La Cagette - CR Réunion RGPD du 26/01/2018.

1ere réunion du comité.

Sujet: Que doit on faire pour respecter la nouvelle réglementation RGPD 2018?

Règlementation Générale des Données Personnelles
(version européanisée de la CNIL)

C'est très bien sur le fond mais ça peut être très lourd pour les structures :

Pour les sites web conçus à partir du 25 mai, la règlementation sera stricte.
Pour les sites web qui existaient déjà, il va falloir prendre des mesures proportionnées mais la CNIL ne mettra pas d'amendes immédiatement à partir du 25 mai. Pour une petite structure on ne devra pas mettre en oeuvre tout à la lettre mais il faut s'attaquer sérieusement à la mise en conformité.

Notion de données sensibles (nous ne sommes a priori pas concerné.e.s) :

- données de santé
- données syndicales
- orientation sexuelle
- opinions politiques
- opinions religieuses
- ...

Quel sera l'impact sur la Cagette, que devrons-nous faire à la Cagette ?

1/ Faire une cartographie des traitements de données personnelles :

quelles données perso a-t-on ? (faire la liste)
comment est-ce qu'on récupère les données,
pourquoi est-ce qu'on les récupère, quelle est la finalité ?
qui y a accès ?
Combien de temps on les garde (droit à l'oubli, sauvegardes…)

remarques : si on n'a pas besoin de les conserver, il faut qu'on les efface. Si on a besoin de les conserver pour une raison légitime, il faut les conserver

2/ Etablir un système de gouvernance

- Nommer un responsable : le DPD. Il peut être extérieur à la structure et il fait un audit permanent. Non obligatoire (cf la Cagette - Documentation et FAQ RGPD).
- mettre en place des procédures internes !
- former les personnes qui sont en contact.
- Avoir un registre des activités de traitement (à définir).
- Formaliser une analyse d'impact relative à la protection des données.

Rem : On est obligé.e.s de recueillir le consentement explicite de la personne avant d'utiliser ses coordonnées (et de les diffuser : c'est pourquoi le fichier coopérateurs, par exemple, doit être en accès très contrôlé)

4/ Les relations avec des tiers (les prestataires…)

Tous les partenaires avec qui nous travaillons doivent respecter la RGPD. Il ne faut pas que les données sortent de l'UE.

Chez nous il va falloir vérifier les contrats de :

- Gandi
- OVH
- Arithmétique
- drive
- Anybox
- Trobz (ils ont eu nos données dans le passé)
- Coopératic / François

5/ Garantir et renforcer la sécurité des traitements

- Principe de privacy by design : à partir du 25 mail, il faut que dès la conception du code de TOUTES les application, la protection des données soit prévue.
- Outils de détection des intrusions : on est obligés de prévenir les personnes dès qu'on détecte un piratage et on doit les prévenir le plus vite possible (24/48h).

Plan d'attaque :

(Copie du mail de Mathieu)

Voilà, j'ai créé quelques documents dans le dossier créé par Antonin, l'ensemble est utilisable et vous pouvez commencer à vous amuser :

- Cartographie des traitements = le fichier où indiquer les données personnelles qu'on récolte et les traitements qu'on leur applique. Il y aura forcément des données qui occuperont plusieurs lignes (emails des coopérateurs dans le Drive + chez sympa + dans Odoo + sauvegardés certainement).

- Documentation RGPD = des liens et des infos utiles, on l'enrichira certainement au fur-et-à-mesure. Il y a notamment les réponses aux questions qu'on avait posées la semaine dernière (pas encore toutes).
- Plan d'action RGPD = une vue générale des différentes étapes du boulot et de leur avancement.

Les prochaines actions :

- Vous pouvez commencer la cartographie dès maintenant.
- Il faudrait qu'on boucle l'étape 1 « Désigner un pilote ». Je ne sais pas si on peut avoir une personne unique ou s'il vaut mieux qu'on ait une équipe.
- Maintenant qu'on a identifié la faille majeure du fait que les coordonnées de coopérateurs sont ouvertes à tous les vents, il faudrait mettre quelques barrières au moins là.
- On a parlé d'un atelier avec les salariés et le 1er cercle. Il faudrait définir ce qu'on y met exactement, pour pouvoir ensuite le planifier.

a+
Mathieu