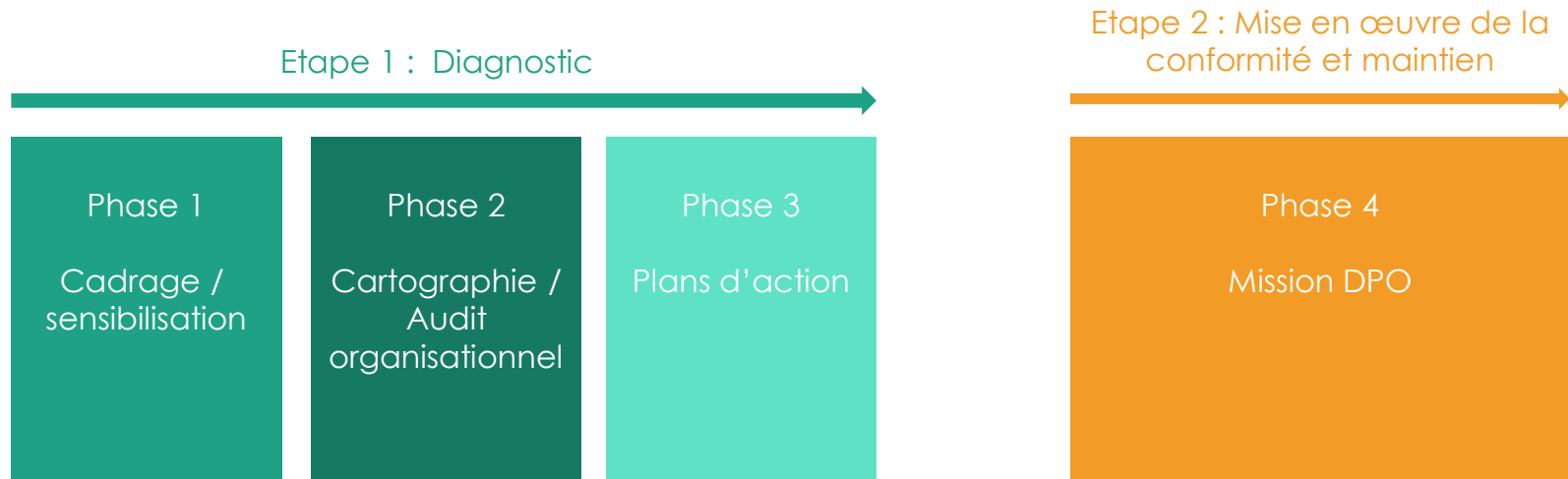
UNE APPROCHE
GLOBALE



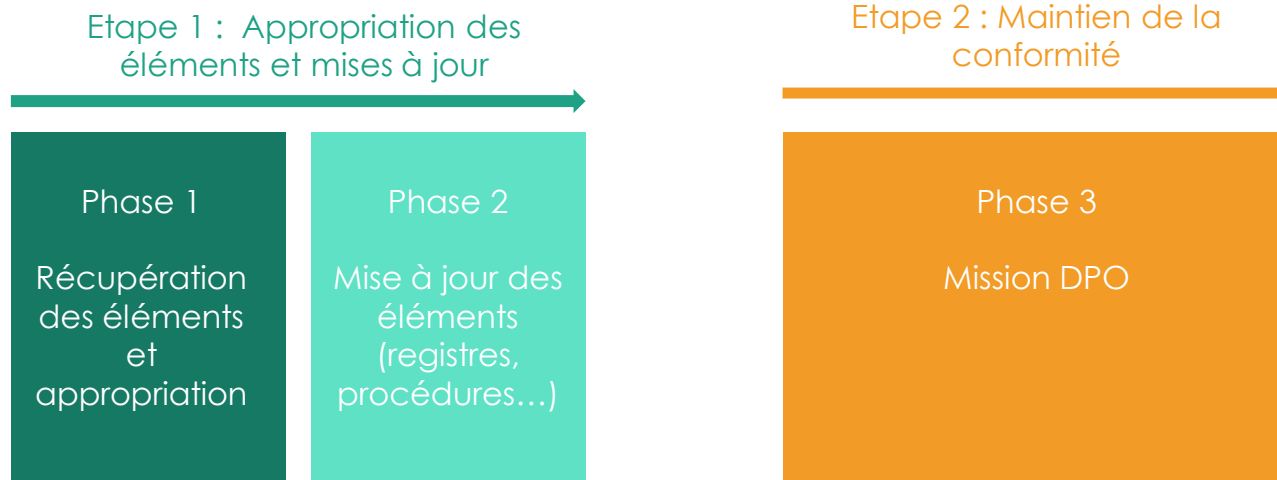
Dans une mission classique

en démarrant d'une page blanche...

- 4 grandes phases ventilées en deux grandes étapes
- Une mission qui se déroule en général à distance et sur site (adaptable en fonction du contexte).

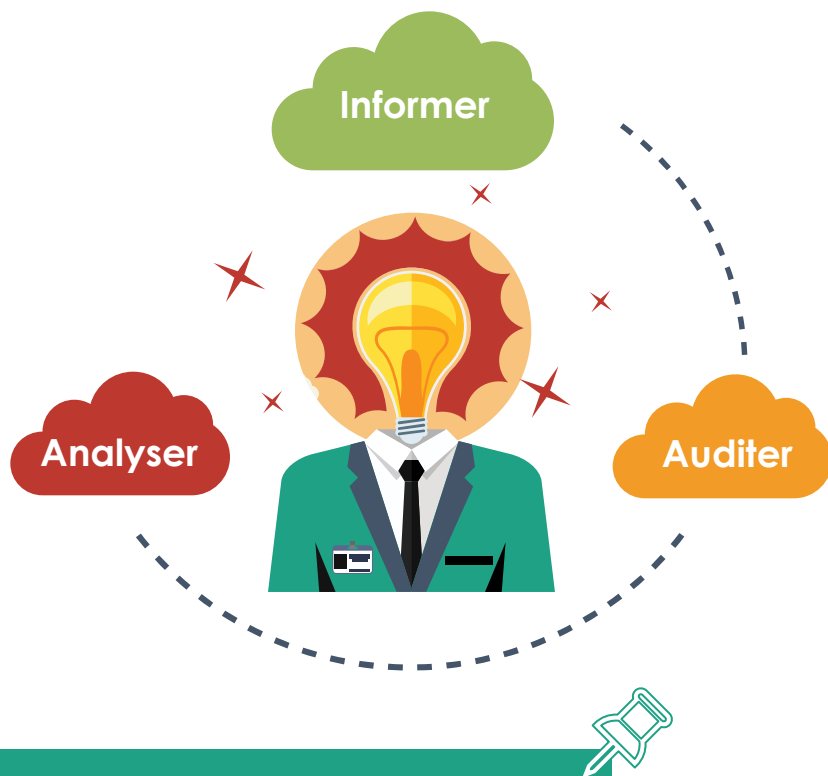


Dans le cadre du marché...



MISSION DPO

Un accompagnement resserré et à la demande



- DPO certifiés ou diplômés

Deux grands types d'intervention pour les DPO :

1. Le pilotage de la mise en conformité Accompagnement à la réalisation des actions préconisées dans les plans d'action

- Animation des réunions de suivi et de pilotage (2 minimum/an)
- Réalisation de certaines actions incombant au DPO

