

RGPD

Règlement général sur la protection des
données

CDG 52

1^{er} juillet 2019

APRES MIDI



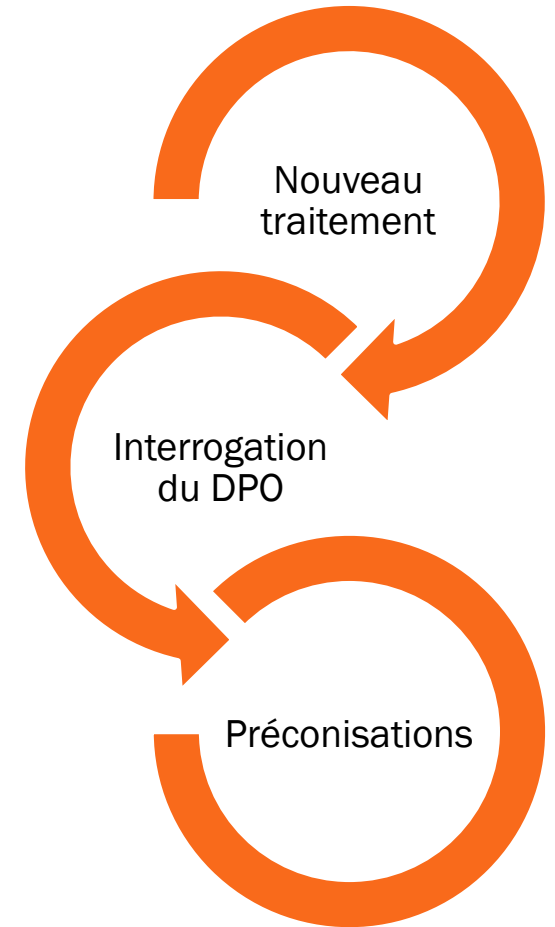
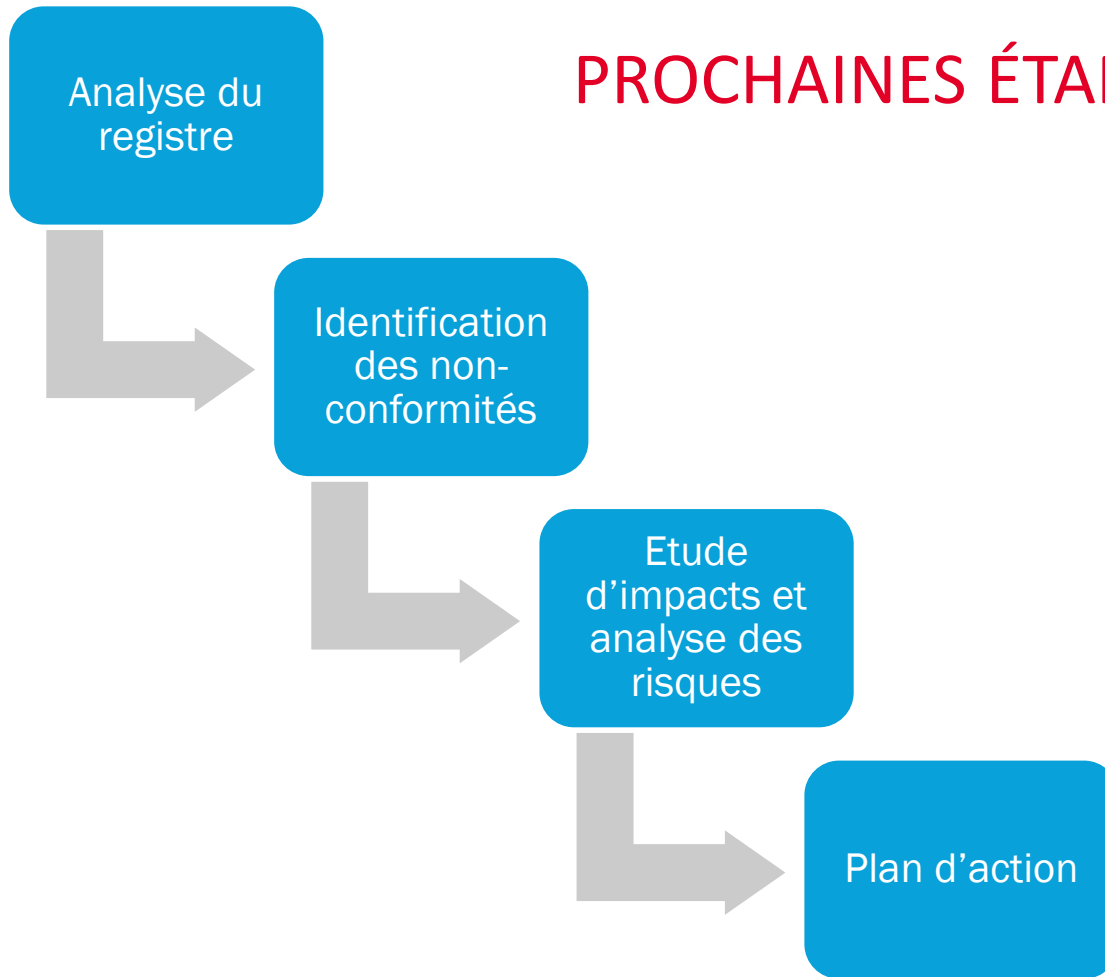
Sommaire

