








Formation RGPD

-  Introduction - Evolution de la protection des données personnelles
-  Tour de table / débat autour du RGPD
-  introduction au RGPD : Enjeux, opportunités, normes
-  Atelier : processus de mise en conformité RGPD
-  Retour d'XP - Rôle du DPO
-  Atelier - Mini audit d'une entreprise
-  Présentation d'un outil - Colibri DPO

Présentation à retrouver sur [Github](#)



Introduction

La protection des données, ça vous évoque quoi ?

Un peu d'histoire

<https://www.youtube.com/watch?v=Th-rzrc3488>



” Qui a le droit de savoir quoi sur qui ?

Source INA (1975)

Création de la CNIL

https://www.youtube.com/watch?v=i_k8ozkY2l4&t=228s



Qu'est-ce que le RGPD ?

- Règlement Général sur la Protection des Données
- Entrée en application: **25 mai 2018**
- 173 considérants, 99 articles

Qu'est-ce qu'une donnée personnelle ?

"Toute donnée permettant d'identifier quelqu'un est considérée comme étant une donnée à caractère personnel"

On distingue 2 types de données à caractère personnel:

- les données personnelles
- les données personnelles dites sensibles

Qui est concerné par le RGPD ?

- Personnes physiques: **citoyens européens**
- Personnes morales: **Toute entreprise européenne ou traitant des données de citoyens européens**

6 droits conférés par le RGPD

- droit d'accès (Art. 15)
- droit de rectification (Art. 16)
- droit d'effacement (droit à l'oubli) (Art. 17)
- droit de limitation du traitement (Art. 18)
- droit à la portabilité des données (Art. 20)
- droit d'opposition (Art. 21)

Droit d'accès (Art.15)

Toute personne concernée peut vous demander une copie de ses données personnelles, ainsi que des informations complémentaires pour l'aider à comprendre comment et pourquoi vous utilisez ses données, et si vous le faites légalement.

Droit de rectification (Art. 16)

Les personnes physiques ont le droit de faire corriger des données personnelles inexactes. Selon les objectifs du traitement des données, les personnes physiques peuvent également avoir le droit d'exiger que leurs données personnelles incomplètes soient complétées (par exemple, en ajoutant une mention complémentaire).

Droit d'effacement (droit à l'oubli) (Art. 17)

Les personnes physiques ont le droit de faire effacer leurs données personnelles. Ce droit n'est pas absolu et ne s'applique que dans certaines circonstances.

Droit de limitation du traitement (Art. 18)

Le RGPD donne aux personnes physiques le droit de limiter la manière dont une organisation utilise leurs données.

Droit à la portabilité des données (Art. 20)

Les personnes physiques ont le droit de recevoir les données à caractère personnel qu'elles ont fournies à un responsable du traitement dans un format structuré, communément utilisé et lisible par une machine. Elles peuvent aussi demander que le responsable du traitement transmette ces données directement à un autre responsable du traitement.

Droit d'opposition (Art. 21)

Les personnes physiques peuvent s'opposer à tout moment au traitement de leurs données à caractère personnel, et le responsable du traitement doit alors cesser de les traiter.

6 grands principes du RGPD

- Licéité, loyauté et transparence
- Limitations de la finalité
- Minimisation des Données
- Exactitude
- Limitations de la conservation
- Intégrité et confidentialité

Licéité, loyauté et transparence

Le traitement doit être traité de manière licite, loyale et transparente au regard de la personne concernée.

Limitations de la finalité

le traitement doit être effectué pour une finalité déterminée, explicite et légitime et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités. Sauf exceptions précisées dans l'article 89, paragraphe 1.

Minimisation de données

Il faut faire en sorte de ne conserver que les données nécessaires à la finalité du traitement. Toute autre donnée doit être supprimée.

Exactitude

Les données du traitement doivent être exacte et si nécessaire, tenues à jour. (Conformément à l'article 5, clause 1(d)). Une protection adéquate et des mesures pour contrer le vol d'identité peuvent être prises dans les bases de références. Des process peuvent être mis en place pour gérer la rectification des données et l'activité d'archivage.

Limitations de la conservation

Il ne faut conserver les données que dans un temps nécessaire à l'exécution de la finalité.

Intégrité et confidentialité

Les sous-traitants doivent traiter les données en garantissant une sécurité appropriée des données à caractère personnel.

Les risques de non-conformité RGPD

Lorsque des manquements au RGPD ou à la loi sont portés à sa connaissance, la formation restreinte de la CNIL peut :

- Prononcer un rappel à l'ordre ;
- Enjoindre de mettre le traitement en conformité, y compris sous astreinte ;
- Limiter temporairement ou définitivement un traitement ;
- Suspendre les flux de données ;
- Ordonner de satisfaire aux demandes d'exercice des droits des personnes, y compris sous astreinte ;
- Prononcer une amende administrative. (pouvant aller jusqu'à 20 millions d'euros ou 4% du CA)

Les enjeux de la conformité RGPD pour une entreprise

Comment se mettre en conformité RGPD ?

