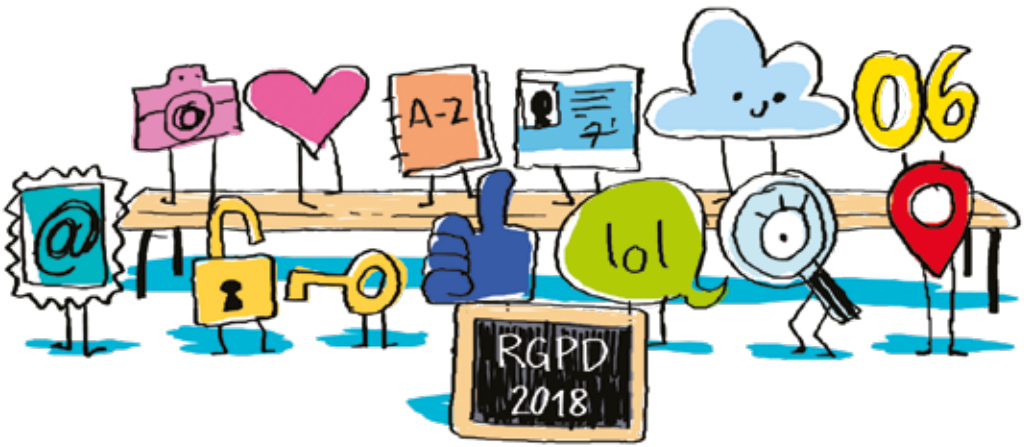
LES DONNÉES À CARACTÈRE PERSONNEL

COMPRENDRE ET APPLIQUER LES NOUVELLES RÉGLEMENTATIONS DANS LES ÉTABLISSEMENTS SCOLAIRES



CANOPÉ ÉDITIONS

03 INTRODUCTION

07 DÉFINITIONS

08 LES GRANDS PRINCIPES DU RGPD

10 LE RESPONSABLE DE TRAITEMENT ET SES OBLIGATIONS

13 LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES ET SES MISSIONS

15 LE RGPD EN QUATRE ÉTAPES

16 RENFORCER L'ÉDUCATION AUX MÉDIAS ET AUX DONNÉES

17 35 QUESTIONS/RÉPONSES SUR L'APPLICATION DU RGPD EN ÉTABLISSEMENT

47 POUR ALLER PLUS LOIN

Directeur de publication :
Jean-Marie Panazol

Directrice de l'édition transmédia :
Stéphanie Laforge

Directrice artistique adjointe :
Gaëlle Huber

Coordination éditoriale :
Benjamin Berut, Kimi Do, Tania Lécuyer et Luc Taramini

Expertise et coordination scientifique : Délégation à la protection des données ; Direction des affaires juridiques, ministère de l'Éducation nationale.

Secrétariat d'édition : Sophie Roué

Mise en pages : Gaëlle Huber

Illustrations : David Tessier

Conception graphique :
DES SIGNES studio Muchir et Desclouds

ISSN : 2426-0207
ISBN : 978-2-240-04895-0

(établissement public à caractère administratif)
Téléport 1 – Bât. @ 4
1, avenue du Futuroscope
CS 80158
86961 Futuroscope Cedex

INTRODUCTION

La généralisation des équipements et des ressources numériques dans les écoles et les établissements scolaires, avec les usages administratifs et pédagogiques qui en découlent, conduit au recueil et à la transmission d'une **très grande quantité de données**. Les données scolaires, dans toute leur variété, peuvent permettre de développer de nouveaux services grâce à la banalisation des objets connectés, à des puissances de stockage et de calcul toujours plus importantes, et aux techniques d'intelligence artificielle qui marquent notre époque. Sous réserve d'une **protection rigoureuse**, ces données peuvent être mieux utilisées qu'à ce jour pour améliorer l'individualisation des parcours de formation et des apprentissages, mettre en œuvre une évaluation plus performante des élèves, offrir aux enseignants de nouveaux outils pédagogiques et aux chefs d'établissement des services de vie scolaire adaptés aux attentes des familles.

Ce « manuel » sur la protection des données à caractère personnel à l'intention des chefs d'établissement, réalisé et diffusé par Réseau Canopé, a pour objectif de répondre aux principales questions auxquelles ils peuvent être confrontés au moment de la mise en œuvre du **Règlement général sur la protection des données** (RGPD) et de l'application des nouvelles dispositions de la loi relative à l'informatique, aux fichiers et aux libertés modifiée le 6 août 2018 par la loi n° 2018-493 du 20 juin 2018, relative à la protection des données personnelles.

Les chefs d'établissement sont doublement concernés par ces textes législatifs :
– d'une part, ils ont pour mission de veiller à ce que les jeunes qui leur sont confiés soient formés aux enjeux sociétaux et économiques de l'utilisation de ces données. En effet, le Code de l'éducation a étendu « aux règles applicables aux traitements de données à caractère personnel » la formation à l'utilisation responsable des outils et des ressources numériques dispensée dans les écoles et les établissements d'enseignement. Cette formation est devenue un volet incontournable de l'éducation aux médias et à l'information ;
– d'autre part, ils sont responsables du respect des principes qui encadrent dorénavant les traitements de données personnelles effectués dans leur établissement (à l'exclusion des applications mises à leur disposition par l'administration centrale ou par les services académiques qui sont respectivement placés sous la responsabilité du ministre ou du recteur). Il leur appartient donc de veiller à la protection des données personnelles de tous les membres de leur communauté éducative – et tout particulièrement de celles des élèves – qui sont nécessaires à la gestion administrative du service public de l'éducation ou aux usages pédagogiques qui s'appuient – et s'appuieront – de plus en plus souvent sur des ressources numériques.

Dans ce domaine, il existe une grande sensibilité des familles, des professeurs et des personnels administratifs. Il appartient au service public de l'éducation de garantir à tous le strict respect du droit applicable aux nombreuses et diverses données personnelles qui sont traitées quotidiennement pour le bon fonctionnement de l'École, sans pour autant limiter les usages qui ne poseraient pas de problème particulier d'un point de vue légal ou éthique. Le rôle des chefs d'établissement est donc essentiel tant par leur qualité de représentant de l'État dans l'établissement que d'organe exécutif de celui-ci. Ils peuvent s'appuyer sur le délégué à la protection des données de leur académie. Ce document n'a d'autre ambition que de les aider à répondre aux questions qui leur seront posées le plus souvent et à mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires à une utilisation responsable des données personnelles dans leur établissement.

Mieux protéger

Malgré la sensibilité croissante du sujet, un rapport des deux inspections générales du ministère de l'Éducation nationale consacré aux données numériques à caractère personnel a récemment montré une faible prise de conscience des membres de la communauté éducative quant à l'utilisation qui est faite des données recueillies, produites et transmises dans le cadre scolaire. La diffusion d'équipements et de ressources numériques comme le développement d'expérimentations utilisant leurs potentialités renforcent la nécessité d'un cadre de confiance clair et partagé par les élèves, les parents, les enseignants et les personnels administratifs.

Le Règlement général sur la protection des données [RGPD] au niveau européen et la loi du 20 juin 2018 relative à la protection des données personnelles contribuent à créer ce cadre par un renforcement des droits des usagers concernant l'utilisation de leurs données personnelles. En particulier, les responsables de traitement ont l'obligation de fournir une information simple, claire et facilement compréhensible par les personnes concernées dont font partie, dans le cadre des activités scolaires, les élèves et leurs familles.

Un délégué à la protection des données [DPD] pour le ministère de l'Éducation nationale et pour le ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation a été nommé conformément au RGPD. De même, chaque académie a procédé à la nomination d'un DPD. Il s'agit d'aider et d'accompagner l'ensemble des acteurs qui utilisent ou souhaitent utiliser des services et des ressources numériques, afin qu'ils aient connaissance de leurs droits et devoirs quant aux traitements effectués sur leurs données personnelles.
Le DPD ministériel et les DPD académiques seront chargés de veiller au respect du cadre légal relatif aux données personnelles, mais aussi de sensibiliser, d'informer et de conseiller les responsables de traitement, notamment les chefs d'établissement et les directeurs académiques des services de l'Éducation nationale [DASEN].

Un accent particulier est mis sur les actions de formation et d'information des chefs d'établissement et des professeurs aux enjeux de l'utilisation des données scolaires numériques [parcours de formation en ligne, guide pour les chefs d'établissement, tel que ce document, etc.].

Par ailleurs, eu égard aux spécificités des données à caractère personnel recueillies dans le cadre scolaire, un code de conduite propre à l'Éducation nationale sera prochainement élaboré puis soumis à la Commission nationale de l'informatique et des libertés [CNIL]. Modalité d'encadrement renforcé prévue par le RGPD pour les secteurs qui le nécessitent, ce code rassemblera tous les éléments qui s'imposeront aux acteurs proposant des services et des ressources numériques aux écoles et établissements scolaires.

Enfin, un comité d'éthique et d'expertise en matière de données numériques sera également créé et placé auprès du ministre de l'Éducation nationale. Cette instance, composée de membres qualifiés, émettra des avis sur l'intérêt public de l'utilisation des données récoltées et traitées dans le cadre scolaire.

Définitions

Qu'est-ce que le Règlement général sur la protection des données ?

Depuis 1978, la **loi relative à l'informatique, aux fichiers et aux libertés** fixe le cadre de la collecte et du traitement des données personnelles. Le **RGPD**, voté en 2016 et entré en application le 25 mai 2018, est la nouvelle réglementation européenne en matière de protection des données directement applicable dans le droit français. La loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles est venue compléter la loi de 1978 qui reste toujours en vigueur.

Le RGPD s'applique pour tous les traitements de données à caractère personnel effectués dans le cadre des activités d'un responsable de traitement établi sur le territoire de l'Union européenne, que le traitement ait lieu ou non sur ce territoire.

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 : 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.

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 apparaître les caractéristiques du traitement, les risques et les mesures adoptées. Il s'agit notamment des traitements contenant des données dites sensibles, des traitements reposant sur « l'évaluation systématique et approfondie d'aspects personnels des personnes physiques », y compris le profilage (art. 35 du RGPD). La CNIL est chargée d'établir une liste des traitements devant nécessairement faire l'objet d'une analyse d'impact, ainsi que ceux qui en seront dispensés.

QUI EST LE RESPONSABLE DE TRAITEMENT ?

Tant par leur qualité de représentants de l'État au niveau du ministère, des rectorats ou des établissements que de l'organe exécutif de ceux-ci :

Au niveau ministériel

Le ministre (les directeurs exercent cette responsabilité par délégation)

Au niveau académique

Le recteur (les DASEN par délégation)

Au niveau du premier degré

Le DASEN par délégation du recteur

Au niveau du second degré (EPLE)

Le chef d'établissement

Au niveau d'un établissement public dépendant du ministère de l'Éducation nationale (Réseau Canopé, CNED...)

Le directeur général de l'établissement

Le périmètre de responsabilité de chaque responsable de traitement est déterminé par les traitements de données dont il a la responsabilité directe.

RELATIONS AVEC L'AUTORITÉ DE CONTRÔLE

Le responsable de traitement et le sous-traitant ainsi que, le cas échéant, leurs représentants **coopèrent avec l'autorité de contrôle** (la CNIL pour la France), à la demande de celle-ci, dans l'exécution de ses missions.

En cas de **violation de données à caractère personnel**, le responsable de traitement doit entrer en communication avec :
– **l'autorité de contrôle (CNIL)**. Le responsable de traitement 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 ;
– **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 de traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais ;
– **le DPD académique pour l'en informer.**

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.

QUI DÉSIGNE LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES ?

Le DPD est désigné par le responsable de traitement. Mais le RGPD laisse la possibilité d'une mutualisation possible. C'est l'orientation prise par le ministère de l'Éducation nationale.

Il est donc proposé aux chefs d'établissement, responsables de traitement pour leur établissement, de mutualiser leur DPD à un niveau académique.

Le ministre de l'Éducation nationale a désigné le DPD de l'administration centrale du ministère. Il est commun avec le ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation.

Les responsables de traitement pour les écoles primaires étant les DASEN (par délégation du recteur), c'est au niveau académique que la nomination du DPD est décidée. Là aussi, la fonction peut être mutualisée.

Chaque recteur a désigné un, parfois deux, DPD pour l'administration de son académie ou de la région académique qui a, la plupart du temps, dans le champ de ses responsabilités, le périmètre des établissements scolaires et des écoles.

Le RGPD en quatre étapes

1. INFORMER LES MEMBRES DE LA COMMUNAUTÉ ÉDUCATIVE DE SON ÉTABLISSEMENT

Présenter les nouvelles obligations aux enseignants et aux personnels administratifs.

En faire un point d'information lors des réunions des représentants légaux des élèves et des délégués de classe.

2. RENSEIGNER LE REGISTRE DE TRAITEMENT

Identifier les traitements opérés dans l'établissement scolaire.

Intégrer les informations nécessaires dans le registre de traitement dont le modèle a été proposé par le rectorat.

Mettre en place les moyens de sa mise à disposition.

3. GÉRER LES RISQUES

Mener une analyse d'impact relative à la protection des données (AIPD) si des risques élevés pour les droits et libertés des personnes ont été identifiés.

4. ORGANISER LES PROCESSUS INTERNES

Prendre en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (faille de sécurité, modification des données, changement de prestataire, etc.).

