Le traitement des données à caractère personnel

cadre juridique et institutionnel

Les Textes:

- Le Règlement Général sur la Protection Données entrée en vigueur au 25 mai 2018.
- Loi n°78-17 du 6 janvier 1978 dite « **loi informatique et liberté** » modifiée par la loi du 20 juin 2018
- Modifiée également en 2004 et enrichie par les dispositions de la 2016-1312 du 07 octobre 2016 dite « **loi pour une république numérique** ».

Une institution en charge du contrôle des pratiques: la Commission Nationale Informatique et Libertés (autorité administrative indépendante) dont le rôle est de veiller à ce que l'informatique ne porte atteinte ni à l'identité humaine, ni à la vie privée, ni aux libertés individuelles ou publiques. Ses outils: informer et conseiller, réglementer, contrôler, sanctionner, anticiper, reflechir.

La protection des données à caractère personnel: un enjeu majeur de société

- La protection des données : un droit fondamental
- Pourquoi une refonte de la législation générale sur la protection des données à l'échelle européenne?
- Un contexte économique et social profondément et durablement bouleversé par l'avènement du numérique dans tous les domaines de la vie courante.
- Un contexte économique et social « globalisé-mondialisé» nécessitant un dispositif juridique adapté face à l'intégration de cette nouvelle échelle « monde » dans la vie courante.
- Un enjeu très fort impliquant une mise en conformité des pratiques actuelles en vue de sensibiliser les « élèves- futurs citoyens numériques »

Une objectif national pris à l'échelon ministériel dans le cadre de l'école de la confiance

- Diffusion de la malette des parents
- Création d'un référentiel CNIL de formation des élèves à protection des données personnelles dont l'objectif est de constituer un socle commun de compétences concrètes et de pratiques en matière de protection des données
- Diffusion d'un guide à l'attention des chefs d'établissement pour comprendre et appliquer les nouvelles réglementations dans les établissements scolaires

Le RGPD pose un principe de responsabilisation de tous les acteurs se traduisant par de nouvelles obligations :

Obligation n°1 : Désignation obligatoire d'un DPD (art 37):

Obligation n°2: **Tenir un registre** (art 30)

Obligation n°3: documenter les actions pour prouver la conformité en effectuant notamment **une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel réalisé par de délégué à la protection des données (art 35)** (devant aboutir respect des principes fondamentaux et garantir une bonne gestion lié à la sécurité des données).

Obligation n°4: organiser l'information et l'accès aux données à caractère personnel (art 13)

Obligation n°5: accompagner la CNIL dans ses démarches en lui notifiant toutes les violations de données rencontrées) la violation = destruction, perte, altération, divulgation, accès non autorisé.

Qu’est ce qu’une donnée à caractère personnel? Qu’est ce qu’un traitement?

Les données concernées:

Art 2 loi de 1978: « *toute donnée relative à une personne physique, qui peut être identifiée par quelqu’un, quel que soit le moyen utilisé* »

- Les données directement ou indirectement identifiantes ou encore les recoupements d’informations anonymes.
- Ex : de données personnelles: photographie, adresse IP, n° de téléphone, adresse mail etc…

Le traitement:

Art 2 loi de 1978: toute opération portant sur des données à caractère personnel quelque soit le procédé utilisé dès lors que ce traitement répond à objectif/finalités qui lui est propre.

Les traitements liés au fonctionnement/gestion: (GRH, Sécurité, gestion financière)

Les traitements liés à une mission ou au cœur d’activité: gestion propre au service

La loi de 2004 élargi le principe en introduisant la notion de « fichier » qui englobe aussi bien les traitements automatisés (informatique) que traitements non automatisés (papier)

Le traitement papier de données nécessite d’être déclaré uniquement en présence de données « sensibles »

Petit lexique RGPD: Les acteurs de la protection de la donnée à caractère personnel dans l'académie en application de l'art 4 du RGPD

Le responsable de traitement (RT) : « *toute personne qui seule ou conjointement avec d'autres détermine les finalités et les moyens du traitement*. »

Il s'agit des responsables juridiques de chaque entité administratives dans l'académie: Le recteur / l'IA-DASEN / Le chef d'établissement en EPLE

À noter: concernant le 1er degré, le responsable de traitement est l'IA DASEN

Le sous traitant (ST) : « *toute personne qui traite des données à caractère personnel pour le compte du responsable de traitement* »:

Tout prestataire extérieur : une entreprise privé / une association / une collectivité ou tout autre personne mandatée par le responsable de traitement.

