RGPD

Guide de mise en route pour protéger les données personnelles de votre structure

Dernière modification le 23.05.18
Version 137

FNOGEC

Vers une culture de la protection des données personnelles

Le Règlement Général sur la Protection des Données (RGPD) entre en vigueur le 25 mai 2018. Les établissements scolaires et les structures territoriales de l'Enseignement catholique sont concernés et doivent se mettre en conformité avec ce dispositif d'extension de la loi Informatique & libertés de 1978.

S'appuyant sur les principes de base de la protection des données personnelles, ce nouveau règlement fait passer les organisations d'une logique déclarative à une démarche proactive et responsable. L'opportunité de bâtir une culture de la protection des données et de la sécurité informatique dans nos établissements.

Ce document a pour objectif de vous donner une méthode, permettant de mettre en œuvre cette nouvelle réglementation dans votre structure. Ce document n'est pas définitif et est susceptible d'évoluer. En effet, d'une part, les ressources documentaires proposées par la Commission nationale de l'informatique et des libertés (CNIL) s'enrichissent régulièrement, d'autre part, vos différents retours nous permettront d'améliorer la démarche proposée. Par conséquent, nous vous conseillons de vérifier de temps en temps qu'une nouvelle version de ce guide n'est pas présente.

Par ailleurs, ce document ne se substitue pas aux ressources officielles communiquées par la CNIL mais permet de décrypter ou démystifier certains dispositifs, au regard de notre secteur d'activité.

• POURQUOI UN NOUVEAU REGLEMENT SUR LA PROTECTION DES DONNEES ?

UNE OBLIGATION DE S'ADAPTER AUX NOUVEAUX ENJEUX DU NUMERIQUE

Face à la numérisation croissante de notre société, nos données personnelles ont pris de plus en plus de valeur et peuvent faire l'objet de dérives (réseaux sociaux) ou de menaces (cybercriminalité).

C'est pourquoi il était nécessaire de réaffirmer l'importance de la vie privée (art. 9 du Code Civil) et de sa protection dans une nouvelle dynamique de sensibilisation collective.

Le RGPD favorise ainsi l'harmonisation au niveau européen des règles applicables à la protection des données.

REAFFIRMER LES FONDAMENTAUX DE LA PROTECTION DES DONNEES

La loi Informatique & Libertés (1978) porte sur la préservation de la sécurité des données personnelles, s'appuyant sur **5 principes fondamentaux qui restent d'actualité** :

- **Finalité** : la collecte et le traitement de données personnelles suivent-ils un objectif connu, légitime et licite ? Ce principe évite la réutilisation à l'infini de données ou le "clonage" de fichiers.
- **Pertinence** : Collecter uniquement les données nécessaires aux objectifs à atteindre (principe de minimisation).
- **Conservation** : Définir les modalités de suppression.
- **Droits** (accès, rectification, opposition, oubli) : informer à priori les usagers de leurs droits.
- **Sécurité** : Assurer la confidentialité des données, notamment par la sécurisation des moyens de stockage et d'accès.

Le Règlement Général sur la Protection des Données (RGPD) réaffirme au niveau européen l'importance fondamentale de ces principes, dans la continuité de cette loi de 1978.

LES NOUVEAUX OUTILS DE LA CONFORMITE

Le RGPD permet de relire ces principes fondamentaux à la lumière d'un nouvel environnement de travail selon 6 axes de conformité.

