

LES BASES DU RGPD

La réglementation générale sur la protection des données



lundi 8 juillet 2024



PLAN

1. DÉFINITION ET ORIGINE
2. DE QUI ET DE QUOI PARLE-T-ON ?
3. LES 8 RÈGLES FONDAMENTALES
4. LES DONNÉES HORS UNION EUROPÉENNE
5. LES DOCUMENTS OBLIGATOIRES
6. LES SANCTIONS
7. LES BONNES PRATIQUES



DÉFINITION ET ORIGINE

- **RGPD** : règlement général sur la protection des données
- Issue de la **loi informatique et libertés** de 1978
- Remanié en 2016
- Applicable depuis **le 25/05/2018**
- Sur le territoire de **l'union européenne**
- Structure autoritaire : **la CNIL**

DE QUI ET DE QUOI PARLE-T-ON ?

Les acteurs du RGPD

- Les personnes physiques
- Les responsables de traitement
- Les sous-traitants
- Les DPO (délégués à la protection des données)
- La CNIL

Traiter des données personnelles

- Collecte
- Enregistrement
- Conservation
- Transmission
- Modification
- Consultation
- Communication



LES 8 RÈGLES FONDAMENTALES

1. La licéité

- La personne consent
- Le traitement est nécessaire à
 - L'exécution
 - L'obligation légale
 - La sauvegarde des intérêts vitaux
 - L'exécution d'une mission d'ordre public
 - L'exécution d'une mission aux fins d'intérêts légitimes

2. La finalité du traitement

- Principe clé
- Doit permettre de définir
 - La raison d'être du traitement
 - L'objectif
 - La méthode
- Si la finalité sort du cadre de licéité, il est obligatoire d'obtenir le consentement

3. La minimisation

- Ne collecter que ce qui est nécessaire à la finalité
- Des informations exactes et à jour
- Limiter les actions de collecte au strict minimum



LES 8 RÈGLES FONDAMENTALES



4. Les données sensibles

- Par principe **interdites**
 - Racial et ethnique
 - Politique
 - Médicales
 - Psychiques et psychologiques
 - Syndicales
 - De genre
 - Génétique
 - Biométrique
- Pénales
- Carte vitale

5. La conservation limitée

- Dans la **base active**
 - Bulletins de paie : 5 ans
 - Données médicales : 10 ans
 - Images de vidéosurveillance : 1 mois
 - Données clients : 3 ans
 - CV : 2 ans
- **Archivage** intermédiaire
- Archivage **définitif**
- **Suppression** des données

6. La sécurisation

- Pseudonymiser ou chiffrer les données
- Sécuriser les accès physiques et numériques
- Assurer
 - La confidentialité
 - L'intégrité
 - La disponibilité

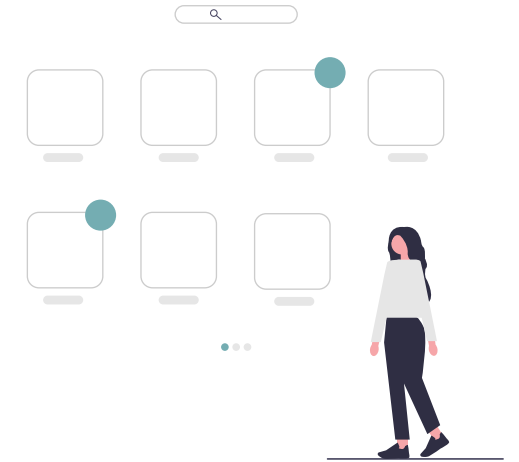
LES 8 RÈGLES FONDAMENTALES

7. La transparence

- Les informations doivent être :
 - Compréhensibles
 - Lisibles
 - Accessibles/disponibles
 - Globales
- Alerter en cas de perte, vol, dommage
 - La CNIL
 - Les personnes concernées
 - Sous 72 h

8. Le respect des droits

- Le droit d'accès
- Le droit de rectification
- Le droit d'opposition
- Le droit à l'effacement
- Le droit à la portabilité
- Le droit à la limitation de traitement
- 1 mois max pour répondre



Gardez en tête les principes suivant :

- *Consentement*
- *Clarté*
- *Sécurité*
- *Limitation*

LES PAYS HORS DE L'UNION EUROPÉENNE

La carte des pays selon leur adéquation au RGPD

Les pays adéquats

- Les données peuvent transiter librement
- Soumises au RGPD

Les pays non adéquats

- Soumis à des documents particuliers :
 - Certificats approuvés
 - Codes de conduite
 - CTT (clauses contractuelles types)
 - Conventions internationales
 - Règles d'entreprise contraignantes





LES DOCUMENTS OBLIGATOIRES

Les registre de traitement

- Renseigner
- Servir de preuve en cas de contrôle
- Éviter les abus
- Prendre conscience et du recul sur les informations collectées
- [Exemple de registre vierge à compléter](#)

La politique de confidentialité

- Recense les données collectées
- Permet la visibilité au public
- Les personnes doivent être informées en cas de modification
- Informe sur les droits et les outils
- Doit être clair, lisible et compréhensible
- [Générateur de politique de confidentialité](#)

L'analyse d'impact

- [Utiliser PIA](#)
- L'AIPD doit recenser :
 - Les événements redoutés
 - Les menaces qui peuvent rendre ces événements possibles
 - Les sources de ces menaces
 - Les impacts potentiels sur les personnes
- L'AIPD est obligatoire en cas de risque élevé
- [Liste des traitement non obligatoires](#)

LES SANCTIONS



Les amendes peuvent aller jusqu'à 4% du chiffre d'affaire annuel de l'entreprise ou 20 millions d'euros en cas de faute grave constatée

- Rappel à l'ordre
- Injonction de mise en conformité
- Limitation temporaire ou définitive du traitement
- Suspension de flux de données vers les pays tiers
- Ordre de satisfaire les droits des personnes
- Retrait d'une certification
- Amende administrative

LES BONNES PRATIQUES À METTRE EN PLACE



- Faire le **tri** dans les données conservées
- S'interroger sur le besoin et/ou l'existence d'une **solution alternative**
- Bannir la **collecte préventive**
- **Anonymiser** les données dès que possible
- **Limiter les commentaires libres** dans les formulaires (favoriser les menus déroulants)
- À la place de la date de naissance, préférer demander la **tranche d'âge**
- Ne pas demander la **carte vitale**
- Mettre en place des procédures de **sécurisation des données**
- Favoriser les **outils de l'UE**
- Garder ses informations **accessibles et à jour**
- **Se faire accompagner** en cas de besoin

BILAN ET TOUR DE TABLE FINAL





MERCI

Copyright @juillet 24 – Stéphanie DUMAS - EI

Tous droits réservés

Le Code de la Propriété Intellectuelle interdit les copies ou reproductions destinées à une utilisation collective « Toute représentation ou reproduction intégrale ou partielle faite par quelque procédé que ce soit, sans le consentement de l'auteur ou de ses ayants cause, est illicite et constitue une contrefaçon, au terme des articles L.335-2 et suivant le Code de la Propriété intellectuelle. »