La protection des données

Débutant



Mission du jour, bonjour !



01

Comprendre le RGPD

Contexte et notion essentielles

02

Droits et obligations

Comment faire pour être conforme ?

03

Mise en pratique & risques

Exemple concret et quiz

C’est quoi le RGPD (GDPR) ?

Règlement européen

Harmonise les règles de protection des données dans l’UE

Application matérielle

Toute opération impliquant des données personnelles (sauf activités domestiques)

Application territoriale

Établissements dans l’UE
ou
Cible des résidents de l’UE





Pourquoi protéger ses données ?

Pour la vie privée

Empêcher que des inconnus aient les données des bénéficiaires et collaborateurs

Pour la sécurité

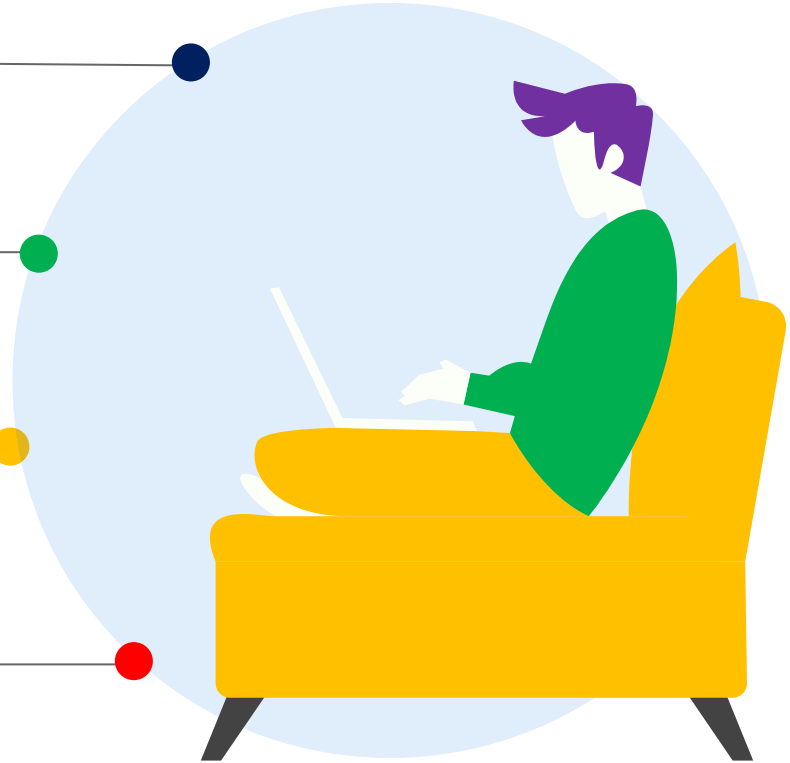
Empêcher les fraudes, fuites ou vol de données

