Le 30 septembre 2020

Objet : Réponse de Cisco Systems, Inc. (Cisco Webex) à la déclaration commune sur les attentes mondiales en matière de confidentialité des entreprises de vidéoconférence

Messieurs et mesdames les commissaires,

Nous vous remercions de nous offrir l'occasion de répondre à la déclaration commune sur les attentes mondiales en matière de politique de confidentialité des données personnelles des entreprises de vidéoconférence (VTC). Nous saluons votre décision d'examiner attentivement les répercussions sur la protection de la vie privée et la sécurité en lien avec la façon dont ces technologies sont développées, déployées et utilisées. L'impératif de distanciation sociale au cours de la pandémie de la COVID-19 a entraîné une augmentation spectaculaire de l'utilisation des technologies de VTC pour permettre, à distance ou par une combinaison de présence physique et virtuelle, aux gens de travailler, d'étudier, d'offrir des soins de santé et de maintenir d'autres fonctions essentielles pour la santé et la sécurité du public, tout en favorisant l'activité économique. Cisco Webex a soutenu, en toute sécurité, 500 millions de participants à des réunions, générant 25 milliards de minutes de réunion en avril seulement, soit plus du triple du volume avant la pandémie. Avec le recours accru à la technologie VTC, la sécurité et la confidentialité sont plus importantes que jamais. Nous comprenons les préoccupations que vous soulevez et nous concentrons nos efforts en matière de protection de la vie privée et de sécurité par conception et par défaut depuis des années. Le président et chef de la direction de Cisco, Chuck Robbins, a déclaré publiquement que « la vie privée est un droit fondamental de la personne » et que nous avons besoin de sécurité, de transparence et de responsabilité pour la protéger. Cisco s'engage à respecter et à protéger les droits à la vie privée de ses clients, partenaires, utilisateurs, travailleurs et autres. Notre programme de protection des données et de la vie privée est ancré sur les principes de transparence, d'équité et de responsabilité, et a été certifié pour s'aligner sur les cadres de confidentialité et les exigences légales à l'échelle mondiale, à savoir les règles d'entreprises contraignantes (Binding Corporate Rules) pour les responsables de données de l'UE (BCR-C) – l'application des règles d'entreprises contraignantes pour les sous-traitants (BCR-P) est à venir –, le bouclier de protection de la vie privée (Privacy Shield) UE/Suisse/Royaume-Uni et États-Unis, le système de règles transfrontalières de protection de la vie privée de l'APEC (Cross-Border Privacy Rules System) et la reconnaissance de la vie privée pour les sous-traitants (Privacy Recognition for Processors). La protection de la vie privée est au coeur de la conception, du développement, du déploiement et de la maintenance de nos réseaux, plateformes, applications et offres, y compris Cisco Webex. Pour en savoir plus sur l'approche de Cisco en matière de confidentialité, nous vous invitons à consulter notre centre de sécurité et de transparence (« Cisco Trust Center ») ici.

Cisco Webex

Le service de vidéoconférence de Cisco Webex, la solution de collaboration la plus déployée au monde, est offert par l'entremise d'une plateforme infonuagique de prestation de services hautement sécurisée offrant des performances, une intégration, une flexibilité, une évolutivité et une disponibilité attendues par un chef de fil de l'industrie tel que Cisco. Cisco Webex est une infrastructure de communication spécialement conçue pour les communications en temps réel sur le Web. Le service permet aux utilisateurs, aux employés et aux équipes virtuelles du monde entier de collaborer en temps réel de n'importe où, en tout temps, sur des appareils mobiles, des PC, des ordinateurs portables ou des systèmes vidéo comme s'ils travaillaient dans la même pièce ou presque. Les solutions offertes comprennent des réunions, des événements, des formations et des services d'assistance.

En réponse aux questions et principes spécifiques soulevés dans votre lettre ouverte, nous vous présentons ci-dessous un bref résumé et un aperçu.