- **Introduction**
 - **Le RGPD : rappel des principes et obligations**
- **Accompagnement par la mission RGPD 54**
 - **Les grandes étapes**
 - **L'espace RGPD**
- **Préconisations**
 - **bonnes pratiques**
 - **procédures**
- **Temps d'échanges et réponses aux questions**

Qu'est-ce que le RGPD ?



PROCHAINES ÉTAPES



ESPACE RGPD

Formulaire de contact

- Saisir le service RGPD
- Poser les questions relatives à la protection des données

Base documentaire

- Modèles de mentions légales
- Formulaire-types

Documents de la conformité

- Registre des traitements
- Evolutions des traitements
- Echanges avec la CNIL



PRÉCONISATIONS GÉNÉRALES

Sensibilisation

- Chaque agent est acteur de la protection des données au quotidien
- Améliorer les pratiques professionnelles
- Concerne tous les services, pas simplement l'informatique

Privacy by design

- Réflexion en amont de la création d'un nouveau traitement
- Interrogation du DPO

Mentions légales

- Information des usagers
- Recueil de consentement

PRÉCONISATIONS GÉNÉRALES

Site internet

- Gestion des cookies
- Politique de protection des données

Purge des données obsolètes

- Durées légales de conservation
- Distinction entre base active et archivage

Anonymisation

- Savoir reconnaître les données personnelles nécessaires (CADA, loi Lemaire...)
- Anonymiser ou supprimer les données facultatives

PRÉCONISATIONS GÉNÉRALES

Marchés publics

- Clauses-types
- Minimiser les documents demandés

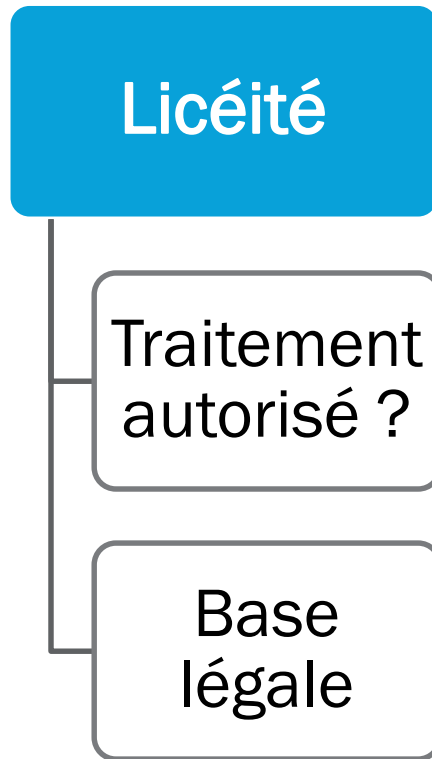
Procédures internes

- Réponse aux demandes des usagers
- Violation de données personnelles

Charte de bonnes pratiques

- Charte informatique
- Charte relative à la protection des données

PRIVACY BY DESIGN : Les 6 règles d'or de la protection des données



Formulaire d'inscription voyage communal

Nom :	Prénom(s) :
Date de naissance :	Téléphone :
Adresse :	

