**B – Mise en place des bonnes pratiques RGPD-CNIL**

1 : Note de synthèse générale sur la réglementation RGPD

*Premièrement, qu’est-ce-que le Règlement Général sur la Protection des Données (RGPD) ?*

Depuis 1978, la **loi relative à l’informatique, aux fichiers et aux libertés,** fixe le cadre de la collecteet du traitement des données personnelles.Le **RGPD**, voté en 2016 et entré en application le25 mai 2018, est la nouvelle réglementation européenneen matière de protection des donnéesdirectement applicable dans le droit français. L’objectif principal du RGPD est de renforcer les droits de la personne, notamment par la création d’un droit à la portabilité des données personnelles et de dispositions propres aux personnes. Ce droit offre à chaque individu la possibilité de récupérer une partie de ses données dans un format ouvert et lisible par n’importe quel ordinateur. Les propriétaires des données peuvent ainsi les stocker ou les transmettre facilement d’un système d’information à un autre, en vue de leur réutilisation à des fins personnelles. Le RGPD cherche à conforter la responsabilité des acteurs traitant les données qu’ils en soient responsables ou sous-traitants. Il offre aussi la possibilité aux autorités en charge de la protection des données d’agir dans un cadre transnational. Cette dimension peut avoir un intérêt pour définir des politiques sur le traitement des données scolaires entre les États à l’échelle européenne.

*Ensuite, qu’appelle-t-on « données personnelles » ?*

Les données personnelles sont des informations qui permettent **d’identifier ou de reconnaître** **directement ou indirectement une personne** **physique**. Elles couvrent divers champs de la vie privée : il peut s’agir d’un nom, d’un pseudonyme, d’une adresse électronique ou physique, d’un numéro de carte de crédit ou de sécurité sociale, d’un historique de navigation web ou encore de données de géolocalisation.

*Qu’entend-on par « traitement » ?*

Pour le RGPD, on appelle « traitement », **toute opération ou tout ensemble d’opérations effectuées ou non à l’aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel**, telles que : lacollecte, l’enregistrement, l’organisation, la structuration,la conservation, l’adaptation ou la modification,l’extraction, la consultation, l’utilisation,la communication par transmission, la diffusion outoute autre forme de mise à disposition, le rapprochementou l’interconnexion, la limitation, l’effacementou la destruction.

* **Les grands principes du RGPD**

Limitation des finalités et minimisation des données

Les données à caractère personnel ne peuvent être traitées qu’en vue d’une finalité déterminée, explicite et légitime au regard des missions de l’établissement. **Seules peuvent être collectées** **les données adéquates et pertinentes au regard** **de ce qui est nécessaire à la finalité du traitement.** Ainsi, la protection dite « privacy by design » est l’idée de protéger les données dès la conception des services, afin d’éviter tout risque juridique ou informatique tandis que la « protection par défaut » entend limiter la quantité de données personnelles traitées, leur accessibilité et leur durée de conservation.

Renforcement de la transparence

Les données concernant des personnes peuvent être collectées à la condition essentielle que ces dernières aient été informées de cette opération. **Une information claire, intelligible et aisément** **accessible aux personnes concernées par** **les traitements de données, en particulier les** **enfants, doit être mise en place.** Cependant, le recueil du consentement n’est pas toujours requis. En effet, les traitements effectués dans le cadre scolaire, à partir du moment où ils sont nécessaires à l’exécution d’une mission d’intérêt public ou relevant de l’exercice de l’autorité publique dont est investi le responsable de traitement, ne nécessitent pas de consentement préalable. La gestion de la vie scolaire entre dans ce périmètre. Si le consentement est nécessaire à l’exécution d’un traitement, celui-ci doit être recueilli de manière libre, éclairé et se matérialiser de manière non ambiguë.

Renforcement du droit des usagers

Les personnes disposent de certains droits qu’elles peuvent exercer auprès de l’organisme qui détient les données les concernant : un droit d’accéder à ces données, un droit de les rectifier et enfin un droit de s’opposer à leur utilisation. Sur ce dernier point, il faut préciser qu’un traitement de données à caractère personnel est licite, notamment lorsqu’il est nécessaire à l’exécution d’une mission d’intérêt public ou relevant de l’exercice de l’autorité publique dont est investi le responsable de traitement. Le droit à la portabilité des données permet à une personne de récupérer les données qu’elle a fournies sous une forme aisément réutilisable et, le cas échéant, de les transférer ensuite à un tiers. L’article 20 du RGPD prévoit que l’exercice de ce droit ne s’applique pas au traitement nécessaire à l’exercice d’une mission d’intérêt public. Par conséquent, le droit à la portabilité ne s’applique pas aux traitements mis en œuvre par le ministère de l’Éducation nationale, les services académiques ou les chefs d’établissement, dès lors que ceux-ci sont mis en œuvre dans le cadre de la mission de service public de l’éducation qui leur est confiée. Les associations actives dans le domaine de la protection des droits et libertés des personnes en matière de protection des données auront **la** **possibilité d’introduire des recours collectifs en** **termes de protection des données personnelles**.