1. Sécurité

Cisco Webex permet aux employés répartis mondialement ainsi qu'aux équipes virtuelles de collaborer en temps réel, et ce, comme s'ils étaient dans la même pièce ou presque. Les entreprises, les établissements, les écoles et les gouvernements à l'échelle internationale font confiance aux solutions Cisco Webex pour simplifier leurs processus d'affaires ainsi que pour améliorer la collaboration et les résultats des équipes de vente, de marketing, de formation, de gestion de projet et de soutien. Pour tous ces clients et utilisateurs, la sécurité et la confidentialité sont des préoccupations de premier plan. Les outils de collaboration en ligne doivent fournir plusieurs niveaux de sécurité en fonction de la sensibilité des données impliquées pour des tâches allant de la planification des réunions à l'authentification des participants et au partage des documents confidentiels.

Chez Cisco, nous nous engageons à créer des solutions fiables dotées d'une sécurité intégrée sur plusieurs plateformes. Le groupe responsable de la sécurité et de la confiance (« Security and Trust Organization ») de Cisco collabore avec différentes équipes de l'entreprise afin d'incorporer la sécurité, la confidentialité, la confiance et la transparence à l'intérieur d'un cadre qui sert de balise pour nos activités liées à la conception, au développement et à l'exploitation de notre infrastructure afin d'atteindre les plus hauts niveaux de sécurité et de confidentialité dans tout ce que nous construisons. Les exigences en matière de protection des données, de protection de la vie privée et du maintien de la sécurité sont intégrées dès la conception des produits et le développement des méthodologies, et ce, tout au long du cycle de vie des produits grâce au cycle de vie sécurisé du développement Cisco (Cisco Secure Development Lifecycle, ou CSDL), appliqué depuis la création du produit au concept d'engagement envers celui-ci, jusqu'au lancement, en passant par le fonctionnement, l'utilisation et la fin du cycle de vie des produits. Le CSDL est un processus reproductible et mesurable conçu pour accroître la résilience et la fiabilité des produits Cisco permettant également de confirmer que les exigences en matière de confidentialité, ainsi que leur impact et les risques qui y sont associés sont traités de manière appropriée. La combinaison d'outils, de processus et de formations de sensibilisation introduites au cours du cycle de vie du développement favorise l'instauration de mécanismes de défense en profondeur, fournit une approche globale de la résilience des produits et établit une culture de sécurité et de confidentialité. Cliquez ici pour en savoir plus sur le CSDL.

Cisco effectue régulièrement des tests de pénétration rigoureux en utilisant des évaluateurs internes et des équipes tactiques. Au-delà de ses propres procédures internes, l'équipe de sécurité de l'information

de Cisco fait également appel à des tiers indépendants pour effectuer des vérifications rigoureuses des politiques, des procédures et de leur application interne à Cisco. Ces audits visent à valider les exigences de sécurité des organisations commerciales et gouvernementales qui sont essentielles à leur mission. Cisco fait également appel de façon continue à des fournisseurs tiers pour effectuer des tests avancés de pénétration et des audits de services poussés assistés par ordinateur. Les utilisateurs sont rapidement informés des mises à jour logicielles (correctifs de sécurité et améliorations des fonctionnalités) et sont invités à installer la dernière version immédiatement.

Des contrôles de sécurité de bout en bout sont intégrés à la plateforme Cisco Webex pour protéger la propriété intellectuelle, la confidentialité et les données. Le service commun d'identité de la plateforme Cisco Webex prend en charge les différentes solutions d'identité d'entreprise (IdP) de plusieurs fournisseurs pour l'authentification des utilisateurs au moyen du protocole normalisé SAML ainsi que pour le provisionnement des utilisateurs par l'entremise du protocole normalisé SCIM. Les clients qui optent pour un fournisseur d'identité d'entreprise peuvent également ajouter, selon leur préférence, tout mécanisme d'authentification multifactorielle (MFA). Pour les clients qui n'utilisent pas leur propre service IdP, Cisco propose une offre de sécurité avancée d'authentification multifactorielle pouvant être ajoutée. Dans le cadre d'une intégration SAML et lorsque l'authentification est effectuée par mot de passe, l'administrateur des services de sécurité informatique ou du fournisseur d'identité détermine les politiques applicables aux mots de passe (longueur, complexité, renouvellement, mots de passe exclus ou précédents, etc.) selon ce que la solution IdP permet. Les administrateurs et les hôtes peuvent déterminer si les participants doivent être authentifiés avant de se joindre, ce qui garantit que seuls les utilisateurs connus et autorisés peuvent participer à la réunion.