Pour l'inscription à un voyage, je n'ai ni base légale, ni intérêt public, donc, je devrai recueillir le consentement des personnes.

Ai-je une base légale (ou un intérêt public) m'autorisant à collecter ces données?

PRIVACY BY DESIGN : Les 6 règles d'or de la protection des données

Formulaire d'inscription voyage communal

Finalité

But du traitement

Définie au départ

Nom :	Prénom(s) :
Date de naissance :	Téléphone :
Adresse :	

J'indique le but du formulaire et je ne réutilise pas les données dans un autre but.



Utilisation de vos données personnelles

Les données recueillies sont nécessaires à la bonne inscription pour ce voyage. Elles sont destinées exclusivement au personnel organisateur du voyage. En aucun cas elles ne seront rendues accessibles à des tiers sans votre accord exprès le cas échéant.

Est-ce que j'utilise bien les données dans le but pour lequel je les ai récoltées ?

PRIVACY BY DESIGN : Les 6 règles d'or de la protection des données

Minimisation

Pertinence

Proportionnalité

Formulaire d'inscription voyage communal

Nom :	Prénom(s) :
Date de naissance :	Téléphone :
Adresse :	

Numéro de sécurité sociale :

Profession :

Pour ce type de formulaire, le recueil de certaines données n'est pas indispensable, voire interdit (numéro Sécu).

Est-ce que toutes les données que je récolte sont indispensables ?

PRIVACY BY DESIGN : Les 6 règles d'or de la protection des données

Formulaire d'inscription voyage communal du 15 novembre 2019

Nom :	Prénom(s) :
Date de naissance :	Téléphone :
Adresse :	

Utilisation de vos données personnelles

Les données recueillies sont nécessaires à la bonne inscription pour ce voyage. Elles sont destinées exclusivement au personnel organisateur du voyage. En aucun cas elles ne seront rendues accessibles à des tiers sans votre accord exprès le cas échéant.

Ces données seront supprimées une fois le voyage effectué.

Dès que le voyage est terminé, je supprime les données car je n'en ai plus l'utilité.

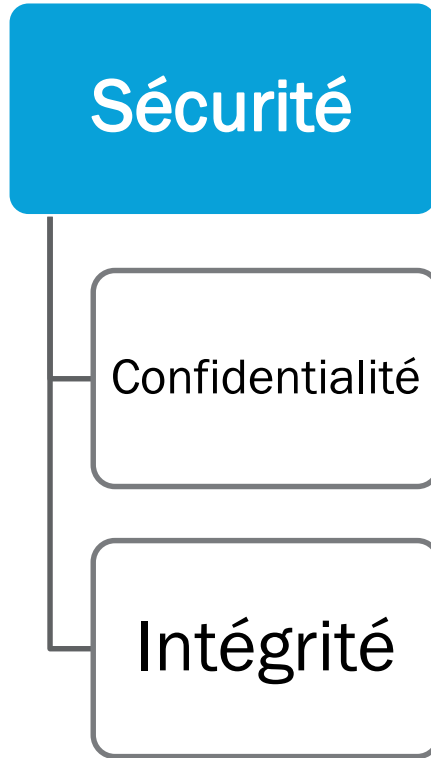
Conservation

Durées
légales

Archivage

Est-ce que j'ai encore besoin des données stockées ?

PRIVACY BY DESIGN : Les 6 règles d'or de la protection des données



Je m'assure que les données collectées dans le formulaire soient stockées et transmises de manière sécurisée.