Pour la confiance

Préserver la réputation et la confiance

Pour la conformité légale

Amendes jusqu'à 20M € ou fermeture temporaire/définitive de l'asbl



RGPD : Guide et Bouclier

Relation de confiance

La confiance est la clé



Encadrer les pratiques

Éviter les abus



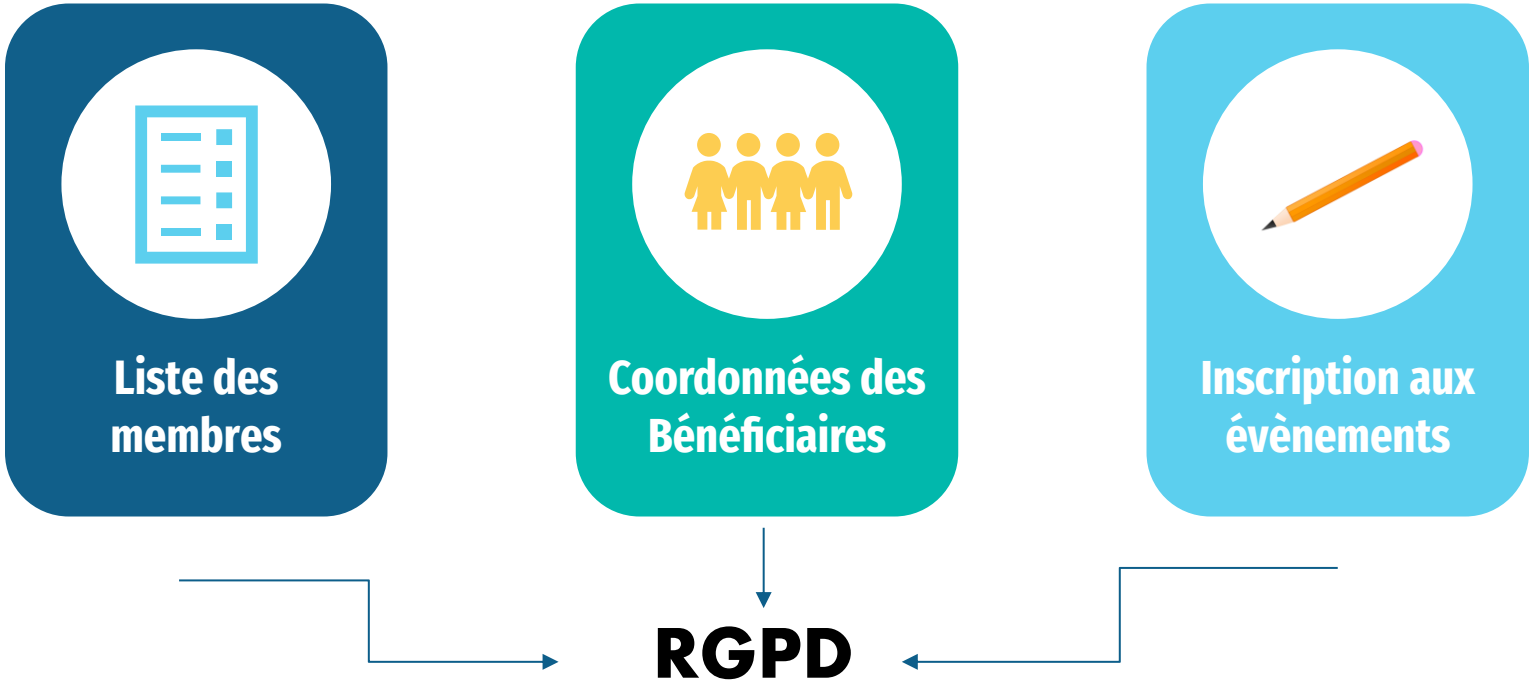
Droits des individus

Droits selon le RGPD





Pourquoi l'ASBl est-elle concernée ?



C’est quoi une “donnée personnelle” ?



Personne identifiée

On la reconnait directement

Définition

Toute information liée à une personne physique identifiée ou identifiable

Personne identifiable

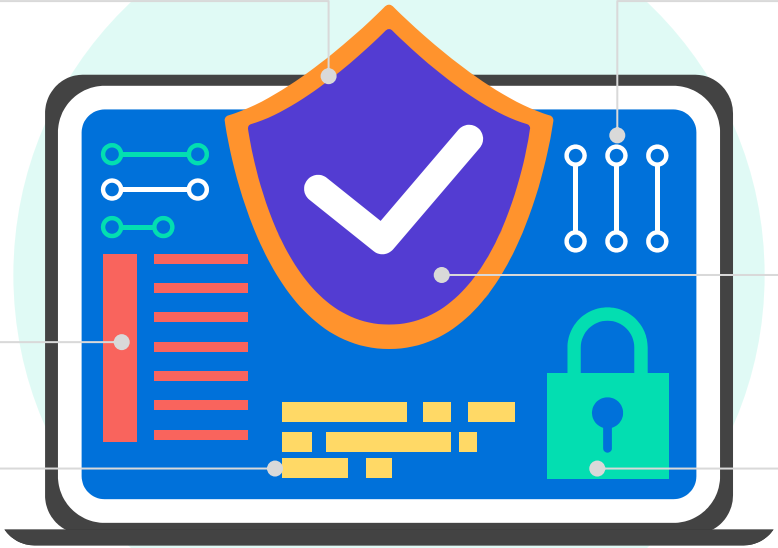
On la reconnait indirectement

Exemples de données personnelles

Nom, prénom

Photo

Âge



Signature

ADN

Couleur des cheveux

Catégories particulières de données

Origine raciale et ethnique

Opinions politiques

Liste des membres d'un groupe militant

Appartenance syndicale

Inscription membres d'un syndicat

Données génétiques

Analyse d'ADN



Données sensibles

Précautions nécessaires ! Traitement interdit SAUF exceptions article 9 (2)

Données biométriques

Empreintes digitales, reconnaissance faciale

Données de santé

Toutes les DP liées à la santé

Orientation sexuelle

Ou vie sexuelle

C’est quoi un “traitement” de données personnelles ?