Toutes les communications entre les applications Cisco Webex et le nuage Cisco Webex se font par le biais de canaux chiffrés conformes aux normes de l'industrie qui utilisent des suites de chiffrement de haute complexité. Tous les flux multimédias (p. ex., VoIP audio, vidéo, partage d'écran et partage de documents) sont cryptés. Les contrôles de sécurité dans Cisco Webex sont conçus selon le principe du moindre privilège ou « besoin de savoir » afin de protéger les renseignements critiques qui pourraient être partagés sur la plateforme.

Pour les réunions standard, les serveurs de médias Cisco Webex peuvent avoir besoin de déchiffrer les médias pour échanger avec le réseau téléphonique public commuté (RTPC), le transcodage et l'enregistrement. Cependant, l'administrateur peut désactiver ces fonctionnalités. Pour les entreprises qui nécessitent un niveau de sécurité plus élevé, les clients de Cisco Webex peuvent opter pour un véritable chiffrement de bout en bout (E2EE) de la vidéo, de l'audio, du texte et du partage de documents. Lorsque E2EE est activé par l'administrateur et que l'hôte de la réunion sélectionne ce mode lors de l'étape de planification, Cisco Webex n'a pas accès aux clés de chiffrement utilisées par les hôtes et les participants de la réunion; il n'est donc pas possible pour la plateforme de déchiffrer les données et les flux multimédias. Avec E2EE, l'application de l'hôte de la réunion génère la clé de chiffrement de la réunion et la distribue en

toute sécurité uniquement avec les participants de la réunion. Bien que l'E2EE offre une sécurité renforcée, les clients perdront certaines fonctionnalités facultatives (p. ex., miniatures d'image, transcription, assistant virtuel, etc.) qui exigeraient que Cisco ait accès au contenu de la réunion.

Pour vérifier et démontrer que notre solution adhère aux plus hauts standards de sécurité, Cisco Webex maintient les certifications SOC2 de type II et ISO 27001, 27017 et 27018. La certification SOC2 Type II comprend le principe du respect de la vie privée et de la confiance, lequel tient compte des préoccupations en lien avec la collecte, l'utilisation, la conservation, la divulgation et l'élimination des renseignements personnels. La certification Cisco Webex ISO 27001 garantit la conformité aux exigences relatives au

système de gestion de la sécurité de l'information, dont la confidentialité fait partie intégrante. Cisco accepte de partager des informations supplémentaires concernant la conformité à ces certifications avec ses clients et leurs principaux intervenants sur demande, en vertu d'un accord de non-divulgation.

2. Respect de la vie privée dès la conception et par défaut

Comme indiqué ci-dessus, Cisco intègre les exigences de protection des données, de confidentialité et de sécurité dans les méthodes de conception et de développement de produits dès leur conception et jusqu'à leur fin de vie à l'aide de la méthodologie CSDL. Respecter la référence de base en lien avec la sécurité des produits, incluant une évaluation des facteurs relatifs à la vie privée (PIA), dans le cadre de la CSDL, est une exigence obligatoire et une partie intégrante du développement de produits chez Cisco. La protection des données dès la conception et par défaut, tels que la minimisation des données, les contrôles d'accès basés sur les rôles, etc., et la garantie que les fonctionnalités permettant de respecter les droits de la personne concernée sur ses données, sont intégrées au coeur même de l'ingénierie de Cisco. Nous utilisons des techniques d'ingénierie et de modélisation des menaces pour évaluer et créer de meilleurs services en nous référant aux principes de la protection des données par défaut. Le processus CSDL qui comprend une évaluation obligatoire de la répercussion sur la vie privée nous permet d'évaluer si un produit traite des données personnelles sensibles ou d'autres données confidentielles et de nous assurer que les contrôles de confidentialité sont intégrés dès le départ. Au fur et à mesure qu'un produit arrive à maturité et évolue, toute modification importante dans la collecte, le traitement ou de l'utilisation des données passe également à travers le processus CSDL et une évaluation des facteurs relatifs à la vie privée (PIA).

