UN CADRE POSSIBLE POUR LA MISE EN ŒUVRE DE SUITES COLLABORATIVES FOR EDUCATION OU D'UN SERVICE NUMÉRIQUE

Les éditeurs internationaux du numérique multiplient les offres destinées aux professeurs ou aux élèves afin de s'intégrer au milieu de l'éducation. L'ensemble des services proposés constitue une offre spécifique dite *for education*.

La satisfaction des besoins de la communauté scolaire, à travers la solution numérique retenue, ne doit pas occulter l'exigence de confiance que l'établissement est en droit d'attendre de l'éditeur, dans le cadre d'un engagement réciproque respectueux de la protection des données personnelles et des libertés individuelles.

Pour mémoire, chaque responsable de traitement détermine les finalités du traitement, les exigences de sécurité, la durée de conservation et les destinataires des données à caractère personnel et choisit ses sous-traitants avec lesquels il contractualise ses exigences conformément au **Règlement Général sur la Protection des Données (RGPD)**.

Ainsi, il lui appartient d'autoriser l'usage de services issus de la société de l'information, pour peu qu'ils soient proposés par des éditeurs, agissant en tant que sous-traitants, et notamment ceux qui proposent une offre spécifique pour l'éducation (Google, Microsoft, Apple, etc.).

Bien conscient de la difficulté pour le responsable de traitement d'apprécier les garanties de chacune des offres, les **délégués à la protection des données (DPD)** de la région académique Auvergne-Rhône-Alpes proposent dans cette publication de leur rappeler les fondamentaux de la protection des données personnelles et attirent leur attention sur les risques qui naissent du choix de recourir à ces solutions.

Afin de protéger chaque responsable de traitement les DPD énumèrent les précautions (valant obligations) et les recommandations réduisant les risques qui pèsent sur lui ou les personnes concernées par les traitements.

académies
Clermont-Ferrand
Grenoble
Lyon

RÉGION ACADÉMIQUE
AUVERGNE-RHÔNE-ALPES

MINISTÈRE
DE L'ÉDUCATION NATIONALE
MINISTÈRE
DE L'ENSEIGNEMENT SUPÉRIEUR,
DE LA RECHERCHE
ET DE L'INNOVATION

Délégué à la protection des données

Délégués à la protection des données de la région académique Auvergne Rhône Alpes

Académies de Clermont-Ferrand, Grenoble et Lyon - Juin 2020

Les risques

Le choix de mise en œuvre d'une offre de services telle qu'une suite collaborative, implique d'équilibrer et de concilier des facteurs comme la productivité des personnels et le cas échéant des élèves, l'efficacité administrative et pédagogique, la conformité, la sécurité, les coûts, etc. Ces préoccupations se sont accrues ces dernières années avec les risques, avérés et croissants, engendrant indisponibilité des services (verrouillage technologique ou de données) et atteintes à la confidentialité..

Risques pour le responsable de traitement

- **Continuité de service**
  - Contrat unilatéral et déséquilibré par lequel le responsable de traitement perd la maîtrise de ses données ;
  - Risque de non-réversibilité, c'est à dire ne pas pouvoir récupérer les données confiées ;
  - Absence de pérennité de l'offre qui peut, notamment, être disponible gratuitement aujourd'hui et proposée à titre onéreux demain ;
  - Possibilité de devoir essuyer un refus légitime d'usage par une personne concernée.
- **Révision du modèle économique**
  - Évolution des conditions de licences, comme la perte de la gratuité ;
  - Révision des garanties et des conditions d'usage sans accord préalable du responsable de traitement.
- **Risque juridique**
  - Manque à l'obligation juridique d'un contrat en bonne et due forme entre les parties ;
  - Signature d'un contrat par une personne non habilitée ;
  - Volatilité des termes d'un contrat d'adhésion (dont les termes sont ajustés régulièrement et unilatéralement par l'éditeur).

- **Risque technique**
  - Incapacité pour le responsable de traitement d'auditer la solution ;
  - Défaut d'administration technique et organisationnelle des services par bridage contractuel des fonctionnalités et manque d'expertise et de moyens humains alloués à cette mission.
- **Risque de non-conformité au RGPD**
  - Difficulté à obtenir les informations de l'offre nécessaires à l'établissement de la fiche de traitement ;
  - Dans le cas d'échanges de données transfrontaliers, risque d'hébergement des données et de leurs sauvegardes en dehors de l'Union européenne ou d'accès des données à des personnes non habilitées par l'effet de loi extra territoriale (*cloud act, patriot act* votés aux USA) ;
  - Difficulté à être informé dans les meilleurs délais par le fournisseur de services de tout évènement considéré comme une violation de données : atteinte en disponibilité (déni de service), intégrité (attaques virales, *ransomware*), confidentialité (fuite / exfiltration de données, consultation par un tiers non autorisé), etc. ;
  - Exploitation des données par le fournisseur de services pour d'autres finalités que celles fixées par le responsable de traitement.
- **Risque d'atteinte à la réputation et/ou de sanctions administratives et pénales**
  - En cas de manquements, perte de confiance de la communauté éducative vis-à-vis de l'établissement ;
  - Exposition aux plaintes des personnes concernées ou à leur représentant (action de groupe).