- **Un transfert de responsabilité** : L'utilisateur final reste propriétaire des données. Avant le RGPD, la loi I&L de 1978 exigeait une déclaration préalable à la CNIL pour tout traitement de fichiers. Aujourd'hui, la déclaration préalable n'est plus obligatoire. Mais l'utilisateur doit désormais documenter en interne un registre de traitement pour prouver le respect de la protection des données en cas de contrôle de la CNIL.
- **La portabilité des données** : Tout doit être mis en œuvre pour permettre aux usagers de récupérer facilement leurs données (fichiers administratifs, bulletins de notes...) quand ils le jugent nécessaire. Ce qui pose la question de la durée légale de conservation des données.
- **Le design de la protection des données** : Lors de la conception d'un nouveau projet qui intègre une collecte et des traitements de données (un voyage scolaire, un développement informatique...), il faut mesurer les risques liés à leur sécurité (privacy by design) et faire en sorte que les paramétrages soient par défaut les plus protecteurs de la vie privée (privacy by default).
- **Un consentement préalable** : Il faut informer les usagers des finalités de la collecte et recueillir expressément leur accord en amont du traitement (opt-in) et non plus uniquement par droit d'opposition (opt-out). La règle du "qui ne dit mot consent" ne s'applique pas en la matière.
- **Un référentiel pour analyser les risques** : Inspirée des logiciels de la CNIL (Privacy Impact Assessment) pour analyser les risques liés aux données personnelles dans une organisation métier, la Fnogec a développé un référentiel de mise en conformité spécifique à nos établissements dans l'application Pilotage.
- **Une responsabilité partagée avec les sous-traitants** : Les sous-traitants sont soumis aux mêmes règles de protection des données que l'organisation pour laquelle ils travaillent et qui est propriétaire des fichiers. Exemple : prestataire de paie, agence informatique... Les contrats doivent être amendées dans ce sens avec des clauses spécifiques.

Le RGPD n'est donc pas une préconisation de solutions techniques mais un référentiel de ce qui est attendu en matière de protection des données à caractère personnel.

Le non-respect de ces règles peut donner lieu à des sanctions par la CNIL qui reste l'autorité de contrôle.

• EN QUOI NOS ETABLISSEMENTS SONT-ILS CONCERNES ?

Toutes les organisations qui collectent et traitent des données à caractère personnel, quelle que soit leur taille, sont concernées.

QU'EST-CE QU'UNE DONNEE A CARACTERE PERSONNEL ?

Toute donnée qui permet l'identification directe et indirecte d'une personne (nom, prénom, date de naissance, adresse, coordonnées téléphoniques, électroniques ou bancaires, n° SS, données de santé, données de géolocalisation, images, adresse IP & cookies, immatriculation…) est une donnée personnelle.

QU'EST-CE QU'UN TRAITEMENT DE DONNEES ?

La protection joue dès lors qu'il y a traitement de données par moyen électronique ou sous forme papier, quel qu'en soit le stade :

- **La collecte**, c'est-à-dire la récupération des données personnelles. Elle doit être faite exclusivement auprès des personnes concernées, avec leur accord préalable, et ce même si les données sont fournies par un partenaire (ex : les noms des parents transmis par l'Ogec à l'Apel). Elle peut être effectuée par le biais d'une fiche de renseignements, d'un bordereau d'inscription, d'un formulaire sur un site internet, par exemple.
- **L'enregistrement** : Une fois les données collectées, l'action de les enregistrer dans une base de données, électronique ou non, est un traitement de données.
- **La conservation** : Dès le stockage d'une donnée personnelle, il est nécessaire de définir la durée de conservation. En effet, il n'est pas utile de garder les données personnelles en dehors de la durée de leurs traitements. Cela accroît le risque de perte ou de violation de données.
- **La communication**, le transfert et l'interconnexion : L'exportation de données personnelles est soumise au RGPD. Il n'est pas autorisé de transférer les données sans autorisation explicite des personnes concernées.

LE DEBUT D'UN PROCESSUS TENDU VERS LE 100% DE CONFORMITE

Son entrée en application est fixée au 25 mai 2018. Il s'agit moins d'une date couperet que le point d'étape d'une dynamique d'amélioration continue.

Extrait du site de la CNIL :

Dans les premiers mois de mise en œuvre du RGPD, la CNIL distinguera lors de ses contrôles deux types d'obligations s'imposant aux professionnels.

***Les principes fondamentaux** de la protection des données restent pour l'essentiel inchangés (loyauté du traitement, pertinence des données, durée de conservation, sécurité des données, etc.). Ils continueront donc à faire l'objet de vérifications rigoureuses par la CNIL.*

*En revanche, pour ce qui est **des nouvelles obligations ou des nouveaux droits résultant du RGPD** (droit à la portabilité, analyses d'impact, etc.), les contrôles opérés auront essentiellement pour but, dans un premier temps, d'accompagner les organismes dans une courbe d'apprentissage vers une bonne compréhension et la mise en œuvre opérationnelle des textes.*

Au-delà de la réglementation stricte (assurer la protection des données et en prouver la matérialité, documenter le suivi), c'est l'opportunité pour nos établissements de :

- Questionner la politique en matière de données personnelles ;
- Responsabiliser davantage les acteurs à tous les niveaux impliqués dans des traitements ;
- Auditer la sécurité des systèmes d'information.

