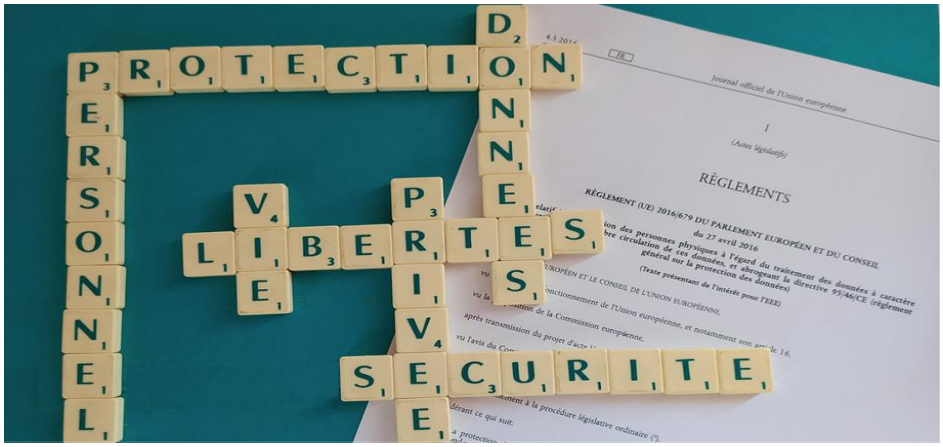
VISIOCONFERENCE

ACADÉMIE
D'AIX-MARSEILLE
Liberté
Égalité
Fraternité

Déléguée à la protection des données

RGPD

Date	version
24/11/2020	V1.2



La visioconférence dans le cadre professionnel ne doit pas négliger la protection des données. Cette fiche présente comment ces réunions distancielles peuvent être conduites.

CHOIX DE L'OUTIL

Outils préconisés par l'institution

L'institution propose plusieurs outils pouvant être utilisés dans le cadre professionnel. Ces outils dont l'utilisation est encadrée ne posent pas de problèmes majeurs en termes de protection des données.

- ✓ Pour les visioconférences avec élèves : Les trois plateformes du dispositif **Ma classe à la maison** (école/collèges/lycées) du CNED sont accessibles, gratuitement, à tous les élèves et à tous les enseignants qui souhaitent les utiliser.
- ✓ Pour les visioconférences entre agents du MENJ **Ma classe virtuelle VIA** https://cvirtuelle.phm.education.gouv.fr/
- ✓ La plateforme Renater propose l'outil Rendez-vous, utilisable à partir de postes de travail individuel (PC, Tablette, smartphone). Ce service permet la mise en relation de 30 participants, possède les fonctionnalités de partage d'écran et de messagerie instantanée et est accessible depuis un navigateur (Chrome, Firefox, ...) sans installation de logiciel
- ✓ Les Webconférences avec Jitsi Meet sont disponibles sur https://apps-Aix-Marseille.beta.education.fr ces solutions peuvent être adaptées aux tenus de conseil de classe.
- ✓ Pour les réunions en audioconférence la plateforme pour les agents de l'état https://audioconf.numerique.gouv.fr/
- ✓ Pour les réunions en audioconférences et jusqu'à 50 personnes, il est possible d'utiliser aussi la solution proposée par OVHCloud https://www.ovh.com/cgi-bin/telephony/webconf.pl
- ✓ Enfin dans les cas de besoin absolu de connexion depuis un matériel de visioconférence ou bien d'un accès téléphonique à votre réunion, il est possible d'utiliser le service RENAvisio.

D'autres outils sont parfois localement promus, les garanties qu'ils offrent en termes de protection des données doivent être analysée avant leur mise en oeuvre.

Outils proposés par des sociétés américaines

La grande majorité de ces outils sont proposés par des société américaines (ZOOM, TEAMS, GOOLE MEET, etc.) avec parfois, comme pour Teams, un hébergement en UE. Au-delà de leurs caractéristiques propres, le degré d'inférence créé par la législation des États-Unis avec les droits fondamentaux doit être pris en compte lorsque la solution fournie par une société américaine du fait de la portée extraterritoriale de ces lois qui concernent ainsi également les hébergements en Union Européenne de ces solutions états-uniennes. Ces solutions sont **inadaptées à une utilisation avec des données à caractères personnelles** en l'état du cadre juridique de l'Union Européenne et des États-Unis.

⇨ **Les réunions ayant pour objet d'échanger des données concernant les élèves leurs responsables ou les personnels, ne doivent pas être tenues sur ces instances.**

Les personnels sont parfois invités à suivre des visioconférences organisées par d'autres entités sur ces solutions états-uniennes. Les personnes concernées doivent alors pouvoir agir **en mode invité (lien générique)**, sans qu'elles ne soient contraintes de donner leurs données* (nom prénom, mail nominatif...) ni d'installer un applicatif non maitrisé sur leur équipement et sous réserve que la solution garantisse la confidentialité des échanges.

* généralement la solution collectera tout de même des données telles que : adresse IP, identifiant de l'appareil, cookies ou technologies analogues…

Alternatives européennes

Des solutions avec un hébergement à l'intérieur de l'UE et non soumises à une législation extra-européenne existent*. Les établissements souhaitant utiliser une de ces solutions sont invités à se rapprocher de leur délégué à la protection des données pour l'analyse des critères de protection des données.

*L'ANSSI a certifié Tixeo pour les administrations. La direction interministérielle du numérique (DINUM) et la Direction Générale de l'Administration et de la Fonction Publique (DGFAP) fournissent un tableau comparatif durant le premier confinement (https://www.numerique.gouv.fr/uploads/outils_webconference-agents-etat.pdf) pour vous accompagner dans le choix d'une solution qui convient à votre besoin.

UTILISATION DE L'OUTIL

Activation de la caméra

De manière générale, la CNIL recommande aux employeurs de **ne pas imposer** l'activation de leur caméra aux salariés en télétravail qui participent à des visioconférences.

Cette recommandation découle du principe de minimisation des données, consacré par l'article 5.1.c du RGPD et selon lequel les données traitées doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées » : or, dans la plupart des cas, une participation via le micro est suffisante.

La diffusion de l'image peut porter atteinte au droit au respect de la vie privée, tout particulièrement pour les autres personnes présentes au domicile.

Conseil à l'utilisateur quand la caméra est activée

Quand ils existent, les outils masquant les arrières plans contribuent à la protection de la vie privée.

En l'absence d'utilisation de ce type d'outil veillez que le champ couvert par la caméra n'interfère pas avec votre vie privée (contrôlez ce champ en amont de la visioconférence).

A la fin de la visioconférence fermer l'application.

Lorsqu'ils ne sont pas utilisés, désactivez le microphone et la webcam (cette dernière peut également être masquée physiquement en apposant un cache sur l'objectif).

Enregistrement de la visioconférence

Aucun enregistrement ne peut avoir lieu à l'insu des participants.

Si un enregistrement de la visioconférence est envisagé la licéité de ce traitement doit être étudiée en amont :

Quelle est la finalité de cet enregistrement ? Combien de temps sera-t-il conservé ? Qui pourra y avoir accès ? -etc. Les établissements ou services souhaitant procéder à l'enregistrement d'une visioconférence sont invités à se rapprocher de leur délégué à la protection des données.