Cisco mène également une variété de campagnes multimédias (en ligne, sur papier, vidéo, etc.) tout au long de l'année pour sensibiliser et former les employés à la protection des données et de la vie privée. Nous maintenons un intranet actif pour la collaboration et les communications à tous les niveaux de l'entreprise. Ces communications touchent la conduite professionnelle, la protection des données, la sécurité, la confidentialité et la formation spécialisée sur le règlement général sur la protection des données (RGPD ou GDPR) et d'autres lois internationales. Au-delà de la formation de sensibilisation de base, Cisco encourage les employés à suivre une formation complémentaire en offrant différentes options telles des sites Web, du contenu multimédia, des cours personnalisés et des certifications externes pertinentes (par exemple, « Certified Information Privacy Professional » [CIPP] de l'IAPP). Toutes les formations sont offertes à tous les employés et sont obligatoires pour ceux qui sont directement responsables des questions en matière de protection de la vie privée. Nous avons actuellement plus de 200 professionnels en matière de protection de la vie privée formés comme CIPP au sein de Cisco. Nous sommes d'avis que la sensibilisation et les compétences des employés dans ces disciplines sont essentielles au succès à long terme de Cisco et à l'importance accordée par tous à la création de produits dotés de mécanismes et fonctionnalités appropriés en matière de la protection de la vie privée.

Cisco Webex comprend de multiples fonctionnalités de protection et d'amélioration de la confidentialité qui sont configurables par le client ou l'administrateur de leur instance afin de répondre à leurs propres exigences de confidentialité. Par exemple, Cisco Webex inclut un accès basé sur les rôles aux réunions, ce qui permet à différents types de participants aux réunions de se faire assigner des autorisations, des accès et des contrôles appropriés. Nous permettons également aux clients de contrôler si leurs utilisateurs peuvent enregistrer des réunions, télécharger des fichiers ou utiliser des fonctionnalités supplémentaires qui entraîneraient une collecte de données additionnelle.

Pour aider les clients à effectuer une analyse d'impact sur la sécurité (SIA) et une évaluation des incidences sur la vie privée (PIA), Cisco peut fournir, sur demande et en vertu d'un accord de confidentialité, des

questionnaires normalisés qui ont été remplis par Cisco comme le « standardized information gathering » (SIG) et le « consensus assessment initiative questionnaires » (CAIQ).

3. Connaître son public

Cisco Webex est utilisé par des clients dans divers secteurs et a été conçu pour répondre à leurs besoins spécifiques. Cisco Webex est un outil essentiel pour les entreprises, les écoles, les établissements médicaux, les gouvernements et autres depuis plus de dix ans. La page Cisco Webex Trusted Platform sur Cisco Trust Center, qui se trouve ici, fournit des détails supplémentaires sur la façon dont les clients dans des secteurs verticaux spécifiques peuvent utiliser Cisco Webex tout en étant conformes à ses propres exigences de sécurité et de confidentialité. Par exemple, Cisco Webex est une solution approuvée par « FedRAMP » à l'usage du gouvernement des États-Unis et a été évaluée pour sa conformité en tant qu'associé en vertu de la loi américaine sur la portabilité et la responsabilité en matière d'assurance en matière de santé (HIPAA).

Cisco Webex est également un outil de confiance à utiliser dans les écoles et répond à la demande croissante de solutions d'enseignement à distance. Cisco fournit une documentation et des conseils détaillés aux écoles, aux arrondissements scolaires, aux universités et autres sur les données recueillies, leur utilisation, les destinataires tiers et la façon dont elles sont sécurisées. Du matériel pédagogique pour aider les parents et les tuteurs à comprendre comment Cisco Webex fonctionne et ce que cela signifie pour leurs enfants est également offert. Nous vous invitons à consulter la page qui se trouve ici pour plus de détails.

Cisco Webex offre un contrôle et une flexibilité complets aux hôtes et aux modérateurs de réunion afin qu'ils puissent mettre en place les mesures nécessaires et offrir des garanties appropriées basées sur le caractère sensible de leur discussion et le contenu qui doit être partagé. De plus, Cisco Webex s'intègre à Cisco Cloudlock, qui est une passerelle d'accès Cloud sécurisé (CASB) pour l'application des politiques de sécurité ainsi qu'à d'autres solutions de passerelle d'accès Cloud sécurisé disponible sur le marché.