Les destinataires: « toute personne qui reçoit communication de données à caractère personnel qu'il s'agisse ou non d'un tiers ».

Une entreprise privé / une association / une collectivité ou tout autre personne extérieure désignée lors de la création du traitement par le responsable de traitement.

A noter: sont destinataires les services d'une même entité qui par définition ne sont pas directement concernés par le traitement.

Les tiers : « *toute personne autre que le RT, le ST et les personnes placées sous l'autorité directe du RT ou du ST autorisée à traiter les données caractère personnel* ».

À noter: la notion de tiers englobe également celle de destinataire. Il est dès lors préférable de la distinguer de celle-ci pour ne comprendre que les personnes non autorisées (à qui les données ne peuvent pas être communiquées) et les personnes autorisées dit « tiers autorisés) que sont les services chargés d'enquête particulière (police / administration fiscale / huissier de justice etc…)

Le Délégué à la protection des données (art 37): le RT et le ST doivent désigner un DPD, lorsqu'il est une autorité ou un organisme publique.

Son rôle : informer et conseiller le RT ainsi que les employés qui procèdent au traitement des données. Il contrôle le respect du RGPD, il dispense des conseils et rend compte de ses activités.

À ce jour pour dans l'académie désignation pour tous les EPLE et services déconcentrés (rectorat) et DSDEN: 1 seul DPD académique M. Nicolas Brus

Les 6 règles d’or de la protection des données

- La finalité du traitement
- La licéité du traitement
- Pertinences des données
- La conservation des données
- Sécurité et confidentialité des données

- Le respect du droit des personnes

La finalité du traitement, pertinence et conservation limitée des données

Préalablement à toute collecte, les finalités d'utilisation des données doivent être déterminées, explicites et légitimes (licites).

Leur utilisation ultérieure ne doit pas être incompatible avec la finalité initiale. (ex: utilisation d'un fichier élève à des fins de communication politique)

Risque pénal important : le détournement de finalité est un délit art 226-1 du code pénal

Les activités de traitement doivent s'inscrire dans le cadre posé par l'article L131-2 due code de l'éducation relatif à l'instruction obligatoire.

La pertinence et proportionnalité des données collectées:

les données sont **adéquates, pertinentes, et non excessives** au regard des finalités. Elles doivent être complètes, exactes et mises à jour

Les données « sensibles »: interdiction de collecter des données faisant apparaitre directement ou indirectement, les origines raciales ou ethnique, les opinions politiques philosophique ou religieuse, l'appartenance syndicale, l'état de santé ou la vie sexuelle. Sauf exception (consentement exprès, intérêt public), pris sur un fondement légal. (ex: traitement des condamnations)

Numéro de sécurité sociale : encadrement strict, utilisation essentiellement limité à la sphère « santé social travail »: sauf dispense de la CNIL, la collecte est toujours soumise à autorisation préalable de CNIL.

Les données comportant des données génétiques, données pénales ou des appréciations sur les difficultés sociales des personnes sont soumises à autorisation préalable de la CNIL qui doit se prononcer dans les 2 mois (son silence vaut rejet).

la durée préalablement définie doit être limitée.

La durée est déterminée par la finalité du traitement. La durée est dans la sphère publique est réglementée. Mais en dehors des cas prévues, un réflexion doit être entamée.

Ex : gestion de la paie 5 ans / video surveillance 30 jours

À l'issue de la durée: destruction ou anonymisation des données

3 phases de conservation à définir: la conversation en base active (utilisation courante), en base intermédiaire (archivage présentant un intérêt administratif), enfin l'archivage définitif (ex: versement aux archives publiques)

Sécurité et confidentialité des données

Obligation de sécurité et confidentialité: les données doivent être entourée de toutes les précautions utiles, au regard des données et des risques présentés par le traitement.

- Pour préserver leur sécurité et garantir leur conservation (intégrité)
- Pour veiller à ce que des tiers non autorisés y aient accès (confidentialité)

Cette obligation implique la mise en œuvre des mesures de sécurité physique et logique et la gestion stricte des habilitations et droits d'accès. (utilisateur, services habilités)

Elle nécessite une identification des destinataires légitimes et des tiers le cas échéant et un encadrement clair des missions du sous traitants.

Un cas particulier: les tiers autorisés (officier de police, administration fiscale etc…)

Le règlement européen: impose une évaluation des niveau de sécurité adapté (art 32 RGPD)

Le respect du droit des personnes

Chaque personne dispose de droits lui permettant de garder la maitrise des informations qui la concerne.

