

LE RGPD EN ESAT

Pourquoi est-on concerné ?

Les ESAT détiennent des données sensibles au même titre que les autres ESSMS. En prendre conscience c'est la base pour bien gérer l'information !

GLOSSAIRE

Données personnelles : ce sont toutes les informations permettant d'identifier une personne physique. Cela peut donc être le nom/prénom, numéro de téléphone, numéro de sécurité sociale, une adresse postale ou courriel, etc.).

Données sensibles : ce sont une catégorie de données personnelles pouvant révéler des informations de santé, d'orientation sexuelle, d'origine ethnique, de condamnation pénale par exemple.

Traitement des données : c'est l'ensemble des opérations (collecte, transfert, consultation, archivage, ...) portant sur des données personnelles (fichier informatique et papier).

Cadre réglementaire : Le Règlement Général sur la Protection des Données (RGPD) est un texte réglementaire européen qui fixe et harmonise les règles de traitement des données à caractère personnel. Les entités qui ne seront pas conformes au RGPD seront sanctionnées.



Les règles de traitement des données personnelles

Pour être en règle, voici les 6 principes du RGPD à respecter.

- 1** Répondre à un **objectif principal** (principe de finalité). Ex : *Gestion de l'admission, gestion de l'accompagnement éducatif et social, gestion des paies...*
- 2** S'appuyer sur l'une des 6 **bases légales**, à savoir : le consentement, l'obligation légale, un contrat, un intérêt légitime, une mission d'intérêt public, la sauvegarde des intérêts vitaux.
- 3** **Minimiser la collecte et l'accessibilité des données** en ne collectant que ce qui est strictement nécessaire à la finalité.
- 4** Respecter le **droit** des personnes : elles doivent être informées de l'utilisation des données les concernant et de la manière dont elles peuvent exercer leurs droits (accès, rectification, suppression, opposition).
- 5** **Sécuriser les données** grâce à des mesures techniques (antivirus, mots de passe robustes, sauvegardes régulières) et organisationnelles (formation du personnel, contrôle des accès).
- 6** Fixer des **durées de conservation des données** en instaurant des mécanismes d'effacement et d'archivage automatique.

La question est de savoir par où commencer. Voici les étapes pour se mettre en conformité.

1 Nommer un délégué à la protection des données

Le rôle du DPO est essentiel au sein des ESAT.

- Il pilote la mise en conformité RGPD de sa structure : rassemble les données traitées au sein d'un registre de traitement, priorise les actions à mener, organise les procédures internes ;
- Il diffuse cette culture et sensibilise les professionnels.

2 Tenir un registre de traitement

Le registre des activités de traitement sert à recenser la façon dont les informations des personnes sont gérées et à offrir une vision globale de l'utilisation qui est faite de leurs données personnelles. Autrement dit, il permet :

- D'avoir une vision claire et une vue d'ensemble ;
- De démontrer une preuve en cas de contrôle que sont respectés et appliqués les principes de conformité ;
- D'élaborer un plan d'action de mise en conformité.

Vos retours d'expérience

« Le paramétrage du DUI ne permet pas toujours de limiter le partage de l'information aux seuls professionnels concernés ».

« Besoin d'identifier les cas d'usages RGPD propres aux ESAT et d'avoir une réponse et un partage des bonnes pratiques ».

« Quelle(s) instance(s)/autorité(s) est en mesure de nous éclairer sur l'application du RGPD dans notre secteur ? »

« Ou mettre les écrits que nous ne souhaitons pas partager à la personne ? Sommes nous en droit de ne pas les partager ? À quels éléments de son dossier la personne peut-elle avoir accès ? »

Et après...

Beaucoup de questions restent à traiter, c'est là où le partage de bonnes pratiques et les échanges sont indispensables !

D'ailleurs le Collectif SI MS Bretagne va prochainement lancer le groupe DPO : un espace d'échanges entre experts sur la question du RGPD. Au programme : partage de bonnes pratiques, échanges avec ses pairs et remonter des besoins terrain.

[Dites-le nous ici si vous souhaitez y participer !](#)

BOÎTE À OUTILS

- [Guide pratique et numérique des ESSMS \(chap.4\)](#)
- [Site de la CNIL](#)
- [Anap : pourquoi le RGPD n'est pas une contrainte ?](#)
- [Modèle de registre de traitement CNIL](#)

