**Règlement Général sur la Protection des Données**

**C’est un règlement de l’Union Européenne qui constitue le texte de référence en matière de protection des données à caractère personnel. Adopté en Avril 2016 il est applicable depuis Mai 2018 dans les 28 États membres de l’UE.**

**Il remplace *la directive sur la protection des données personnelles* qui agissait seulement en France et a pour objectif d’accroitre la protection des personnes concernées par un traitement de leurs données à caractère personnel et aussi, accroitre la responsabilité des acteurs de ce traitement.**

**Mise en œuvre** :

**Les organisations doivent pouvoir garantir et prouver leur conformité en matière de protection des données personnelles.**

**Pour pouvoir garantir et prouver leur conformité, la CNIL (Commission Nationale de l’Informatique et des Libertés) conseille 6 étapes.**

1. **Nommer un délégué à la protection des données.**

* Si des données personnelles transitent dans votre entreprise, celui-ci est chargé d’un rôle d’information, de conseil et de contrôle interne.

EXEMPLE : Projet Franprix, nous ne collectons pas de données, tous les micros-services développés tapent dans les bases de données Franprix. Sur ce projet onepoint n’a pas de délégué à la protection des données, mais nous pouvons supposer que Franprix oui.

1. **Recenser les traitements des données**

* Faire un registre des traitements de données effectués.

EXEMPLE : Quelles données sont passées par nous et qu’en avons-nous fait.

1. **Définir les actions correctives**

* Il est nécessaire de déterminer quelles sont les actions prioritaires à mettre en œuvre. La priorisation est déterminée en fonction du niveau de risque et grâce au registre des traitements (voir étape 2).

1. **Analyser les risques**

* Gérer les risques pouvant avoir des conséquences sur la sécurité des données.

EXEMPLE : Faille de système permettant de dumper les données

1. **Etablir des procédures internes**

* Il s’agit ici de constamment assurer la protection des données personnelles, anticiper les évènements éventuels pouvant impacter les traitements en cours.

1. **Tenir une documentation**

* La documentation permet de justifier la conformité d'une entreprise au règlement. Il est également essentiel de fréquemment reconsidérer et ajuster les actions et documents afin de garantir une protection des données durable.

**Sanctions** :

**Pour les organisations qui ne respectent pas le RGPD, les sanctions sont graduelles et dépendent de la gravité des actions constatées et qui sont contraires au RGPD.**

1. **Avertissement ou mise en demeure de l’entreprise accompagné d’un rappel des règles.**
2. **Injonction, ordre de cessation immédiate des violations constatées.**
3. **Limitation ou suspension temporaires des traitements ou des flux de données.**
4. **Sanction administrative pour les entreprises qui n’ont pas respecté l’injonction**

🡪 Déf injonction : ordre d'un tribunal visant à obliger une personne à faire ou ne pas faire quelque chose en l'attente du jugement final.

Documentation référence du RGPD :

* <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460>
* <https://www.cnil.fr/fr/les-outils-de-la-conformite> (Le CNIL est aussi joignable par téléphone, où l’on peut même avoir un de leur juriste directement.)

CE QU’IL MANQUAIT DANS MON SONDAGE :

* Contact pour avoir accès à ses données ?
* L’obligation de remplir le questionnaire est un mensonge.
* Le sondage ne mentionne pas clairement la finalité du traitement des données personnelles, les destinataires des données, leur durée de conservation.
* Question sur la mixité raciale : en France le principe des « races » chez l’être humain n’est pas reconnu + question hors sujet, aucun rapport avec le sondage.
* Question sur l’orientation sexuelle : question hors sujet, aucun rapport avec le sondage.

Il est là : <https://docs.google.com/forms/d/e/1FAIpQLSdS-wyCdTbnTL2vsnKoekJB6LP_Xlc5DJhbb6KXMD5BttCl8w/viewform?vc=0&c=0&w=1>

<https://www.koban.cloud/rgpd-mention-traitement-de-donnees/>

**La sécurité informatique**

Elle a plusieurs objectif, liés aux types de menaces ainsi qu’aux type des ressources.

On peut noter les points suivants comme les objectifs principaux :

* Empêcher la divulgation non-autorisée de données
* Empêcher la modification non-autorisée de données
* Empêcher l’utilisation non-autorisée de ressources réseau ou informatique de façon générale

La « sécurité informatique » est un terme très large qui s’applique dans différents champs d’application.

* La sécurité physique (gestion d’accès physique, prévenir/détecter les intrusions)
* La sécurité humain (\*prévenir des risques liés à l’humain, avec des formations par ex.)
* La sécurité procédurale (audit, procédures informatiques …)
* La sécurité des émissions physiques (écrans, câbles, courbes de consommation de courant …)
* La sécurité des systèmes d’exploitation
* La sécurité des communications

**Pour remédier aux failles et pour contrer les attaques, la sécurité informatique se base sur un certain nombre de services**, à ce moment il ne s’agit que d’un niveau d’abstraction visant à déployer une politique de sécurité optimale.

* La confidentialité
* L’authentification
* L’intégrité (des machines, des données ou des flux)
* Le contrôle d’accès (= autorisation, à ne pas confondre avec l’authentification)
* La non-répudiation (avec preuve d’émission ou avec preuve de réception)

🡪 Déf répudiation : rompre un lien qui lie deux partis par volonté unilatérale.

<https://malovsky.github.io/HackMe/>