Centre national de la recherche scientifique

07/05/2021

Guide des bonnes pratiques pour l'utilisation des

outils de visioconférence proposés au CNRS

0 – Préambule

Différents outils de communication sont aujourd'hui proposés par divers fournisseurs, ils ne sont néanmoins pas tous adaptés aux besoins de sécurité des données du CNRS.

La robustesse de ces outils, les risques associés à leur utilisation (compétition internationale, risques sur la sécurité des postes de travail, risques pour les données personnelles et/ou sensibles, notamment), les usages souhaités sont autant de facteurs à prendre en compte dans le choix du ou des outils, pour les échanges par visioconférences.

L'actualité depuis le début de l'année 2020 relative à la sécurité des supports, outils, systèmes de communication met en exergue la difficile compatibilité de la qualité du service et de la protection légitime de nos activités de recherche.

A l'issue de nombreuses analyses des offres existantes et des besoins des laboratoires, le CNRS a décidé de proposer différents outils de visioconférence, afin d'être en adéquation avec les besoins de sécurité divers et de garantir une meilleure résilience (un seul outil disponible est une mauvaise idée…).

Ce guide des bonnes pratiques est destiné à fournir à chacun des éléments (analyse de la sensibilité des données, objet, nombre de participants, ….) pour le choix de l'outil opportun pour l'usage prévu.

A savoir

Qu'est-ce qu'une donnée sensible ?

→ De manière absolue : une donnée sensible est une donnée dont la divulgation à des tiers non autorisés peut avoir des conséquences, plus ou moins graves, sur l'accomplissement des missions ou l'image de l'établissement ou des personnes concernées.

La classification du niveau de sensibilité des informations relève des mesures PDI-1 et PDI-2 de la PSSI du CNRS. La cible de diffusion des informations est encadrée par la réglementation PPST (protection du potentiel scientifique et technique), le secret des affaires, la propriété intellectuelle et industrielle, le code du patrimoine etc…

→ Selon la règlementation sur la protection des données

Les données à caractère personnel sensibles sont : les données qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les données de santé, les convictions religieuses, …. Les données relatives aux infractions et condamnations pénales, le numéro de sécurité sociale.

Les données hautement personnelles nécessitent également des mesures de protection et sécurité adaptées.

Voir articles 4, 9, 10 du règlement européen sur la protection des données personnelles UE 2016/679

1 – Les outils préconisés par le CNRS

A date de finalisation du guide

	Capacité	Usages
BBB*	Jusqu'à 150 utilisateurs	Possible pour tous les usages
Rendez-vous	Jusqu'à 30 utilisateurs	Possible pour tous les usages
Renavisio**	Accessible en salle de visio, 20 connexions simultanées	Possible pour tous les usages
Zoom (instance CNRS)	Pour les visio réunissant plus de 100 personnes	Exclusivement pour les données non sensibles

*Voir la disponibilité de BBB avec la délégation de proximité ou l'institut

** Produit en cours de refonte chez Renater.

Pour en savoir plus sur l'utilisation des outils :

https://intranet.cnrs.fr/Cnrs_pratique/si/pratique/Pages/Outils-communication.aspx

La plupart des outils sont accessibles au moyen d'un logiciel dédié installable sur votre poste, et d'un navigateur web. La solution du navigateur web est toujours à privilégier car elle présente moins de risques d'intrusion sur le poste de travail. Le logiciel dédié peut présenter des vulnérabilités parfois critiques qui peuvent compromettre totalement votre poste.

NOTA : Dans le cas de Zoom, il existe un paradoxe :

- Le logiciel installable de Zoom est le seul qui permet de réaliser des réunions avec chiffrement des données de bout en bout (voir plus loin). Il est donc le seul à pouvoir garantir une confidentialité des données relative ;
- Mais ce logiciel est régulièrement affecté de failles importantes qui mettent en danger les données sur le poste de travail.

2 – Une attention à porter aux conditions d'utilisation des outils

Pour ce qui concerne BBB, Rendez-vous et Renavisio, le CNRS a pu vérifier et garantir l'adéquation des dispositions contractuelles avec les enjeux de protection des données personnelles et sensibles et s'assurer d'une maîtrise des risques pour l'établissement et les personnes.

Pour ce qui concerne les services de mise en relation en temps réel offerts en cloud public (Zoom, MS Teams, GotoMeeting, Whereby, Discord…), ces services présentent tous des risques inhérents à leur mode de mise à disposition et à la territorialité du droit associé aux sociétés émettrices

- Soumission à des réglementations permettant aux Etats un accès aux données des utilisateurs
- Stockage ou transit des données par des territoires où la protection des données personnelles ne se situe pas à un niveau adéquat comme défini par la CNIL
- Commerce des données et métadonnées collectées par l'opérateur du service vers des sociétés tierces

Chaque outil dispose, en général, d'un lien en bas de page de connexion vers les conditions générales d'utilisation (*terms of service*) et de protection des données personnelles (*data privacy agreement, privacy policy*). Lisez ces documents et demandez l'avis du service de la Déléguée à la Protection des Données /du Responsable de la Sécurité des Systèmes d'Information CNRS en cas de question ou de doute sur la portée des engagements.

3 – Une attention à porter à la confidentialité des données et des échanges

L'utilisation des outils de visioconférences implique, dans tous les cas, la collecte de données personnelles : à minima celles permettant la connexion (authentification) et les données techniques liées à la mise en relation comme l'adresse IP (métadonnées).

