



Se mettre en conformité avec le RGPD, conseils d'Aurélie Banck (août 2019)

Après 4 ans de négociation au niveau européen, le RGPD (Règlement général sur la protection des données) est entré en application depuis le 25 mai 2018, a soufflé sa première bougie.
Mais votre association n'a encore rien fait ?

Aurélie Banck, directrice du département **Conformité RGPD Banque et Assurance** du cabinet Lexing et responsable pédagogique du Diplôme d'Université Data Protection Officer de l'Université de Paris Nanterre vous donne quelques conseils.

Quelles démarches faut-il entreprendre de toute urgence, si l'association n'a encore rien fait pour se mettre en conformité ?
Entamez les démarches recommandées par la CNIL (Commission Nationale Informatique et Liberté).

1/ Désignez un pilote qui va s'occuper de toute la procédure suivante

2/ Faire un état des lieux pour constituer un registre des traitements de données

A chaque activité recensée, expliquer l'objectif poursuivi, catégoriser les données collectées, dire qui a accès à ces données et indiquer leur durée de conservation.

Exemple pour un fichier d'adhérents : quelles informations personnelles collectez-vous (nom, prénom, adresse, e-mail, âge...) ?

Comment : via un formulaire en ligne ou papier ?

Où est hébergée la base de données : dans le cloud ou sur un ordinateur ?

3/ A partir de cet état des lieux, mettre en place des procédures pour prioriser

Faites un tri pour ne garder que les données essentielles, vérifiez que vous n'avez pas de données sensibles qui nécessitent un traitement particulier, assurez-vous que les données ne sont pas accessibles à tous, regardez la durée de conservation des données.

4/ Respectez les droits des personnes

Dès que vous collectez des données, le support (formulaire, questionnaire...) doit expliquer pourquoi, qui a accès, combien de temps, comment exercer ses droits d'opposition et précisez si des données sont transférées hors de l'Union européenne.

Attention au risque de détournement des données.

Par exemple, si un élu local souhaite utiliser votre fichier d'adhérent pour mener sa campagne. C'est bien évidemment punissable.

Ajoutons qu'aucune organisation n'est à l'abri d'un dépôt de plainte si des membres particulièrement sensibles à leurs données constatent que l'association n'est pas dans les clous.

5/ Sécurisez les données

Attention, par exemple, si vous détenez des certificats médicaux pour pratiquer un sport et si l'accès à ces données n'est pas correctement sécurisé car nous entrons dans des données sensibles.

Si l'association rencontre un problème : piratage, fuite des données... elle a **72h pour alerter la CNIL**.

Quels risques sont encourus, si on ne fait rien ?

Vous risquez jusqu'à **20 000 millions d'euros d'amende ou de 2 à 4 % du chiffre d'affaire mondial**.

La CNIL inspecte aussi les associations.

Et un mois après son entrée en vigueur, l'ADEF (Association pour le Développement des Foyers) s'est vue infligée une sanction de 75 000 € pour faille de sécurité de son site Web.

D'autres associations ont aussi été épinglées.

Est-il obligatoire de nommer un DPO (Délégué à la Protection des Données) ?

Il n'y a pas d'obligation mais le chef de projet (étape 1) pourrait naturellement devenir le DPO de l'association.

Veillez à éviter les conflits d'intérêt.

Le DPO ne peut pas être celui qui s'occupe de la sécurité de la base de données de vos adhérents.

Ses fonctions de conseil et de contrôle doivent s'exercer en toute neutralité.

Mon conseil

Sensibiliser et former plusieurs personnes dans l'association.

Par exemple : les chargés de campagnes car les collectes de dons drainent des collectes de données.

Propos recueillis par Évelyne Jardin pour Associathèque

- Pour en savoir plus :
- [Dossier thématique RGPD](#)
- [Entamer les démarches](#)
- [Conseils et modèle de registre](#)
- [Infos sur le DPO](#)
- [Suivre le MOOC de la CNIL](#)
- [Sur le 1^{er} anniversaire du RGPD](#)

Et aussi : Aurélie Banck, RGPD : la protection des données à caractère personnel, 18 fiches pour réussir votre mise en conformité, Gualino, 2019, 2^{ème} édition.