RGPD

Règlement général sur la protection des données

Présentation

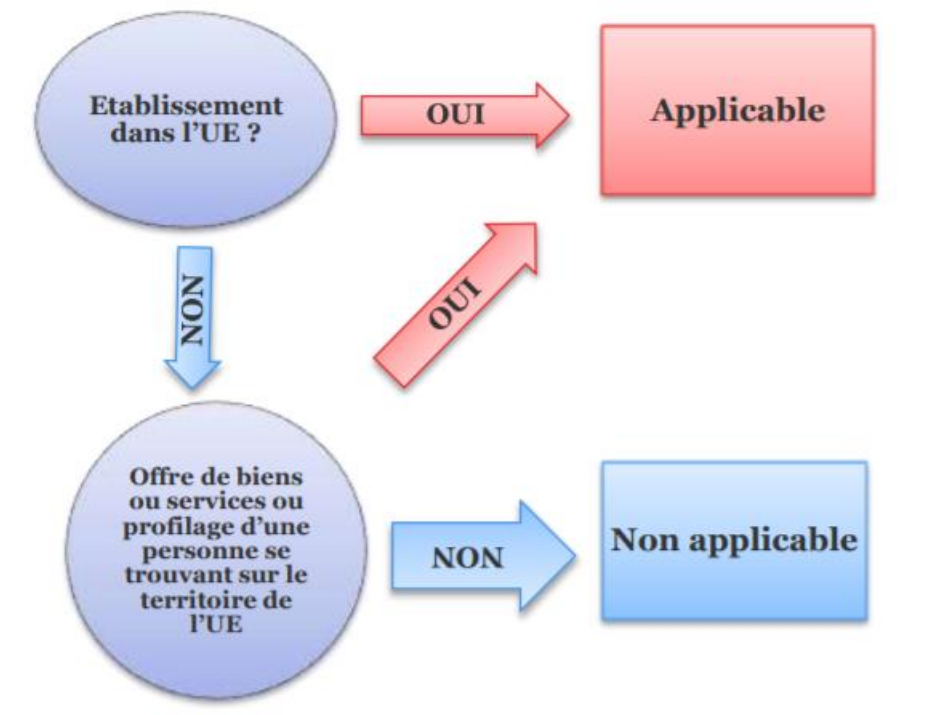
Qu'est-ce que le RGPD ?

- Règlement européen adopté le 14 avril 2016 et entrant en application le 25 mai 2018.
- Modifie et unifie les lois en matière de protection des données personnelles.
- Apporte un caractère **obligatoire** au respect de ces nouvelles normes.
- Renforce le pouvoir de sanction de la CNIL.

Champ d'application du RGPD

Qui est concerné par le RGPD ?

- Critère d'établissement : tout établissement effectuant des traitements de données personnelles et situé sur le territoire de l'UE.
- Critère du ciblage : tout établissement traitant des données personnelles concernant des résidents de l'UE afin de leur faire une offre de services ou de biens.



Les 6 règles d'or de la protection de données

Licéité
- Le traitement est-il licite ?
- Recueil de consentement, contrat, intérêt public, obligations légales…

Finalité
- Dans quel(s) but(s) les données sont-elles collectées/utilisées ?

Minimisation
- Pertinence et proportionnalité des données
- Sont-elles toutes indispensables ?

Durée de conservation
- Les durées sont-elles optimales et en adéquation avec les préconisations légales ?

Intégrité et confidentialité
- Obligation de sécurité, les mesures de sécurité sont-elles suffisantes ?