La confidentialité des échanges ne peut être garantie de manière indiscutable que si le service offre un chiffrement des échanges « de bout en bout », audité par un tiers de confiance.

En termes de **chiffrement**, il faut distinguer :

- Le chiffrement du transport des données (à l'image de protocole « HTTPS » utilisé sur le web en lieu et place du classique « HTTP » non chiffré). Ce chiffrement crée un canal de communication chiffré dans lequel les données passent en clair. Le détournement de canal est assez facile, en particulier par l'opérateur du réseau d'accès à Internet utilisé (WiFi local, réseau 4G etc…)
- Le chiffrement des données elles-mêmes : dans ce cas, sur un canal de transport chiffré, les données sont chiffrées à partir d'une clé qui ne quitte jamais le poste de travail de l'émetteur. Même si le canal de transport était compromis, la donnée reste inintelligible pour le pirate.

On préfèrera toujours utiliser un outil capable de réaliser un chiffrement de la donnée de bout en bout.

A savoir : les fournisseurs doivent fournir l'information sur l'utilisation des données personnelles (voir lien dans la rubrique dédiée aux conditions d'utilisation)

Les données contenues dans les échanges, les fichiers peuvent revêtir un caractère confidentiel, sensible. Dans une unité impactée par le dispositif ZRR, les échanges autour des activités ayant conduit au classement en ZRR doivent utiliser des outils sécurisés (chiffrés de bout en bout et non soumis à des réglementations extra nationales) validés par le CNRS. Zoom est ici exclu.

A savoir : le niveau de confidentialité et la nature des échanges forment un critère du choix de l'outil à utiliser

Réflexe : Ne pas publier sur les réseaux sociaux ou les sites web publics des unités les codes d'accès aux réunions organisées par l'unité

Réflexe : Vérifier régulièrement la liste des présents/connectés à la réunion

4 – Le choix des outils

Plusieurs éléments sont à prendre en compte dans le choix de l'outil.

→ Situation 1 : Vous êtes à l'initiative d'une visioconférence

	Données non sensibles	**Données sensibles et très sensibles**
Nombre de participants < 100	BBB Rendez-vous Renater	BBB Rendez-vous Renater
Nombre de participants ≥100	BBB (jusqu'à 150) Zoom	BBB

→ Situation 2 : Vous êtes invité

BBB : Préconisé

Rendez-vous : Préconisé

Renater : Préconisé

Zoom : Analyse de la sensibilité des échanges ; possibilité de proposer un autre outil (Renater, BBB si proposé par la délégation régionale ou l'institut)

Préconisation : Discuter du choix des outils en conseil de laboratoire. Définir les échanges qui nécessitent sans ambiguïté le choix d'un outil sécurisé en fonction des informations qui sont échangées.

5 – Dispositions spécifiques liées à l'utilisation des outils de visioconférence

Le service Zoom fourni par le CNRS a été paramétré pour atteindre le meilleur niveau possible de sécurité dans l'accès aux conférences. Certains paramètres sont verrouillés au niveau central et ne peuvent être modifiés. **Il est conseillé de ne modifier aucun paramètre dans la console utilisateur**.

Voici quatre rappels importants :

- Le mode réunion chiffrée de bout en bout (E2EE) est préconisé mais non obligatoire (car il nécessite l'installation du client local pour tous les participants – même les invités externes)
- Toute réunion doit avoir une salle d'attente et un mot de passe d'accès
- Le partage du bureau est interdit – on ne peut partager qu'une application à la fois
- L'enregistrement des conversations (tchat) est interdit

L'accès à Zoom au moyen d'un compte utilise l'authentification centralisée du CNRS (Janus).

Rappel des dispositions qu'il vous est demandé d'accepter à la création de votre compte :

L'usage des services « Zoom » dans le contexte du CNRS est soumis au strict respect des règles ci-dessous.

Zoom ne doit pas être utilisé pour des échanges :

- relevant du secret de la défense nationale ou de la classification « Diffusion Restreinte » ;
- en lien avec l'activité de recherche des unités sensibles ;
- dont la divulgation pourrait mettre en cause l'image ou la responsabilité de l'établissement ;
- dont la divulgation pourrait porter atteinte à la vie privée des participants, en particulier dans les activités de recherche en sciences humaines et sociales.

Le service a été paramétré à la création de votre compte de manière automatique par le CNRS afin de sécuriser au mieux son usage. Les paramètres de sécurité qui ont été positionnés sont verrouillés et ne peuvent être modifiés.

Il est **interdit d'enregistrer** les réunions à l'insu des participants. Si un enregistrement est nécessaire, vous devez informer les participants de la finalité et de l'usage (ex : rediffusion pour un autre public) et obtenir leur autorisation au préalable via un formulaire de droit à l'image/ à la voix. La rediffusion des enregistrements à d'autres fins est interdite.

Il vous est demandé de **ne fournir aucune donnée à caractère personnel à « Zoom »** qui n'aurait pas été automatiquement transmise par le CNRS au service lors de votre demande de création de compte.

En cas de doute, **vous devez utiliser un autre service** de visioconférence : Renavisio, Rendez-vous de Renater, instance BigBlueButton (BBB) fournie par votre délégation régionale ou votre institut.

Pour toute question ou information, merci de contacter :

- le Fonctionnaire Sécurité et Défense du CNRS : fsd@cnrs.fr
- La Déléguée à la protection des Données Personnelles du CNRS : dpd-demandes@cnrs.fr
- le RSSI du CNRS : rssi@cnrs.fr