RAPPELS SUR LA MISE EN ŒUVRE DES OUTILS COLLABORATIFS (VISIOCONFERENCE, MESSAGERIE, ETC.) DANS L'ESR

À RETENIR

En période de plan de continuité d'activité, et considérant les risques induits par la dématérialisation rapide des procédures réalisées pour assurer la continuité pédagogique des établissements, il importe de rappeler certains fondamentaux quant à la protection des données dans l'enseignement supérieur et la recherche :

- les traitements relatifs aux outils collaboratifs sont **mis en œuvre par l'établissement**, qualifié de responsable de traitement au sens du Règlement général sur la protection des données (RGPD) ;
- l'utilisation de solutions proposées par des **entreprises non-européennes n'est pas interdit** par le RGPD ;
- le choix de l'outil doit être **adapté au risque**.

Outils collaboratifs et RGPD : fondamentaux

- **Les traitements relatifs aux outils collaboratifs sont mis en œuvre par l'établissement, qualifié de responsable de traitement au sens du Règlement général sur la protection des données (RGPD)**.

  A ce titre, l'établissement aura à répondre des conséquences juridiques éventuelles du non-respect du RGPD ou d'une violation des traitements de données dont il a déterminé les finalités et les moyens.

  Les analyses proposées par différents DPO ou référents RGPD non affiliés à l'établissement et qui ont vocation à mutualiser les bonnes pratiques doivent toujours être adaptées aux problématiques internes de l'établissement. L'établissement est tenu responsable des traitements de ses propres systèmes d'information et des mesures techniques et organisationnelles qu'il a lui-même décidées pour son compte propre.

- **L'utilisation de solutions proposées par des entreprises non-européennes n'est pas interdite par le RGPD. En revanche, elle nécessite la mise en place de mesures techniques et organisationnelles particulières** (dont des mesures juridiques pour obtenir des garanties appropriées selon la situation (e.g. pays adéquats, Privacy Shield[1], clauses contractuelles types de l'Union Européenne, etc.) en sus des mesures classiques (informations des personnes, paramétrages applicatifs, etc.).

[1] https://edpb.europa.eu/our-work-tools/our-documents/other/eu-us-privacy-shield-second-annual-joint-review-report-22012019_fr

En pratique, et sans mésestimer la question de l'expérience utilisateur, il reste très important de faire reposer ses choix d'outils sur :

- une analyse d'impact sur la protection des données et une analyse des risques sur les systèmes d'information, notamment si interconnexion avec le SI existant (authentification, email, annuaire, groupes, etc.) à réaliser avec votre DPO et votre RSSI,

- un contrat entre l'établissement et le sous-traitant (ce point étant impératif).

- **Le choix de l'outil doit être adapté au risque** : l'approche sera donc nécessairement différente, et la politique plus ou moins stricte, qu'il s'agisse de conserver un lien avec les différentes populations de la communauté (étudiants, enseignants, chercheurs et collègues confinés), de mener des enquêtes RPS, ou d'accompagner les recherches internationales sur des domaines sensibles (risque majeur PPST). Les logiciels libres sont utilisés en priorité[2].

  ⇨ La sécurité d'un traitement de données repose sur :

  - le sous-traitant (éditeur, intégrateur, hébergeur)
  - les mesures techniques et organisationnelles mises en place par l'établissement (e.g. paramétrages applicatifs, procédures écrites et suivies, etc.)
  - l'usage des outils / de la solution / des données par les utilisateurs

⛔ **Outils interdits :** Outils grands publics sans contrat institutionnel, sans paramétrage de sécurité et vie privée. **L'implémentation d'outils sans concertation avec le DPO et le RSSI est risquée pour l'établissement, les personnels et les étudiants.**

❌ **Outils déconseillés :** Outils collaboratifs sans négociation précontractuelle entre l'établissement et le sous-traitant. Leur utilisation doit être limitée aux échanges non sensibles, non confidentiels, et hors projets de recherche.

✔ **Conseillé :** Outils mis en oeuvre par l'établissement, solutions libres respectueuses de la vie privée, et/ou libres.

✅ **Recommandé :** Solutions ESR (Tixeo, certifiée par l'ANSSI, Renater, etc.). On rappelle que Renater a mis en service une instance *Rendez-Vous* dédiée aux réunions institutionnelles.

Attention !

- aux outils qui utilisent les contenus échangés pour d'autres finalités que la prestation (e.g. finalités commerciales, marketing, profilage, etc.). La mission de service public d'un établissement n'est pas compatible avec ces finalités.

- à l'utilisation des réseaux sociaux par les communautés de travail. Le partage de copies d'écran ou des identifiants ou liens d'accès des réunions de visioconférence sur les réseaux sociaux. La responsabilité de l'établissement est engagée : Clarifiez les règles auprès de vos utilisateurs.

[2] art. L123-4-1 du Code de l'Éducation

Mettre en conformité son outil collaboratif (visio-conférence, messagerie, etc.)

- **Base légale** : Mission d'intérêt public (continuité académique en période de crise sanitaire).

  La mise en œuvre d'un outil collaboratif (messagerie, visioconférence, etc.) est considérée comme par nature déterminée, explicite et légitime (cf. mise en place d'un ENT, ancienne norme CNIL RU-003), dans la mesure où les traitements mis en œuvre sont décrits dans le plan de continuité de l'établissement.

  Attention ! Ne pas se perdre dans la multiplication des outils collaboratifs et de visioconférence proposés aux mêmes membres d'un établissement.