Droits des personnes
- Les procédures sont-elles conformes aux nouvelles normes pour faciliter et répondre aux demandes d'exercice des droits (modification, suppression, portabilité…)

Principe général et obligations

Nommer un DPO (ou DPD)

- Obligatoire pour tout établissement public
- Conseille et pilote les démarches de mise en conformité
- Peut être mutualisé

Registre des traitements

- Liste des traitements de données personnelles mis en œuvre par la collectivité
- Document obligatoire et central pour la conformité

Mise à jour des procédures

- Révision des contrats de sous-traitance
- Procédure en cas de violation de données
- Règles de bonnes pratiques, charte informatique

Principe général et obligations

Analyses d'impacts et analyses des risques

- Principe de privacy by design (protection de la vie privée dès la conception du traitement)
- Les traitements à risques doivent faire l'objet d'une étude d'impact
- Obligation d'analyser les risques et de déterminer des mesures correctives AVANT la mise en œuvre du traitement

Conformité permanente et dynamique

- Principe d'accountability (nécessité de rendre compte)
- Nécessité de pouvoir prouver à tout moment son implication dans la protection de données personnelles
- Documentation systématique des actions et décisions au regard du RGPD

L’offre du CDG 54 via le CDG 52

DPO (data protection officer) **mutualisé**

- Mise à disposition du DPO mutualisé du CDG 54.
- Accompagne les collectivités dans leur démarche de mise en conformité.

Questionnaire d’audit

- Le DPO mutualisé fournit à la collectivité un lien vers un questionnaire d’audit recensant les traitements de données personnelles mis en œuvre.
- Les réponses saisies par la collectivité servent de base essentielle à toute la démarche (autodiagnostic)

Création du registre des traitements

- Le DPO mutualisé crée le registre des traitements de la collectivité après récupération des réponses au questionnaire.
- Le DPO mutualisé analyse le registre et dispense les premières préconisations.

L'offre du CDG 54 via le CDG 52

Analyses d'impacts

- Le DPO mutualisé identifie les traitements nécessitant des analyses d'impacts.
- Les collectivités bénéficiant de leur registre des traitements avant le 25 mai 2018 disposent d'un délai de **3 ans pour réaliser les analyses d'impacts.**