Le droit d'information (art 32 loi de 1978 / art 12 RGPD) : un principe général de loyauté dans la collecte du traitement impliquant une information préalable, claire et précise des personnes concernées sur :

- La finalité du traitement
- Le caractère obligatoire ou facultatif des réponses et des conséquences d'un défaut de réponse
- L'identité du responsable du traitement (le recteur)
- Les destinataires des données
- Leurs droits (accès, rectification, opposition + droit de définir le sort en cas de décès)
- La durée de conservation ou des critères pour la déterminer

Le recueil du consentement des personnes concernées: le consentement est une démarche active, explicite et de préférence écrite qui doit libre, spécifique et informée. Ce consentement est requis dans les cas suivants:

- En cas de collecte de données sensibles
- De réutilisation des données à d'autres fins que celles initialement prévues

Le droit d'opposition (art 38 loi de 1978):

Toute personne a le droit de s'opposer, pour un motif légitime, au traitement de ses données, sauf si le traitement répond à une obligation légale (ex: impôts)

Pas de définition d'un motif légitime: un appréciation au cas par cas ex:

Le droit à la tranquillité: toute personne a le droit de s'opposer sans frais et sans motif légitime, à l'utilisation de ses données à des fins de prospection, (commerciale, politique, syndicale)

Le droit d'accès et de rectification (art 39-40 loi de 1978): (RGPD droit à l'oubli)

Toute personne peut directement auprès du responsable de traitement (sauf exception) avoir accès à l'ensemble des informations la concernant, en obtenir une copie et exiger qu'elles soient selon les cas rectifiées, complétées, mise à jour ou supprimées.

Le droit à l'oubli (des anciens mineurs): une personne mineure au moment de la collecte de données peut obtenir auprès des plateformes, l'effacement des données problématiques dans les meilleurs délais.

Les limites:

- Il est possible de refuser la demande d'accès en la motivant en fait et en droit (décision défavorable)
- Les demandes manifestement abusives par leur nombre ou leur caractère répétitif ou systématique.
- L'accès doit se faire dans le respect du droit des tiers (garantir la confidentialité de leurs données)

La transmission de données à des tiers

Les données ne peuvent être traitées ultérieurement de manière incompatible avec la finalité initialement prévue.

Ainsi seuls sont destinataires les personnes habilitées à recevoir communication des données autre que la personne concernée, le sous traitant et la personne chargée de traiter les données en raison de leur fonction, afin de garantir la confidentialité des données.

- Ces personnes doivent être précisément identifiées et déclarées dans les formalités préalables (obligation de transparence)
- Ces personnes doivent être portées à la connaissance des personnes concernées (obligation d'information).

Une seule exception: les tiers autorisés par la loi (police, impôts etc..)

Les tiers autorisés

Obligation de transmettre des informations demandées

Seule condition à la communication : les demandes doivent être Ponctuelle, Précise et Motivée.

Précaution à prendre afin de garantir la confidentialité:

Solliciter un écrit pour s'assurer de la qualité du demandeur et contrôle la légalité de la requête (fondement légal de la requête!)

- Aucune information préalable des personnes concernées n'est à accomplir
- Aucune information des destinataires

Les tiers non autorisés

Aucune obligation de transmission

Des précautions: vérifier la légalité de la demande et de la transmission

Condition de légalité d'une transmission acceptée:

Respect du droit des personnes: information et possibilité d'opposition pour motif légitime, voir droit de consentement

Respect des obligations de sécurité: chiffrement des données lors de leur transmission

Rappeler au tiers (nouveau destinataire) ses obligations: déclaration de traitement, information des personnes et prise en compte de leurs droits

Formalité à accomplir: intégrer ce nouveau destinataire dans la déclaration initiale

Solution alternative de transmission:

Anonymisation des données sollicitées: dans le cas le RGPD ne s'applique pas

La transmission directe au tiers par les personnes concernées: le responsable de traitement informe de la demande du tiers de son souhait et les invite si elle le souhaite à lui communiquer ces données.

Si vous êtes vous-même un tiers

Assurez vous du caractère licite et loyal de la collecte et de la transmission que vous sollicitez:

Le transmetteur a-t-il bien informé les personnes concernées? Le traitement est il bien déclaré?

Procéder vous-même aux obligations qui vous incombent en devenant destinataire.