Renforcer l'éducation aux médias et aux données

Même si le programme d'éducation aux médias et à l'information (EMI) au cycle 4 aborde déjà la question des données personnelles via la compétence « comprendre ce que sont l'identité et la trace numériques », que les orientations pour les cycles 2 et 3 évoquent l'attention aux traces numériques et que le programme d'enseignement moral et civique (EMC) au lycée permet d'aborder les questions relatives aux données personnelles, il convient sans doute aujourd'hui d'approfondir la question de la protection des données à caractère personnel en abordant avec les élèves :

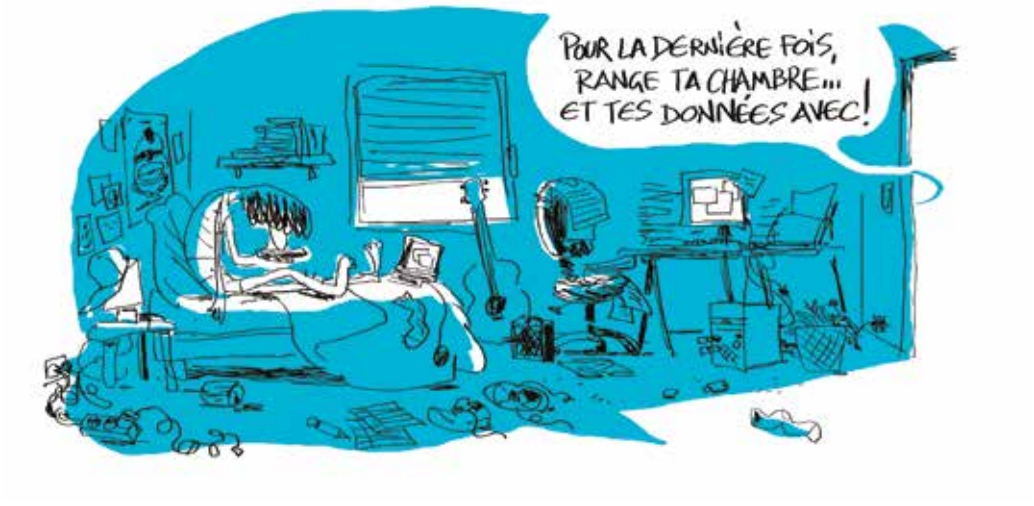
– la question de la protection des données à caractère personnel ;

– la place prise par les algorithmes dans notre société ;

– et plus globalement les dimensions éthiques, sociales et économiques de l'utilisation des données numériques et de leurs traitements.

De nombreux exemples de l'actualité permettent de le faire.

L'éducation aux médias et à l'information n'est pas affectée à une discipline, ce sont les équipes pédagogiques qui doivent s'en emparer. C'est à la fois une force pour permettre de montrer que les enjeux traversent l'ensemble des champs d'études, mais c'est aussi un point de fragilité, car cette diversité d'acteur rend complexe sa mise en œuvre. Aussi, comme le préconise le récent rapport de l'inspection générale sur le sujet (voir « Pour aller plus loin », p. 38), les chefs d'établissement devront renforcer le pilotage de cet enseignement si l'on veut espérer former efficacement les élèves aux enjeux actuels et futurs de la collecte et du traitement des données personnelles. Ils peuvent s'appuyer à cette fin sur les équipes du Centre de liaison d'éducation aux médias et à l'information (CLEMI), service de Réseau Canopé.



35 questions/ réponses sur l'application du RGPD en établissement

QUESTIONS RELATIVES AUX USAGES PÉDAGOGIQUES

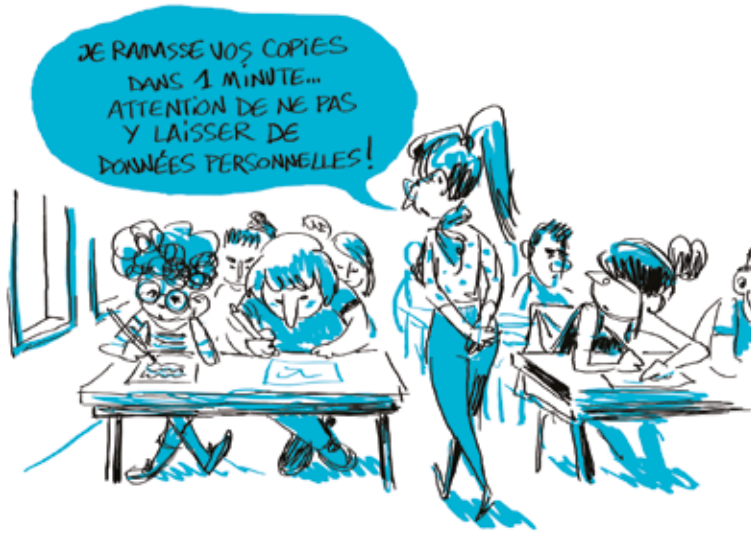
1. Un enseignant peut-il ouvrir un blog hébergé par une entreprise privée pour partager ses cours et des vidéos créées par lui, et permettre à ses élèves de travailler chez eux plus facilement, sachant qu'aucune information liée aux élèves n'est mise en ligne ? Si oui, sous quelles conditions ?

À titre liminaire, il convient de rappeler qu'un blog est par défaut un site internet accessible à tous. Dans le cadre d'une utilisation à des fins pédagogiques, il peut apparaître souhaitable d'en restreindre l'accès aux seules personnes autorisées, ce qui implique nécessairement, dans ce cas, la création de comptes utilisateurs avec identifiant et mot de passe, et donc la collecte de données à caractère personnel.

Par ailleurs, si le blog est un outil interactif permettant des échanges entre les utilisateurs, notamment pour commenter les publications qui y sont faites, la qualification de traitement de données à caractère personnel n'est exclue que s'il n'y a aucune possibilité d'identification directe ou indirecte des personnes qui se connectent ou contribuent sur le blog et si aucune donnée pouvant permettre, directement ou indirectement, l'identification des élèves n'est publiée.

Un blog constituant un site internet, il est soumis au droit applicable à tout service de communication en ligne tel qu'il est défini dans la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) et notamment aux dispositions de l'article 6 de cette loi, qui ont été précisées par le décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne. Ces dispositions font notamment obligation à toute personne physique ou morale assurant le stockage de signaux, d'écrits, d'images, de sons ou de messages pour mise à disposition du public, de détenir et de conserver pendant un an les données de connexion des utilisateurs de nature à permettre l'identification de quiconque a contribué à la création de contenu en ligne. De ce fait, si les élèves ou leurs responsables sont autorisés à intervenir sur le blog, leurs données de connexion devront nécessairement faire l'objet d'un traitement de données à caractère personnel.

Par conséquent, sauf dans l'hypothèse où un enseignant ouvre un blog auquel personne ne peut contribuer et sur lequel aucune donnée à caractère personnel (par exemple la photographie d'un élève) n'est mise en ligne, l'ouverture d'un blog dans le cadre scolaire constitue un traitement de données à caractère personnel auquel s'appliquent les dispositions du RGPD du 27 avril 2016



et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

En pratique, ce traitement de données à caractère personnel devra faire l'objet d'une inscription sur le registre de l'établissement public local d'enseignement (EPLE) qui le met en œuvre ou sur le registre tenu par les directions des services départementaux de l'Éducation nationale (DSDEN) ou les rectorats d'académie (en fonction de l'organisation choisie) pour les traitements mis en œuvre dans les écoles.

Par ailleurs, l'entreprise privée qui héberge les données à caractère personnel doit alors être regardée comme un sous-traitant au sens du RGPD. Par conséquent, une convention de sous-traitance doit être conclue entre l'établissement et cette entreprise, selon les modalités qui sont définies à l'article 28 du règlement.

En outre, en application du 2° de l'article R. 421-23 du Code de l'éducation qui prévoit que le conseil d'administration donne son avis sur les principes de choix des manuels scolaires, des logiciels et des outils pédagogiques, l'ouverture d'un blog à des fins pédagogiques au sein d'un EPLE devrait nécessiter l'avis préalable du conseil d'administration avant de pouvoir être inscrit sur le registre des activités de traitement de l'établissement scolaire.

Enfin, il est utile de rappeler que toute mise en ligne de photos ou de vidéos dans lesquelles apparaîtraient les élèves nécessite d'obtenir préalablement l'autorisation de la personne si elle est majeure ou de ses responsables légaux si elle est mineure, en application de l'article 9 du Code civil qui dispose que « chacun a droit au respect de sa vie privée ». Il est en effet de jurisprudence constante que le droit au respect de la vie privée permet à toute personne de s'opposer à la diffusion, sans son autorisation expresse, de son image.

Les contenus publiés par l'enseignant doivent également être libres de droit ou être la propriété de l'enseignant. Si le contenu est protégé par des droits d'auteur détenus par une tierce personne, il convient alors d'obtenir l'autorisation de cette personne avant de le publier.

2. Un enseignant peut-il utiliser en classe un service en ligne de questionnaires ou d'évaluations nécessitant d'identifier ses élèves, afin d'offrir des parcours et des résultats personnalisés ?

Dans la mesure où un tel outil implique nécessairement l'identification des élèves et la collecte d'un certain nombre d'informations à caractère personnel,

notamment relatives à l'évaluation des élèves, son utilisation en classe génère la mise en œuvre d'un traitement de données à caractère personnel au sens du RGPD et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Comme tout traitement de données à caractère personnel mis en œuvre dans une école ou un établissement scolaire, il devra dès lors, préalablement à sa mise en œuvre, faire l'objet d'une analyse au regard de la réglementation applicable en matière de protection des données personnelles, avec l'appui du délégué à la protection des données (DPD), et d'une inscription sur le registre d'activités de traitement par le responsable de traitement, à savoir le directeur académique des services de l'Éducation nationale (DASEN) agissant par délégation du recteur d'académie pour les traitements mis en œuvre dans les écoles, et le chef d'établissement pour les traitements mis en œuvre dans les établissements publics d'enseignement du second degré.

Dans les établissements du second degré, l'utilisation d'un tel outil pédagogique sera par ailleurs soumise à l'avis préalable du conseil d'administration, en application du 2° de l'article R. 421-23 du Code de l'éducation.

Dans l'hypothèse où le fournisseur du service en ligne serait amené à traiter ou à héberger des données, un contrat de sous-traitance doit également être établi entre le responsable de traitement et ce fournisseur, dans les conditions prévues par l'article 28 du RGPD.

Une attention particulière doit aussi être accordée dans le choix de ces outils en ligne. Beaucoup d'entre eux reposent en effet sur une analyse des traces d'apprentissage et des comportements des élèves, appelées « *learning analytics* », qui pourrait être qualifiée de « traitement de profilage », dont la mise en œuvre est particulièrement encadrée par les dispositions du RGPD.

Il convient par ailleurs de s'assurer que les données des élèves ne seront pas utilisées ultérieurement par les fournisseurs de services pour une finalité autre que celle définie par le responsable de traitement.

Les personnes concernées par le traitement (les élèves et leurs responsables s'ils sont mineurs) devront, en outre, être dûment informées par le responsable de traitement des caractéristiques de ce traitement dans les conditions prévues par les articles 13 et 14 du RGPD.

3. Un enseignant peut-il utiliser une application de réseau social pour une utilisation pédagogique ? Si oui, quelles précautions doit-il prendre et sous quelles conditions ?

L'utilisation d'une application de réseau social en classe entraîne nécessairement la mise en œuvre d'un traitement de données à caractère personnel au sens du RGPD et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Pour pouvoir mettre en œuvre un tel traitement, il convient donc, en premier lieu, que le responsable de traitement puisse justifier que ce traitement est nécessaire à l'exercice d'une mission d'intérêt public ou relève de l'exercice de l'autorité publique dont il est investi, au sens du e) du 1 de l'article 6 du RGPD. En d'autres termes, il faut pouvoir être en mesure de justifier que l'utilisation d'une telle application entre pleinement dans le champ du service public du numérique éducatif défini à l'article L. 131-2 du Code de l'éducation.

Si tel n'est pas le cas, pour que le traitement soit licite, il est nécessaire de recueillir le consentement des personnes concernées en application du a) du 1 de l'article 6 du RGPD. Conformément aux dispositions de l'article 7-1 de la loi du 6 janvier 1978 issu de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, il convient ainsi d'obtenir le consentement du mineur s'il est âgé de quinze ans ou plus ou le consentement du mineur et des titulaires de l'autorité parentale s'il est âgé de moins de quinze ans.

Il paraît toutefois difficile de recueillir le consentement des mineurs, quel que soit leur âge, dans le cadre scolaire. En effet, le 11) de l'article 4 du RGPD précise que le consentement consiste en une « manifestation de volonté libre, spécifique, éclairée et univoque, par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ». Or, il est permis de s'interroger sur la question de savoir si, dans le cadre scolaire, l'élève peut être regardé comme donnant valablement son consentement compte tenu de l'autorité qu'exerce sur lui l'enseignant qui propose l'utilisation d'une application numérique en classe.

Par ailleurs, le fait qu'un ou plusieurs élèves ou les titulaires de l'autorité parentale pour les mineurs de moins de quinze ans ne consentent pas à la collecte de leurs données personnelles conduit nécessairement à ce que les élèves ne puissent pas suivre l'enseignement et interagir dans le cours dans les mêmes conditions que les autres élèves, ce qui présente le risque d'une rupture d'égalité entre les élèves.