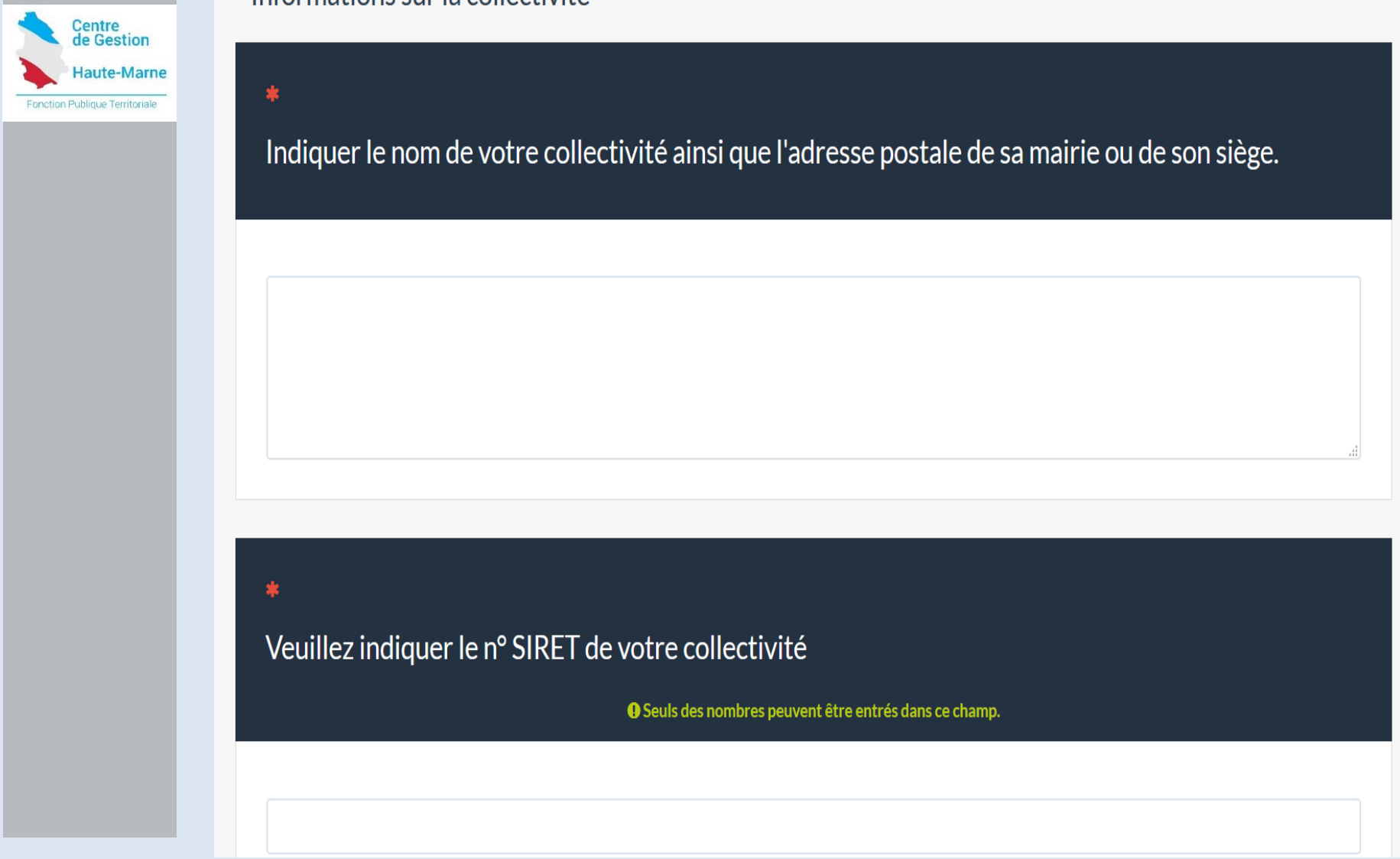
Extranet en ligne

- La collectivité reçoit un accès sécurisé à un extranet créé spécifiquement.
- L'extranet regroupe les documents importants de la conformité RGPD ainsi qu'une **base documentaire d'informations utiles à la compréhension des enjeux de la protection de données.**

