fédération des conseils de parents d'élèves
des écoles publiques

Veille juridique

Réglementation Générale sur la Protection des Données

FCPE – Mai 2018

Contenu

1. Qu'est-ce que la RGPD ? ***2***

2. Qui est concerné par la RGPD à la FCPE ? ***2***

3. Qu'est-ce que ça change ? ***2***

4. Comment se mettre en conformité ? ***3***

4. Impact de la RGDP sur NORMA ? ***4***

5. Impact sur BAL/BAF ***5***

6. que faire si vous gérez une base de données ? ***5***

1. Qu'est-ce que la RGPD ?

Le 25 mai 2016, une nouvelle règlementation européenne sur la protection des données personnelles a été mise en place.
Communément appelée RGDP, la Règlementation Générale des Données personnelles entre en vigueur en France le 25 mai 2018.
C'est une réglementation qui s'applique à toutes les entités qui collectent, traitent et stockent des données personnelles dont l'utilisation peut directement ou indirectement identifier une personne.

Attention :

Un simple nom est une donnée personnelle. De ce fait, une liste de personnes adhérentes d'une association rentre dans le cadre de la nouvelle réglementation et doit s'y conformer. Ainsi, à partir du moment où une association collecte des informations sur ses membres (par exemple : le nom, le prénom, l'adresse e-mail, l'adresse postale, le numéro de téléphone, …), elle doit, à la date du 25 mai 2018, avoir au moins entrepris les actions nécessaires à la mise en conformité de votre base de données.

2. Qui est concerné par la RGPD à la FCPE ?

Ainsi que précisé précédemment, toutes les structures sont concernées dès lors que l'on tient une liste d'adhérents.

- La fédération est en premier lieu concernée car elle est détentrice de la base NORMA qui contient les données personnelles des adhérents mais aussi de leurs enfants. A ce titre, des règles très strictes de la CNIL sont déjà en application et devront être renforcées
- les CDPE dès lors qu'ils détiennent des listes d'adhérents ou de bénévoles via des fichiers Excel, des fichiers partagés en cloud, ou autre.
- les conseils locaux qui tiennent des listes de leurs adhérents ou qui sont amenés à détenir et/ou utiliser d'autres listes comme ceux des effectifs par classe, etc.

3. Qu'est-ce que ça change ?

Les 6 principales nouveautés apportées par la RGPD sont :
1 : Le renforcement des droits des personnes : *il impose de recueillir et conserver le consentement au traitement des données personnelles.*
2 : L'obligation d'information : *il impose aux structures victimes d'un piratage des données personnelles d'informer dans les 72 heures la Commission Nationale de l'Informatique et des Libertés (CNIL) et les personnes concernées dont les informations ont été volées.*
3 : Des sanctions lourdes : *il met en place des sanctions dissuasives, pouvant aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire mondial d'une organisation. Le montant le plus élevé étant celui retenu.*
4 : Le principe de minimisation des données collectées : *il impose de ne collecter que les renseignements strictement nécessaires au regard des finalités pour lesquelles elles sont traitées.*
5 : Le droit de portabilité des données : *les personnes, dont les informations ont été collectées, ont le droit de demander à recevoir les données à caractère personnel les concernant.*

6 : Le registre des données : *il oblige les organisations à tracer l'ensemble des traitements des données personnelles mis en œuvre au sein de l'organisation.*

Attention : lorsque vous mettez en place un formulaire en ligne à remplir avec ne serait-ce qu'une adresse mail, vous collectez des données personnelles donc vous êtes soumis à la RGPD.

Dans votre formulaire, une case à cocher doit être prévue pour que la personne qui remplit le formulaire indique son consentement pour l'utilisation des données qu'elle fournit. De plus, un texte inclut ou non dans les conditions d'utilisation du formulaire doit expliquer ce que le CDPE ou le CL fera des données en question, de sorte que la personne qui coche la case le fasse en toute connaissance.

La case ne doit pas être pré-cochée. Les données collectées doivent permettre de connaître la date à laquelle la personne à accepter l'utilisation de ses données personnelles, donc ces informations doivent aussi être conservées.

Si le consentement a été donné sur un bulletin d'adhésion, il faudra conservé ce bulletin d'adhésion pendant toute la durée de la présence de la personne dans la base de données.

4. Comment se mettre en conformité ?

La CNIL a mis en place un guide complet pour rappeler les précautions à prendre en la matière.
Il en ressort 4 étapes :

- ***Recenser les données personnelles traitées****, les supports et emplacements où sont conservées ces données. Définir une personne responsable du traitement de ces données. Par défaut, ce sera le/la président(e) du CDPE ou du CL s'il est en association*
- ***Répertorier les risques potentiels*** *engendrés par les données conservées. (comprendre le type de données traitées, les impacts potentiels du traitement de ces informations sur les droits et libertés des personnes concernées, analyser les mesures prises ou à prendre pour se prémunir de ces risques potentiels (contrôle d'accès, chiffrement...) et leur gravité potentiel.*
- ***Mettre en place et tester les mesures*** *prises pour se mettre en conformité.*
- ***Réaliser des audits externes*** *de sécurité pour tester régulièrement le niveau de sécurité*