En tout état de cause, qu'il soit mis en œuvre sur le fondement du consentement de la personne concernée ou de l'exercice d'une mission d'intérêt public, tout traitement de données à caractère personnel mis en place au sein d'une école ou d'un établissement public du second degré doit être regardé comme étant sous la responsabilité du DASEN agissant par délégation du recteur d'académie dans le premier degré et du chef d'établissement dans le second degré.

Or, conformément aux dispositions de l'article 4 du RGPD, le responsable de traitement doit être en capacité de déterminer les finalités et les moyens du traitement. Cependant, les conditions générales d'utilisation (CGU) des réseaux sociaux sont le plus souvent élaborées unilatéralement par le fournisseur de services et ne permettent pas au DASEN ou au chef d'établissement d'exercer le moindre contrôle sur le traitement de données qu'il met en œuvre dans son établissement, ce qui n'est pas conforme à la réglementation applicable.

Aussi, pour pouvoir utiliser un réseau social dans le cadre scolaire, ou tout autre service numérique en ligne, il est nécessaire que les conditions générales d'utilisation du service fassent l'objet d'un contrôle par les services du ministère ou du rectorat d'académie et présentent des garanties suffisantes, notamment en termes de sécurité des données. Il convient notamment que les fournisseurs de services acceptent d'avoir la qualité de sous-traitants et de ne pouvoir traiter ou héberger les données que sur instruction du responsable de traitement. En dehors d'un tel cadre, qui implique donc des CGU spécifiques négociées par les services du ministère, dites « CGU éducation », il ne paraît pas possible pour le chef d'établissement ou le DASEN de garantir aux élèves et à leurs responsables que les services qu'ils mettent en œuvre au sein de l'établissement scolaire respectent les conditions de sécurité adéquates en matière de protection des données à caractère personnel et les droits des personnes concernées.

Comme tout traitement de données à caractère personnel, l'utilisation d'un réseau social en classe doit en outre faire l'objet d'une inscription sur le registre du responsable de traitement et d'une information des personnes concernées conformément aux dispositions des articles 13 et 14 du RGPD.

4. Un enseignant peut-il ouvrir un compte nominatif pour ses élèves sur un service de messagerie, une plateforme de travail coopératif ou de stockage et d'échange de documents développés par une entreprise privée et, si oui, quelles sont les règles à respecter dans ce domaine ?

Dès lors qu'un enseignant ouvre un compte nominatif permettant ainsi d'identifier les élèves avec leurs nom et prénom, il met en œuvre un traitement de données à caractère personnel. L'utilisation de ces services entraîne d'ailleurs la collecte et le traitement d'autres données à caractère personnel, telles que des photos ou des productions scolaires.

Par conséquent, les mêmes considérations que celles qui ont été décrites précédemment s'appliquent à ces traitements, à savoir :
– pouvoir justifier que le traitement est nécessaire à l'exécution d'une mission de service public ou recueillir le consentement des personnes concernées, avec toutes les réserves déjà rappelées précédemment ;
– s'assurer que les conditions générales d'utilisation permettent au responsable de traitement (DASEN ou chef d'établissement) de garder la maîtrise des données à caractère personnel collectées ;
– s'assurer que le service ou la plateforme présente les garanties suffisantes, notamment en termes de sécurité.

Le traitement fait par ailleurs l'objet des mêmes obligations d'inscription sur le registre des activités de traitement et des modalités d'information prévues aux articles 13 et 14 du RGPD.

5. Dans le cadre d'un cours ou d'un voyage scolaire, la classe réalise des photos, de petites vidéos et des enregistrements audio qui seront mis en ligne sur le site internet de l'établissement ou sur une plateforme d'échange privée. Quelles précautions prendre ? Doit-on obtenir l'accord des représentants des élèves? Des élèves eux-mêmes?

Toute mise en ligne de photos ou de vidéos dans lesquelles apparaîtraient des élèves nécessite d'obtenir préalablement l'autorisation de l'élève s'il est majeur ou de ses responsables s'il est mineur en application de l'article 9 du Code civil qui dispose que « chacun a droit au respect de sa vie privée ». Il est en effet de jurisprudence constante que le droit au respect de la vie privée permet à toute personne de s'opposer à la diffusion, sans son autorisation expresse, de son image.

L'autorisation de diffusion doit être écrite, spéciale et suffisamment précise quant aux conditions d'utilisation de l'enregistrement ou de la photo, de la durée de publication et du territoire d'exploitation concerné. L'autorisation étant spéciale, toute utilisation différente de celle qui a été autorisée par la personne nécessite une nouvelle autorisation.

Il est, par conséquent, possible de publier sur le site internet de l'établissement des photographies ou enregistrements qui illustrent une activité pédagogique telle qu'une sortie scolaire, sous réserve que les élèves pour lesquels l'autorisation de diffusion n'a pas été obtenue n'apparaissent pas ou soient « floutés ».

Dans un souci de protection des élèves, il est toutefois grandement préférable de privilégier une publication sur un site intranet ou sur un site disposant d'un accès restreint plutôt que sur un site internet.

Par ailleurs, l'image d'une personne constituant une donnée à caractère personnel dès lors qu'elle se rapporte à une personne identifiée ou identifiable, un site internet ou intranet sur lequel sont publiées des photos et des vidéos d'élèves constitue un traitement de données à caractère personnel soumis aux dispositions du RGPD du 27 avril 2016 et à la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Les sites intranet ou internet des établissements scolaires collectent et traitent, en outre, beaucoup d'autres données à caractère personnel, telles que des adresses électroniques ou des données d'identification des personnels des établissements. Il convient dès lors de veiller à ce que les traitements de données à caractère personnel relatifs à la mise en œuvre par un établissement scolaire d'un site intranet ou internet fassent l'objet d'une inscription sur le registre du responsable de traitement (le DASEN sur délégation du recteur d'académie dans le premier degré ou le chef d'établissement dans le second degré) et d'une information des personnes concernées dans les conditions prévues par les articles 13 et 14 du RGPD.

Si l'établissement a recours à une entreprise privée pour l'hébergement ou le transfert des données, cette entreprise doit être considérée comme un sous-traitant au regard de la réglementation applicable en matière de droit des données à caractère personnel. Un contrat de sous-traitance doit donc être conclu dans les conditions prévues par l'article 28 du RGPD.

6. Des enseignants peuvent-ils échanger sur une messagerie, personnelle ou privée, au sujet d'un élève?

Les échanges effectués par un enseignant par le biais d'une messagerie personnelle ou privée relèvent de sa vie personnelle. En application du c) du 2 de l'article 2 du RGPD du 27 avril 2016, le règlement n'est pas applicable aux traitements de données à caractère personnel effectués par une personne physique dans le cadre d'une activité strictement personnelle ou domestique.

Une messagerie privée n'est donc pas un traitement de données à caractère personnel soumis aux dispositions du RGPD.

7. Un enseignant peut-il refuser de transmettre au responsable de traitement, au nom de la liberté pédagogique, les applications numériques effectuant des traitements de données à caractère personnel de ses élèves ?

Un traitement de données à caractère personnel ne peut pas être mis en œuvre sans que les dispositions du RGPD du 27 avril 2016 et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés aient été respectées, notamment l'inscription du traitement sur le registre des activités de traitement prévu à l'article 30 du RGPD. Dans ces conditions, le responsable de traitement (le DASEN sur délégation du recteur dans le premier degré et le chef d'établissement dans le second degré) doit être informé des applications numériques utilisées en classe avec les élèves si celles-ci génèrent la mise en œuvre d'un traitement de données à caractère personnel. Il convient de rappeler qu'en application du 1 de l'article 24 du RGPD, le responsable de traitement « met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au [...] règlement ».

La liberté pédagogique de l'enseignant est encadrée : comme le rappelle l'article L. 912-1-1 du Code de l'éducation, elle s'exerce « dans le respect des programmes et des instructions du ministre chargé de l'Éducation nationale et dans le cadre du projet d'école ou d'établissement avec le conseil et sous le contrôle des membres des corps d'inspection ».

Dans le second degré, l'article R. 421-23 du Code de l'éducation précise d'ailleurs que le conseil d'administration, sur saisine du chef d'établissement, donne notamment son avis « sur les principes de choix des logiciels et des outils pédagogiques ».

L'enseignant est donc libre de choisir les outils pédagogiques qu'il souhaite utiliser dans le cadre de sa mission éducative, mais le conseil d'administration de l'établissement public local d'enseignement (EPLE) est appelé à émettre un avis sur les principes qui guident ses choix.

De même, dans le premier degré, l'article D. 411-2 du Code de l'éducation prévoit qu'une information doit être donnée au conseil d'école sur les principes de choix des manuels scolaires ou de matériels pédagogiques divers.

8. Pour les enseignements professionnels, les professeurs ont à choisir des solutions numériques liées au métier auquel prépare la formation. La plupart de ces solutions sont aujourd'hui proposées en ligne par les éditeurs. Les élèves (ou étudiants) sont susceptibles de les utiliser sous leur propre identité. Quels sont les points de vigilance auxquels sensibiliser les professeurs pour les aider dans leur choix ?

Dans la mesure où les élèves utilisent leur nom, un identifiant ou encore une adresse électronique pour accéder au service proposé, ces solutions numériques constituent des traitements de données à caractère personnel au sens du RGPD du 27 avril 2016 entré en vigueur le 25 mai 2018 et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Par conséquent, comme tout traitement de données à caractère personnel mis en œuvre dans un établissement scolaire, il doit faire l'objet d'une analyse au regard de la réglementation applicable en matière de protection des données personnelles avec l'appui du délégué à la protection des données (DPD) et d'une inscription sur le registre des activités de traitement tenu par le responsable de traitement, à savoir le chef d'établissement dans les établissements du second degré.

Dans le cas où les solutions numériques sont gérées par un prestataire de service, celui-ci doit être regardé comme un sous-traitant au sens de l'article 28 du RGPD.

Un contrat doit donc être conclu entre le responsable de traitement et ce prestataire dans les conditions prévues par l'article 28 du RGPD.

Le responsable de traitement doit en effet être en mesure de s'assurer que le sous-traitant présente des

garanties suffisantes, de manière à ce que le traitement réponde aux exigences du RGPD.

Il est donc impératif de sensibiliser les professeurs sur la nécessité de choisir une solution numérique proposée par un éditeur qui s'engage notamment à :
– respecter les règles instaurées par le RGPD. Par exemple, certains éditeurs peuvent appliquer un code de conduite approuvé ou un mécanisme de certification approuvé, ce qui constitue un élément pour démontrer l'existence de garanties suffisantes (cf. point 5 de l'article 28) ;
– respecter les mesures de sécurité instaurées par le RGPD (article 32). Il s'agit, par exemple, de la pseudonymisation et du chiffrement des données à caractère personnel ;
– informer le responsable de traitement en cas de violation de données à caractère personnel (cf. point 2 de l'article 33).
– n'avoir recours qu'à des sous-traitants soumis aux mêmes obligations que celles prévues dans le contrat de sous-traitance initial.

Par ailleurs, dans la mesure où ces solutions numériques entrent dans le champ du service public du numérique éducatif défini à l'article L. 131-2 du Code de l'éducation, le traitement est nécessaire à l'exercice d'une mission d'intérêt public au sens du e) du 1 de l'article 6 du RGPD. Le consentement des personnes concernées n'a donc pas à être préalablement recueilli.

En outre, les personnes dont les données sont collectées doivent être informées des principales caractéristiques du traitement par le responsable de traitement, conformément aux articles 13 et 14 du RGPD.

Ces personnes doivent ainsi être informées de l'identité et des coordonnées du responsable de traitement, des coordonnées du délégué à la protection des données, des finalités du traitement, de sa base juridique, du caractère obligatoire ou facultatif du recueil des données et des conséquences pour la personne en cas de non-fourniture de ces données, des destinataires des données collectées, de la durée de conservation de ces données. De même, les personnes dont les données sont collectées doivent être informées de leurs droits d'opposition, d'accès, de rectification, d'effacement, de limitation et de la possibilité dont elles disposent d'introduire une réclamation (plainte) auprès de la Commission nationale de l'informatique et des libertés (CNIL).

Le cas échéant, les personnes dont les données sont collectées doivent également être informées de l'existence d'une prise de décision automatisée ou d'un profilage, des informations utiles à la compréhension de l'algorithme et de sa logique, du fait que les données sont requises par la réglementation, de la faculté d'accéder aux documents autorisant le transfert de données hors de l'Union européenne (par exemple, les clauses contractuelles types de la Commission européenne).

De surcroît, des informations supplémentaires doivent être communiquées aux personnes concernées en cas de collecte indirecte de données (autrement dit, données qui ne sont pas collectées directement auprès des personnes concernées), à savoir : les catégories de données recueillies et les sources des données (en indiquant notamment si elles sont issues de sources accessibles au public).

Enfin, le choix de ces outils doit être soumis au conseil d'administration de l'EPLE, conformément à l'article R. 421-23 du Code de l'éducation qui dispose que le conseil d'administration pour les collèges et les lycées, sur saisine du chef d'établissement, donne son avis notamment « sur les principes de choix des logiciels et des outils pédagogiques ».