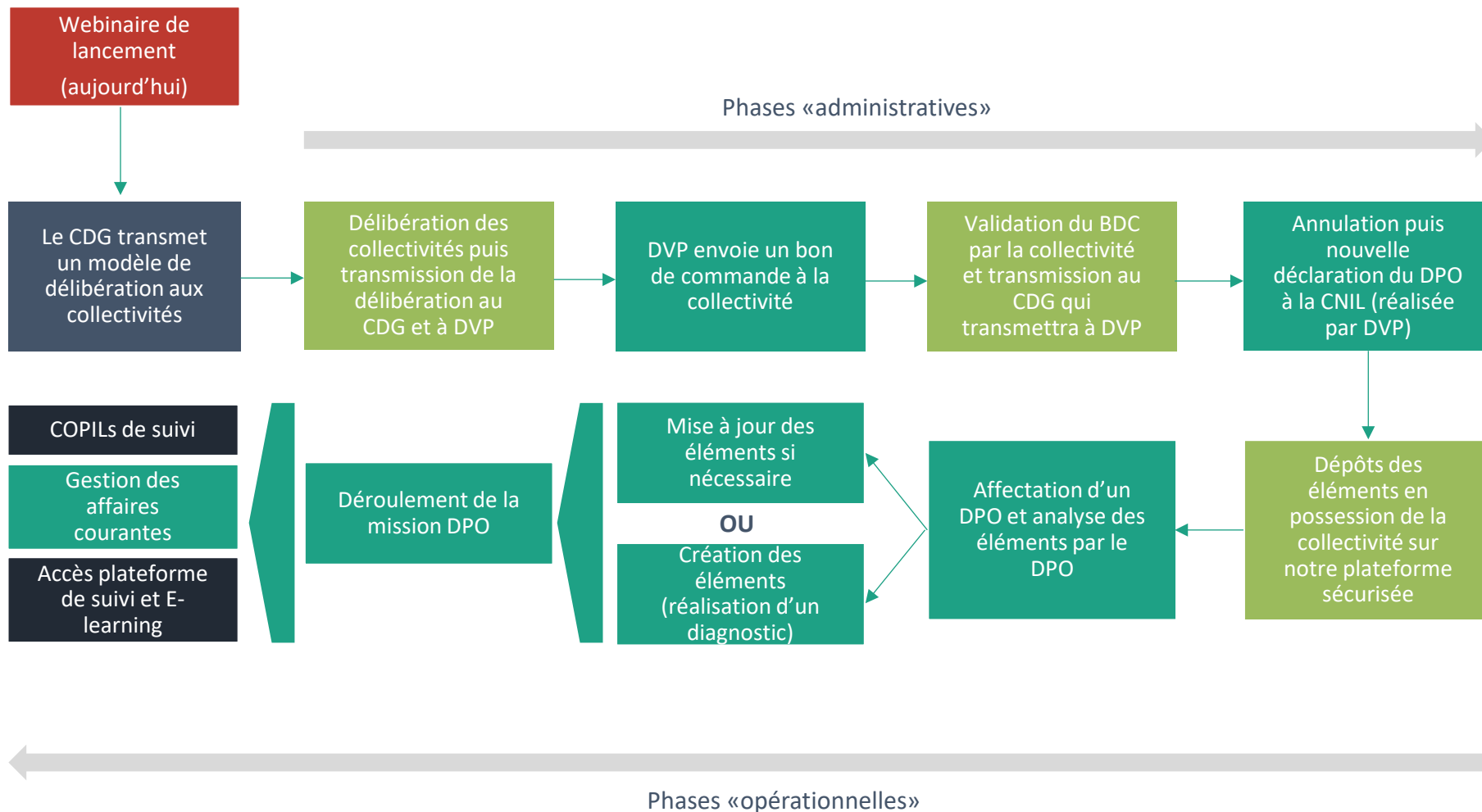
2. Assistante à la gestion des « affaires courantes »

- Tenue du registre des activités de traitement
- Assistance à la gestion des demandes de droits des personnes
- Suivi à mettre en œuvre en cas de violation de données
- Réponses aux questions posées par les collaborateurs de la structure
- Veille juridique
- ...

Les DPO seront mobilisables pour répondre à **toutes questions 5j/7**. Un accès à notre outil collaboratif pourra être mis en place.

Mise à disposition aux clients le désirant d'un espace dédié sur notre outil de gestion de projet incluant une plateforme d'E-learning

Et la suite...



Des questions ?



DATAVIGI
PROTECTION
SÉCURITÉ ET CONFORMITÉ RGPD

