POUR L'ÉCOLE
DE LA CONFIANCE

La protection des données à caractère personnel dans l'éducation nationale

Gilles Braun IGEN, DPD MENJ et MESRI

Eidos, janvier 2019

MINISTÈRE
DE L'ÉDUCATION
NATIONALE

Une faible sensibilisation sur le sujet

- Un sujet souvent lointain des préoccupations des personnels de direction et d'encadrement, des enseignants et des administrations.

- Former rapidement les enseignants et les chefs d'établissement sur l'utilisation des données scolaires numériques dans des situations pédagogiques et administratives avec une attention particulière aux traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques dans le sens de l'article 9 du RGPD (données dites « sensibles »).

Le RGPD : un changement de paradigme

- **La responsabilisation des acteurs**

Mise en place d'un régime où les responsables des traitements et les sous-traitants de données personnelles doivent analyser les conséquences des traitements dont ils ont la charge et en assumer les responsabilités vis-à-vis des usagers.

Données à caractère personnel

- « Toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. »

- « Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable de traitement ou tout autre personne. »

- « Toute information »: englobe potentiellement toute sorte d'informations, tant objectives que subjectives, sous forme d'avis ou d'appréciations, à condition que celles-ci « concernent » la personne en cause.

Traitement de données

- 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 la collecte, 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 ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

- "Est dénommée traitement automatisé d'informations nominatives toute opération aboutissant à la constitution informatique de fichiers ou de bases de données, et ce quel que soit le moyen ou le support informatique, ainsi que toute procédure de consultation, de télétransmission d'informations nominatives, quel que soit le moyen de télécommunication utilisé ".

- Le RGPD s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

Les grands principes

- Les principes de licéité, de loyauté et de transparence : il convient en particulier de s'assurer que les données sont traitées de manière licite, c'est-à-dire qu'elles doivent être légalement collectées.

- le principe de limitation des finalités : 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 ;

- le principe de minimisation des données : seules peuvent être collectées les données adéquates et pertinentes au regard de ce qui est nécessaire à la finalité du traitement

- Principes concernant le cycle de vie de la donnée : sécurité, durée d'archivage, portabilité et droit à l'oubli (les données doivent être transférées et sauvegardées dans un lieu sûr et, pour certaines, ne peuvent être gardées indéfiniment voire pouvoir être transmise).

Les bases légales d'un traitement (dans le secteur public)

- Le consentement libre, spécifique, éclairé et univoque de la personne
- L'intérêt vital de la personne concernée
- Respect d'une obligation légale
- L'exécution d'une mission d'intérêt public ou relevant de l'autorité publique dont est investi le responsable de traitement
- La nécessité contractuelle

- Un traitement de données peut s'appuyer sur différentes bases légales suivant la situation dans laquelle il s'effectue.

Données « sensibles »

Informations concernant :

- **l'origine raciale ou ethnique**
- **les opinions politiques,**
- **les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique.**
- **la santé,**
- **la vie sexuelle ou l'orientation sexuelle d'une personne physique.**

Ainsi que les caractéristique physique ou biologique permettant d'identifier une personne (ADN, contour de la main, empreintes digitales...).

Principe : pas de traitement sauf dans des cas très particuliers (par ex. consentement, sauvegarde de la vie humaine, données rendues publiques par la personne concernée, statistique publique ou intérêt public sous certaines conditions)

Le responsable de traitement

- Le responsable du traitement est "la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens" .

- Pour les ministères, le(s) responsables de traitement sont le ministère de l'éducation nationale ou le ministère de l'enseignement supérieur, de la recherche et de l'innovation, ie l'État en tant que personne morale, et non une personne physique.

- Tant par leur qualité de représentants de l'État dans les rectorats ou les établissements que de l'organe exécutif de ceux-ci
  - Le recteur (les dasen par délégation au niveau du département)
  - Le chef d'établissement pour les EPLE
  - Pour le primaire : le recteur (et si délégation, le DASEN)
  - Pour les établissements publics sous tutelle du MEN (Canopé, CNED, Onisep, CIEP, CNOUS…) : le directeur général
  - Pour l'enseignement privé sous contrat avec l'État : le directeur de l'établissement
- Le périmètre de responsabilité de chacun est déterminé par les traitements de données dont il a la responsabilité directe.

Le responsable de traitement

- Les responsables de traitements doivent mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles.

- La tenue d'un registre des traitements.

- L'adhésion à des codes de conduite (quand ils existent).

- Pour tous les traitements à risque, le responsable de traitement devra conduire une étude d'impact complète, faisant apparaître les caractéristiques du traitement, les risques et les mesures adoptées. Concrètement, il s'agit notamment des traitements de données sensibles et de traitements reposant sur « l'évaluation systématique et approfondie d'aspects personnels des personnes physiques », c'est-à-dire notamment de profilage

Périmètre des traitements concernés

- **Traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous - traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union.**

- **Traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées :**

  - **a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes,**

  - **b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.**

Traitements nationaux/ Traitements académiques/EPLE : le principe

- S'il n'a pas été effectué un traitement local au niveau d'une académie (ou d'un établissement), il n'est pas nécessaire d'"inscrire le traitement national ou (académique) dans le registre académique (ou de l'établissement). Le responsable du traitement est alors le ministre (ou le recteur)

- On appelle paramétrage local, un traitement (et non pas une catégorie de données nouvelles) qui aurait été ajouté ou modifié par rapport à l'application initiale (même une condition d'hébergement différente de celle préconisée).