9. Pour les enseignements professionnels, certains référentiels recommandent ou imposent l'usage d'un outil de suivi des compétences acquises par les élèves ou les étudiants (portefeuille, passeport ou encore livret). Quelles sont les précautions à prendre pour l'usage de tels outils, qu'ils soient hébergés dans l'établissement ou en ligne ?

L'usage de tels outils, qui implique la collecte de données à caractère personnel relatives aux élèves ou aux étudiants, constitue un traitement de données à caractère personnel au sens du RGPD et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Par conséquent, comme tout traitement de données à caractère personnel mis en œuvre dans un établissement public d'enseignement, quel que soit le mode d'hébergement des données, il doit faire l'objet d'une inscription sur le registre des activités de traitement tenu par le responsable de traitement, à savoir le chef d'établissement dans les établissements du second degré.

Si l'éditeur est amené à traiter (par exemple, dans le cadre d'une prestation de maintenance ou d'aide à l'utilisateur) ou à héberger des données à caractère personnel, celui-ci doit être regardé comme un sous-traitant. Il convient donc de conclure un contrat de sous-traitance conformément à l'article 28 du RGPD.

Le responsable de traitement doit en effet être en mesure de s'assurer que le sous-traitant présente des garanties suffisantes, de manière à ce que le traitement réponde aux exigences du RGPD.

En outre, les personnes dont les données sont collectées doivent être informées des principales caractéristiques du traitement par le responsable de traitement, aux termes des articles 13 et 14 du RGPD.

Ces personnes doivent ainsi être informées de l'identité et des coordonnées du responsable de traitement, des coordonnées du délégué à la protection des données, des finalités du traitement, de sa base juridique, du caractère obligatoire ou facultatif du recueil des données et des conséquences pour la personne en cas de non-fourniture de ces données, des destinataires des données collectées, de la durée de conservation de ces données. De même, les personnes dont les données sont collectées doivent être informées de leurs droits d'opposition, d'accès, de rectification, d'effacement, de limitation et de la possibilité dont elles disposent d'introduire une réclamation (plainte) auprès de la Commission nationale de l'informatique et des libertés (CNIL).

Le cas échéant, les personnes dont les données sont collectées doivent également être informées de l'existence d'une prise de décision automatisée ou d'un profilage, des informations utiles à la compréhension de l'algorithme et de sa logique, du fait que les données sont requises par la réglementation, de la faculté d'accéder aux documents autorisant le transfert de données hors de l'Union européenne (par exemple, les clauses contractuelles types de la Commission européenne).

De surcroît, des informations supplémentaires doivent être communiquées aux personnes concernées en cas de collecte indirecte de données (autrement dit, données qui ne sont pas collectées directement auprès des personnes concernées), à savoir : les catégories de données recueillies et les sources des données (en indiquant notamment si elles sont issues de sources accessibles au public).

Enfin, le choix de l'outil de suivi des compétences doit être soumis au conseil d'administration de l'EPLE, conformément à l'article R. 421-23 du Code de l'éducation qui dispose que le conseil d'administration pour les collèges et les lycées, sur saisine du chef d'établissement, donne son avis notamment « sur les principes de choix des logiciels et des outils pédagogiques ».

QUESTIONS D'ORDRE ADMINISTRATIF

10. Dans le cadre du RGPD, qui est responsable du traitement des données à caractère personnel pour une école, un collège, un lycée, public ou privé ?

Le 7° de l'article 4 du RGPD définit le responsable de traitement comme « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ».

Sauf dans l'hypothèse où le traitement fait l'objet d'un paramétrage local, qui est susceptible de justifier une responsabilité conjointe, les traitements mis en œuvre par le ministère de l'Éducation nationale dans les établissements scolaires relèvent uniquement de la responsabilité du ministre chargé de l'Éducation nationale.

Ce principe s'applique aux traitements mis en œuvre dans les établissements publics mais également dans les établissements privés sous contrat, dès lors que les traitements mis en œuvre relèvent de la compétence du ministre chargé de l'Éducation nationale (par exemple, la gestion des personnels).

Pour les traitements mis en œuvre dans les écoles ou les établissements scolaires à l'initiative d'un personnel (par exemple, un enseignant), la responsabilité incombe à la personne ayant la capacité juridique de représenter l'établissement, notamment en justice dans l'éventualité d'un recours.
Dans les établissements publics du second degré, qui ont la personnalité morale, c'est le chef d'établissement qui, en sa qualité d'organe exécutif de l'établissement conformément à l'article R. 421-9 du Code de l'éducation, doit être regardé comme le responsable des traitements mis en œuvre dans son établissement.

En revanche, dans les écoles publiques, les directeurs n'ayant pas la capacité juridique de représenter l'école (cf. les articles 2 à 4 du décret n° 89-122 du 24 février 1989 relatif aux directeurs d'école), ce sont les directeurs académiques des services de l'Éducation nationale (DASEN), agissant sur délégation des recteurs d'académie qui, en application de l'article R. 222-19-3 du Code de l'éducation, doivent être regardés comme responsables des traitements mis en œuvre.

S'agissant enfin des traitements mis en œuvre dans les écoles, collèges et lycées privés, il ne peut y avoir de réponse de principe, dans la mesure où la qualité de responsable de l'établissement dépend du mode de constitution et de fonctionnement de ces établissements.

11. Chaque responsable de traitement doit-il nommer un délégué à la protection des données (DPD) ?

En application du 1 de l'article 37 du RGPD, les responsables de traitement et les sous-traitants sont tenus de désigner un DPD lorsque le traitement est effectué par une autorité publique ou un organisme public, ou lorsque l'activité de base de l'organisme consiste en un suivi systématique à grande échelle de personnes ou en un traitement à grande échelle de catégories particulières de données à caractère personnel.

Les responsables des traitements mis en œuvre dans les écoles, les collèges et les lycées publics sont donc tenus de désigner un DPD.

Toutefois, le 3 du même article prévoit que « lorsque le responsable de traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille ».

Une mutualisation du DPD au niveau académique, infra-académique ou de la région académique est donc tout à fait possible.

En revanche, les établissements d'enseignement privés sous contrat, qui ne relèvent d'aucune des dispositions du 1 de l'article 37 du RGPD, ne sont pas soumis à l'obligation de désignation d'un DPD.

La désignation d'un DPD dans les établissements d'enseignement privés sous contrat n'est donc qu'une faculté prévue par le 4 de l'article 37 du RGPD.

Si les lignes directrices concernant les délégués à la protection des données adoptées le 13 décembre 2016 par le groupe de protection des personnes à l'égard du traitement des données à caractère personnel, dénommé « G29 », recommandent aux organismes privés chargés d'une mission de service public de désigner un DPD, il ne s'agit néanmoins que d'une recommandation et non pas d'une obligation.

12. Quels sont les traitements qu'un chef d'établissement doit inscrire dans le registre ? Ce registre doit-il être accessible au public ?

Le RGPD s'applique à tous les traitements de données à caractère personnel effectués dans le cadre des activités d'un responsable de traitement établi sur le territoire de l'Union européenne, que le traitement ait lieu ou non dans l'Union européenne.

Les chefs d'établissement n'ont pas à déclarer les traitements qui sont mis en œuvre par des applications nationales ou académiques fournies et diffusées par la direction du numérique pour l'éducation ou les services académiques qu'ils installent sur leurs propres hébergements, dans la mesure où ils sont exploités conformément à leur documentation et n'ont pas été modifiés au niveau de l'établissement. Pour ces applications nationales ou académiques, le périmètre fonctionnel est défini par les directions métiers de l'administration centrale ou du rectorat qui en sont les responsables de traitement.

En revanche, si les établissements utilisent des données issues des applications nationales, académiques ou recueillies au niveau de l'établissement dans des applications locales ou des services numériques développés indépendamment de l'administration centrale ou du rectorat, ils doivent déclarer ces traitements.

En application de l'article L. 121-4-1 du Code de l'éducation, ce registre doit être mis à la disposition du public.

13. Quelles sont les informations qu'un responsable de traitement doit inscrire dans le registre ?

L'article 30 du RGPD prévoit que chaque responsable de traitement tient un registre des activités de traitement effectuées sous sa responsabilité.

Ce registre doit comporter le nom et les coordonnées du responsable de traitement et du délégué à la protection des données.

Le registre est composé d'une fiche registre pour chaque activité de traitement qui comporte les informations suivantes :
– les finalités du traitement (l'objectif en vue duquel les données sont collectées) ;
– les personnes dont les données sont collectées ;
– les catégories de données traitées (par exemple, l'identité et des informations professionnelles : nom, prénom et adresse électronique…) ;
– les destinataires des données ;
– les transferts éventuels de données à caractère personnel vers un pays tiers ou une organisation internationale et les garanties prévues pour ces transferts ;
– les durées de conservation des données collectées ;
– une description générale des mesures de sécurité techniques et organisationnelles mises en œuvre pour l'activité de traitement.

14. Quand le responsable de traitement doit-il demander le consentement des parents, des élèves ou des personnels sous sa responsabilité, pour utiliser un logiciel ou un service numérique ?

Le 1 de l'article 6 du RGPD du 27 avril 2016 prévoit qu'un traitement de données à caractère personnel n'est licite que dans la mesure où l'une des conditions suivantes est remplie :
« a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;
b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable de traitement est soumis ;
d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
e) le traitement 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 ;
f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable de traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant. »

Les traitements mis en œuvre dans les établissements d'enseignement relèvent en principe de l'exécution de la mission d'intérêt public dont est investi le responsable de traitement au sens du e) de cet article. En effet, l'utilisation d'un logiciel ou d'un service numérique à des fins pédagogiques s'inscrit dans le champ du service public du numérique éducatif défini à l'article L. 131-2 du Code de l'éducation.

Le responsable de traitement n'est, par conséquent, pas tenu de recueillir le consentement des parents, des élèves ou des personnels sous sa responsabilité pour mettre en œuvre un tel traitement.

Toutefois, si le responsable de traitement n'est pas en mesure de justifier que le traitement qu'il souhaite mettre en œuvre rentre bien dans le champ de la mission d'intérêt public dont il est investi, hypothèse qui apparaît marginale, il est tenu d'obtenir le consentement des personnes concernées par le traitement.

Ce type de traitement devrait cependant rester exceptionnel, car sa mise en œuvre risquerait d'aboutir à des situations de traitement différencié des élèves. En effet, si un parent ou un élève refuse de consentir à la mise en œuvre du traitement en question, l'élève ne pourra pas participer au cours dans les mêmes conditions que les autres élèves, ce qui présente un risque de rupture d'égalité entre les élèves.

15. Qu'entend-on par un traitement « nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique » ?

Le RGPD du 27 avril 2016 ne définit pas la notion de « mission d'intérêt public » mentionnée au e) du 1 de l'article 6. Il semble, en outre, que cette notion n'est que la traduction littérale du terme anglais « *public interest* ».

La notion de « mission d'intérêt public » n'est pas utilisée en droit français. On peut toutefois la rapprocher de la notion de « mission de service public », qui est

d'ailleurs l'expression utilisée au 3° de l'article 7 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

En matière d'enseignement ou d'éducation, un traitement peut être regardé comme « nécessaire à l'exécution d'une mission d'intérêt public » s'il entre dans le champ de la notion générale de « service public de l'enseignement » ou de celle, plus restrictive, de « service public du numérique éducatif » définie à l'article L. 131-2 du Code de l'éducation.

Aucune disposition à caractère législatif ou réglementaire ne définit précisément la notion de « service public de l'enseignement ». Toutefois, un titre est expressément consacré aux « Objectifs et missions du service public de l'enseignement » dans le Code de l'éducation (titre II du livre premier de la première partie). Les commentaires du Code Dalloz en proposent la définition suivante : « Les missions du service public de l'enseignement ou de l'éducation [...] consistent [...] à apporter au titulaire du droit à l'éducation les prestations qui lui permettent d'acquérir un savoir [...], un savoir-faire [...] et un savoir être [...] »

Au regard de cette définition qui apparaît comme pertinente, pourrait être regardé comme « nécessaire à l'exécution d'une mission d'intérêt public » tout traitement de données à caractère personnel qui aurait pour objet la mise en œuvre d'un outil ou d'un service numérique permettant l'acquisition d'un savoir, d'un savoir-faire ou d'un savoir être.

16. Doit-on effectuer des démarches particulières pour utiliser un logiciel de vie scolaire [gestion des absences, conception d'emploi du temps, etc.] développé par une entreprise privée ?

Dans la mesure où ce type de logiciel implique nécessairement la collecte de données relatives à l'identité et à la vie scolaire des élèves, un tel fichier, qu'il soit ou non diffusé sur le réseau local de l'établissement, constitue un traitement de données à caractère personnel au sens du RGPD et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Par conséquent, comme tout traitement de données à caractère personnel mis en œuvre dans une école ou dans un établissement public d'enseignement, il doit faire l'objet d'une inscription sur le registre des activités de traitement tenu par le responsable de traitement, à savoir le directeur académique des services de l'Éducation nationale (DASEN), agissant sur délégation du recteur d'académie, dans le premier degré, ou le chef d'établissement, dans le second degré.

Dans le cas où le logiciel de vie scolaire est géré par un prestataire de services, celui-ci doit être regardé comme sous-traitant au sens de l'article 28 du RGPD.