La CNIL précise également les mesures à prendre :

1. *Sensibiliser les utilisateurs c'est-à-dire la/les personnes(e) qui gère(nt) la base de données*
2. *Authentifier les utilisateurs*
3. *Gérer les habilitations, c'est-à-dire les droits d'accès*
4. *Tracès les accès et gérer les incidents c'est-à-dire pouvoir dire à tout moment qui a accéder aux données, à quel moment et pourquoi y faire*
5. *Sécuriser les postes de travail par des mots de passe pour s'assurer que les données ne seront pas accessibles à toute personne qui accède à ces postes de travail*
6. *Sécuriser l'informatique mobile*
7. *Protéger le réseau informatique interne*
8. *Sécuriser les serveurs*
9. *Sécuriser les sites web*
10. *Sauvegarder et prévoir la continuité d'activité (par des sauvegardes et archives externes)*
11. *Archiver de manière sécurisée*

12. *Encadrer la maintenance et la destruction des données*
13. *Gérer la sous-traitance*
14. *Sécuriser les échanges avec d'autres organismes*
15. *Protéger les locaux*
16. *Encadrer les développements informatiques*
17. *Chiffrer, garantir l'intégrité ou signer*

Pour la taille des données collectées par les CDPE et surtout les CL, il convient :
- de disposer d'un tableau précis sur la nature des données collectées
- d'informer les personnes concernées que leurs données qui seront précisées sont détenues et qu'ils ont un droit de modification à ces données
- d'identifier avec précision auprès de qui et par quels moyens ces données sont stockées et sauvegardées
- de s'assurer que les ordinateurs et/ou serveurs contenant ces données sont accessibles seulement à des utilisateurs identifiés (accès personnalisé)

Attention :
Pour la taille des données collectées par les CDPE et surtout les CL, il convient :
- de disposer d'un tableau précis sur la nature des données collectées
- d'informer les personnes concernées que leurs données qui seront précisées sont détenues et qu'ils ont un droit de modification à ces données
- d'identifier avec précision auprès de qui et par quels moyens ces données sont stockées et sauvegardées
- de s'assurer que les ordinateurs et/ou serveurs contenant ces données sont accessibles seulement à des utilisateurs identifiés (accès personnalisé)

4. Impact de la RGDP sur NORMA ?

La base Norma a la particularité d'être déjà bien encadré par les dispositions de la CNIL.
Avec la mise en place de l'espace adhérent, chaque adhérent a accès à ses données personnelles collectées par la FCPE et pourra en demander la modification et/ou la suppression comme c'est déjà le cas actuellement.

Les adhérents sont déjà informés de l'utilisation que fait la FCPE de leurs données au travers du bulletin d'adhésion.

Vous pouvez adresser le texte ci-dessous en plus à vos adhérents en complément :

« Les informations collectées par le CDPE du XXXXX , directement auprès de vous, font l'objet d'un traitement informatique [gestion et de suivi de ses adhérents]…… par le CDPE du XXXX et la fédération nationale. Vos informations sont à destination du CDPE, de la FCPE et du conseil local et sont conservées pendant 3 ans à l'issue de votre dernière année d'adhésion
Conformément au Règlement (UE) 2016/679 relatif à la protection des données à caractère personnel, vous disposez des droits suivants sur les données vous concernant : droit d'accès, droit de rectification, droit à l'effacement (droit à l'oubli), droit d'opposition, droit à la limitation du traitement, droit à la portabilité. Vous pouvez également définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après votre décès.
Vous pouvez, pour des motifs tenant à votre situation particulière, vous opposer au traitement des données vous concernant.

Pour exercer vos droits, merci d'adresser votre courrier à FCPE du XXXX, adresses à compléter, ou par courriel à informatique@fcpe.asso.fr et le mail du CDPE……
Sous réserve d'un manquement aux dispositions ci-dessus, vous avez le droit d'introduire une réclamation auprès de la CNIL. »

Cette information sera renforcée sur l'adhésion en ligne pour répondre aux obligations en la matière.

Sur le logiciel BAL, des dispositions ont été prises :

5. Impact sur BAL/BAF

Dans le cadre du Règlement Général de Protection des Données (RGPD), applicable à partir du 25 Mai 2018, la protection des données a été renforcée dans le logiciel Bourse aux Livres :

- *Fichier d'import Norma crypté et protégé par mot de passe*
- *sauvegarde cryptée et protégée par mot de passe.*
- *cryptage des données lorsque le logiciel n'est pas utilisé.*
- *journalisation des opérations effectuées.*
- *création d'un droit de gestion de base de données pour les utilisateurs.*

Une procédure spécifique est fournie aux utilisateurs de BAL.

6. que faire si vous gérez une base de données ?

Créez des utilisateurs par opérateur et non par poste.

Se déconnecter de la base de données après chaque utilisation

Site réseau : fermez la base de données quand la session de travail est finie.

N'attribuez les droits de Gestion de bases de données qu'à des personnes de confiance.

Changez le mot de passe de l'utilisateur ADMIN. Ne conservez pas celui donné par défaut.

Ne stockez pas vos sauvegardes dans les mêmes lieux que votre ordinateur.