• COMMENT PASSER A L'ACTION ?

Afin de protéger les données à caractère personnel de votre structure, nous vous proposons UNE méthode, basée sur notre expérience de mise en place du RGPD au sein de vos instances nationales (en lien avec un cabinet spécialisé) et sur les recommandations de la CNIL.

Cette méthode est actuellement visible sur votre plateforme d'aide à la gestion : Isidoor, au travers de l'application Pilotage.

Les chefs d'établissement ainsi que les directeurs diocésains sont en mesure de se connecter directement à la plateforme Isidoor avec leur identifiant Gabriel; les présidents d'Ogec peuvent demander leur code d'accès à leur Udogec ou Urogec.

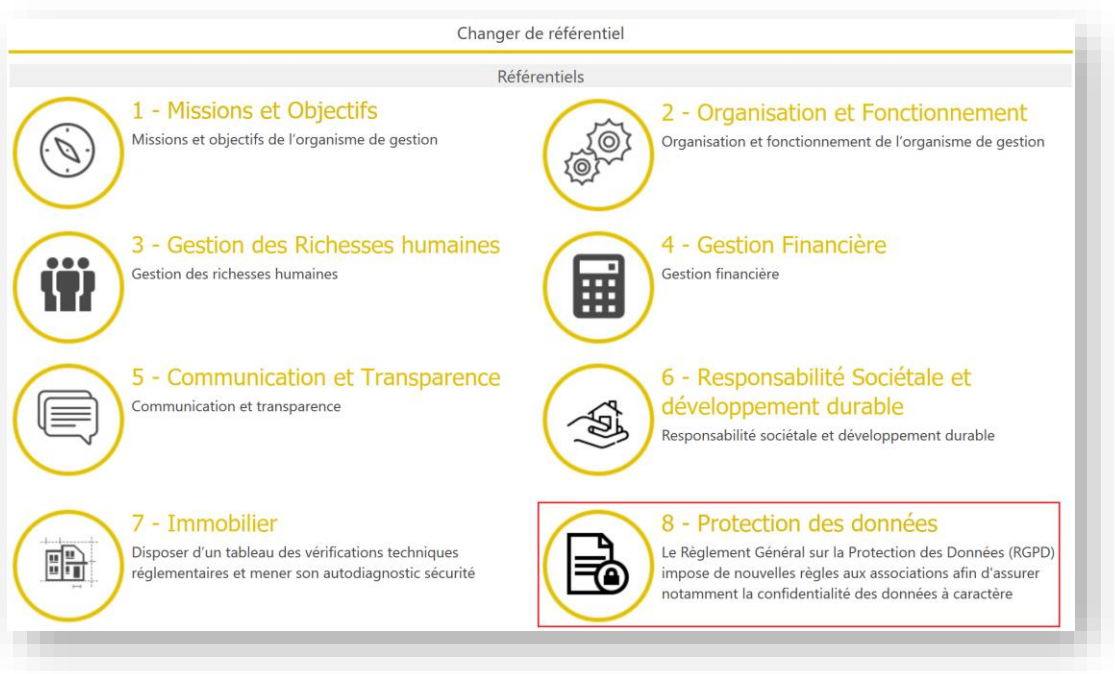
Si vous êtes salarié d'un Ogec, vous pouvez obtenir votre code d'accès à Isidoor auprès de votre chef d'établissement.

Un tutoriel est disponible sur l'espace documentaire d'Isidoor, sous la forme d'une vidéo de moins d'une minute pour expliquer la démarche de gestion des accès Isidoor pour votre structure.

