Fédération des Églises Adventistes du septième jour du Nord de la France
Règlement général sur la protection des données

Le RGPD, pour Règlement Général sur la Protection des Données, est un règlement de l'Union européenne. Celui-ci concerne directement toutes les entités françaises qui récoltent et rassemblent des données personnelles**.** Le règlement pose un cadre juridique plus sécurisant autour du consentement, des responsabilités et des obligations de chacune des parties que sont les entreprises, les fondations, les organismes, les associations, etc., d'un côté, et les particuliers et leurs données, de l'autre. Il est entré en vigueur le 25 mai 2018.

L'objectif principal de cette nouvelle réglementation est d'accroître la protection des personnes quant au traitement de leurs données personnelles. Il s'agit de (re)donner aux citoyens le contrôle de leurs données à caractère personnel**.**

La notion de données personnelles

Une distinction est à faire entre « données personnelles », « données publiques » et « données sensibles ».

Les « données personnelles » sont toutes les informations se rapportant à une personne physique identifiée, comme son adresse, son numéro de téléphone, sa date de naissance, etc. En tant qu'église, et donc en tant qu'associations cultuelles et culturelles (ACSA), il s'agit principalement des éléments fournis par les membres d'église et les personnes intéressées (visiteurs).

Les « données publiques » sont disponibles pour tous, produites par l'État ou une collectivité territoriale. Par exemple, ce sont des adresses mail disponibles sur un site web. Les églises ne sont pas concernées par ces données.

Les « données sensibles » concernent, par exemple, des éléments liés à la santé des individus, éléments qui doivent rester entre le milieu médical et la personne prise en charge par ce milieu (et sa famille le cas échéant). Ou encore, autre domaine, la géolocalisation. À nouveau, les églises ne sont pas concernées par ce domaine.

Et les données papier, même combat ?

Comme pour les données informatiques, les éléments papier sont concernés par la réglementation qui est même plus contraignante pour les documents physiques. Par exemple, il faut systématiquement détruire les données de personnes qui n'ont pas répondu à plusieurs sollicitations, comme une invitation à participer à une activité de l'église, depuis plus de trois ans.

Mettre en œuvre le RGPD

Mettre en œuvre le RGPD au sein de l'église, et ses associations, nécessite de :

1. Nommer un DPO

Première étape, il faut désigner un(e) responsable RGPD au sein de l'église pour les deux associations (cultuelle et culturelle). Cette personne doit être un bon pilote pour mener à bien la mise en conformité de l'église : elle doit posséder les qualités requises : rigueur, sens de l'organisation, connaissance du fonctionnement de l'église et connaissance du RGPD. Le plus simple, c'est qu'il s'agisse d'un des responsables de l'association (le/la secrétaire semble être la solution la plus pertinente, car elle gère plusieurs des listings de l'église). Ce responsable devient alors le DPO pour "Data Protector Officer" en anglais, soit le "Responsable de la protection des données" en français, de l'église et de ses associations. Il est l'unique référent et l'interlocuteur principal pour toutes les questions relatives à la protection des données au sein de l'église.

2. Identifier les différents fichiers et documents et déterminer leur utilité

Ensuite, deuxième étape, il s'agit d'identifier les différents fichiers et documents contenant les données nécessaires à la bonne organisation de l'église et de ses associations. Il s'agit d'établir une cartographie, appelée aussi « registre des données » faisant ressortir les fichiers et/ou documents nécessaires au fonctionnement de l'église, ainsi que le but de leur existence.

Compte tenu du fonctionnement habituel d'une église adventiste, il semble nécessaire d'avoir les listes suivantes, qui sont justifiées pour sa bonne organisation :

- Liste des membres (cultuelle et culturelle, listes identiques),
- Liste des donateurs (dîmes – pour l'établissement des reçus fiscaux),
- Liste des donateurs (dons dédiés – pour la mise aux normes des bâtiments servant aux églises – pour l'établissement des reçus fiscaux),
- Liste des intéressés afin de pouvoir les contacter et les inviter à une activité de l'église/de l'ACSA,
- Liste des nominations (cultuelle et culturelle),

- Liste des jeunes (antenne locale de la FFJAN),
- Liste des membres de telle ou telle entité, par exemple la chorale, un groupe, les personnes âgées, pour l'organisation de leurs activités.

Cette étape doit amener à ne conserver que les fichiers absolument nécessaires et à supprimer tout le reste ! Il faut faire apparaître les informations récoltées et, surtout, dans quel but elles le sont, et donc leur nécessité, pour la vie des deux associations qui servent de support à l'église.

Il convient également de pouvoir expliquer qui a accès à ces données et pourquoi.

Ainsi, avec cette cartographie, il est possible d'anticiper un éventuel contrôle (effectué par la Commission Nationale Informatique et Libertés – la CNIL) en créant et en mettant à jour régulièrement les documents à présenter le jour de cette vérification.