Cisco Webex respecte les exigences en matière d'accessibilité et a été testé par rapport au modèle volontaire d'accessibilité des produits (VPAT) 2.1 afin de se conformer à la section 508 du US Rehabilitation Act. Cisco garde à jour les modèles de documents VPAT et autres documents relatifs sur notre site Web public pour s'assurer que nos produits répondent aux besoins d'accessibilité en constante évolution.

4. Transparence et équité

La transparence et l'équité sont les piliers du programme de protection des données et de confidentialité de Cisco. Notre déclaration de confidentialité en ligne donne un aperçu de la façon dont les renseignements personnels sont traités globalement à l'échelle de l'entreprise. Pour obtenir ces renseignements pour des produits spécifiques, nous avons également créé des fiches de données de confidentialité et des cartes qui complètent notre déclaration de confidentialité générale et fournissent des renseignements plus détaillés et propres au produit sur la façon dont les renseignements personnels sont recueillis, utilisés, traités, transférés, sécurisés et supprimés.

En outre, des notifications et des avis sont fournis dans l'application de manière proactive lorsque certaines fonctionnalités sont utilisées. Par exemple, si l'hôte de la réunion décide d'enregistrer une réunion, tous les participants en sont avertis par une fenêtre contextuelle et un message vocal automatisé. Cette notification est également envoyée aux nouveaux participants lorsqu'ils rejoignent la réunion. Une icône de cercle rouge est également visible pour tous les participants et demeure visible tant que l'enregistrement est activé.

5. Contrôle par l'utilisateur

Cisco est fermement convaincue que les particuliers doivent avoir le contrôle de leurs propres données et fournit un guide des meilleures pratiques pour des réunions sécurisées adressé aux administrateurs de site et aux hôtes afin de les aider à appliquer nos paramètres et pratiques recommandées pour renforcer la sécurité et la confidentialité.

La plateforme Cisco Webex Meetings a été conçue dans le respect de la vie privée des individus. Dès le début de l'expérience de réunion, les utilisateurs sont invités à activer l'accès à leur vidéo et à leur microphone (tous deux désactivés par défaut) puis, pour accéder aux fonctionnalités accessibles durant la réunion, telles que l'enregistrement, le sous-titrage et la transcription. Des icônes multilingues et accessibles avec des infobulles sont présentes dans toute l'interface utilisateur pour attirer l'attention sur ces fonctionnalités, ce qui permet à un individu de les activer ou désactiver à sa discrétion.

Pour s'assurer que les individus bénéficient d'une vision transparente sur la façon dont la plateforme Cisco Webex gère les données qui peuvent être collectées à l'aide de fonctionnalités basées sur la collaboration cognitive, Cisco a créé le papier blanc suivant pour décrire les données qui sont collectées, utilisées et stockées ainsi qu'expliquer comment les utilisateurs individuels peuvent activer ou désactiver ces services.

Nous tenons à vous remercier à nouveau de nous avoir donné l'occasion de répondre à votre déclaration et de nous permettre de vous exposer notre approche en lien avec la protection de la vie privée et notre produit de vidéoconférence Cisco Webex. Nous sommes déterminés à fournir à travers Cisco Webex, un outil de collaboration de calibre mondial qui assure une sécurité et une confidentialité élevées, protégeant et améliorant les fonctionnalités pour tous nos clients et utilisateurs. Si vous souhaitez obtenir des informations supplémentaires à mesure que vous vous penchez sur ces questions importantes, n'hésitez pas à communiquer avec le bureau de la protection de la vie privée de Cisco en envoyant un courriel à l'adresse privacy@cisco.com. Nous serions ravis de pouvoir travailler avec vous et vos équipes afin de vous assurer que la vie privée est respectée et protégée de manière appropriée lors de l'utilisation des technologies de vidéoconférence.

Veuillez accepter nos salutations les plus distinguées,

Harvey Jang
Vice-président et chef de la protection des renseignements personnels Cisco Systems, Inc.