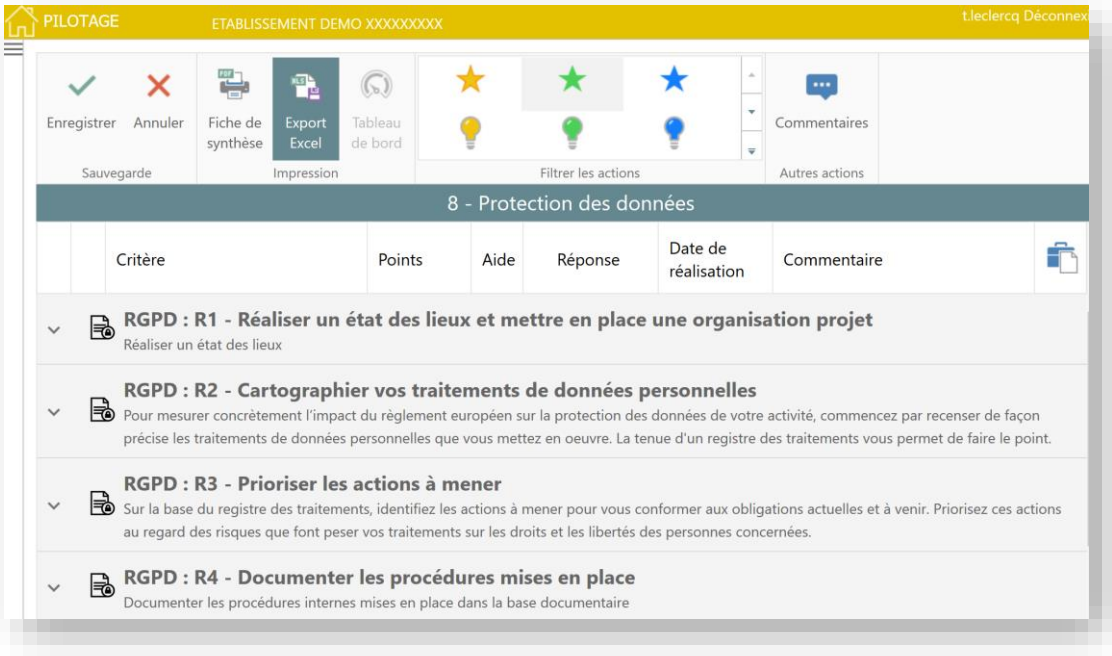
SUIVRE LE PLAN D'ACTION :

Une fois dans l'application Pilotage, cliquez sur le menu « **Indiquez les objectifs réalisés** » :

Plusieurs référentiels apparaîtront, choisissez celui intitulé « **Protection des données** » :



Les étapes de mise en place du RGPD apparaissent au début du référentiel selon cette progression :



1 - Par défaut, toutes les actions à réaliser obligatoirement apparaîtront et il suffit de les réaliser pas à pas. Ces actions obligatoires sont symbolisées par ★.

Quand un grand nombre d' ★ apparaît, cela signifie que l'action est importante.

Plus tard, quand vous aurez terminé de réaliser chaque action obligatoire, vous pourrez découvrir d'autres actions plus avancées (★ puis ★), mais également des bonnes pratiques en matière de sécurité de vos données (💡)

Pour résumer :

★ L'étoile concerne les **réglementations,**

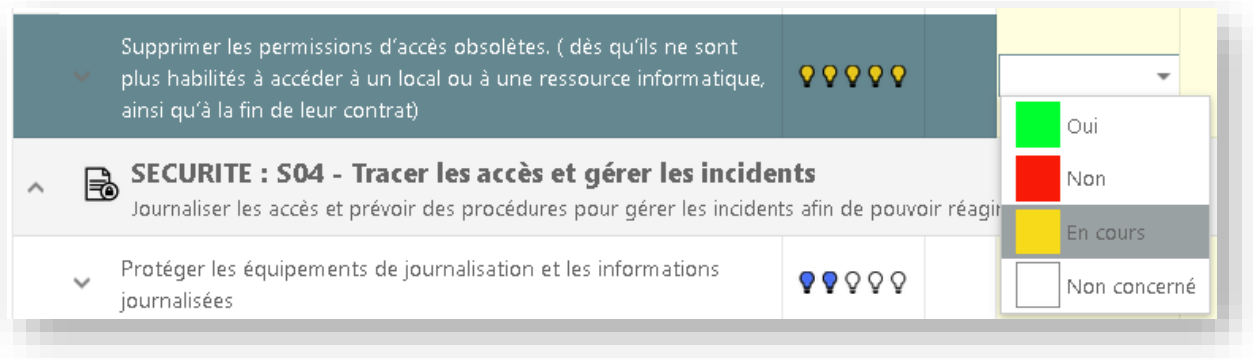
💡 L'ampoule concerne les bonnes **pratiques**.

