

## Fiche réglementation n° 2 : la protection des données à caractère personnel – les principes à respecter

### Références :

- Règlement général sur la protection des données de l'Union européenne (RGPD) du 27 avril 2016 – art. 5 et 6
- Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés

### Destinataires de la présente fiche :

Ensemble des acteurs de l'académie

La démarche de conformité prévue par le RGPD passe par la mise en œuvre de sept grands principes. L'élaboration du registre des traitements pour chaque responsable de traitement de l'académie (rectorat, DSDEN et établissements) permettra de s'interroger sur ces principes et, le cas échéant, permettra de déterminer les actions nécessaires pour mieux protéger les données personnelles utilisées par les services académiques et les établissements.

Chaque application ou chacun des fichiers contenant des données à caractère personnel doit satisfaire aux conditions ci-dessous.

Conditions juridiques d'usage de la donnée personnelle	Conditions d'utilisation de la donnée personnelle
<p>Le traitement de données personnelles doit reposer sur une <b>base juridique</b> qui sera le plus souvent l'exercice d'une mission de service public prévu par le code de l'éducation ou le respect d'une obligation légale.</p> <p>⚠ Le consentement comme base juridique doit être utilisé avec précaution car il peut conduire à une rupture d'égalité entre les usagers (par exemple, le refus de certains parents d'inscrire leur enfant à une application conduirait à exclure ces derniers du dispositif).</p> <p>Par contre, le consentement est la base juridique adéquate pour l'inscription d'usagers à une newsletter.</p> <p>⚠ Un élève doit consentir seul à un traitement de ses données personnelles à compter de l'âge de 15 ans. En dessous de cet âge, le consentement doit être donné « conjointement » par les représentants légaux et l'élève (art. 7-1 loi informatique et libertés).</p>	<p>Les données personnelles ne peuvent être utilisées que pour une <b>durée préalablement déterminée</b> (principe de conservation limitée).</p> <p>Ainsi, dès lors que des informations personnelles ne sont plus utiles, celles-ci doivent être détruites.</p> <p>⚠ Ce principe de destruction peut être écarté par la législation relative à l'archivage.</p> <p>⚠ L'usage d'un destructeur de documents est conseillé pour les données personnelles.</p>
<p>Le traitement doit respecter les <b>droits des personnes</b>. Ces droits qui seront définis dans une prochaine fiche sont :</p> <ul style="list-style-type: none"> <li>- droit d'information</li> <li>- droit d'accès</li> <li>- droit de rectification</li> <li>- droit de portabilité</li> <li>- droit d'opposition</li> <li>- droit de limitation</li> <li>- droit d'effacement</li> </ul>	<p>Le traitement de données doit reposer sur des <b>finalités</b> "déterminées, explicites et légitimes" (le « pourquoi » du traitement).</p> <p>Exemple de finalités : « gestion de la scolarité », « gestion de la carrière des agents »</p>
	<p>Les données traitées dans un fichier doivent être <b>exactes</b>, et au besoin corrigées.</p>

## Qualité de la donnée personnelle

Les données collectées doivent être **utiles et nécessaires** à la réalisation d'une activité (finalité). Cette utilité doit pouvoir être justifiée à l'usager ou à l'agent qui en fait la demande.

Ainsi, demander dans un formulaire des renseignements « au cas où » ceux-ci pourraient être utilisés plus tard n'est pas une pratique conforme avec le RGPD.

Par exemple, la demande du numéro de sécurité social ou de la date de naissance des parents pour inscrire un enfant à la cantine n'est pas en adéquation avec le but recherché et donc à bannir.

Les données doivent être **sécurisées** (cryptage de données, armoire fermée à clé...).

Le degré de protection doit être adapté au niveau du risque encouru ainsi qu'au niveau de sensibilité de la donnée concernée. Par exemple, les dossiers RH des agents doivent être rangés dans des armoires fermées à clé.