



Mesures de sécurité pour les conférences audio et vidéo

En Suisse comme dans le monde entier, la crise du virus coronaire nous rappelle que certains événements peuvent chambarder nos habitudes et nos comportements du jour au lendemain, en l'occurrence en nous empêchant de rencontrer nos proches ou d'avoir des réunions avec nos collègues. Les particuliers et les entreprises ont été contraints de trouver rapidement des solutions pour communiquer par conférences audio et vidéo. Même si cela s'est parfois fait à la hâte, les réunions professionnelles, les conversations avec les enfants et les grands-parents et même les petites rencontres festives ont pu être transposées dans le monde virtuel. Il est néanmoins important de veiller à la sécurité des informations et à la protection des données dans le cadre de ces conférences. Le présent document énumère certaines règles à appliquer dans la sphère professionnelle comme privée.

Le PFPDT recommande dans un premier temps de prendre des mesures pour utiliser de la manière la plus sûre possible les solutions adoptées dans l'immédiat dans le cadre du confinement. Plus tard, ou déjà lors de cette utilisation, il est recommandé d'analyser, en se fondant sur le droit de la protection des données, les risques que présentent les services et produits disponibles, ce qui permettra éventuellement d'opter pour un produit plus approprié. Vous trouverez ci-dessous des instructions pour choisir et mettre en œuvre une solution respectueuse de la protection des données.

Mesures pour l'utilisation de solutions de conférence audio et vidéo

Ne pas publier les identifiants de réunion

Un identifiant de réunion est un numéro unique attribué à une réunion. Veillez à ne pas publier cet identifiant sur Internet (médias sociaux compris). Même si cette solution devait vous sembler pratique, elle pourrait permettre à des *personae non gratae* d'accéder à la réunion.

Utiliser à chaque fois un identifiant différent et verrouiller les réunions

N'utilisez pas le même identifiant pour des réunions consécutives et verrouillez l'accès à la réunion dès que tous les participants s'y sont connectés. Les participants de la réunion suivante ne pourront ainsi pas se connecter et vous écouter.

Utiliser un mot de passe de réunion

Définir un mot de passe pour l'accès à la réunion permet de renforcer la sécurité. Seules les personnes autorisées pourront alors se connecter. Évitez d'envoyer l'identifiant de la réunion et le mot de passe dans le même courriel.

Vérifier régulièrement qui est connecté

Vérifiez régulièrement qui est connecté à la réunion. Si vous remarquez des personnes inconnues, demandez-leur de décliner leur identité.

Toujours informer les participants avant d'enregistrer la réunion

Les participants doivent être explicitement prévenu en cas d'enregistrement de la réunion (son, image). Ils doivent pouvoir, sans subir de préjudice, formuler des objections et, si nécessaire, quitter la réunion.

Faire attention au hameçonnage

Si vous recevez un lien pour une réunion par courriel ou par un réseau social, contactez l'expéditeur afin de vérifier son identité. N'ouvrez jamais de liens ou de pièces jointes provenant d'adresses inconnues.

Obstruer la caméra lorsqu'elle n'est pas utilisée et vérifier son champ de vision

Il est recommandé d'obstruer la caméra lorsque vous ne l'utilisez pas pour être à l'abri de toute tentative d'observation sournoise. Avant de l'activer, vérifiez ce qui entre dans son champ de vision, et donc ce que les participants pourront voir (par ex. murs blancs, images, inscriptions sur un tableau). Il existe des fonctions permettant de flouter l'arrière-plan.

Partager l'écran

Ne partagez que les informations nécessaires pour la réunion. Fermez donc les contenus, fenêtres et onglets inutiles. Plutôt que le bureau dans son intégralité, présentez uniquement le programme concerné. Vous pouvez aussi créer un bureau distinct sans liens ni fichiers.

Vérifier la politique de confidentialité du fournisseur

Certains fournisseurs transmettent des données personnelles à des tiers ou leur mettent à disposition des métadonnées comme la durée et le lieu des réunions ou le nombre de participants et leurs identifiants. Si le fournisseur de la solution que vous utilisez partage ce genre de données, il doit le signaler dans sa politique de confidentialité. Lisez ce document et, si nécessaire, usez de votre droit d'obtenir des informations sur les données partagées.