Les règles d'or du RGPD

01

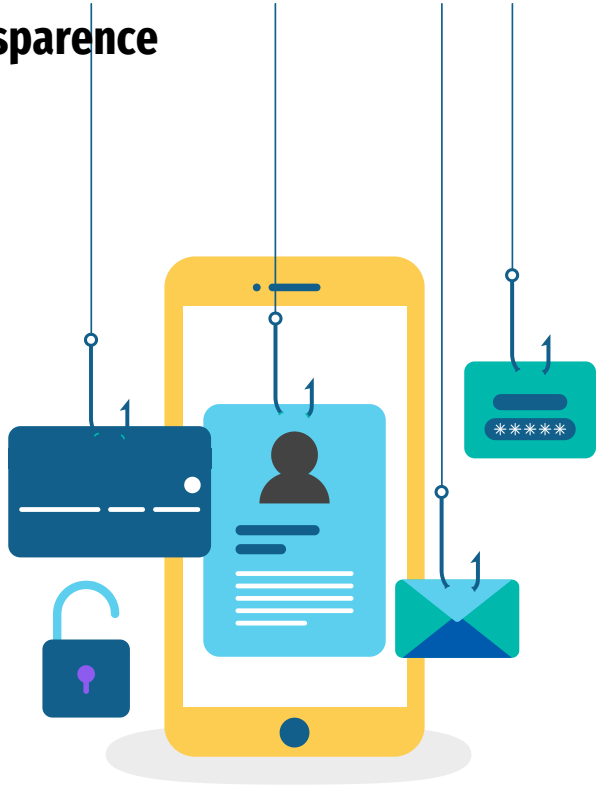
Licéité, Loyauté, transparence

Informer clairement sur l'usage des données

02

Limitation

Utiliser les données que pour le but défini



03

Minimisation

Ne collecter que ce qui est nécessaire.

04

Exactitude

Maintenir les données à jour

05

Conservation

On garde les données le moins longtemps possible

06

Sécurité

On protège les données au mieux

Les bases légales

Pas de base légale, pas de traitement de données !

1	2	3	4	5	6
Demande d'autorisation claire	Execution d'un contrat	La loi vous oblige à traiter des données	Pour atteindre un objectif légitime	Question de vie ou de mort	Exécution d'une mission d'intérêt publique
Consentement	**Contrat**	**Obligation légale**	**Intérêt légitime**	**Intérêt vitaux**	**Mission d'IP**



Les rôles définis par le RGPD

Qui fait quoi ?



- Les personnes concernées
- Le responsable de traitement
- Le sous-traitant
- Le délégué à la protection des données (DPO)

Sous-traitant de données



Bien choisir ses sous-traitants

Fiables et conformes

Établir un contrat de sous-traitance

Obligatoire

Clauses spécifiques

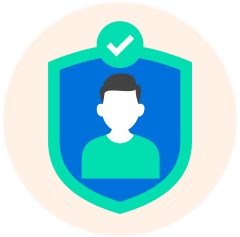
Superviser les sous-traitant

Contrôler périodiquement

Documenter la conformité

Exemple

L'ASBL utilise le sous-traitant D-Health pour le stockage de ses dossiers patients (Lifeline)



01

Choix du sous-traitant

D-Health respecte-t-il le RGPD ?



02

Contrat de sous-traitance

Signature d'un contrat de protection des données entre l'ASBL et D-Health



03

Supervision

L'ASBL vérifie le respect continu du RGPD par D-health et réalise un audit périodique ou en cas de besoin.

Les droits des personnes concernées

Accès

Savoir quelles données sont détenues et comment elles sont utilisées.

Effacement

Demander la suppression des données

Portabilité

Recevoir ses données dans un format réutilisable

Retrait du consentement

Retirer son accord à tout moment (seulement pour cette base légale)



Rectification

Corriger des données inexactes ou incomplètes

Limitation

Suspendre temporairement le traitement des données

Opposition

Refuser un traitement (ex. newsletter, cookies)

