Fiche de synthèse concernant les questions de conformité au RGPD

Source : François BOCQUET - Chef de projet Veille et Prospective - Bureau du soutien à l'innovation et à la recherche - Sous-direction de la transformation numérique - Direction du Numérique pour l'Éducation au Ministère de l'Éducation Nationale

Tél. : +33 155 557 781 ou +33 6 35 48 21 13 - Bureau 116A au 107 rue de Grenelle à Paris

Mèl. : francois.bocquet@education.gouv.fr - Portfolio : http://fr.linkedin.com/in/fbocquet/

Les paragraphes qui suivent rappellent les points essentiels quels que soient les traitements réalisés dès lors qu'il s'agit de traitements de données à caractère personnel.

1. Un rappel de ce qu'est une donnée à caractère personnel (DCP)

Toute information se rapportant à une personne physique identifiable de façon directe ou indirecte.

C'est-à-dire non seulement les données identifiantes de type nom prénom ou adresse mail ou encore adresse postale ou IP du domicile, mais bien toutes les données en relation avec une personne physique comme un pseudonyme, des notes ou des appréciations, une production pédagogique, etc.

2. L'application du RGPD

Le RGPD s'applique dés lors qu'il y a un traitement numérique ou analogique (sur papier) réalisé dans un cadre professionnel. Il n'y a pas d'usage personnel en contexte professionnel.

Donc même la création d'un compte pour un service par un enseignant ou un ERUN ne peut en aucun cas être considéré comme personnel si ce compte a une finalité professionnelle (se former, produire des documents, tenir des listes, publier un site web, un blog ou un wiki, etc…).

Les prénoms et noms des professionnels exerçant dans notre institution, par exemple, et toutes données les concernant (enseignants, formateurs, etc.) sont-ils des données personnelles à "protéger" ?

En fait, toute donnée à caractère personnel (DCP) fait l'objet du même niveau d'exigence de protection que le traitement soit numérique ou analogique (sur papier). Cela concerne les enseignants et les adultes comme les élèves que ce soit pour des données à caractère personnel « normales » ou « sensibles ». Le RGPD prend en compte l'analyse de risque ainsi que des critères qui peuvent justifier des analyses d'impacts sur la protection des données (AIPD).

En synthèse rapide lire : https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd

Le traitement relatif à des personnes vulnérables (les mineurs) et à des grandes échelles (tous les élèves d'une commune ou tous les enseignants d'une circonscription) sont des critères de vigilance accrue.

Les traitements concernant les élèves sont bien sûr à gérer avec encore plus de prudence (augmentation du risque par le fait qu'il s'agit de mineurs et par le fait que les responsables légaux peuvent demander des comptes au responsable de traitement, au DPD qu'il a désigné, à la CNIL voir à la justice…).

3. Les traitements

Depuis le 25 mai 2018, seuls les traitements inscrits au registre du responsable de traitement (DASEN) peuvent être mis en œuvre.

Par exemple, un service monté sur son serveur perso ne peut être conforme, pas plus qu'un service proposé par un éditeur commercial ou une association qui n'aurait pas signé un contrat de sous-traitance au sens de l'article 28 du RGPD.

À titre d'exemple, les services Framasoft ne sont pas utilisables car il est impossible pour le responsable de traitement d'obtenir un contrat de sous-traitance au titre de l'article 28.

La maîtrise des données professionnelles nécessite également de ne pas manipuler nos données avec n'importe quel outil non maîtrisé et validé par l'institution.

Dans la jungle Internet et logicielle, il est de plus en plus complexe de distinguer les outils et sites "safe" en terme de respect des données que l'on peut être amené à y déposer plus ou moins volontairement de ceux qui ne le sont pas, tout ce qui est gratuit cachant quasi fatalement un modèle économique non neutre.

Rappelons encore que les outils et surtout les services (outils mis en œuvre par quelqu'un quelque part) doivent impérativement faire l'objet d'une fiche de traitement sur le registre du responsable de traitement.

Tout traitement mis en œuvre est bien illégal s'il n'est pas porté au registre et ce n'est pas qu'une question d'information du responsable de traitement mais bien une responsabilité administrative et pénale du responsable de traitement. Si un traitement est mis en œuvre par une équipe dans un département ou une académie, on peut raisonnablement penser qu'il a fait l'objet d'une inscription au registre, mais il vaut mieux le vérifier de toute façon.

4. L'utilisation de services

Seuls les services proposés par le ministère, un rectorat ou une DSDEN peuvent être utilisés car, a priori, déjà porté au registre de leur responsable de traitement, sous réserve de vérifierqu'ils sont bien au registre, surtout si ce sont des services proposés par des prestataires privés (associations ou entreprises) ou par une collectivité (si accord de sous-traitance ou accord de responsabilité conjointe).

5. Le responsable de traitement

Attention de ne pas confondre le nom d'un logiciel (Sphinx ou LimeSurvey par exemple) et celui d'un service mis en œuvre :

Par qui est-il exploité ? Par l'académie ? Par un tiers ? Dans ce dernier cas, est-ce un éditeur ou un opérateur du Ministère (comme le CNED, l'Onisep, Canopé, …) ?

L'éditeur du logiciel n'est pas responsable du traitement alors que l'éditeur du service (celui qui met en œuvre le logiciel pour rendre un service) est obligatoirement soit responsable de traitement (c'est le cas de Framasoft) soit sous-traitant (c'est le cas de Canopé avec la Quizinière normalement).