Vous pouvez filtrer ces actions en cliquant sur l'icône correspondante dans le menu ***Filtrer les actions*** :

2 - Pour chaque action à mener, vous aurez souvent le symbole vous indiquant qu'une explication est apportée pour réaliser cette action.

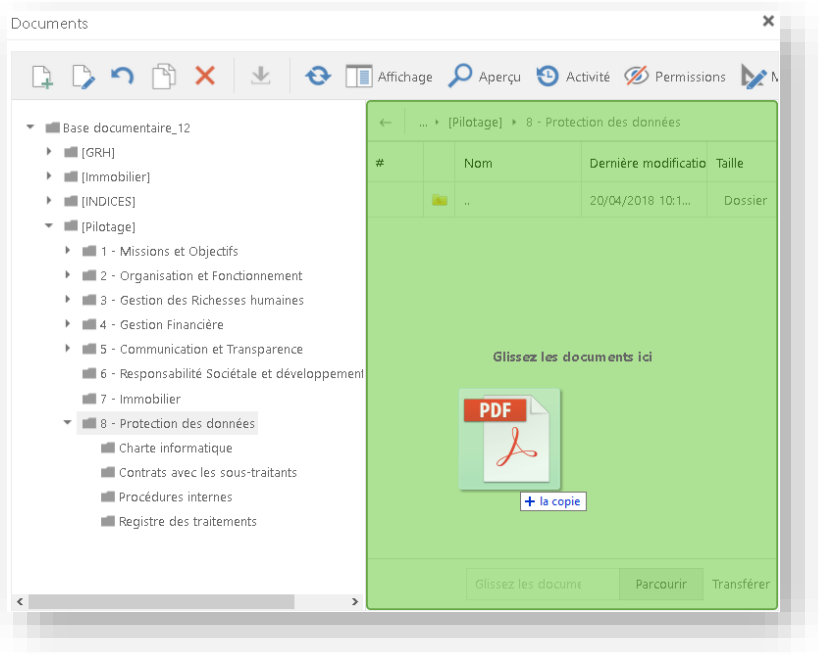
Ce symbole peut également vous renvoyer vers un modèle de document ou un lien vers un site internet de référence (Site de la Cnil, ...).

3 - Vous pouvez indiquer l'état de votre avancement en renseignant la colonne **Réponse** :



4 - Vous pouvez également indiquer un commentaire dans la colonne correspondante.

