ACCUEIL DES VILLES FRANÇAISES

AVF

ACCUEIL DU NOUVEL ARRIVANT

FICHE ACTION N° 12.1.

RGPD

URAVF PACA

◊ QUOI ?

Création par l'URAVF PACA d'un « Pôle de compétences régional RGPD » conduit par un « Référent régional RGPD », pour accompagner les AVF dans la mise en œuvre du dispositif de Protection des Données.

◊ POURQUOI ?

Le RGPD (Règlement du Parlement européen et du Conseil, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données) est applicable depuis le 25 mai 2018, y compris dans le monde associatif.

Mais les responsables associatifs qui, souvent, ont une connaissance incomplète du RGPD et des règles à respecter dans la gestion des données personnelles de leurs adhérents, même s'il ne s'agit pas de données « sensibles », ont, soit sous-estimé les dispositions à mettre en œuvre dans leur secteur (une simple mention dans le bulletin d'inscription ou sur le site n'est pas suffisante), soit, à l'inverse, été freinés par une apparente complexité du dispositif.

◊ POUR QUI ?

- Les responsables des AVF de la région,
- Leur éventuel Délégué à la Protection des Données (DPD).

◊ QUI ?

- À la demande de l'Union Régionale, un adhérent, Délégué à la Protection des Données (DPD) *(ou DPO pour Data protection Officer)* déjà formé et inscrit à la CNIL, assure une sensibilisation à la mise en œuvre du dispositif de conformité des données. Il est assisté de personnes motivées et formées pour assurer la diffusion dans toute la région et composer un pôle de compétences. L'objectif est d'aboutir à l'identification et à la mise en place de responsables du RGPD dans chaque AVF et à la mise en œuvre du dispositif.
- L'adhérent assure également la fonction de DPD pour l'URAVF.

◊ COMBIEN ?

- Toute l'équipe du « Pôle de compétence RGPD » est bénévole.
- Les séances de sensibilisation proposées aux responsables des AVF sont prises en charge par la région.

➔➔ Voir l'exemple pratique de l'URAVF PACA au dos.

Expérience de l'*URAVF Provence-Alpes-Côte d'Azur*

Les organisations doivent pouvoir garantir et prouver leur conformité en matière de protection des données personnelles. Pour les guider, la Commission Nationale de l'Informatique et des Libertés (CNIL), l'autorité de surveillance numérique française, conseille les associations afin de faire face à cette responsabilité accrue.

Étape	Détail
Étape 1 : identifier un responsable de la protection des données	La désignation d'un référent ou d'un DPD / DPO, chargé de piloter les démarches de mise en conformité au RGPD n'est pas obligatoire pour les associations. Pour autant, afin de consolider les relations de confiance avec les personnes concernées, et limiter les risques juridiques et d'image liés à une mauvaise utilisation des fichiers, elles ont tout intérêt à se doter d'une telle fonction ou à confier à une personne la mission de veiller au bon respect par la structure des règles applicables en la matière.
Étape 2 : Recenser les fichiers	Un registre des fichiers comportant des données personnelles est une documentation qui permet de faire le bilan sur l'effet du règlement.
Étape 3 : Faire le tri dans les données	Ce tri permet de vérifier que les données traitées sont bien pertinentes et nécessaires à l'objectif poursuivi, que seules les personnes habilitées ont accès aux données dont elles ont besoin et que des mesures de sécurité adaptées sont mises en place et que les données ne sont pas conservées plus longtemps que nécessaire
Étape 4 : Faire preuve de transparence	Les personnes doivent être informées à chaque fois que des données personnelles sont recueillies, sous format papier, numérique (questionnaires, bulletins d'adhésion, bulletins d'abonnement, etc.). Il est recommandé une information orale en plus d'une information écrite afin de s'assurer de la bonne compréhension par la personne concernée des informations communiquées.
Étape 5 : Organiser et faciliter l'exercice des droits des personnes	Toute personne concernée a des droits sur ses données. Elle peut notamment obtenir la confirmation que vous traitez ou non des informations la concernant, accéder à celles-ci et en obtenir la copie, ou faire effacer ses données.
Étape 6 : Sécuriser les données	Les incidents, internes ou externes, malveillants ou accidentels, peuvent avoir des conséquences importantes pour les personnes dont les données sont concernées (réputation, chantage, etc.). Pour limiter les risques, vous devez mettre en place des mesures de sécurité pour empêcher : • l'accès illégitime à des données (atteinte à la confidentialité) ; • leur modification non désirée (atteinte à l'intégrité) ; • leur disparition (atteinte à la disponibilité).

ACTIONS POUR LA MISE EN ŒUVRE

- Séances de sensibilisation,
- Accompagnement à la mise en œuvre avec exemple concret d'un AVF (sur site ou en atelier),
- Information sur la sécurisation physique des données.

PÔLE ASSISTANCE

Réponses aux questions des responsables AVF ou des webmestres.

➔ ➔**Pour plus de renseignements, vous pouvez vous adresser à Philippe Régnier : *phr-avf@hotmail.fr***