Points à contrôler lors de l'évaluation des solutions et des préparatifs en vue de leur utilisation

Se renseigner sur la réputation du fournisseur

Cherchez sur Internet des informations sur le produit du fournisseur : la satisfaction des clients, les fonctions particulières, les éventuels problèmes de sécurité, etc. En cas de doute, optez plutôt pour un fournisseur reconnu sur le marché.

Vérifier la politique de confidentialité

Vérifier aussi la politique du fournisseur en matière de transmission des données personnelles à des tiers. Si le fournisseur est établi ailleurs qu'en Suisse ou dans l'UE et que les données sont transmises dans un État tiers, vérifier si cet État ou si le fournisseur garantit une protection adéquate (bouclier de protection des données

pour les entreprises américaines, par exemple, ou toute autre clause standard de protection des données).

Vérifier l'utilisation des métadonnées par le fournisseur

Faites attention à ce que le fournisseur ne collecte pas de métadonnées, n'en traite pas à des fins propres et n'en transmette pas à des tiers. Outre les informations déjà évoquées, à savoir la durée et le lieu des réunions ainsi que le nombre de participants et leurs identifiants, les métadonnées portent sur les adresses électroniques d'autres contacts figurant dans le carnet d'adresses, le type d'appareil utilisé ou encore le navigateur.

Chiffrer les données

Toutes les données doivent être sauvegardées et transmises sous forme chiffrée. Au minimum : transmission chiffrée ; au mieux : chiffrement de bout en bout.

Vérifier la sécurité physique

Où se trouvent les centres de données du fournisseur ? REMPLISSENT-ILS LEURS exigences de sécurité ? En particulier si votre solution fonctionne selon un stockage centralisé des données, assurez-vous que les centres sont sécurisés en permanence, qu'ils sont régulièrement contrôlés et qu'ils sont protégés contre les intrusions physiques. Privilégiez les fournisseurs ayant leurs serveurs en Suisse ou dans l'UE.

Utiliser des instruments de sécurité

Certaines solutions permettent de détecter efficacement les tentatives d'abus, par exemple en remarquant et en bloquant les tentatives répétées d'identification. Certaines signalent à tous les participants les entrées et sorties dans une réunion. Une fonction pratique est celle permettant à tous les participants de voir en tout temps qui est connecté. Des fonctions de délégation permettent de confier la surveillance ou la direction de la réunion à un participant.

Paramétrer la protection des données

Uniformisez les paramètres de protection des données dans votre organisation pour prévenir les traitements de données indésirables. Remettez à cet effet des instructions à tous les utilisateurs.

Points à vérifier au moment de mettre une solution en service

Enregistrer ou annoncer

Il est très pratique d'utiliser une solution en ligne dans un navigateur sans enregistrement ni annonce. Cela évite de devoir installer un programme sur les machines. Néanmoins l'identification des participants n'est alors pas optimale. C'est pourquoi de telles solutions ne devraient pas être utilisées pour la communication interne.

Empêcher les accès indésirables aux données personnelles

Beaucoup d'applications, surtout sur les appareils portables, veulent accéder à des données personnelles sans que cela ne soit utile. Adaptez les paramètres de

confidentialité pour éviter tout traitement de données indésirables. Veillez aussi à configurer, documenter et surveiller les accès aux applications de manière détaillée (ne donner des accès que si l'utilisation que vous faites de l'application le requiert).

Édicter un règlement d'utilisation

Sans règlement, l'utilisation de la solution à des fins privées reste une question floue. Sans limitation ou interdiction expresses, les collaborateurs sont en droit de penser qu'ils peuvent l'utiliser à des fins privées dans la mesure du raisonnable sans être surveillés.

Informé sur la surveillance et les enregistrements

L'employeur n'est pas tenu d'édicter un règlement d'utilisation, mais il doit informer les collaborateurs de manière transparente s'il surveille et enregistre les communications effectuées au moyen de la solution, car il s'agit d'une atteinte à la sphère privée (principe de la bonne foi, art. 4, al. 2, LPD).

Berne, avril 2020

Informations supplémentaires

Liste de produits pour la [collaboration par voie numérique](#), avril 2020, Préposé à la protection des données du canton de Zurich.