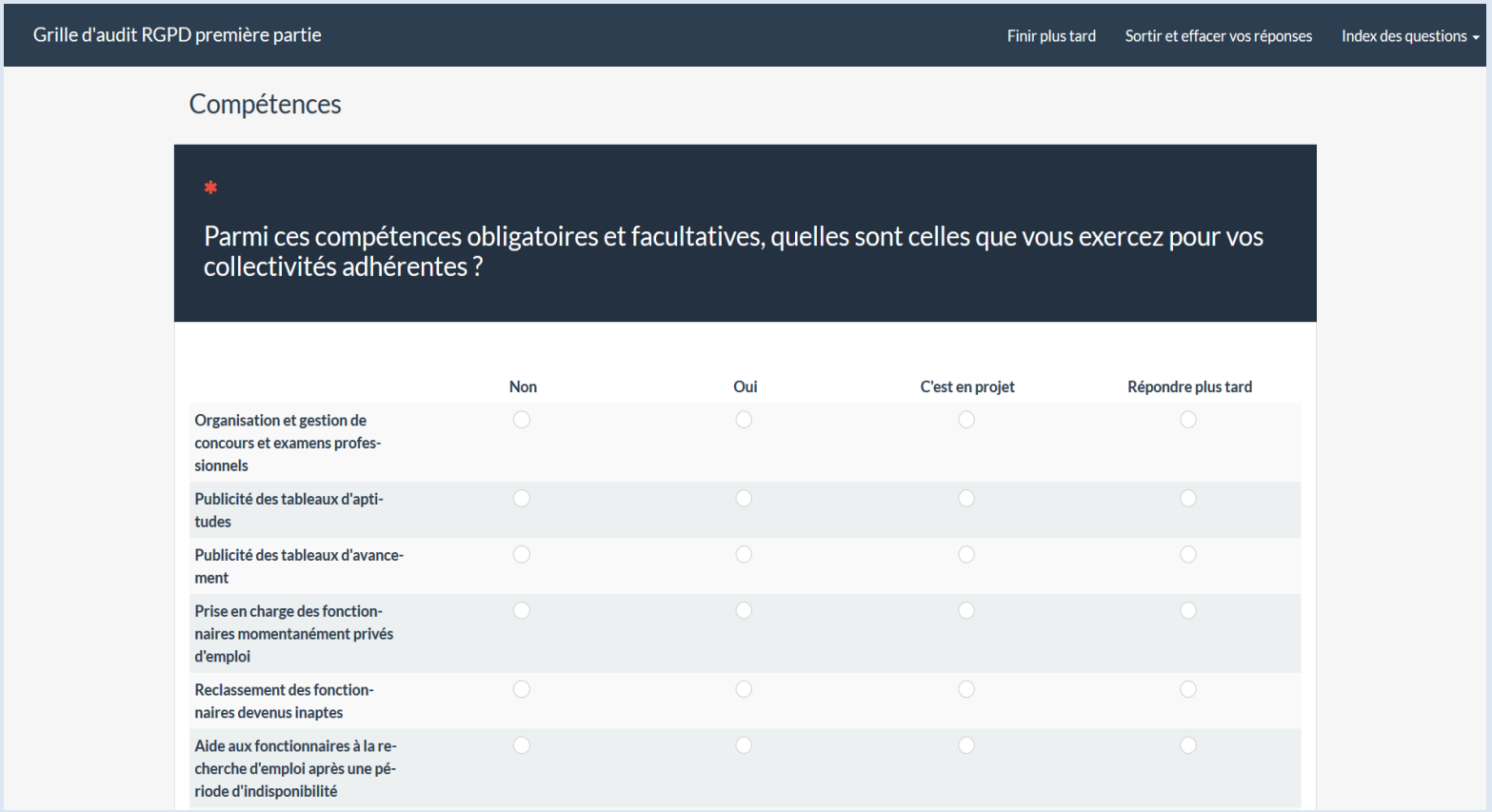
Pilotage de la mise en conformité

- Le DPO mutualisé propose **un plan d'action** annuel adapté à la collectivité, en fonction des soucis de conformité identifiés.
- Un formulaire de contact en ligne est disponible tout au long de la mission afin de répondre aux questions des collectivités.

Captures d’écran : questionnaire d’audit



Captures d’écran : questionnaire d’audit



Captures d'écran : questionnaire d'audit

Quels sont les **destinataires** de ces données ?

Ajoutez un commentaire seulement si vous sélectionnez la réponse.

- [ ] Tous les agents de la collectivité
- [ ] Un ou plusieurs agent(s)/service(s) en particulier de la collectivité
- [ ] Un sous-traitant
- [ ] Un établissement/entreprise/association (public ou privé) effectuant pour son propre compte des traitements sur ces données
- [ ] Destinataire(s) hors UE

Pour chaque case cochée, merci d'inscrire les détails dans la zone de commentaire correspondante (par exemple si le destinataire est le service ressources humaines de votre collectivité, cochez la case "un ou plusieurs agent(s)/service(s) en particulier" et inscrivez "ressources humaines" en commentaires).

Veillez à ne pas donner de noms d'agents en particulier, identifiez simplement leur fonction.

Est considéré comme sous-traitant tout établissement ou entreprise réalisant pour vous certains traitements basés sur les données que vous lui fournissez (analyse statistique, gestion de la paie, hébergement des données...).

*

Quelle(s) catégorie(s) de personnes sont **concernées** par les données traitées ?