Un contrat doit donc être conclu entre le responsable de traitement et ce prestataire dans les conditions prévues par l'article 28 du RGPD.

Le responsable de traitement doit en effet être en mesure de s'assurer que le sous-traitant présente des garanties suffisantes de manière à ce que le traitement réponde aux exigences du RGPD, notamment en termes de sécurité.

Par ailleurs, les personnes dont les données sont collectées doivent être informées des principales caractéristiques du traitement par le responsable de traitement, aux termes des articles 13 et 14 du RGPD.

Elles doivent ainsi être informées de l'identité et des coordonnées du responsable de traitement, des coordonnées du délégué à la protection des données, des finalités du traitement, de sa base juridique, du caractère obligatoire ou facultatif du recueil des données et des conséquences pour la personne en cas de non-fourniture de ces données, des destinataires des données collectées, de la durée de conservation de ces données.
Enfin, les personnes dont les données sont collectées doivent être informées de leurs droits d'opposition, d'accès, de rectification, d'effacement, de limitation et de la possibilité dont elles disposent d'introduire une réclamation (plainte) auprès de la Commission nationale de l'informatique et des libertés (CNIL).
Le cas échéant, les personnes dont les données sont collectées doivent également être informées de l'existence d'une prise de décision automatisée ou d'un profilage, des informations utiles à la compréhension de l'algorithme et de sa logique, ainsi que des conséquences pour la personne, du droit de retirer son consentement à tout moment, du fait que les données sont requises par la réglementation, par

un contrat ou en vue de la conclusion d'un contrat, de la faculté d'accéder aux documents autorisant le transfert de données hors de l'Union européenne (par exemple, les clauses contractuelles types de la Commission européenne).

Enfin, des informations supplémentaires doivent leur être communiquées en cas de collecte indirecte de données, à savoir : les catégories de données recueillies et les sources des données (en indiquant notamment si elles sont issues de sources accessibles au public).

17. Quand le chef d'établissement, responsable de traitement, doit-il demander une étude d'impact? Qui la réalise?

L'article 35 du RGPD prévoit que la réalisation d'une analyse d'impact relative à la protection des données (AIPD) s'impose « lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques ».

Le règlement énonce, en outre, que la réalisation d'une analyse d'impact est particulièrement requise dans trois cas :
– « l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire » ;
– « le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 » ;
– « la surveillance systématique à grande échelle d'une zone accessible au public ».

Par ailleurs, le règlement charge les autorités de contrôle, autrement dit, en France, la Commission nationale de l'informatique et des libertés (CNIL), d'établir des listes des opérations de traitement soumises à une analyse d'impact ou au contraire pour lesquelles aucune analyse d'impact n'est requise.

Ces listes sont toutefois toujours en cours d'élaboration par la CNIL à ce jour.

Dans l'attente de la publication de ces listes, il convient de se référer aux lignes directrices concernant l'analyse d'impact relative à la protection des données et la manière de déterminer si le traitement est susceptible d'engendrer « un risque élevé » aux fins du RGPD, lignes directrices qui ont été adoptées le 4 avril 2017 par le groupe de protection des personnes à l'égard du traitement de données à caractère personnel, dénommé « G29 ».

Ces lignes directrices sensibilisent les responsables de traitement sur les neuf critères suivants :
– évaluation ou notation, y compris les activités de profilage et de prédiction ;
– prise de décision automatisée avec effet juridique ou effet similaire significatif ;
– surveillance systématique ;
– données sensibles ou données à caractère hautement personnel (sont visées, à ce titre, les données mentionnées aux articles 9 et 10 du RGPD, outre les données liées aux communications électroniques, les données de localisation ou encore les données financières) ;
– données traitées à grande échelle (notamment au regard du nombre de personnes concernées, du volume de données collectées, de la durée du traitement et de son étendue géographique) ;
– croisement ou combinaison d'ensembles de données ;
– données concernant les personnes vulnérables (enfants, demandeurs d'asile, par exemple) ;
– utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles ;
– traitements qui empêchent l'exercice d'un droit ou emportent l'exclusion d'un contrat.

Le G29 estime nécessaire la réalisation d'une AIPD lorsqu'au moins deux de ces neuf critères sont réunis.

Le responsable de traitement doit donc, dès la conception du traitement, se poser la question de la nécessité de réaliser une étude d'impact, en analysant l'ensemble des éléments qui viennent d'être exposés.

Il est toutefois à noter qu'une seule et même analyse d'impact peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés identiques.

Dans les établissements publics d'enseignement, l'AIPD doit être effectuée par le chef d'établissement, en sa qualité de responsable de traitement, avant la mise en œuvre du traitement. À cette fin, il peut demander conseil au délégué à la protection des données qui a également pour mission de vérifier la bonne exécution de cette analyse.

La maîtrise d'ouvrage, la maîtrise d'œuvre et la personne chargée de la sécurité des systèmes d'information peuvent également intervenir dans la réalisation de l'AIPD. De la même manière, lorsqu'un sous-traitant intervient dans le traitement, il doit fournir son aide et les renseignements nécessaires à la réalisation de l'AIPD.

Le RGPD prévoit, en outre, la possibilité pour les responsables de traitement de consulter les personnes concernées.

Il convient enfin de rappeler que la CNIL a décidé de laisser aux responsables de traitement un délai de trois ans à compter du 25 mai 2018 pour se mettre en conformité avec la réglementation relative à l'analyse d'impact lorsqu'un traitement déjà mis en œuvre et régulièrement déclaré avant le 25 mai 2018 (récépissé, autorisation, avis de la CNIL ou inscription au registre d'un correspondant informatique et libertés) est susceptible de relever des conditions de réalisation de l'AIPD.

En revanche, dans tous les autres cas où elle est requise, une AIPD devra être réalisée immédiatement :
– pour les traitements antérieurs au 25 mai 2018 n'ayant pas fait l'objet de formalités préalables auprès de la CNIL ;
– pour les traitements antérieurs au 25 mai 2018 et régulièrement mis en œuvre, mais qui ont fait l'objet d'une modification substantielle depuis l'accomplissement des formalités préalables qui leur étaient applicables ;
– pour tout nouveau traitement de données mis en œuvre après le 25 mai 2018.

La CNIL met à disposition des guides facilitant la réalisation de ces études d'impact (www.cnil.fr/fr/PIA-privacy-impact-assessment). Si un sous-traitant intervient dans le traitement, il doit fournir son aide et les informations nécessaires à la réalisation de l'étude. Le responsable de traitement peut s'appuyer sur les conseils du délégué à la protection des données de son académie.

18. Un CPE peut-il créer des fichiers au nom des élèves dans le système informatique, afin de suivre de manière annuelle, voire pluriannuelle, certains élèves « à problèmes » ?

Dans la mesure où il implique la collecte de données relatives à l'identité des élèves, un tel fichier constitue un traitement de données à caractère personnel au sens du RGPD du 27 avril 2016 et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Comme tout traitement de données à caractère personnel, il doit, avant sa mise en œuvre, faire l'objet d'une analyse au regard de la réglementation applicable et d'une inscription sur le registre des activités de traitement du chef d'établissement, dans les conditions prévues à l'article 30 du RGPD.

En effet, un conseiller principal d'éducation (CPE) n'a pas la capacité juridique de représenter l'établissement scolaire.

En l'espèce, pour pouvoir mettre en œuvre un tel traitement, plusieurs points prévus à l'article 5 du RGPD devraient faire l'objet d'une attention particulière de la part du responsable de traitement.

La finalité du traitement devrait être précisée. En effet, la notion « d'élèves à problèmes » est trop floue pour pouvoir être regardée comme déterminée, explicite et légitime au sens du b) du 1 de l'article 5 du RGPD. Il conviendrait de mentionner précisément l'objet de ce traitement.

Il convient par ailleurs de veiller à ne collecter que des données adéquates, pertinentes et limitées à ce qui est nécessaire à la finalité du traitement dans le respect du

principe de minimisation des données prévu au c) du 1 de l'article 5 du RGPD. Cela implique, par exemple, que le traitement en question ne pourrait pas traiter de données relatives à la religion des personnes concernées ou des données relatives à la prévention, la recherche, la constatation ou la poursuite des infractions pénales dont le traitement est réservé à certains organismes prévus à l'article 9 de la loi du 6 janvier 1978 et qui ne peut être autorisé que par un acte réglementaire en application de l'article 26 de la loi du 6 janvier 1978.

Il est également nécessaire de faire preuve d'une vigilance particulière si le fichier comporte des champs de commentaires libres. La Commission nationale de l'informatique et des libertés (CNIL) rappelle, en effet, de façon constante, que les appréciations mentionnées dans les champs libres doivent toujours être objectives et jamais excessives ou insultantes. Le responsable de traitement doit être informé que ces zones de commentaires ne doivent pas comporter de données sensibles au sens de l'article 9 du RGPD ou de l'article 8 de la loi du 6 janvier 1978. Par exemple, lorsqu'il s'agit de suivre des élèves présentant des troubles psychiatriques, les données de santé les concernant constituent des données sensibles, dont le traitement est en principe interdit, sauf exception prévue par le RGPD concernant les traitements mis en œuvre par les acteurs de santé dont ne fait pas partie un CPE. Les données de santé ne peuvent donc en aucun cas apparaître dans les champs de commentaires libres.

En application du e) du 1 de l'article 5 du RGPD, la durée de conservation des données ne devrait pas excéder celle nécessaire au regard des finalités pour lesquelles les données sont traitées. Il faudrait, par conséquent, que le chef d'établissement soit en mesure de justifier la conservation pluriannuelle des fichiers.

Enfin, les personnes concernées devraient être dûment informées des caractéristiques du traitement dans les conditions prévues aux articles 13 et 14 du RGPD.

19. Il existe des logiciels de gestion de flottes de tablettes ou d'ordinateurs portables qui permettent, dans le cadre d'un travail de classe, de projeter l'écran d'une tablette ou d'un ordinateur à l'écran, de vérifier quels sont les élèves qui sont connectés ou pas, de regarder le travail qu'ils effectuent. Ces « gestionnaires » font partie intégrante de nombreux systèmes utilisés dans les écoles. Peut-on les utiliser et sous quelles conditions ?

Les logiciels de gestion de flottes et les outils de gestion de classe sont des traitements de données à caractère personnel.

Les logiciels de gestion de flottes ont notamment pour objet de gérer le parc d'équipements informatiques (tablettes ou ordinateurs fixes et mobiles) et son déploiement, ainsi que de contrôler certaines fonctions du matériel et du système.

Les outils de gestion de classe peuvent, quant à eux, avoir pour finalités de permettre aux enseignants de diffuser des documents aux élèves, d'autoriser ou de restreindre les accès aux ressources en fonction des objectifs pédagogiques de la séquence, de visualiser l'écran des élèves sur le poste de l'enseignant, de créer des groupes de discussion ou encore de gérer des sessions de discussion (messagerie instantanée).

La mise en œuvre de tels traitements nécessite un examen préalable approfondi au regard de la réglementation applicable en matière de protection des données à caractère personnel et une inscription sur le registre du responsable de traitement dans les conditions prévues à l'article 30 du RGPD.

Pour aider les responsables de traitement dans le choix de ces outils, le ministère de l'Éducation nationale a édité deux référentiels – le « Cadre de référence pour l'accès aux ressources pédagogiques via un équipement mobile » (CARMO) et le « Cadre de référence des services d'infrastructure numérique » (CARINE) – qui donnent des recommandations sur les mesures techniques, organisationnelles et de sécurité devant être respectées.

Par ailleurs, le ministère de l'Éducation nationale travaille depuis plusieurs mois en étroite collaboration avec la Commission nationale de l'informatique et des libertés (CNIL) à l'élaboration d'un référentiel qui pourrait servir de base à l'analyse de ces traitements par les responsables de traitement.

En attendant l'élaboration d'un tel référentiel, il convient d'analyser chaque traitement au regard de la réglementation applicable et, notamment, de s'interroger sur la nécessité de procéder ou non à une analyse d'impact avant la mise en œuvre d'un tel traitement.

Une attention particulière doit également être portée sur les traitements qui entraîneraient le transfert de données à caractère personnel dans un État en dehors de l'Union européenne (par exemple, dans l'hypothèse d'un hébergement de données dans un « cloud » en dehors de l'Espace économique européen). Il faut alors s'assurer que ces transferts présentent des garanties suffisantes en matière de sécurité et sont couverts par des documents juridiques adéquats (par exemple, clauses contractuelles types dûment signées).

Par ailleurs, les personnes dont les données sont collectées doivent être informées des principales caractéristiques du traitement par le responsable de traitement, conformément aux dispositions des articles 13 et 14 du RGPD.

Elles doivent ainsi être informées : de l'identité et des coordonnées du responsable de traitement, des coordonnées du délégué à la protection des données, des finalités, de la base juridique du traitement, des destinataires, de la durée de conservation des données, du droit des personnes concernées (opposition, accès, rectification, effacement, limitation), du droit d'introduire une réclamation (plainte) auprès de la CNIL, du transfert éventuel de données hors de l'Union européenne et de la faculté d'accéder aux documents autorisant le transfert de données hors de l'Union européenne.

Enfin, des informations supplémentaires doivent leur être communiquées en cas de collecte indirecte de données, à savoir : les catégories de données recueillies et les sources des données (en indiquant notamment si elles sont issues de sources accessibles au public).