Pas de décision automatisée

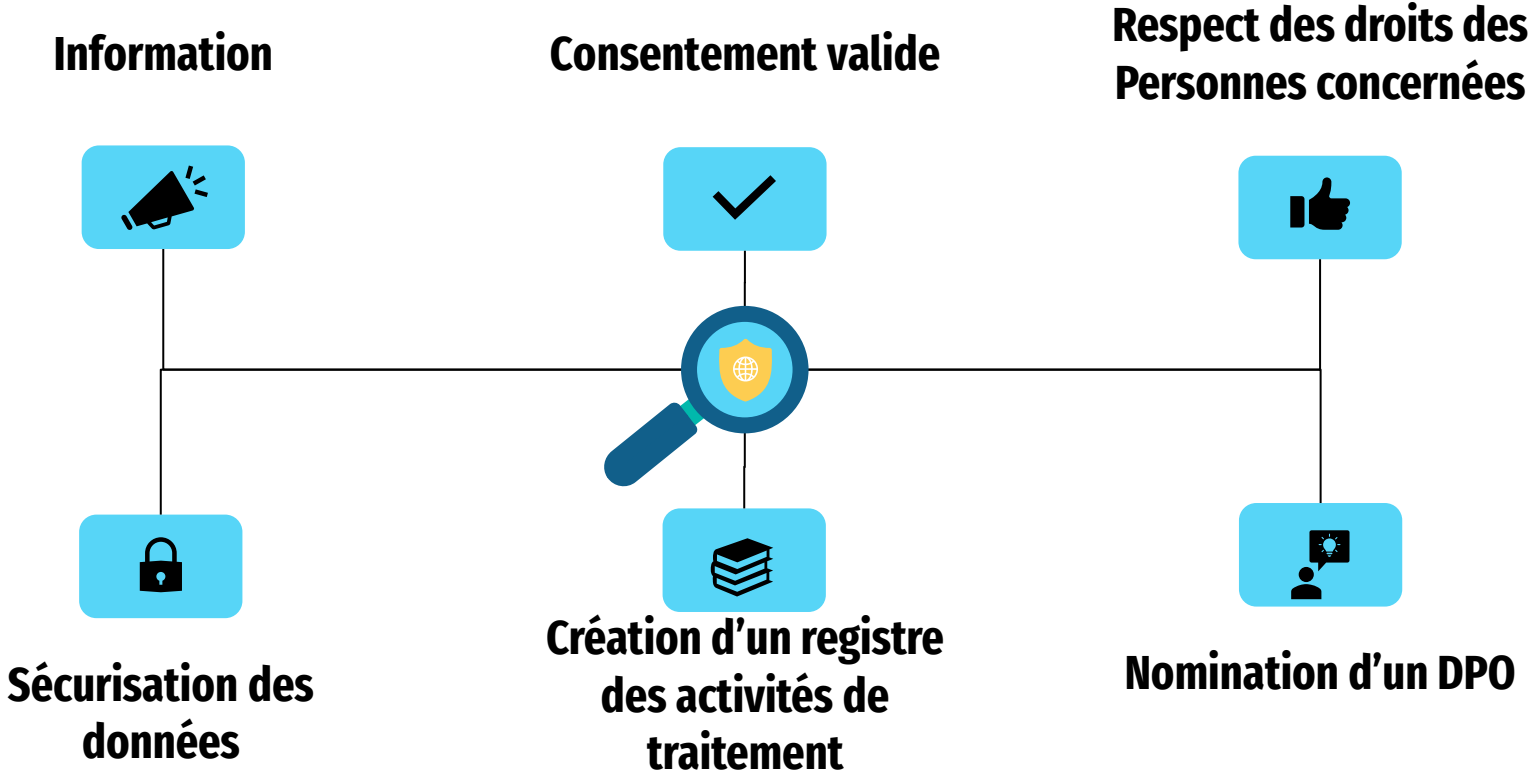
S'opposer à des décisions prises par des systèmes automatisés (IA)

En tant qu'ASBL, comment respecter les droits des personnes concernées ?



- Communication transparente
- Procédure interne définie
- Respect des délais légaux
- Suivi et archivage
- Gratuité des droits

Mise en pratique du RGPD



Qu’est-ce qu’une fuite de données ?

Définition :
« ***Tout incident entraînant perte, destruction, altération, divulgation non autorisée ou accès à des données personnelles*** »

Peux être **accidentelle** ou **malveillante**

Exemples :
- Piratage / phishing
- Envoi de fichiers à la mauvaise personne
- Vol d’ordinateurs ou supports (ex. clé USB)
- Erreur technique.



⚠️ **Prévenir immédiatement la direction et/ou Pierre !**
Prévenir permet d’agir correctement et d’éviter de graves conséquences.

Fuite grave : qui prévenir et quoi faire



Autorité de protection des données

Notifier aux autorités compétentes

Délai : **72 heures** après avoir pris connaissance de la violation.

Contenu : nature de la violation, catégories et nombre de personnes concernées, conséquences probables, mesures prises.

Informer les personnes concernées

Obligatoire si la violation est susceptible d'engendrer un **risque élevé pour les droits et libertés.**

10 bons réflexes pour éviter une fuite de données

1. 🔒 Mots de passe forts et uniques
2. 📱 Activer la double sécurité (MFA)
3. 🔑 Sécuriser son poste et ses documents en cas d'absence
4. 🔄 Maintenir à jour les outils utilisés
5. 📧 Vigilance sur les communications
6. 🗂️ Ne garder que l'essentiel
7. ☁️ Utiliser les outils officiels de l'ASBL
8. 🤫 Discrétion dans et hors des locaux
9. 💾 Stocker et sauvegarder correctement
10. 🚨 Signaler rapidement un incident



Quiz pratique : Protection des données (RGPD)?