ÉGLISE CATHOLIQUE DANS L'OISE | Service du catéchuménat

BONNES PRATIQUES EN MATIERE DE COLLECTES DE DONNEES PERSONNELLES

INDICATIVES ET NON-EXHAUSTIVES

Collecter et traiter des données personnelles implique avant tout **d'informer les personnes sur ce que vous faites de leurs données et de respecter leurs droits.**

En tant que responsable d'un traitement de données, vous devez prendre des mesures pour **garantir une utilisation de ces données respectueuses de la vie privée des personnes concernées.** Il est donc obligatoire d'inscrire une clause « protection des données personnelles » dans tous les documents où sont transmis des données personnelles (nom, prénom, numéro de téléphone, mail, adresse, religion, date de naissance …) qu'ils soient en format numérique ou papier.

Les données que vous collectez entrant dans la catégorie des données sensibles (convictions religieuses, santé) au sens du règlement général sur la protection des données (RGPD) et concernant parfois des mineurs, il est indispensable d'entreprendre une démarche au niveau paroissial pour mettre en conformité ces traitements vis-à-vis du RGPD et de la loi Informatique et Libertés.

Vous trouverez ci-dessous quelques bons réflexes à suivre, tels que peut les préconiser la Commission nationale informatique et libertés (CNIL) dans son guide pratique de sensibilisation au RGPD !

1- Ne collectez et conservez que les données vraiment nécessaires

Il est nécessaire de bien préciser quelles sont les données qui sont indispensables par rapport à celles qui ne sont qu'utiles (il est possible de les distinguer par une couleur, un astérisque etc.).

Posez-vous les bonnes questions : Quel est mon objectif ? Quelles données sont indispensables pour atteindre cet objectif ? Ai-je le droit de collecter ces données ? Est-ce pertinent ? Les personnes concernées sont-elles d'accord ?

En ce qui concerne la durée de conservation des données et tri des données avant archivage, il faut une durée de conservation appropriée pour chaque donnée. Rappel, il n'est pas nécessaire de conserver toutes les données → cela passe par la formation des personnes en charge des dossiers

2- Soyez transparent

Une information claire et complète constitue la base de la confiance réciproque qui vous lie avec les personnes dont vous traitez les données.

Ainsi quand on collecte des données personnelles, le support doit contenir

- Une finalité
- Un fondement juridique ou une utilité légitime (à justifier)
- les noms des personnes qui y auront accès
- Leur durée de conservation
- Les modalités pour permettre aux intéressés d'exercer leurs droits (effacement, portabilité …) la CNIL recommande un temps de réponse très rapide pour faire droit à la demande d'une personne.

3- Pensez aux droits des personnes

Vous devez répondre dans les meilleurs délais (1 mois maximum), aux demandes de consultation, de rectification ou de suppression des données. Il est donc indispensable de mettre en place un processus interne permettant de garantir l'identification et le traitement des demandes dans ces délais courts. (Déterminer qui prévenir, le nom de la personne à contacter, courriel et adresse)

4- Gardez la maîtrise de vos données

Le partage et la circulation des données personnelles doivent être encadrés, sécurisés, afin de leur assurer une protection à tout moment :

- Vérifiez que seules les personnes habilitées ont accès aux données dont elles ont besoin (code d'accès)
- Evitez les photocopies et l'enregistrement des fichiers sur des clés USB
- Assurez-vous que vous ne conservez pas les données au-delà de ce qui est nécessaire

5- Identifiez les risques

Certaines données ou certains types de traitement nécessitent une vigilance particulière. C'est le cas des données dites « sensibles » (religion, origine raciale, santé…) ou celles qui concernent des mineurs, qui ne peuvent être utilisées que sous certaines conditions strictement encadrées par la loi.

6- Sécurisez vos données

Les mesures de sécurité, informatique (code d'accès, identifiant de connexion, éviter le « cloud » …) mais aussi physique (documents papiers ou listing informatique rangés dans une pièce, ou un tiroir fermé à clef), doivent être adaptées en fonction de la sensibilité des données et des risques qui pèsent sur les personnes en cas d'incident.

Minimisez les risques de pertes de données ou de piratage informatique par la mise à jour des logiciels, changement des mots de passe qui doivent être complexes, sécurisation des serveurs, chiffrement des données.

Il faut penser à toutes ces informations et règles dès le moment de la création des dossiers numériques, il est donc nécessaire de sensibiliser les responsables à ces questions lors de leur recrutement.