20. Une école primaire peut-elle créer un fichier sur un tableur recensant les nom et prénom des élèves, leur classe et leurs demi-journées de présence/absence ? Ce fichier a vocation à être soit diffusé sur le réseau local de l'école afin d'être complété par les enseignants pour leurs classes respectives, soit conservé uniquement sur le poste informatique de direction [et complété par la directrice]. Est-ce autorisé ? Et si oui, quelles sont les démarches à effectuer ?

Dans la mesure où il implique la collecte de données relatives à l'identité et à la vie scolaire des élèves, un tel fichier, qu'il soit ou non diffusé sur le réseau local de l'établissement, constitue un traitement de données à caractère personnel au sens du RGPD et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Comme tout traitement de données à caractère personnel mis en œuvre dans une école, il doit donc faire l'objet d'une inscription sur le registre des activités de traitement tenu par le responsable de traitement, à savoir le directeur académique des services de l'Éducation nationale (DASEN), agissant sur délégation du recteur d'académie.

Les personnes concernées par le traitement doivent être informées des caractéristiques de ce traitement dans les conditions prévues par les articles 13 et 14 du RGPD.

Elles doivent ainsi être informées de l'identité et des coordonnées du responsable de traitement, des coordonnées du délégué à la protection des données, des finalités, de la base juridique du traitement, du caractère obligatoire ou facultatif du recueil des données et des conséquences pour la personne en cas de non-fourniture des données, des destinataires, de la durée de conservation des données, du droit des personnes concernées (opposition, accès, rectification, effacement, limitation), du droit d'introduire une réclamation (plainte) auprès de la Commission nationale de l'informatique et des libertés (CNIL).

Le cas échéant, les personnes concernées doivent également être informées de l'existence d'une prise de décision automatisée ou d'un profilage, des informations utiles à la compréhension de l'algorithme et de sa logique, ainsi que des conséquences pour la personne concernée, du droit de retirer son consentement à tout moment, du fait que les données sont requises par la réglementation, par un contrat ou

en vue de la conclusion d'un contrat, de la faculté d'accéder aux documents autorisant le transfert de données hors de l'Union européenne (par exemple, les clauses contractuelles types de la Commission européenne).

Enfin, des informations supplémentaires doivent leur être communiquées en cas de collecte indirecte de données, à savoir : les catégories de données recueillies et les sources des données (en indiquant notamment si elles sont issues de sources accessibles au public).

21. L'échange de courriels entre les membres de la communauté éducative (élève/élève, professeur/parents, etc.) via une messagerie mise en œuvre par une école est-il considéré comme privé ?

Il résulte d'une jurisprudence constante de la Cour de cassation que les fichiers et courriels échangés par un salarié à l'aide d'un outil informatique mis à sa disposition par l'employeur pour les besoins de son travail sont présumés revêtir un caractère professionnel, sauf si le salarié les a expressément identifiés comme revêtant un caractère personnel (ex. : Cass. soc., 16 mai 2013, n° 12-11866).

Le Conseil d'État n'a, jusqu'alors, pas eu l'occasion de prendre position sur cette question.

La cour d'appel de Rennes, statuant en matière pénale, a quant à elle considéré que les courriels échangés par un agent public par le biais d'une messagerie professionnelle sont présumés revêtir un caractère professionnel, sauf à ce que leur contenu intéresse de manière évidente la vie privée de leur auteur (CA Rennes, 14 janvier 2010, n° 972010).

Le caractère professionnel d'un message peut autoriser l'employeur, dans certaines conditions et notamment dans le respect de la réglementation en matière de protection des données à caractère personnel, à exercer un contrôle sur la messagerie de l'agent.
En revanche, dès lors que l'objet du courriel échangé par un enseignant avec un parent d'élève mentionne son caractère privé, il doit être regardé comme une correspondance privée couverte par le secret des correspondances prévu par l'article L. 32-3 du Code des postes et des communications électroniques et par le droit au respect de la vie privée reconnu par l'article 8 de la Convention européenne des droits de l'homme.

Les échanges de courriels entre élèves ont, quant à eux, par nature un caractère privé. Ce principe de protection des correspondances des enfants ressort de l'article 16 la Convention relative aux droits de l'enfant. Il n'est donc pas possible de contrôler leurs courriels, y compris lorsqu'ils utilisent la messagerie qui a été mise à disposition par l'école.

À toutes fins utiles, il est indispensable de rappeler que les messageries électroniques et les dispositifs de contrôle de l'utilisation de ces dernières constituent des traitements de données à caractère personnel au sens de l'article 4 du RGPD et doivent, par conséquent, être inscrits sur le registre des activités de traitement.

22. Un élève peut-il créer un site internet pour sa classe, afin de relayer des informations pour ses camarades (changements de cours, professeurs absents, etc.) ?

Il convient tout d'abord de rappeler qu'un site internet est *a priori* accessible à tous. Dans le cadre de la diffusion d'informations concernant la vie interne d'un établissement scolaire, il est préférable de privilégier la diffusion sur un site intranet dont l'accès est restreint aux seules personnes concernées par l'information.

Même s'il est créé par un élève, un site relayant des informations relatives à des changements de cours ou des absences de professeurs à destination de l'ensemble des élèves de la classe ne peut pas être regardé comme un traitement de données effectué par une personne physique dans le cadre d'une activité strictement personnelle ou domestique au sens du c) du 2 de l'article 2 du RGPD du 27 avril 2016. S'il comporte des données à caractère personnel (par exemple, le nom des professeurs et la discipline enseignée), un tel traitement est donc soumis aux dispositions du RGPD et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

S'agissant d'un traitement concernant le fonctionnement de l'établissement, seuls les directeurs académiques des services de l'Éducation nationale (DASEN) pour les écoles et les chefs d'établissement pour les collèges et lycées pourraient le mettre en œuvre régulièrement.

Le traitement ne pourrait être mis en œuvre que dans le respect des exigences du RGPD, notamment de son article 5 : finalité déterminée, explicite et légitime, minimisation des données, durée de conservation n'excédant pas celle nécessaire à la finalité du traitement, etc. Il devrait, en outre, faire l'objet d'une inscription sur le registre du responsable de traitement dans les conditions prévues à l'article 30 du RGPD. Les personnes concernées devraient, par ailleurs, être informées des caractéristiques de ce traitement dans les conditions prévues par les articles 13 et 14 du RGPD.

23. Un chef d'établissement peut-il faire une extraction de l'annuaire de son établissement pour fournir aux enseignants la liste des élèves de leurs classes ? Si oui, quelles informations peuvent y figurer?

Un annuaire constitue un traitement de données à caractère personnel placé sous la responsabilité du chef d'établissement s'il est mis en œuvre directement par un établissement public local d'enseignement et doit, à ce titre, faire l'objet d'une inscription au registre des activités de traitement conformément aux dispositions de l'article 30 du RGPD.
Pour que le chef d'établissement puisse transmettre via une extraction de cet annuaire la liste des élèves de leurs classes aux enseignants de l'établissement, il faut que les mentions contenues dans le registre pour l'annuaire considéré le permettent. Autrement dit, il faut que cette finalité (l'extraction de données pour les enseignants) soit compatible avec les finalités de l'annuaire et que les enseignants aient été désignés comme destinataires des données du traitement. Il faut en outre que les personnes dont les données personnelles sont traitées, ou leurs représentants légaux s'il s'agit d'élèves mineurs, aient eu connaissance de la transmission des données les concernant à un nouveau destinataire conformément aux articles 13 et 14 du RGPD.

Il sera enfin rappelé que si les données concernées par la demande d'export sont collectées dans le traitement de données à caractère personnel intitulé « SIÈCLE », il conviendra de se référer aux mentions contenues dans le registre du ministère de l'Éducation nationale.

24. Un directeur d'école ou un chef d'établissement peut-il transmettre l'annuaire de son école ou de son établissement à une municipalité ou une collectivité territoriale ? À une association de parents d'élèves ?

Un annuaire constitue un traitement de données à caractère personnel placé sous la responsabilité du chef d'établissement s'il est mis en œuvre directement par un établissement public local d'enseignement ou du directeur académique des services de l'Éducation nationale (DASEN) pour les traitements de données à caractère personnel mis en œuvre dans les écoles et doit, à ce titre, faire l'objet d'une inscription au registre des activités de traitement conformément aux dispositions de l'article 30 du RGPD.

Pour que le chef d'établissement ou le DASEN puisse transmettre cet annuaire à une collectivité territoriale ou à une association de parents d'élèves, il faut que la fiche registre le permette.

Autrement dit, il faut que cette finalité (l'extraction des données pour des collectivités territoriales ou des associations de parents d'élèves) soit compatible avec les finalités de l'annuaire et que les collectivités territoriales ou les associations de parents d'élèves aient été désignées comme destinataires des données du traitement. Il faut en outre que les personnes dont les données personnelles sont traitées, ou leurs représentants légaux s'il s'agit d'élèves mineurs, aient eu connaissance de la transmission des données les concernant à un nouveau destinataire conformément aux articles 13 et 14 du RGPD.

Il convient toutefois de rappeler que lorsque les données concernées par la demande d'export sont collectées dans les traitements de données à caractère personnel intitulés « ONDE » pour le premier degré ou « SIÈCLE » pour le second degré, il faut se référer aux mentions contenues dans le registre du ministère de l'Éducation nationale.

25. Quelles démarches sont à entreprendre pour être conforme à la loi en cas de mise en œuvre d'une plateforme d'e-learning sur laquelle sont enregistrés les élèves ou les stagiaires de la formation continue [nom, prénom, adresse électronique et les dates et durées de connexions aux cours] pour des raisons d'obligation au titre du financement de la formation et/ou pour le conseil régional, afin de bien prouver la réalité de l'action de formation?

Dès lors qu'elles collectent des données relatives à l'identité des élèves, les plateformes d'e-learning constituent des traitements de données à caractère personnel. Ces traitements doivent, par conséquent, faire l'objet d'un enregistrement sur le registre des activités de traitement par le responsable de traitement, conformément à l'article 30 du RGPD.

Il est utile de rappeler que les traitements ayant pour objet de permettre aux élèves ou aux enseignants d'effectuer des formations en ligne (e-learning) entrent sans aucun doute dans le champ du service public du numérique éducatif défini à l'article L. 131-2 du Code de l'éducation.

Leur mise en œuvre dans les établissements scolaires relève, de ce fait, de l'exécution d'une mission de service public au sens du e) de l'article 6 du RGPD. Le responsable de traitement (DASEN pour le premier degré, chef d'établissement pour le second degré) n'est donc pas tenu de recueillir le consentement des personnes concernées pour pouvoir mettre en œuvre un tel traitement de données à caractère personnel.

Il convient de préciser que dans le cas où la plateforme est gérée par un prestataire de services, celui-ci doit être regardé comme sous-traitant au sens de l'article 28 du RGPD. Un contrat doit donc être conclu entre le responsable de traitement et ce prestataire dans les conditions prévues par l'article 28 du RGPD.

Le responsable de traitement doit, en effet, être en mesure de s'assurer que le sous-traitant présente des garanties suffisantes de manière à ce que le traitement réponde aux exigences du RGPD, notamment en termes de sécurité.

Par ailleurs, les personnes dont les données sont collectées doivent être informées des principales caractéristiques du traitement par le responsable de traitement, aux termes des articles 13 et 14 du RGPD.

Elles doivent ainsi être informées de l'identité et des coordonnées du responsable de traitement, des coordonnées du délégué à la protection des données, des finalités, de la base juridique du traitement, du caractère obligatoire ou facultatif du recueil des données et des conséquences pour la personne en cas de non-fourniture des données, des destinataires, de la durée de conservation des données, du droit des personnes concernées (opposition, accès, rectification, effacement, limitation), du droit d'introduire une réclamation (plainte) auprès de la Commission nationale de l'informatique et des libertés (CNIL).

Le cas échéant, les personnes concernées doivent également être informées de l'existence d'une prise de décision automatisée ou d'un profilage, des informations utiles à la compréhension de l'algorithme et de sa logique, ainsi que des conséquences pour la personne concernée, du droit de retirer son consentement à tout moment, du fait que les données sont requises par la réglementation, par un contrat ou en vue de la conclusion d'un contrat, de la faculté d'accéder aux documents autorisant le transfert de données hors de l'Union européenne (par exemple, les clauses contractuelles types de la Commission européenne).

Enfin, des informations supplémentaires doivent leur être communiquées en cas de collecte indirecte de données, à savoir : les catégories de données recueillies et les sources des données (en indiquant notamment si elles sont issues de sources accessibles au public).

26. Un chef d'établissement peut-il renseigner des régimes alimentaires suivis par les élèves et les professeurs dans une application de gestion de cantine développée par une collectivité territoriale ou une entreprise privée ?

Conformément au c) de l'article 5 du RGPD du 27 avril 2016 et au 3° de l'article 6 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, les données collectées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont collectées (principe de minimisation).
L'indication des régimes alimentaires suivis par les élèves et les professeurs a pour objet de permettre aux responsables des cantines scolaires d'être en mesure de proposer des plats de substitution ou des repas spéciaux.

Un chef d'établissement peut donc renseigner les régimes alimentaires suivis par les élèves et les professeurs dans une application de gestion de la restauration scolaire à la condition qu'aucune donnée relative à la santé ou faisant apparaître l'opinion religieuse ne soit collectée.