Pour être plus clair, le logiciel utilisé par Framaform n'est pas utilisable s'il est hébergé par Framasoft ou n'importe quel « chaton » ou encore si vous l'installez sur votre serveur personnel.

Il peut être conforme s'il est exploité par un service académique ou par un éditeur de service (association ou entreprise) acceptant de signer un accord de sous-traitance.

6. Le registre de traitement

Le seul bon réflexe à avoir est de consulter le registre des traitements et des sous-traitants de votre responsable de traitement en y cherchant le traitement dont vous avez besoin.

Vous pouvez également rechercher sa disponibilité en montant d'un cran (service académique) ou de deux (service national).

S'il n'y est pas, vous pouvez seulement recommander à votre responsable du traitement (via l'IEN de votre département en charge du Numérique) de faire appel à tel ou tel sous-traitant ou de mettre en exploitation tel ou tel logiciel par les services de l'académie ou de la collectivité.

Mais tant que ce nouveau traitement n'est pas inscrit au registre et que les mesures d'informations des personnes concernées ne sont pas disponibles, toute mise en œuvre reste illégale au regard du RGPD.

7. Les services et applications gratuites

Pour ce qui est du gratuit il est nécessaire d'avoir une analyse un peu plus nuancée et bien repérer le modèle mis en œuvre.

- Le gratuit payé par l'impôt : fonction publique, subventions publiques, avec service internalisé (sur les serveurs d'un rectorat) ou externalisé (ENT).
- Le gratuit financé par des dons d'argent (Wikipedia ou Framasoft).
- Le gratuit financé par des dons de temps et du bénévolat réellement désintéressé (en dehors du fait d'aider ou de faire connaître telle ou telle idée militante).
- Le gratuit financé par un pied dans la porte à court terme (modèle freemium du type Beneylu ou Mathador visant à transformer un pourcentage d'utilisateurs gratuits en utilisateurs payants ou encore modèle avec services associés du type Toutemonannée.com avec transformation sur l'édition d'albums de photos de classe).

  Le service gratuit ne fait qu'une publicité parfois discrète pour son modèle payant.
- Le gratuit financé par un pied dans la porte à long terme, c'est-à-dire sans recherche immédiate de nouveaux clients payants, mais surtout pour occuper la place vis-à-vis des concurrents en activité sur le même secteur et proposant le même service (Google Workpace Education et Microsoft Office 365 Education sont sur ce modèle ou encore SAP et CEGID pour les ERP ou Cathia de Dassault pour la CAO).

  On peut dire que c'est du « mécénat intéressé » ou de la « responsabilité sociale d'entreprise ». Ça n'est possible que si l'assise principale du modèle économique est déjà financée par des contrats solvables par ailleurs (dans l'industrie en particulier).
- Le gratuit financé par la réutilisation (sans revente) des données à des fins publicitaires, soit sur le service lui-même (affichage de publicité dans le service), soit via des régies publicitaires tierces. Dans ce cas seuls les emplacements sont vendus aux enchères sans revente des données elles-mêmes.
- Enfin le gratuit financé par la revente des jeux de données (le plus bas niveau de modèle économique qui génère par exemple les spams).

Seul le gratuit des deux dernières catégories, i.e. avec réutilisation des données pour une autre finalité que pour rendre le service lui-même, posent un problème rédhibitoire.

Ce qui signifie que tout service proposant des bandeaux de pub ou des cookies en relation avec des régies publicitaires devrait être banni des usages (infraction au code de l'éducation sur la neutralité commerciale).

Par ailleurs, les modèles de convention de sous-traitance de type article 28 du RGPD interdisent normalement la réutilisation des données pour des finalités autres que celles du service.

8. Cas pratiques

Des parents d'élèves filment la fête de fin d'année scolaire

Le directeur ou les enseignants ne peuvent autoriser ou interdire que pour ce qui est fait au sein de l'école par eux-mêmes. Par exemple, filmer les activités de la classe.

Pour toute autre situation, notamment spectacle d'école, sortie scolaire, etc., ils ne peuvent et ne doivent se borner qu'à rappeler les règles. Ils n'ont aucun pouvoir de police et de contrôle, et tenter de le faire les mettrai en situation bien fâcheuse.

C'est à la personne à qui une prise de vue déplaira d'engager les démarches pour faire appliquer le droit.

Les règlements mis en jeu ici sont :

- ✔ la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, telle que modifiée le 1er juin 2019, le cas échéant mise à jour ;
- ✔ le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données abrogeant la directive 95/46/CE.

Ceux-ci sont très simples et précisent les bénéfices que chacun peut en attendre.

- ➢ Les droits pour contrôler l'usage qui est fait de ses données personnelles.

  Chacun peut notamment demander à accéder aux données le concernant, les faire rectifier, modifier, supprimer (à exercer auprès du DPD académique).

- ➢ Le droit de retrait à exercer à tout moment de ces vidéos ou de ces photographies si on le juge utile.

  Concernant un reportage presse ou réalisé par un tiers, la demande est à adresser directement au média / à la personne physique ou morale responsable de la publication.

  Si cette démarche reste sans réponse dans un délai de 1 mois ou en cas de réponse insatisfaisante, on peut alors saisir la CNIL.

La réglementation est faite pour protéger les personnes, pas pour dissuader.