Les données dites sensibles

Une donnée sensible est une information qui révèle les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, l’appartenance syndicale, la santé ou la vie sexuelle d’une personne physique. Les données scolaires ne sont donc pas considérées comme des données sensibles dans leur ensemble, par contre certaines données scolaires peuvent bien évidemment être des données sensibles. Elles font l’objet d’une protection légale renforcée ; ainsi leur collecte et leur traitement ne peuvent se faire que dans certains cas très précis et doivent être justifiés au regard des objectifs recherchés (cf. art. 9 du RGPD).

Sécurité et confidentialité

Le responsable de traitement est tenu de prendre les dispositions nécessaires pour **préserver la** **sécurité des données et notamment empêcher** **qu’elles soient déformées, endommagées** **ou que des personnes non autorisées y aient** **accès**. Des mesures de sécurité physiques, telles que la sécurité des accès aux locaux, ainsi que des mesures de sécurité informatiques (antivirus, sécurisation des mots de passe) doivent être mises en place. Ces mesures de sécurité sont à déployer au regard de la nature des données et des risques présentés par le traitement.

* **Le responsable de traitement et ses obligations**

Qu’est-ce qu’un responsable de traitement ?

Le responsable de traitement est « la personne, l’autorité publique, le service ou l’organisme qui détermine ses finalités et ses moyens ». Pour l’Éducation nationale, il s’agit de la personne morale (et non la personne physique, voir page 11) qui détermine la réponse aux deux questions suivantes :

– À quoi va servir le traitement ?

– Comment l’objectif fixé sera atteint ?

Quelles sont les obligations du responsable de traitement ?

Ses obligations sont :

– **la mise en œuvre** de toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles ;

– **la tenue d’un registre** des traitements en relation avec le délégué à la protection des données (voir exemple de registre, p. 45) ;

– **l’adhésion à des codes de conduite** (quand ils existent). Le ministre de l’Éducation nationale a ainsi annoncé, dans son discours du 21 août 2018 à Ludovia, la prochaine création d’un code de conduite pour l’Éducation nationale ;

– pour tous les traitements à risque, **la conduite d’une étude d’impact complète**, faisant apparaîtreles caractéristiques du traitement, les risqueset les mesures adoptées. Il s’agit notamment destraitements contenant des données dites sensibles,des traitements reposant sur « l’évaluationsystématique et approfondie d’aspects personnelsdes personnes physiques », y compris le profilage(art. 35 du RGPD). La CNIL est chargée d’établir uneliste des traitements devant nécessairement fairel’objet d’une analyse d’impact, ainsi que ceux quien seront dispensés.

* **Le délégué à la protection des données et ses missions**

Qu’est-ce qu’un délégué à la protection des données ?

Le délégué à la protection des données (DPD), ou *data protection officer* en anglais (DPO), est le « chef d’orchestre » de la conformité en matière de protection des données au sein de son organisme. La nomination d’un DPD est **obligatoire pour toute** **autorité ou tout organisme public.**

Quelles sont ses missions ?

Le délégué à la protection des données est en charge de plusieurs missions.   
**Veiller au respect du cadre légal** : le DPD veille en toute indépendance au respect du RGPD et plus largement de l’ensemble des normes applicables par les responsables de traitement ou des sous-traitants en matière de protection des données à caractère personnel. Ses analyses et conseils s’étendent aux sous-traitants et prestataires prenant part aux traitements mis en place par les responsables de traitement. Il est obligatoirement consulté avant la mise en œuvre d’un nouveau traitement ou la modification substantielle d’un traitement en cours et peut faire toute recommandation aux responsables de traitement de l’administration centrale des deux ministères.   
**Sensibiliser, informer et conseiller** les écoles, les établissements et l’administration, ainsi que les salariés/agents sur les obligations qui leur incombent en vertu du RGPD et de la loi relative à l’informatique, aux fichiers et aux libertés. Il doit pouvoir organiser des actions de communication, de sensibilisation, de dialogue et de concertation avec l’ensemble de la communauté éducative, y compris, dans une certaine mesure, auprès des élèves et des parents, afin de leur apporter toutes les informations sur leurs droits et sur les garanties mises en œuvre. **Contrôler** le degré de conformité au RGPD ainsi qu’à l’ensemble des textes applicables, et **alerter** **les responsables de traitement**. En cas de manquement aux obligations légales, le DPD ne peut pas être tenu pour responsable : c’est le responsable de traitement (ou le représentant légal) qui devra répondre de ses obligations.   
**Dispenser des conseils** en ce qui concerne les **analyses d’impact** relatives à la protection des données quand elles sont nécessaires et vérifier leur **exécution**.   
**Coopérer avec l’autorité de contrôle** (la CNIL pour la France) et faire office de point de contact pour les personnes concernées sur toute question en lien avec les traitements. Il se charge des médiations entre les personnels quand cela est nécessaire.   
**S’assurer de la bonne tenue de la documentation** relative aux traitements.   
**Rédiger et présenter un rapport** annuel au ministre ou au recteur suivant son niveau d’intervention.