<https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes>

- Etape 1: DÉSIGNER UN PILOTE
- Etape 2: CARTOGRAPHIER
- Etape 3: PRIORISER
- Etape 4: GÉRER LES RISQUES
- Etape 5: ORGANISER
- Etape 6: DOCUMENTER

1. DÉSIGNER UN PILOTE

Pour piloter la gouvernance des données personnelles de votre structure, vous aurez besoin d'un véritable chef d'orchestre qui exercera une mission d'information, de conseil et de contrôle en interne : le délégué à la protection des données. En attendant 2018, vous pouvez d'ores et déjà désigner un « correspondant informatique et libertés », qui vous donnera un temps d'avance et vous permettra d'organiser les actions à mener.

2. CARTOGRAPHIER VOS TRAITEMENTS DE DONNÉES PERSONNELLES

Pour mesurer concrètement l'impact du règlement européen sur la protection des données que vous traitez, commencez par recenser de façon précise vos traitements de données personnelles. L'élaboration d'un registre des traitements vous permet de faire le point.

3. PRIORISER LES ACTIONS À MENER

Sur la base de votre registre, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.

4. GÉRER LES RISQUES

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une analyse d'impact relative à la protection des données (AIPD).

5. ORGANISER LES PROCESSUS INTERNES

Pour assurer un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire).

6. DOCUMENTER LA CONFORMITÉ

Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

Le RGPD, 3 axes

- Axe juridique
- Axe technique
- Axe organisationnel

Axe juridique (requis)

- Politique de confidentialité
- Politique de protection des données
- Politique de conservation des données
- Politique relative aux cookies
- Conditions générales d'utilisation
- Informations de contact
- Conditions de transfert de données vers des pays hors UE

Axe juridique (optionnel)

- Politique de suppression des données
- Politique de sauvegarde et de continuité des activités
- Politique de contrôle d'accès au système
- Politique de contrôle du chiffrement
- Politique de récupération et de continuité des activités
- Politique de résiliation des utilisateurs
- Politique d'audit
- Politique d'évaluation des risques
- Politique de sensibilisation et de formation

Axe technique

- Données hébergées en Europe
 - Privacy by default / Privacy by design
 - Sécurité des réseaux
 - Chiffrement des bases de données
 - Chiffrement des données en transit (HTTPS, IPSec, TLS, PPTP, SSH, etc...)
 - Contrôle d'accès (physique et technique)
 - Prévention et détection des intrusions
 - Surveillance d'état
 - Sauvegarde régulières
 - Chiffrement des sauvegardes
 - Authentification multifacteur, autorisations strictes
 - Solution antivirus
 - Analyse régulière des infrastructures
-
- Politique d'installation des logiciels, politique de mise à jour des logiciels, politique de mise à niveau des équipements

Axe organisationnel

- Gestion du registre des activités de traitement
- Gestion des violations de données personnelles
- Gestion des demandes d'exercices de droit
- Gestion des sous-traitant
- Gestion de la formation/sensibilisation de toutes les parties prenantes
- Gestion de projet (plan d'action)
- Conduite d'audits et d'analyses d'impact

Registre des activités de traitements (Art. 30)

<https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement>

1. le cas échéant, le **nom et les coordonnées** du responsable conjoint du traitement mis en œuvre
2. les **finalités** du traitement, l'objectif en vue duquel vous avez collecté ces données
3. les catégories de **personnes concernées** (client, prospect, employé, etc.)
4. les catégories de **données personnelles** (exemples : identité, situation familiale, économique ou financière, données bancaires, données de connexion, données de localisation, etc.)
5. les **catégories de destinataires** auxquels les données à caractère personnel ont été ou seront communiquées, y compris les sous-traitants auxquels vous recourez
6. les **transferts** de données à caractère personnel vers un pays tiers ou à une organisation internationale et, dans certains cas très particuliers, les garanties prévues pour ces transferts ;
7. les **délais prévus pour l'effacement** des différentes catégories de données, c'est-à-dire la durée de conservation, ou à défaut les critères permettant de la déterminer
8. dans la mesure du possible, une **description générale des mesures de sécurité** techniques et organisationnelles que vous mettez en œuvre

Atelier

Violations de données

https://www.ina.fr/video/S720117_001/fuite-des-donnees-personnelles-une-crainte-vieille-de-50-ans-video.html



Atelier

Gestion des demandes d'exercices de droit

Atelier

Gestion des sous-traitants

Rôle du DPO - Gestion de projet

- Nomination DPO (Art. 37)
- Pas obligatoire, sauf Big Data, administration publique ou traitements de données sensibles

Atelier

Analyse d'impact sur la vie privée



pia

analyse d'impact sur la protection des données
privacy impact assessment

L'approche qualité - Amélioration continue

Présentation de Colibri DPO