Guide de survie pour être (à peu près) conforme au RGPD

Lucie Anglade – L’apéro du web – Janvier 2024

Lucie Anglade

- Ingénieure en informatique 👩‍💻
- Développeuse logiciels libres
- Consultante RGPD 🇪🇺
- Présidente de l'AFPy 🐍
- Organisatrice des meetups Python sur Lyon

- Avant le RGPD
- C’est quoi le RGPD ?
- Les choses à faire
- Les sanctions possibles
- Par où commencer ?

Avant le RGPD

Le projet SAFARI

- **S**ystème **A**utomatisé pour les **F**ichiers **A**dministratifs et le **R**épertoire des **I**ndividus
- projet du gouvernement en 1973
- recenser et recouper les informations détenues par les différents pouvoirs publics de chaque citoyen
- fait la une du Monde en 1974
- projet abandonné
- création d’une commission chargée de proposer un cadre pour l’utilisation des données personnelles

La Loi Informatique et Libertés

- **6 janvier 1978**
- inscrit l'informatique dans le cadre des droits de l'homme
- crée la Commission Nationale de l'Informatique et des Libertés (CNIL)
- définit les données personnelles, le consentement
- définit le reponsable de traitement et ses obligations
- définit les droits des personnes sur leurs données
- et plein d'autres choses

Les directives 95/46/CE et 2002/58/CE

- Tentent d’harmoniser les lois des pays membres
- interdisent le spam avec le principe d’**opt-in**
- instaurent le principe d’**opt-out** pour les cookies
- sont transposées dans le droit français en 2004

Le RGPD

C’est quoi le RGPD ?

- **R**èglement **G**énéral sur la **P**rotection des **D**onnées
- adopté par le Parlement Européen en 2016
- **directement applicable dans les pays membres à partir du 25 mai 2018**

Les objectifs du RGPD 🎯

- Augmenter la protection des personnes concernées par un traitement de données
- augmenter la responsabilisation des acteurs du traitement
- donner plus de pouvoir aux autorités de contrôles
- uniformiser la loi dans les pays membres

Qui est concerné ?

Tous les organismes, publics ou privés, peu importe le pays d'implantation du moment que :

- l'organisme est établi en Union Européenne
- ou que son activité cible directement des résidents européens

Les choses à faire

C’est quoi une donnée personnelles ?

« Toute information se rapportant à une personne physique identifiée ou identifiable »

C’est quoi un traitement de données ?

« Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, … »

Un traitement de données **n’est pas forcément informatisé**, il doit **avoir une finalité** et **une base légale**.

Le registre des traitements de données 📖

C’est un document **obligatoire pour tous les organismes** qui permet de démontrer sa conformité avec le RGPD.

Le registre liste tous les traitements effectués sur les données personnelles.
Il peut être « réduit » pour les organismes de moins de 250 personnes.

Il permet de présenter les informations relatives à chaque traitement.

C’est quoi un sous-traitant ?

Un organisme est sous-traitant du moment qu’il **traite des données personnelles pour le compte et sur instruction d’un autre organisme** ayant la qualité de responsable de traitement.

Le registre de sous-traitance 📖

C’est un document **obligatoire pour tous les organismes sous-traitants** qui permet également de montrer sa conformité.

Le registre recense toutes les catégories d'activités de traitement effectuées pour le compte des clients.

C’est quoi une violation de données ?

« une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données »

En cas de violation de données

Pour les personnes concernées, la violation entraine	Aucun risque	Un risque	Un risque élevé
Documentation interne	X	X	X
Notification à la CNIL (max. 72h)		X	X
Information aux personnes concernées			X

C’est fini pour les registres… mais il y a encore des choses !

Le·la DPO

Le délégué à la protection des données (Data Protection Officer) met en œuvre le RGPD dans l'organisme.

Le DPO peut être interne ou externe à l'organisme, ou mutualisé avec d'autres organismes. Dans tous les cas, **le DPO est désigné de façon indépendante**.

Le DPO n'est pas obligatoire pour tous les organismes.

Les analyses d’impact 🧐

Une analyse d’impact est une étude qui se fait avant de mettre en place un traitement.

Dans certains cas, il est obligatoire de faire une analyse d’impact.

Une analyse d’impact permet d’évaluer la proportionnalité d’un traitement, les risques liés et les mesures de sécurité envisagées.

Encore une dernière chose !

Informer les gens 📣

- Sur les traitements qui les concernent
- sur leurs droits
- sur les incidents éventuels

En veillant à avoir une information **accessible** à tout le monde.

Est-ce que je peux être sanctionné ?

Les sanctions possibles 💸

- Détournement de finalité : 300 000€ d’amende et 5 ans d’emprisonnement
- détournement de finalité : 20 millions d’€ ou 4% du CA annuel mondial
- violations de données / analyses d’impact : 10 millions d’€ ou 2% du CA annuel mondial

Par où commencer pour se mettre en conformité ?

S’informer

Vous avez déjà commencé ! 😁

Recenser les traitements de données 📝

- identifier les activités qui utilisent des données personnelles
- identifier et discuter avec les responsables opérationnels
- analyser les sites, applications...
- commencer à remplir les différents registres

Faire le tri 🚮

- les données sont-elles toutes utiles ? Sont-elles toujours pertinentes ?
- combien de temps les données sont conservées ?

Définir une politique de sécurisation des données

- identifier les risques qu’il peut y avoir sur les traitements
- garantir l'intégrité des données
- limiter les risques de violations de données

La politique de sécurisation des données concerne aussi bien les données numériques que les **données physiques**.

Respecter les droits des personnes

- les informer
- leur permettre d'exercer leurs droits facilement

Quels sont ces droits ?

Les personnes disposent de droits sur les données les concernant :

- accès
- rectification
- opposition
- effacement
- portabilité
- limitation
- ne pas faire l’objet d’une décision fondée exclusivement sur un traitement automatisé

Comment faire tout ça ? 😱

- Avoir une personne en interne
- se faire accompagner
- se former
- sensibiliser les personnes

Combien de temps ça va me prendre ?

C’est un travail continu. Le plus dur, c’est de s’y mettre ! 💪

Et bien sûr, rester en conformité !

Merci ! Des questions ?