FOCUS

RGPD ?[1]

Et si on faisait le point ?

Que vise ce règlement ?

L'objectif de ce règlement est de protéger les données personnelles des citoyens européens et également de réglementer le transfert des données en dehors de l'Union européenne.

Le RGPD vise **trois objectifs** :
- L'uniformisation européenne de la règlementation sur la protection des données ;
- La responsabilisation des entreprises ;
- Le renforcement du droit des personnes.

Qui est concerné par le RGPD ?

Toutes les structures qui traitent des données à caractère personnel sont concernées par cette nouvelle réglementation.

Peu importe la taille de la structure ou de son secteur d'activité.
Les Ecoles de Devoirs doivent donc se conformer au RGPD.

Que signifie « Donnée à caractère personnel » ?

Toute information se rapportant à une personne physique identifiée ou identifiable[2].
Par exemples : nom et prénom, adresse, lieu et date de naissance, numéro de registre national, ...

Que signifie « Traiter les données » ?

Le traitement est défini comme toute opération ou tout ensemble d'opérations effectuées ou

1. Réglement général sur la protection des données
2. Par exemple, par un numéro client.

non à l'aide de procédés automatisés et appliqués à des données ou des ensembles de données à caractère personnel.
Par exemples : collecte, enregistrement, organisation, structuration, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission, diffusion, mise à disposition, rapprochement ou interconnexion, limitation, effacement ou destruction.

Comment vous conformer ?

En tant qu'employeur, vous avez la casquette de **responsable du traitement**.

1. Cartographier vos traitements de données personnelles

Pour effectuer cet état des lieux, il faut mener une réflexion générale sur l'ensemble des données personnelles traitées nécessaires pour chacune de vos activités (exemples : données des enfants, gestion du personnel, recrutement...).

Cette étape est importante pour mettre en place votre plan d'actions.

2. Prioriser les actions à mener

▶ Registre des données

Sur base de l'inventaire que vous avez effectué, vous devez constituer un **registre de vos traitements de données**[3]. Pour ce faire, nous vous proposons d'utiliser le modèle présenté par la CNIL.

La CNIL propose une méthode pour la mise en place du registre sur base de 6 questions.
Pour chaque traitement de données opéré, le registre devra contenir les informations spécifiques suivantes :

- **Qui s'en occupe ?** Identifiez le responsable de traitement.
- **Quoi ?** Identifiez les catégories de données traitées.
- **Pourquoi ?** Indiquez la ou les finalités pour lesquelles vous collectez ou traitez ces données. Autrement dit, les raisons et objectifs.
- **Où ?** Déterminez le lieu où les données sont conservées. Indiquez dans quels pays les données sont éventuellement transférées.
- **Jusqu'à quand ?** Indiquez, pour chaque catégorie de données, le délai de conservation
- **Comment ?** Quelles mesures de sécurité sont mises en œuvre pour minimiser les risques d'accès non autorisés aux données et donc d'impact sur la vie privée des personnes concernées ?

Le registre va permettre d'avoir une vision globale sur l'ensemble de vos traitements. Il permet également de vous interroger sur le besoin réel de traiter les données par votre EDD. Cela permet de renforcer votre politique de protection des données en vous demandant si :

- les données traitées sont-elles nécessaires à vos activités ?
- les accès aux données sont-ils limités aux seules personnes habilitées ?
- la conservation des données est-elle bien limitée ?

▶ Communication

Vous devez informer les personnes concernées des traitements de données à caractère personnel. Pour ce faire, chaque fois que vous collectez des données personnelles (par exemple, les données médicales des enfants),

3. La tenue du registre est obligatoire pour les entreprises de 250 employés ou plus, et pour les plus petites entreprises qui traitent régulièrement des données ou qui traitent des données sensibles. En école de devoirs, nous pouvons être amené à traiter des données sensibles.

vous devez préciser, sur le support utilisé (formulaire, fiche, questionnaire...), un ensemble de mentions d'information :
- la ou les finalité(s) du traitement ;
- la personne gérant l'accès aux données et les modalités d'exercice des droits des personnes concernées ;
- le temps de conservation de ces données ;
- les destinataire(s) des données.

Cette information doit être claire et compréhensible pour tout un chacun.
Il est important d'obtenir **le consentement** de la personne concernée. En cas de traitement de données d'enfant mineur, il y a lieu d'obtenir l'accord du/des parent(s) ou du/des tuteur(s) pour le traitement.

▶ Droit des personnes concernées

Vous devez mettre en place l'ensemble des procédures internes pour consacrer les droits des personnes concernées : droit d'accès, de rectification, d'opposition, d'effacement, à la portabilité et à la limitation de ces données.

Il y a lieu de vérifier si les procédures actuelles dans votre structure prévoient tous les droits que la personne concernée peut invoquer. Dans la négative, vous devez déterminer les modalités d'exercice de ces droits (comment faire, qui se charge des demandes, quelles procédures suivre).

▶ Politique interne de protection des données

De manière générale, il faut établir un ensemble de règles contraignantes, d'outils et de bonnes pratiques en matière de protection des données. Cela peut être réalisé par le biais d'un code de conduite.
La politique doit traduire les principes de protection des données à savoir :
- les données doivent être traitées loyalement et licitement ;
- elles peuvent être collectées uniquement pour des finalités limitées et explicites ;
- les données collectées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles ont été collectées ;
- elles doivent être exactes et, si nécessaire, mises à jour ;
- elles doivent être conservées pendant une durée n'excédant pas celle nécessaire ;
- elles doivent être traitées conformément aux droits de la personne concernée ;
- elles doivent être conservées de manière sécurisée ;
- elles ne peuvent pas être transférées à des tierces parties sans précautions adéquates.

▶ Sécuriser les données

Il y a lieu de prévoir les mesures nécessaires pour garantir au mieux la sécurité des données.

A quoi faut-il penser ?

- Antivirus à jour ;
- Utilisation de mots de passe et login ;
- Mise à jour régulière des systèmes informatiques ;
- Bâtiment et bureaux sécurisés ;
- Garantir la sécurité des données transmises ;
- Restreindre les accès (wifi, Dropbox, Google drive)
- Sécuriser l'accès aux équipements de réseau ;
- Règles d'utilisation disques durs, clés USB,... .

▶ Prévoir les procédures de fuites des données

Il y a lieu de prévoir les procédures adéquates pour détecter, rapporter et analyser des fuites de données à caractère personnel.

Il faut prévoir le document pour informer d'une faille de sécurité. Ce document (notification de fuites) doit être rédigé dans un langage clair et simple.