En effet, la collecte de telles données, qui sont considérées comme des données sensibles au sens de l'article 9 du RGPD et de l'article 8 de la loi du 6 janvier 1978, pourrait apparaître comme excessive au regard de la finalité du traitement.

Pour que le principe de minimisation des données soit respecté, les mentions relatives au régime alimentaire doivent, par conséquent, être le plus neutre possible.

Par exemple, les mentions « sans porc » ou « sans viande » peuvent être indiquées dans un tel traitement, mais les mentions « halal » ou « casher » ne doivent pas apparaître, dans la mesure où elles révèlent l'appartenance religieuse des intéressés et excèdent ainsi la finalité pour laquelle elles ont été collectées.

De même, les mentions « sans gluten » ou « sans arachides » peuvent être renseignées ; en revanche, les mentions « allergique au gluten » ou « allergique aux

arachides » ne peuvent pas apparaître puisqu'elles constituent des données relatives à la santé qui excèdent la finalité du traitement.

Ces points étaient précisés dans l'ancienne norme simplifiée 58 (NS 58) « Affaires scolaires, périscolaires, extrascolaires et petite enfance » issue de la délibération n° 2015-433 du 10 décembre 2015 portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les collectivités territoriales et les personnes morales de droit public et de droit privé gérant un service public aux fins de gérer les services en matière d'affaires scolaires, périscolaires, extrascolaires et de petite enfance, consultable sur le site de la Commission nationale, de l'informatique et des libertés (CNIL).

Même si cette norme n'a plus de valeur juridique eu égard à la suppression des formalités préalables de déclaration depuis le 25 mai 2018, elle peut utilement servir de cadre pour la mise en œuvre d'un traitement relatif à la restauration scolaire et extrascolaire. En effet, en application des dispositions du a) bis du 2° du I de l'article 11 de la loi du 6 janvier 1978, la CNIL envisage de convertir les anciennes normes simplifiées en référentiels destinés à faciliter la mise en conformité des traitements de données à caractère personnel avec les textes relatifs à la protection des données à caractère personnel.

La NS 58, qui devrait devenir un référentiel, prévoyait notamment que lorsque la prise en charge sanitaire et psychologique du mineur ou du professeur nécessite de collecter des renseignements portant sur les allergies et pathologies, les informations relatives à la santé doivent être fournies de manière facultative et ne peuvent être recueillies qu'après avoir obtenu le consentement exprès de la personne concernée, ou dans le cas d'un élève mineur, celui de son représentant légal.

Comme tout traitement de données à caractère personnel, une application de gestion de cantine qui serait mise en œuvre par un établissement scolaire et non par une collectivité territoriale doit faire l'objet d'une inscription sur le registre des activités de traitement tenu par le responsable de traitement, à savoir le directeur académique des services de l'Éducation nationale (DASEN), agissant sur délégation du recteur d'académie pour les écoles, et le chef d'établissement pour les établissements scolaires.

Les personnes concernées par le traitement doivent en outre être informées des caractéristiques de ce traitement dans les conditions prévues par les articles 13 et 14 du RGPD.

Elles doivent ainsi être informées de l'identité et des coordonnées du responsable de traitement, des coordonnées du délégué à la protection des données, des finalités, de la base juridique du traitement, du caractère obligatoire ou facultatif du recueil des données et des conséquences pour la personne en cas de non-fourniture des données, des destinataires, de la durée de conservation des données, du droit des personnes concernées (opposition, accès, rectification, effacement, limitation), du droit d'introduire une réclamation (plainte) auprès de la CNIL.

Le cas échéant (selon que le consentement est ou non nécessaire à la mise en œuvre du traitement pour certaines données), les personnes concernées doivent également être informées du droit de retirer leur consentement à tout moment.

Enfin, des informations supplémentaires doivent leur être communiquées en cas de collecte indirecte de données, à savoir : les catégories de données recueillies et les sources des données (en indiquant notamment si elles sont issues de sources accessibles au public).

27. Pendant combien de temps un chef d'établissement peut-il conserver des informations contenant des données à caractère personnel ?

L'article 5 du RGPD prévoit que les données à caractère personnel doivent être conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles ces données sont traitées.

La durée de conservation des données à caractère personnel dépend, par conséquent, de la nature des données et des objectifs poursuivis par le traitement. Cette durée de conservation doit donc nécessairement être déterminée dès la conception du traitement par le responsable de traitement, sauf si un texte impose une durée précise.

28. Quels sont les principes à respecter quand on installe un système de vidéoprotection dans un établissement ? La mise en service du système doit-elle uniquement s'opérer lorsque personne n'est censé être présent dans l'établissement?

À titre liminaire, il est utile de rappeler que les formalités à effectuer sont différentes selon que le système de vidéosurveillance est mis en œuvre dans un lieu public ou dans un lieu non ouvert au public.

En effet, les systèmes de vidéosurveillance mis en œuvre dans un lieu public relèvent des dispositions des articles L. 251-1 et suivants du Code de la sécurité publique.

Un établissement scolaire ne peut être regardé comme un lieu ouvert au public au sens de l'article 251-2 du Code de la sécurité intérieure. Par conséquent, un système de vidéosurveillance mis en œuvre à l'intérieur d'un établissement scolaire ne relève pas des dispositions des articles L. 251-1 et suivants du Code de la sécurité intérieure. En revanche, dès lors que le système mis en place permet l'enregistrement d'images permettant l'identification des personnes, il constitue un traitement de données à caractère personnel soumis aux dispositions du RGPD et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Dans les écoles, la décision de mettre en place un système de vidéosurveillance relève du maire de la commune dans laquelle est implanté l'établissement lorsqu'il s'agit de protéger les biens et les locaux, en dehors de la présence des élèves, en application de l'article L. 212-4 du Code des collectivités territoriales selon lequel la commune est propriétaire des locaux des écoles publiques.

Dans l'hypothèse où la vidéosurveillance serait mise en œuvre dans le but d'assurer la sécurité des élèves, la décision est soumise à l'avis du conseil d'école en application du g) du 3° de l'article D. 411-2 du Code de l'éducation. Au regard des dispositions de l'article 4 du décret n° 89-122 du 24 février 1989 relatif aux directeurs d'école qui dispose que « le directeur contribue à la protection des enfants en liaison avec les services compétents », la mise en place d'un tel dispositif paraît relever de la compétence conjointe de l'État, représenté par le directeur académique des services de l'Éducation nationale (DASEN), et de la collectivité locale.

Dans les collèges et les lycées, la décision de mettre en place un tel dispositif relève de la compétence du chef d'établissement après délibération du conseil d'administration en application du c) du 7° de l'article R. 421-20 du Code de l'éducation.

Comme tout traitement de données à caractère personnel, tout système de vidéosurveillance installé dans une école ou un établissement scolaire doit être mis en œuvre dans le respect des exigences des dispositions du RGPD et de la loi du 6 janvier 1978.

Ainsi, avant d'inscrire le traitement sur le registre, dans les conditions prévues à l'article 30 du RGPD, le responsable de traitement doit définir précisément la finalité du traitement, ne collecter que des données pertinentes, adéquates et nécessaires à la sécurité des personnes et des biens, veiller à ce que seules les personnes habilitées aient accès aux données collectées et fixer une durée de conservation de ces données strictement nécessaire à la finalité. Sur ce point, la Commission nationale de l'informatique et des libertés (CNIL) a précisé, dans sa délibération n° 94-056 du 21 juin 1994 portant adoption des recommandations concernant les dispositifs de vidéosurveillance, qu'une conservation des données pendant une durée maximale de quinze jours est suffisante pour assurer la sécurité d'un lieu et qu'il est préférable de paramétrer cette durée dans le système pour donner lieu à un effacement automatique.

Par ailleurs, dans l'hypothèse où le traitement aurait pour objet la surveillance systématique de personnes, notamment de mineurs, il serait soumis à une analyse d'impact relative à la protection des données, en application des dispositions de l'article 35 du RGPD.

Il convient toutefois de préciser que la CNIL juge que des systèmes de vidéosurveillance qui filmeraient en permanence les lieux de vie des établissements (par exemple, cour de récréation, cantines, préaux, jardins, foyers des élèves) constituent une atteinte excessive à la vie privée des personnes. Elle considère en effet que l'utilisation des caméras doit rester limitée, dans la mesure où il existe selon elle des moyens moins intrusifs d'assurer la sécurité des personnes. Elle admet toutefois que des circonstances

exceptionnelles puissent justifier la vidéosurveillance des lieux de vie, notamment les actes de malveillance fréquents et répétés dans ces lieux.

Les personnes concernées doivent être dûment informées des caractéristiques du traitement dans les conditions prévues par les articles 13 et 14 du RGPD.

29. Un établissement peut-il mettre en place un système biométrique pour gérer les entrées et les sorties de l'établissement scolaire ou l'accès à la cantine ?

Par principe, le paragraphe I de l'article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dans sa version issue de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles interdit le traitement des données biométriques aux fins d'identifier une personne physique de manière unique.
Le II du même article prévoit toutefois un certain nombre de dérogations à cette interdiction lorsque la finalité du traitement l'exige, notamment lorsque la personne concernée a donné son consentement exprès.

Avant l'entrée en vigueur du RGPD, le 25 mai 2018, la mise en œuvre de traitements automatisés de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du contour de la main pour accéder aux restaurants scolaires était autorisée sous réserve que ces traitements répondent aux conditions fixées par l'autorisation unique AU-009 issue de la délibération de la CNIL n° 2006-103 du 27 avril 2006 et que le responsable d'un tel traitement adresse à la CNIL un engagement de conformité à cet acte. Cette autorisation unique prévoyait en particulier la possibilité, pour les élèves opposés à l'utilisation du dispositif biométrique, de se voir délivrer un badge ou tout autre moyen d'accès à la cantine.

Depuis l'entrée en vigueur du RGPD, cette autorisation unique n'a plus de valeur juridique.

Nouveaux traitements mettant en place un système biométrique d'accès : les traitements qui mettent en place un système biométrique pour gérer l'accès des élèves à la cantine doivent être fondés sur le consentement préalable des personnes concernées. Il conviendra toutefois de veiller à ce que la mise en place de tels dispositifs ne conduise pas à exclure de la cantine les élèves dont les responsables n'auraient pas donné leur consentement à la mise en œuvre du traitement et donc de garantir une possibilité d'accès alternative au service de restauration scolaire (par la délivrance d'un badge, par exemple, ou tout autre système d'accès).

Ensuite, dans la mesure où la mise en place d'un système biométrique pour gérer les entrées et les sorties de l'établissement ou l'accès à la cantine nécessite la collecte de données particulières, au sens de l'article 9 du RGPD, relatives à des mineurs, il doit être considéré comme susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Par conséquent, conformément à l'article 35 du RGPD, le responsable de traitement doit effectuer, avant la mise en œuvre du traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

Systèmes de biométrie mis en œuvre avant le 25 mai 2018, date d'entrée en vigueur du RGPD, pour gérer les accès : s'agissant enfin des systèmes de biométrie gérant les accès à l'établissement ou à la cantine mis en œuvre avant l'entrée en vigueur du RGPD, il est nécessaire de recueillir dans les meilleurs délais le consentement des personnes concernées. En cas d'opposition à l'utilisation du dispositif biométrique, les élèves concernés pourront utiliser les modalités alternatives d'accès, d'ores et déjà mises en œuvre, en application de l'autorisation unique AU-009.
Pour ces traitements en cours, qui ont déjà fait l'objet d'un contrôle a priori et donc d'une formalité préalable avant le 25 mai 2018 (autorisation, déclaration avec délivrance d'un récépissé, ou engagement de conformité à une autorisation unique ou norme simplifiée), aucune analyse d'impact relative à la protection des données n'est en revanche exigée dans l'immédiat. Toutefois, il appartient aux responsables de traitement, au terme d'une évaluation du risque, de procéder à une telle analyse d'impact dans un délai de trois ans à compter du 25 mai 2018.
Enfin, en cas de modification substantielle du traitement, l'analyse d'impact devra être effectuée avant la mise en œuvre de la modification dans tous les cas où elle apparaît nécessaire, sans qu'il y ait lieu de distinguer selon que cette nécessité découle de la modification ou des caractéristiques du traitement préexistant.

30. Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, que doit faire le chef d'établissement?

La violation de données se caractérise principalement par la perte de disponibilité, d'intégrité ou de confidentialité de données personnelles, de manière accidentelle ou illicite.

L'article 33 du RGPD impose au responsable de traitement, en l'espèce le chef d'établissement, de notifier à l'autorité de contrôle (la Commission nationale de l'informatique et des libertés – CNIL – en France) dans les meilleurs délais et, si possible au plus tard 72 heures après en avoir pris connaissance, les violations présentant un risque pour les droits et libertés des personnes.

Cette notification doit comporter les éléments suivants :
– une description de la nature de la violation de données à caractère personnel y compris, si possible, des catégories et du nombre approximatif de personnes concernées par la violation de leurs données personnelles, et des catégories et du nombre approximatif de données à caractère personnel concernées ;
– le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
– une description des conséquences probables de la violation de données à caractère personnel ;
– une description des mesures prises ou que le responsable de traitement propose de prendre pour remédier à la violation des données à caractère personnel, y compris, le cas échéant, des mesures pour en atténuer les éventuelles conséquences négatives.