Est-ce que j'ai correctement stocké ou transmis les données collectées ?

PRIVACY BY DESIGN : Les 6 règles d'or de la protection des

Droit des personnes

Information

Respect

Utilisation de vos données personnelles

Vos droits

Conformément à la Loi Informatique et Libertés ainsi qu'aux dispositions du Règlement Général sur la Protection des Données (RGPD), vous bénéficiez :

- **d'un droit d'accès, de rectification ou de suppression des informations vous concernant**
- **du droit à la portabilité de vos données**
- **du droit à la limitation d'un traitement vous concernant**
- **du droit, pour motifs légitimes de vous opposer à ce que vos données fassent l'objet d'un traitement**

Tout exercice de ces droits peut s'effectuer sur simple demande en vous adressant à [adresse mail ou postale du service en charge du traitement de ces demandes]. Un justificatif d'identité sera requis pour toute demande d'exercice de droit.

Pour aller plus loin

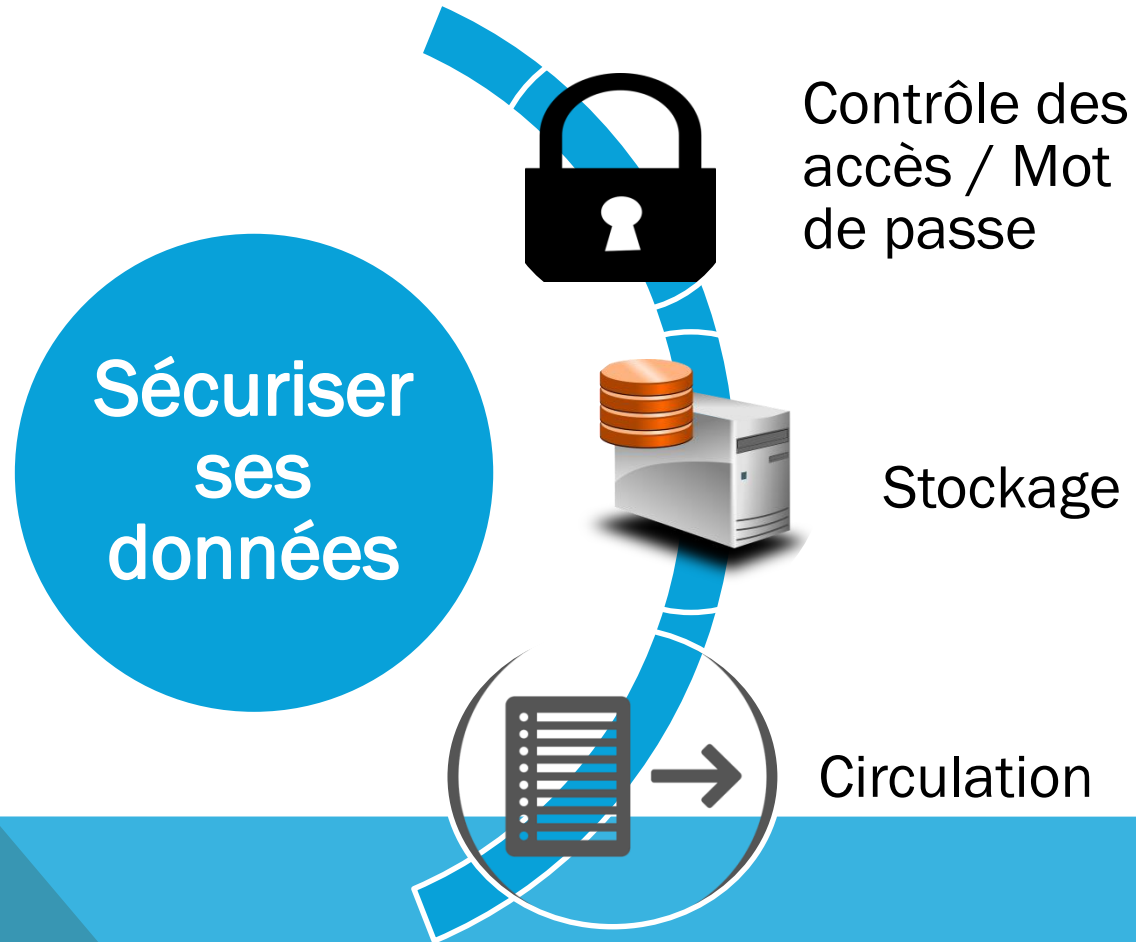
Si vous souhaitez plus d'informations sur la protection des données personnelles et vos droits en la matière, vous pouvez :