3. Recueillir le consentement

C'est l'élément central de ce nouveau règlement. Il faut faire apparaître la demande de consentement sur chaque récolte de données. Celui-ci devra prendre la forme d'un texte qui doit clairement présenter les informations collectées et, surtout, dans quel but. Ce consentement doit être demandé explicitement aux personnes fournissant leurs données, par exemple via une case à cocher sur une carte à remplir lors d'un effort d'évangélisation ou au travers d'une signature (nettement plus probant que la case à cocher) comme sur la fiche de renseignements des membres (voir les fichiers fournis par la Fédération). Il en est de même pour les pages web du site Internet de l'église (exemple : envoi d'une newsletter mensuelle).

Il convient dans ce cadre de bien faire comprendre aux membres d'église quel sera l'usage de leurs données personnelles, comment elles seront stockées et qui y aura accès… Et que – sans ces éléments – la vie de l'église, ainsi que leur implication dans celle-ci, peut s'avérer compliquée…

4. Préservation de la confidentialité

Bien évidemment, les listes de membres ne sont pas à diffuser à tous les membres de l'église, même si certains les demandent ! Au contraire, ces listes ne devraient être en possession que des personnes définies, selon chacune de ces listes, dans l'unique cadre du bon fonctionnement de l'église et de l'ACSA tel qu'explicité au point 2. Par exemple, la liste des membres avec leurs coordonnées complètes ne devrait être accessible qu'au pasteur (président des deux associations), au/à la secrétaire et au trésorier de l'église.

Par ailleurs, autre exemple, pour le bon fonctionnement des nominations, le/la secrétaire de l'église fournit au président de la commission de nominations (le pasteur, généralement) la liste des personnes nommées sortantes ainsi que celle des membres de l'église, en version simplifiée : nom, prénom, poste de responsabilité.

Quand les nominations ont été votées par l'église, elles sont envoyées à la Fédération pour son usage interne uniquement (envoi de documentations, publicité pour les activités organisées par

la Fédération à relayer dans les églises, convocations, etc.), ce qu'il est important également de souligner auprès des frères et sœurs nommées en obtenant leur consentement (voir les fichiers des listes de nominations à adresser à la Fédération). Dans ce cadre, il convient de conserver localement un double de ces fichiers avant de les adresser à la Fédération. Cette dernière, elle aussi, met en place les éléments nécessaires à la mise en conformité de la réglementation de la RGPD !

Une remarque ici, afin d'être le plus explicite possible : même s'il n'est pas possible d'obliger une personne qui est sollicitée pour être nommée à telle ou telle responsabilité dans l'église à fournir les éléments qui la concerne (adresse, téléphone, email), il convient de bien préciser que le fonctionnement normal de l'église et de la Fédération implique l'acceptation pour ce frère ou cette sœur du fait que ses données personnelles sont conservées durant son mandat au sein de l'église locale et de la Fédération. En cas de refus, comment est-il possible pour la Fédération d'avoir une communication efficace avec les églises qu'elle regroupe ?

5. Sécurisation

La sécurité des données est essentielle ! L'ordinateur de l'église doit être protégé par un mot de passe connu uniquement des personnes qui sont censées l'utiliser : pasteur, secrétaire, trésorier, par exemple. Dans une pièce dont l'accessibilité est, elle aussi, limitée (clé). Et si cet ordinateur est connecté à Internet, il est équipé des pare-feu et antivirus nécessaires, et même, encore mieux d'un VPN (Virtual Private Network), limitant les risques de piratage des données.

En cas de difficultés dans ce domaine, il faut faire un signalement à la CNIL dans les 72 heures qui suivent la découverte du problème en question, et prévenir également les personnes concernées, celles qui ont fourni leurs données personnelles.

Dans le même domaine, attention aux fiches papier et autres documents physiques, à leur stockage et à leur accès qui doit être, là encore, limité aux seules personnes autorisées à les consulter (placards fermés à clé, coffre-fort, etc.).

Pour résumer

Pour une église, et ses deux associations, être en conformité avec le RGPD signifie :

- Nommer une personne qui soit le DPO de l'église
- Collecter uniquement les renseignements nécessaires
- Tracer l'ensemble des documents et fichiers mis en place servant au traitement des données personnelles : cartographie en indiquant le but de la collecte de ces données
- Demander et sauvegarder le consentement des personnes pour le traitement de leurs données, en leur laissant la possibilité de connaître les éléments que vous conservez sur elles, en gérant bien ce qui concerne l'église locale et ce qui concerne la Fédération
- Respecter la confidentialité des personnes et de leurs données
- Sécuriser les données collectées (stockages physique et numérique)
- Informer (dans les 72 heures maximum) la CNIL et les personnes concernées si leurs données personnelles dans votre base ont été volées (documents) ou/et piratées (fichiers informatiques).

Voir le site de la CNIL : https://www.cnil.fr/fr/rgpd-par-ou-commencer