Comment être condamné par la CNIL

Date : 12 avril 2023
Speakers : Juliette Audema (Aircall)
Format : Université (45mn)
Newsletter : womenonrails.substack.com

Les bases

La **CNIL** : Commission Nationale Informatique et Liberté créée en 1978. Autorité indépendante de l'état chargée de veiller à la protection des données personnelles. 18 membres à la Commission et en 2021 : 250 agents
La CNIL de condamne pas, elle fait des mises en demeures et sanctionne

Ses missions :

1. Informer, protéger les droits
2. Accompagner la conformité / conseiller
3. Anticiper et innover
4. Contrôler et sanctionner

Moyens légaux

- On dit Le **RGPD** (et non pas La) : Règlement Général sur la Protection des Données mise en application en mai 2018

Qui est concerné par le RGPD : toute organisation publique ou privée qui traite des données personnelles dès lors qu'elle opère sur le territoire européen ou qu'elle propose des services à des européens. Le RGPD s'applique également aux sous-traitants.

Données personnelles : toute information se rapportant à une personne physique identifiée ou identifiable : exemple numéro de carte vitale, ou croisement de données : une femme qui habite à telle adresse

Au sein des données personnelles, on retrouve les données sensibles :

- Données relatives à la santé des individus
- Données concernant la vie ou l'orientation sexuelle
- Données qui révèlent une prétendue origine raciale ou ethnique
- Opitions politiques, syndicales …
- …

Traitement des données personnelles : opération ou ensemble d'opérations portant sur des données personnelles, quelque soit le procédé utilisé : collecte ; enregistrement, utilisation, consultation rapprochement, mise à disposition, extraction, adaptation, organisation …

Tout traitement doit être justifié

- Par un contrat
- L'intérêt légitime
- Le consentement

Les outils de la conformité au RGPD :

- Le registre des traitements et la documentation interne. Le responsable légal est le dirigeant de l'entreprise
- La cybersécurité et la notification de certains incidents : prévenir la CNIL et les utilisateurs dans certains cas
- AIPD : analyse d'impact sur la protection des données pour les traitements pouvant être sensibles
- Rôle de Délégué à la Protection des données (DPO)

La chaîne répression de la CNIL

4 étapes :

1. Le signalement :
    a. Plaintes d'utilisateur réalisées sur le site de la CNIL
    b. Autosaisine
    c. Presse
    d. Coopération au niveau Européen
2. Le contrôle :
    a. Sur place : des agents de la CNIL viennent demander l'accès aux données
    b. En ligne
    c. Convocation dans les bureaux de la CNIL
    d. Sur pièces
3. Les suites du contrôle
    a. Clôture
    b. Manquements : la présidente de la CNIL peut faire un rappel des obligations légales ou mettre en demeure
4. Mesures
    a. Rendre publique mise en demeure ou sanction (sur le site de la CNIL ou Légifrance)
    b. Non publique
    c. Pécuniaire (max de 4% du CA mondial ou 20Millions d'euros)
    d. Non pécuniaire

En 2022 : 345 contrôles, 147 mises en demeure et 21 sanctions pour un montant de 101 277 900 €.
Le tiers des sanctions concernent la sécurité des données personnelles.
2 REX de contrôle :

1. Alan (Charles Gorintin) : collaboration intelligente
2. Fidzup -> clé sous la porte

L'intégration avec les users

En tant que dév, comment faire pour respecter la RGPD ?
La CNIL a sorti un guide pour les équipes de dév : avec bonnes et mauvaises pratiques
Être clair et transparent auprès de ses utilisateurs et utilisatrices.
L'information doit être facile d'accès.
Les utilisateurs doivent pouvoir exercer leurs 7 droits :

1. Droit d'accès
2. Droit de rectification
3. Droit d'opposition :
4. Droit à l'effacement
5. Droit à la limitation
6. Droit à la portabilité
7. Droit à l'intervention humaine

Un site doit guider la personne sur la manière dont elle peut exercer ses droits.

Les mauvais élèves :

- 13/02/2023, 2 établissements de l'enseignement supérieur ont été mis en demeure pour leur non-conformité à la RGPD
- Refuser les cookies doit être aussi simple que les accepter : une vingtaine d'organismes mises en demeure le 25/05/2021
- Clearview AI siphonnait les photographies trouvées sur le web sans avoir le consentement des utilisateurs
- Brico Privé : compte désactivé mais données non supprimées
- Monsanto : fichier de lobbying avec une liste de personnes notées de 1 à 5 sur leur niveau d'influence
- Google Analytics : les données sont envoyées vers les Etats-Unis

Recommandations techniques

- La CNIL donne des conseils basiques sur les bonnes pratiques de code : versionning, utilisation de branche, ne pas commiter des secrets et des mots de passe, utiliser des clés SSH, utiliser des noms de variables et fonctions explicites, tester son code, mettre en place une CI, disposer de métriques, ne pas utiliser de données de prod pour les tests, respecter les exigences de sécurité de données (recommandations relatives aux mdp), faire attention aux injections
- Gestion des profils utilisateurs et collaborateurs
    - Identifications uniques et propres à chaque individu
    - Authentification avant accès à des données personnelles
    - Utilisation de compte root à proscrire, y associer une politique de mdp fort

- Documenter / automatiser les procédures de mouvement des collaborateurs
- Politique de gestion d'accès aux données (habilitations)

La CNIL recommande de minimiser le nombre de données collectées. Ne pas collecter certaines données si non nécessaires, supprimer la donnée une fois sa date de péremption dépassée