- consulter le site de la CNIL : <https://www.cnil.fr/>
- contacter le Délégué à la Protection des Données de la collectivité : <https://www.agirhe.cdg54.fr/TDB/rgpd.aspx>

Bien veiller à informer les personnes de leurs droits dans le formulaire.

Est-ce que j'ai bien informé des personnes de leurs droits ?

SECURISER SES DONNEES



INFORMER



Informer ses agents



Informer ses usagers



Transparence

PROCÉDURE : NOTIFICATION D'UNE VIOLATION DE DONNÉES

Etape 1 : dès le constat de la violation (piratage, virus, faille de sécurité, erreur humaine, intrusion dans les locaux...) **informer immédiatement son référent et le DPO.**

Etape 2 : le DPO remplit la **notification initiale auprès de la CNIL** (délai maximum de 72h après le constat) et contacte le référent pour toute information complémentaire.

Etape 3 : enquête interne pour **définir précisément les causes de la violation** ainsi que la liste la plus précise possible des données et des personnes concernées.

Etape 4 : communication des éléments (y compris techniques) au DPO. Définition et mise en place de **mesures correctives** si nécessaire. Le DPO complète la notification initiale.

Etape 5 : obligation d'**informer les personnes concernées** si la violation présente un risque élevé pour leur vie privée. Il est toutefois préconisé de les informer même si la violation est minime.

PROCÉDURE : RÉPONSE À UNE DEMANDE DE DROIT D'ACCÈS

Etape 1 : **s'assurer de l'identité du demandeur** (pièce justificative, rappel d'identifiants...). En cas de personne mineur, la demande peut être effectuée par un parent / un tuteur légal. La vérification doit alors porter sur l'identité du parent / tuteur ET sur celle du mineur. Une personne peut également mandater un tiers pour effectuer un droit d'accès en son nom. Il convient alors de vérifier que le mandat précise clairement l'exercice du droit d'accès et vérifier les identités du mandant ainsi que du mandataire.

Etape 2 : fournir impérativement au demandeur un **récépissé (daté) de réception** de la demande.

Etape 3 : **informer immédiatement le référent et le DPO**. Vérifier, en consultation avec le DPO, la recevabilité de la demande. Si la demande est jugée irrecevable, répondre au demandeur pour l'en informer et lui indiquer le plus clairement possible les raisons (demande abusive, répétitive, violant une obligation légale...).

PROCÉDURE : RÉPONSE À UNE DEMANDE DE DROIT D'ACCÈS

Étape 4 : si la demande est valide, définir en consultation avec le DPO le délai maximum légal de réponse.

Une demande simple et/ou précise (ex : « je souhaite accéder à mon dossier RH ») bénéficiera d'un délai de réponse maximum autorisé de 1 mois.

Une demande vaste ou complexe (enregistrement vidéo présentant plusieurs personnes, accès à l'ensemble des données de plusieurs services...) verra son délai de réponse maximum porté à 3 mois (article 12.3 du RGPD).

ATTENTION : en cas d'accès à des données de santé, le délai de réponse est régi par le Code de la santé publique, à savoir : si les données remontent à plus de 5 ans, 2 mois pour répondre ; si les données remontent à moins de 5 ans, la réponse doit être effectuée dans un délai compris entre 48h minimum en guise de temps de réflexion prévu par la loi dans l'intérêt de la personne et 8 jours maximum.

TEMPS D'ÉCHANGE ET RÉPONSES AUX QUESTIONS