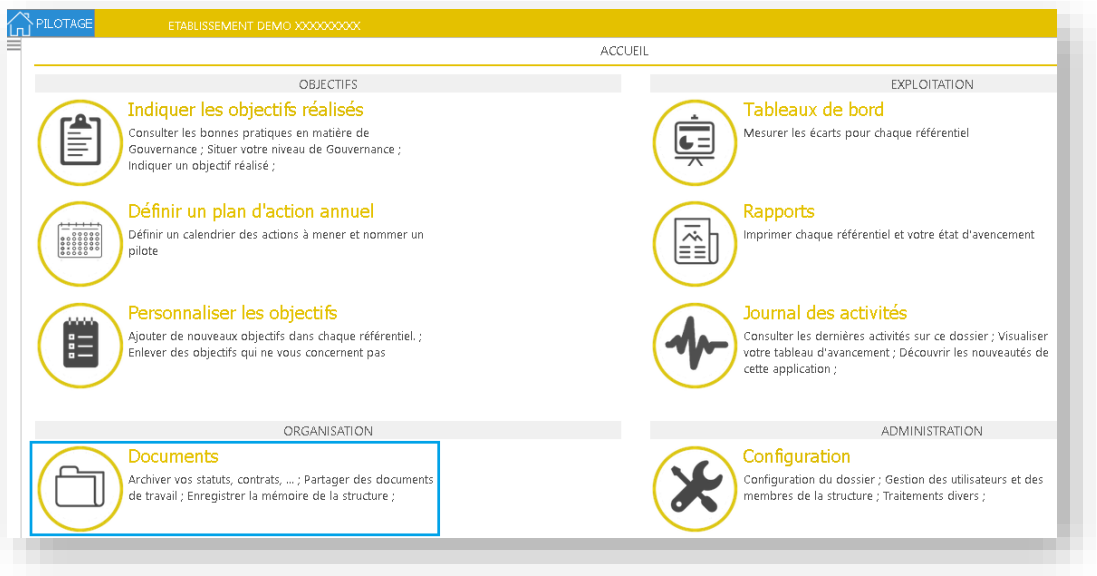
5 - En cas d'achèvement d'une action, vous pouvez, si c'est possible déposer le document qui prouve que cette action a été réalisée dans une base documentaire spécifique  . Nous vous rappelons que c'est un fondement essentiel du RGPD de prouver que vous respectez bien la réglementation :



N'oubliez pas d'enregistrer vos modifications lorsque vous avez terminé :

LA BASE DOCUMENTAIRE :

Vous pouvez également gérer/consulter le contenu de votre base documentaire en cliquant sur le menu **Documents** de la page d'accueil :

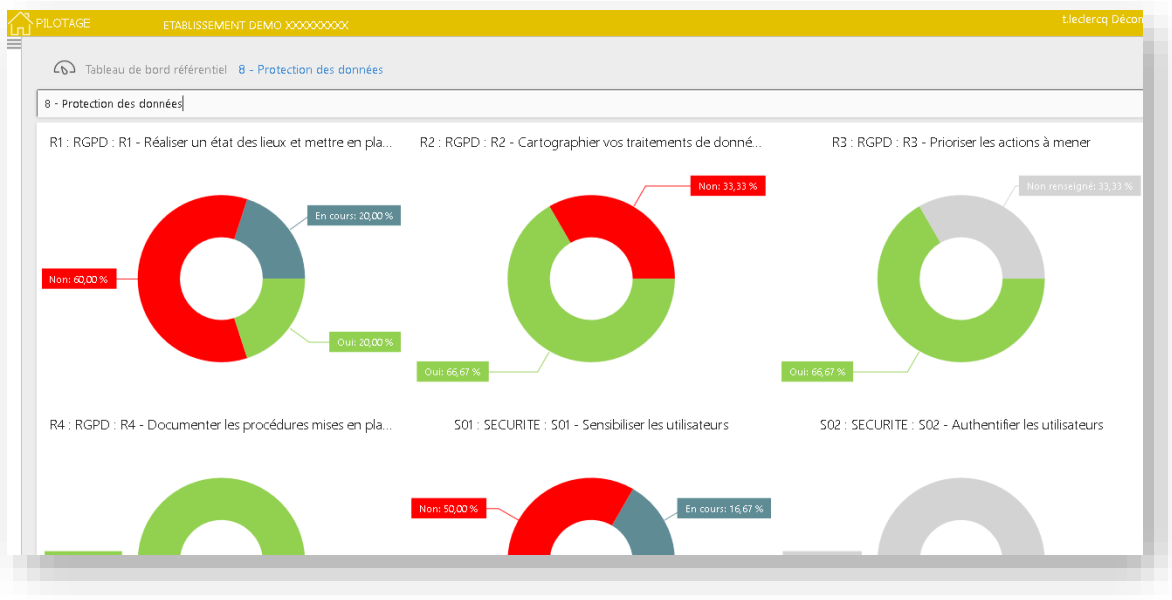


TABLEAUX DE BORD :

Enfin, afin d'avoir une vision générale de votre progression sur le référentiel RGPD à des fins d'autodiagnostic, plusieurs tableaux de bord ont été mis en place. Ils sont accessibles sur la page d'accueil de l'application Pilotage en cliquant sur le menu **Tableaux de bord** :