Risques pour les personnes concernées

- **Droit des personnes**
  - Manque de transparence du traitement ;
  - Réutilisation éventuelle des données pour d'autres fins que celles prévues ;
  - Difficulté à faire valoir ses droits (droit d'accès, de modification, d'effacement, ...).
- **Qualité des personnes**
  - Offre potentiellement inadaptée aux personnes vulnérables (mineurs numériques de moins de quinze ans, mineurs, salariés).
- **Violation de données**
  - Évaluation difficile du préjudice subit ;
  - Complexité voire incapacité à faire valoir ses droits notamment pour les traitements hors UE.

Fort de ce constat, il revient au responsable de traitement l'obligation de prendre les mesures techniques et organisationnelles nécessaires, pour diminuer autant que possible le niveau de risque à l'égard des droits, des libertés et des données personnelles des utilisateurs de chaque solution numérique.

Conseils

Conseils circonstanciés

- S'assurer de pouvoir évaluer les limites de responsabilité de chacun des services intégrés à l'offre ;
- Évaluer l'impact de la politique en nuage ("cloud") retenue en fonction de la sensibilité des données à stocker ;
- Veiller à obtenir les garanties d'un stockage des données dans les pays de l'Union européenne ;
- Se donner les moyens d'assurer l'administration des services souscrits ;
- Prévoir la formation des usagers aux règles de sécurité des services, à la politique de protection des données et aux règles de partage ;
- S'assurer de la conformité au RGPD en matière de politique de confidentialité des données notamment en satisfaisant aux obligations qui incombent au responsable de traitement.

Obligations du responsable de traitement

- Pour les établissements scolaires, recueillir l'avis du conseil d'administration et conseil d'école pour le recours aux services et acter la décision d'emploi ;
- Etablir et mettre à disposition des usagers les mentions légales d'information sous une forme concise et compréhensible, et le cas échéant, obtenir leur consentement ;
- Ne pas se contenter de valider les conditions générales d'utilisation (CGU) mais établir un contrat en bonne et due forme ;
- Identifier et choisir les options du contrat qui permettent de répondre à ses obligations comme :
  - Prévoir qu'en cas de conflit, la législation européenne prend le dessus sur la législation non européenne ;
  - Garantir l'hébergement/stockage des données dans les pays de l'UE ou à défaut, faire valoir obligatoirement les clauses contractuelles types de l'Union européenne ;
  - Établir la liste des services applicatifs inclus avec la description des responsabilités de chaque partie pour chacune des application (datée) ;
  - S'assurer que le responsable de traitement peut gérer la suppression des données chez l'hébergeur, etc.
- Amender la charte numérique de l'établissement annexée au règlement Intérieur (nécessaire à son opposabilité) en intégrant le recours à ces suites collaboratives et prévoir un processus permettant de s'assurer que les utilisateurs ont bien lu et accepté cette charte ;
- Exiger une gestion des accès à partir de comptes nominatifs avec identifiants et mots de passe individuels ;
- Documenter les traitements de données et maintenir à jour le registre de traitements de l'établissement.

En cas de négociations bilatérales possibles avec le fournisseur de services, faire valoir les clauses de sécurité de la **direction des achats de l'État** dans les marchés publics nécessaires pour la conclusion d'un marché relatif à la mise en place de sauvegardes externalisées.

Position des délégués à la protection des données

La communauté des DPD n'est, ni à même de juger du bien-fondé du choix du service retenu, ni habilitée à le certifier conforme au RGPD, notamment en raison de la libre concurrence qui doit s'exercer sur ce marché. Le rôle des DPD auprès du responsable de traitement est avant tout un rôle de conseil pour porter à sa connaissance les risques auxquels il s'expose, afin qu'il puisse prendre une décision éclairée dans le respect de la nécessaire protection des données personnelles qui lui sont confiées.

Par exemple, l'utilisation de solutions proposées par des entreprises non-européennes, du type for education, n'est pas interdite par le RGPD mais nécessite de s'assurer de garanties adéquates.

Face aux différents risques exposés, il s'agit de donner au responsable de traitement les moyens de les prendre en compte pour les réduire au mieux tout en s'acquittant de l'ensemble des obligations qui lui incombent.