Traitements nationaux/ Traitements académiques/EPLE : le principe

- **Communication d'une violation de données à caractère personnel**
  - **à l'autorité de contrôle: en cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.**
  - **à la personne concernée : Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.**

- **Coopération avec l'autorité de contrôle**
  - **Le responsable du traitement et le sous-traitant ainsi que, le cas échéant, leurs représentants coopèrent avec l'autorité de contrôle, à la demande de celle-ci, dans l'exécution de ses missions.**
  - **Pour les ministères MEN et MENSRI : DPD point de contact avec la CNIL**

Les traitements effectués par les enseignants

- Certains outils utilisés par les enseignants, dans le cadre de leur liberté pédagogique, peuvent conduire à un traitement de certaines données personnelles de leurs élèves (en particulier les adresses internet souvent utilisées pour s'inscrire sur ces services... mais pas uniquement...).

- Exemple l'utilisation de système de communication (Skype, MSN, Hangout), des plateformes de travail collaboratif (tableau virtuel partagé, textes collaboratifs, ...), des blogs, questionnaires automatisés ...

- Les enseignants doivent transmettre au chef d'établissement la liste de ces traitements pour qu'ils soient reportés dans le registre des traitements.

- Avec les contraintes éventuelles que cela représente : analyse d'impact, demande éventuelle de consentement, etc.

À propos de la liberté pédagogique

- **Des textes qui en précisent les contours**
  - **1er degré : Article D411-2 du code de l'éducation**
    Qui définit les compétences **du conseil d'école** dans les mises en œuvres pédagogiques

    Article D401-1, 2 et 3 du code de l'éducation
    Qui définit les compétences **du conseil école collège**

  - **2nd degré :**
    Article R421-23 du code de l'éducation
    Qui définit les compétences **du conseil d'admin**istration pour le pilotage pédagogique
    Article R421-41 du code de l'éducation
    Qui définit les compétences **du conseil pédagogique**

Risques encourus

- Les amendes ne s'appliquent pas aux traitements mis en œuvre par l'État. Il en résulte que les amendes ne sont pas applicables à ceux mis en œuvre par les services déconcentrés ainsi que par les chefs d'établissement pour ce qui est des traitements réalisés au nom de l' État/ en qualité de représentant de l' État.

- La question qui se pose actuellement et qui reste à expertiser (elle dépasse évidemment le périmètre de nos seuls ministères…) est celle de savoir si les chefs d'établissement mettant en œuvre un traitement non pas au nom de l' État mais de l'EPLE pourraient se voir infliger des amendes administratives en cas de violation des dispositions relatives à la protection des données….

- Des sanctions pénales sont prévues par les textes : « le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. »

LE DPD

- le DPO (Data Protection Officer) ou DPD (délégué à la protection des données) obligatoire pour toute autorité publique ou tout organisme public (collectivités territoriales, État, établissements publics, etc.).

- 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 des traitements 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.

- Alerter les responsables de traitement : Le DPD informe sans délai les responsables de traitement de tout risque que le non-respect de ses recommandations ou toute initiative des utilisateurs ou de concepteurs de traitements feraient courir à l'institution. Il veille à formaliser une procédure pour informer directement les responsables de traitement d'une non-conformité majeure.

- Analyser, investiguer, auditer et contrôler : Le DPD pilote, de façon maîtrisée et indépendante, toute action permettant de juger du degré de conformité au RGPD, de mettre en évidence les éventuelles non-conformités, de vérifier la bonne application de procédures, méthodes ou consignes relatives à la protection des données personnelles. Il est en relation avec le DPD ministériel sur ces questions.

LE DPD

- **Établir et maintenir une documentation sur les traitements effectués : Le DPD s'assure de l'existence d'une documentation relative aux traitements de données à caractère personnel (dont le registre des traitements) et de sa bonne conservation et veille à son accessibilité par l'autorité de contrôle (CNIL).**
- **Assurer la médiation avec les personnes concernées : Le DPD reçoit les réclamations éventuelles des personnes concernées par les traitements et veille au respect du droit des personnes. Il traite ces réclamations et plaintes avec impartialité, ou met en œuvre les procédures propres à assurer leur bon traitement en lien avec les services académiques.**
- **Accompagner et sensibiliser : le DPD assure une mission d'information et de sensibilisation des services académiques au travers notamment d'actions de formation et de diffusion de supports de communication sur la protection des données personnelles.**
- **Interagir avec l'autorité de contrôle : Le DPD est, pour l'académie, le point de contact privilégié de l'autorité de contrôle (CNIL), avec laquelle il communique en toute indépendance sur les questions relatives aux traitements mis en œuvre.**
- **Présenter un rapport annuel au recteur : Le DPD rend compte de son action en présentant chaque année un rapport au Recteur**

Le sous-traitant

- **Responsabilisation du sous-traitant (art. 28 du RGPD)**

- **Obligation d'expliciter clairement la chaine de sous-traitance et interdiction de recruter un autre sous-traitant sans l'autorisation écrite du responsable de traitement.**

- **Le traitement par un sous-traitant est régi par un avenant au contrat détaillant avec précision:**

  - **Les modalités de transfert de données vers des pays-tiers**
  - **La mise en place de mesures de sécurité adéquates**
  - **Prévient le RT de toute violation de données dans les meilleurs délais**
  - **Participe, le cas échéant, aux études d'impact**

Des questions ?

POUR L'ÉCOLE
DE LA CONFIANCE

Gilles Braun
IGEN, DPD

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'ÉDUCATION
NATIONALE