L'article 34 du RGPD prévoit en outre que lorsque la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable de traitement notifie également à la personne concernée, dans les meilleurs délais, la violation de données à caractère personnel.

La communication à la personne concernée doit décrire, en des termes clairs et simples, la nature de la violation des données, ses conséquences probables et les mesures prises ou que le responsable de traitement propose de prendre pour y remédier. Elle doit également contenir le nom et les coordonnées du délégué à la protection des données.

Il convient de signaler que la communication à la personne concernée n'est toutefois pas nécessaire si le responsable de traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et que ces mesures ont été appliquées aux données personnelles affectées par la violation.

De la même manière, cette communication n'est pas exigée si le responsable de traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes physiques concernées n'est plus susceptible de se matérialiser.

Enfin, si cette communication exige des efforts disproportionnés, il pourra être procédé à une communication publique ou à une mesure similaire permettant aux personnes physiques concernées d'être informées de manière tout aussi efficace.

Dans tous les cas, lorsqu'une violation de données à caractère personnel a lieu, le responsable de traitement doit indiquer précisément en quoi a consisté l'incident en décrivant ses circonstances, ses effets et les mesures prises pour y remédier.

Il doit enfin être rappelé que le sous-traitant a l'obligation de notifier au responsable de traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

31. Quelles informations le chef d'établissement doit-il donner aux membres de son conseil d'administration ?

Le 2° de l'article R. 421-23 du Code de l'éducation prévoit que le conseil d'administration, sur saisine du chef d'établissement, donne son avis sur les principes de choix des manuels scolaires, des logiciels et des outils pédagogiques.

L'avant-dernier alinéa du même article prévoit par ailleurs que le chef d'établissement peut consulter le conseil d'administration sur les questions ayant trait au fonctionnement administratif général de l'établissement.

Par conséquent, le chef d'établissement doit consulter le conseil d'administration préalablement à la mise en œuvre d'un logiciel ou d'un outil pédagogique et peut le consulter sur tout projet de traitement de données à caractère personnel ayant pour finalité le fonctionnement général de l'établissement.

Pour que le conseil d'administration puisse se prononcer en toute connaissance de cause, il paraît opportun que le chef d'établissement lui présente toutes les caractéristiques du traitement qu'il souhaite mettre en œuvre. Il peut ainsi utilement donner aux membres du conseil toutes les informations qui doivent figurer dans le registre des activités de traitement en application de l'article 30 du RGPD.

QUESTIONS RELATIVES AUX RELATIONS AVEC LES REPRÉSENTANTS LÉGAUX DES ÉLÈVES

32. Des parents ne souhaitent pas que soit utilisé le livret scolaire unique numérique pour leur enfant. Peuvent-ils le refuser ?

L'exercice du droit d'opposition est strictement encadré par le RGPD et par la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

En effet, l'article 21 du RGPD prévoit que la personne dont les données sont collectées a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement de données à caractère personnel la concernant nécessaire à l'exécution d'une mission d'intérêt public. Dans ces conditions, le responsable de traitement ne traite plus les données à caractère personnel, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne dont les données sont collectées.

Il résulte de ces dispositions du RGPD que si les parents de l'élève dont les données personnelles sont traitées dans le livret scolaire unique numérique entendent s'opposer à ce traitement, ils ne peuvent le faire qu'à la condition d'exposer des raisons tenant à leur situation particulière, ce qui exclut des raisons tenant à des considérations d'ordre général.

Dans une telle hypothèse, il appartiendra alors au responsable de traitement, en l'espèce le ministère de l'Éducation nationale pour le livret scolaire unique numérique, de démontrer qu'il existe des motifs légitimes et impérieux à traiter les données de leur enfant dans le livret scolaire unique numérique.

33. Un représentant légal d'un élève peut-il demander qu'un service numérique privé ne soit pas utilisé par un enseignant ?

Dès lors qu'un service numérique utilisé par un enseignant est mis en œuvre sur le fondement du e) du 1 de l'article 6 du RGPD (traitement nécessaire à l'exécution d'une mission d'intérêt public), le représentant de l'élève a le droit de s'opposer à tout moment à ce traitement de données à caractère personnel, en application des dispositions du 1 de l'article 21 du RGPD, pour des raisons tenant à sa situation particulière, c'est-à-dire pour des raisons tenant à la situation personnelle de l'élève ou de ses responsables, ce qui exclut les oppositions de principe à la mise en œuvre d'un traitement de données. Une demande non motivée au regard de la situation particulière de l'intéressé peut donc être rejetée.

En revanche, dans l'hypothèse où la personne concernée a suffisamment motivé sa demande au regard de sa situation personnelle, il appartient au responsable de traitement, pour pouvoir continuer à traiter les données, de démontrer qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée.

Par ailleurs, lorsque le service numérique n'est pas nécessaire à l'exécution d'une mission de service publique, sa mise en œuvre nécessite le recueil du consentement des responsables des élèves ou des élèves s'ils sont majeurs.

Dans cette hypothèse, le responsable de l'élève pourra refuser de donner son consentement ou le retirer à tout moment.

34. Un représentant légal d'un élève peut-il demander à disposer des données à caractère personnel recueillies par l'établissement scolaire ?

L'exercice du droit d'accès prévu à l'article 39 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés permet à

toute personne physique de savoir si des données la concernant sont traitées et d'en obtenir la communication dans un format compréhensible. Il permet également de contrôler l'exactitude des données et, au besoin, de les faire rectifier ou effacer.

La délivrance d'une copie des données détenues par le responsable de traitement sur une personne physique constitue ainsi une modalité d'exercice de ce droit d'accès.

En l'espèce, le responsable de traitement, ou le service auprès duquel s'exerce le droit d'accès, doit ainsi être en mesure de faire parvenir à l'élève concerné, ou à son représentant légal s'il est mineur, une copie des données qu'il détient sur lui et de le renseigner sur :
– les finalités d'utilisation de ces données ;
– les catégories de données collectées ;
– les destinataires ou catégories de destinataires qui ont pu accéder à ces données ;
– la durée de conservation des données ou les critères qui déterminent cette durée ;
– l'existence des autres droits (droit de rectification, d'effacement, de limitation, d'opposition) ;
– la possibilité de saisir la Commission nationale de l'informatique et des libertés (CNIL) ;
– toute information relative à la source des données collectées si celles-ci n'ont pas directement été collectées auprès de l'intéressé ;
– l'existence d'une prise de décision automatisée, y compris en cas de profilage, et la logique sous-jacente, l'importance et les conséquences pour la personne d'une telle décision ;
– l'éventuel transfert des données vers un pays tiers (non-membre de l'Union européenne) ou vers une organisation internationale.

Cette demande de droit d'accès peut s'exercer par divers moyens (voie électronique ou courrier) et doit être accompagnée de tout document permettant de prouver l'identité du demandeur. Lorsque le responsable de traitement ou le sous-traitant a des doutes raisonnables quant à l'identité de cette personne, il peut toutefois demander des informations supplémentaires sur l'identité du demandeur, y compris, lorsque la situation l'exige, la photocopie d'un titre d'identité portant la signature du titulaire.

35. Quand un établissement souhaite mettre en place, directement ou via une prestation, un système d'information traitant des données à caractère personnel, quelles sont les mesures de sécurité à mettre en place ?

Les mesures de sécurité doivent, au possible, être identifiées en amont des projets (*security by design*), elles peuvent être techniques, organisationnelles ou portant sur la sensibilisation des différents acteurs du système (chef de projet, développeurs, utilisateurs, gestionnaire…). La Commission nationale de l'informatique et des libertés (CNIL) met à disposition un guide de la sécurité des données personnelles détaillant les différentes mesures dans des fiches thématiques. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) propose un ensemble de documentations et de ressources plus opérationnelles pour accompagner la sécurisation des systèmes.

—

Guide de la CNIL : www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles

Ressources ANSSI : www.ssi.gouv.fr/administration/reglementation/rgpd-renforcer-la-securite-des-donnees-a-caractere-personnel/

Exemple de registre de traitement

Description du traitement	
Nom / sigle	
N° / Réf	
Réf CNIL	
Date de création	
Mise à jour	

Acteurs	Nom	Adresse	CP	Ville	Pays	Tél
Maîtrise d'ouvrage						
Délégué à la protection des données						
Représentant						
Responsable(s) conjoint(s)						

Finalité(s) du traitement effectué	
Finalité	
Finalité statistique (OUI / NON)	

Mesures de sécurité	
Mesures de sécurité techniques	
Mesures de sécurité organisationnelles	

Personnes concernées	Liste ou catégories de données traitées Y compris données de connexion (adress IP, logs, etc.)	Destinataires	Délai d'effacement
Personne 1			
Personne 2			

Destinataires	Description	Type de destinataires	
Destinataire 1			
Destinataire 2			

Transferts hors UE	Destinataire	Pays	Type de garanties	Lien vers le document
Organisme 1				
Organisme 2				

Sites et documents officiels

Le RGPD sur le site de la CNIL
www.cnil.fr/fr/reglement-europeen-protection-donnees

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, version consolidée le 12 septembre 2018
www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460

Pour accompagner la rentrée scolaire des parents et des chefs d'établissement
www.cnil.fr/fr/rentree-scolaire-ce-que-les-etablissements-scolaires-et-periscolaires-peuvent-vous-demander

Braun Gilles et Merriaux Jean-Marc (dir.), « Données numériques à caractère personnel au sein de l'Éducation nationale », rapport de l'inspection générale, 2018.
www.ladocumentationfrancaise.fr/var/storage/rapports-publics/184000536.pdf

Bibliographie

Abiteboul Serge et Peugeot Valérie, *Terra Data : qu'allons-nous faire des données numériques ?*, Paris, Éditions le Pommier/Cité des sciences et de l'industrie, 2017.

Agacinski Daniel, Brun Félix, Isart Céline *et al.*, « L'école sous algorithmes », 2016. En ligne :
http://tnova.fr/etudes/l-ecole-sous-algorithmes

Cardon Dominique, *À quoi rêvent les algorithmes : nos vies à l'heure des big data,* Paris, Seuil/La République des idées, 2015.

Piolle Guillaume, « La protection des données personnelles vue par un informaticien », 2015. En ligne : http://guillaume.piolle.fr/doc/Piolle15a.pdf

Audiovisuel

Bernet David, *Democracy, la ruée vers les datas*, documentaire, Arte, 2016.
En ligne : www.edutheque.fr

Parcours M@gistère

« Les données à caractère personnel au cœur des établissements »

m@gistère

Le nouveau cadre juridique concernant la protection des données à caractère personnel impose, depuis l'entrée en vigueur du RGPD le 25 mai 2018, aux responsables de traitement, que sont les chefs d'établissement dans le 2nd degré et les DASEN dans le 1er degré, de prendre des mesures pour s'assurer d'être en conformité avec la législation. Il s'agit notamment de mettre à disposition des élèves, de leurs représentants légaux et du personnel, l'ensemble des traitements de données.

Ce parcours M@gistère, en autoformation d'une durée de 3 heures, a été conçu précisément pour les responsables de traitement. Il présente le nouveau cadre législatif et ses évolutions, les mesures à prendre pour être conforme et des pistes d'actions à destination de l'ensemble de la communauté éducative.

magistere.education.fr

La mallette des parents

Les données scolaires sont placées au cœur de la stratégie numérique du ministère de l'Éducation nationale qui doit impérativement s'assurer que les flux, les traitements et l'hébergement de ces données scolaires respectent la vie privée des élèves et de leur famille, mais aussi des enseignants et des autres personnels.

Le sujet est sensible, d'où la nécessité de donner un cadre de confiance clair et partagé par toute la communauté éducative.

Le nouveau site de « La mallette des parents » est dédié aux parents et aux professionnels de l'éducation.

– La fiche « **La protection des données des enfants** », accessible depuis « l'espace parents », présente le nouveau cadre juridique et le traitement des données scolaires. Elle est complétée par une infographie.
https://mallettedesparents.education.gouv.fr/fr/parents/ID251/la-protection-des-donnees-des-enfants

– La fiche « **La protection des données personnelles à l'école** », accessible dans « l'espace professionnel », donne des éléments de communication aux chefs d'établissement pour aborder la question des données à caractère personnel avec les familles, mais aussi avec les équipes éducatives. Une infographie vient là aussi compléter la page dédiée.
https://mallettedesparents.education.gouv.fr/fr/professionnels/ID208/la-protection-des-donnees-personnelles-a-l-ecole

NOTES

En complément du présent manuel, accédez gratuitement aux contenus du dossier en ligne sur www.reseau-canope.fr/notice/les-donnees-a-caractere-personnel :

- les réponses pratiques aux questions d'ordre administratif ou pédagogique auxquelles les responsables de traitement peuvent être confrontées ;
- le documentaire de David Bernet, *Democracy, la ruée vers les datas* (Arte, 2016, 100 min) disponible sur le portail Éduthèque sur simple identification ;
- la version téléchargeable de ce manuel.

Imprimé par mcc graphics
Dépôt légal : septembre 2018

ÉCLAIRER

Pour décrypter
l'essentiel

ISSN 2426-0207
ISBN 978-2-240-04895-0
Réf. W0013059
Gratuit