Captures d'écran : questionnaire d'audit

*

Exploitez vous des **fichiers de données personnelles liées aux RESSOURCES HUMAINES et MATERIELLES de votre collectivité ?**

	Non	Oui	C'est en projet
Gestion interne (administrative, financière, carrière...) des agents	○	○	○
Gestion de la paie	○	○	○
Géolocalisation des véhicules	○	○	○
Suivi d'activité et contrôle des horaires/temps de travail des agents par un système de badges/pointeuse	○	○	○
Contrôle des accès (locaux, salles, annexes, archives...) par un système de badges, code d'accès ou reconnaissance biométrique	○	○	○
Ecoute/enregistrement des conversations téléphoniques sur le lieu de travail	○	○	○
Recrutement	○	○	○
Comité d'établissement (CNAS, CE...)	○	○	○
Gestion des comptes personnels de formation	○	○	○
Remboursement de frais	○	○	○

Captures d'écran : questionnaire d'audit

*

Possédez-vous des **LISTES** (sous format papier ou numérique) de personnes appartenant à certaines catégories ?

	Non	Oui	C'est en projet
Liste des syndicats et de leurs membres	○	○	○
Listes des associations et de leurs membres	○	○	○
Liste des personnes d'un certain âge	○	○	○
Liste des personnes en difficultés (sociales, financières...)	○	○	○
Liste des personnes en situation de handicap	○	○	○
Liste des personnes bénéficiant de services sociaux	○	○	○
Liste de personnes condamnées par la justice	○	○	○

Captures d’écran : questionnaire d’audit

Logiciels installés sur vos ordinateurs (paie, gestion interne...)	○	○	○
Logiciels en ligne	○	○	○
Contrôle d'activité des agents (historiques, logs...)	○	○	○
Autre(s)	○	○	○

Cochez "oui" pour tous les traitements de données listés que votre collectivité exploite et qui comportent des données à caractère personnel.

Cochez "C'est en projet" si vous avez en projet de créer ce traitement de données personnelles au sein de votre collectivité durant l'année en cours.

*

Comment sont hébergées les données du Système d'Information ?

Veuillez sélectionner une réponse ci-dessous

- ○ Serveurs physiques en interne, dans les locaux de la collectivité
- ○ Serveurs physiques hébergés chez un prestataire
- ○ Données stockées sur le cloud

Captures d'écran : questionnaire d'audit

*

Exploitez vous des **fichiers de données personnelles liées à la SECURITÉ PUBLIQUE** de votre collectivité ?

	Non	Oui	C'est en projet
Conseil Local de Sécurité	○	○	○
Chiens dangereux	○	○	○
Système d'alerte des populations	○	○	○
Traitement des infractions pénales (stationnement, tabac, amendes…)	○	○	○
Vidéosurveillance de l'espace public	○	○	○
Registre des fourrières	○	○	○

Captures d'écran : questionnaire d'audit

*

Veuillez détailler quelles MESURES DE SECURITE techniques et organisationnelles sont mises en place au sein de votre collectivité afin de garantir la sécurité des données

	Non	Oui	C'est en projet
Locaux à accès contrôlé (badges, code d'accès...)			
Vidéo protection des locaux			
Ordinateurs verouillés par des sessions uniques (chaque utilisa-teur possède un identifiant et un mot de passe unique)			
Données numériques stockées sur des serveurs sécurisés			

L'offre du CDG 54 via le CDG 52

Le respect de la mise en œuvre de cette obligation

- **Pour toutes les collectivités, affiliées ou non**
- **Par simple convention tripartite : CDG 52, CDG 54, Collectivité**

L'optimisation de la mutualisation de cette mission entre CDG au profit des collectivités de la Haute-Marne

- **Mutualisation des coûts de conception des outils de travail (questionnaire, extranet dédié, analyse des réponses)**
- **Une adaptation de la mission et donc de son coût à la taille de la collectivité suivant le montant de sa masse salariale (aucun coût fixe pour les collectivités)**

L'optimisation de la mutualisation de cette mission entre CDG au profit des collectivités de la Haute-Marne

- **La garantie de disposer des compétences spécifiques en matière juridique et informatique; la mise à disposition de personnel dédié à cette mission**
- **Une étude et des préconisations suivant les réponses données au questionnaire d'état des lieux**