- **Conformité contractuelle** (obligatoire) : l'établissement doit assortir des garanties juridiques appropriées -par exemple des clauses contractuelles types de l'UE- à la commande réalisée, dès lors que le choix d'outil collaboratif donne lieu à des flux de données hors Union européenne

  + d'information sur la page *Transférer des données hors de l'UE* de la CNIL

- **Information des personnes** (obligatoire), à prévoir dans :

  - les conditions générales / une charte utilisateur complémentaire à celle du service collaboratif utilisé
  - les guides utilisateurs
  - les FAQ
  - la charte informatique / charte numérique de l'établissement

  Ces documents doivent clarifier les obligations des utilisateurs du service mis en place par l'établissement. Ils doivent également clarifier l'étendue des enregistrements.

  Attention ! Un message de l'établissement à tous ses membres peut se révéler nécessaire pour leur rappeler les bonnes pratiques et les obligations en matière de protection des données, droit à l'image et droit d'auteur sur les outils collaboratifs. Cette initiative est encouragée par SupDPO.

- **Consentement des personnes :** obligatoire dès lors que des enregistrements vidéos sont lancés car cette procédure participe à la bonne information des personnes.

  Il est préconisé de clarifier les règles en matière d'enregistrement (autorisation/interdiction) dans le Règlement intérieur, le Règlement de scolarité et le Règlement des admissions. D'une manière générale, en l'absence d'accords/règles d'établissement spécifiques ayant donné lieu à une consultation des instances représentatives, les participants devraient toujours en mesure de suspendre leur caméra et leur micro, et d'interrompre leur participation à la réunion.

- **Droits des personnes :** les services d'assistance des éditeurs d'outils collaboratifs ne doivent pas se substituer à l'établissement lors d'une difficulté technique d'un utilisateur ou lorsqu'il exerce ses droits RGPD. L'adresse générique du DPO et l'adresse du service d'assistance technique de l'établissement doivent être proposés en première intention aux utilisateurs.

- **Cycle de vie des données :** l'établissement doit prévoir des règles de stockage et archivage et veiller aux règles d'accès aux données enregistrées.

- **Minimisation et proportionnalité des traitements de données :** l'établissement doit limiter les enregistrements au strict nécessaire, à la continuité de ses activités. Il n'est pas conseillé a priori d'opter pour des enregistrements par défaut de toutes les réunions ni de tous les cours. Pour autant, chaque établissement peut être en mesure de justifier telle ou telle nécessité d'enregistrement (décalage horaire, limite des matériels des participants, contrat de service public préexistant entre l'étudiant et l'établissement, etc.). Ceci n'est donc pas interdit en soi.

  SupDPO conseille aux participants de réunions enregistrées de :

  - couper leur caméra et leur micro ;
  - veiller à ce qu'aucun document confidentiel ne soit ouvert sur le bureau virtuel de l'animateur/l'hôte de la réunion/le participant partageant son écran ;
  - changer leur pseudo;
  - refuser et demander l'accès à l'enregistrement (ce refus engendrant l'exclusion du participant à la réunion, il reste cependant préférable de couper la caméra et le micro et d'utiliser un pseudo si souhaité) ;
  - ne jamais partager des copies d'écran des réunions, par exemple sur les réseaux sociaux, ni les enregistrer avec des matériels personnels (smartphone, enregistreur etc.) : leur responsabilité juridique est engagée ;
  - veiller à ce que leur caméra soit orientée de telle sorte qu'elle ne porte pas atteinte à leur vie privée ou celle de tiers ;
  - d'être vigilants sur les conversations écrites qui sont assimilables à des zones bloc notes et commentaires ;
  - demander aux organisateurs des réunions de rappeler ces recommandations aux participants.

  Si la participation des étudiants est naturellement conseillée pour la bonne continuité des enseignements, SupDPO conseille aux établissements dont les réunions sont enregistrées et pour lesquelles les étudiants ne souhaiteraient pas participer, de s'assurer de leur accès aux enregistrements en lecture et de s'assurer que cela ne conduise à aucune pénalité sur leur scolarité.

- **Sécurité et confidentialité :** faire reposer le choix de l'outil sur une analyse de risque (vie privée/RGPD/sécurité des SI) réalisée avec le DPO et le RSSI afin de s'assurer de la sécurité par défaut des outils utilisés.

  Attention ! En cas de risque identifié, rédiger un courrier juridique à l'adresse du sous-traitant pour exiger le rétablissement d'un niveau de sécurité et conformité, dans le respect du RGPD.

  En cas de violation de données, le DPO et le RSSI et la Direction de la communication doivent participer à la cellule de crise.

En savoir plus

Pour les DPO de l'ESR, consulter les ressources disponibles sur le wiki :

- Page dédiée "COVID-19" (bonnes pratiques, analyses d'impact, documentation,...)
- Conseils et propositions aux établissements d'enseignement supérieur et de recherche concernant le choix et la mise en œuvre des suites collaboratives "For Education"
- AIPD et analyse du contrat Gsuite (incl. HangOut Meet),
- O365 (incl. Teams),
- AIPD Outil de visioconférence Zoom.

Pour le public, consulter :

- la fiche *COVID-19 : les conseils de la CNIL pour utiliser les outils de visioconférence sur le site de la CNIL ;*
- les *Outils de la continuité pédagogique : les conseils de la CNIL* sur EducNum ;
- les AIPD O365 et l'analyse du Clusif.