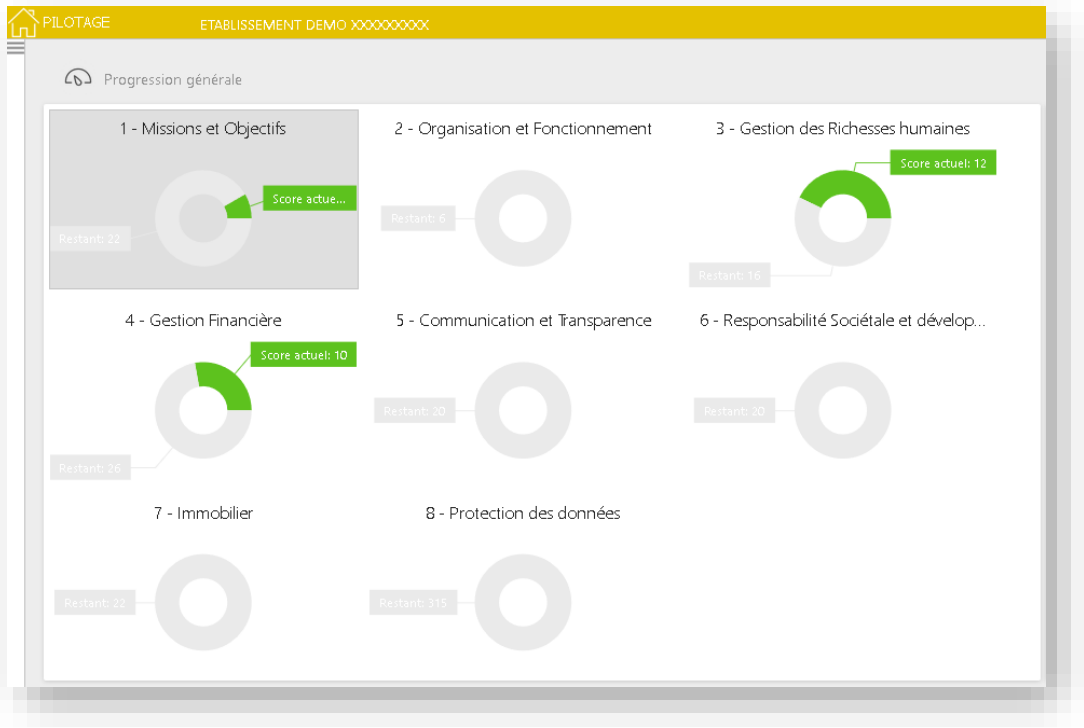
Un tableau de bord du référentiel :

Pour chaque référentiel, les catégories de données sont restituées graphiquement afin d'avoir une idée précise de l'avancement par thème :



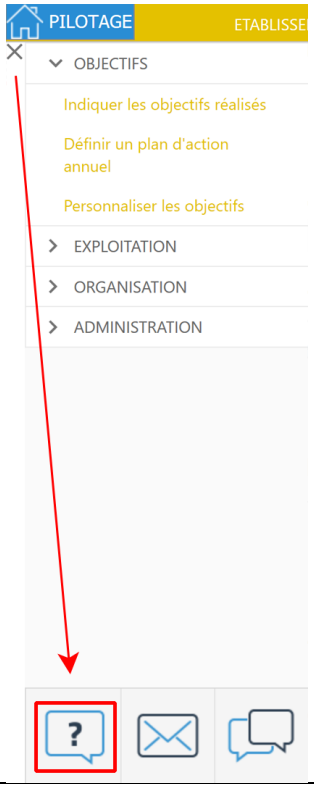
Un tableau de bord de tous les référentiels :

Comme la capture d'écran le montre, la progression de l'ensemble des référentiels est consolidée dans un tableau dans lequel chaque tâche réalisée apparait en vert.



NOUS CONTACTER :

Pour obtenir des informations sur l'utilisation de l'application Pilotage, vous pouvez consulter la documentation en ligne en cliquant sur :

1. Ouvrez le panneau latéral	2. Cliquez sur l'icône « Aide » :
	

Vous pouvez également nous envoyer des demandes à l'adresse **rgpd@isidoor.org**