COUR DE JUSTICE
DE L'UNION EUROPÉENNE

Analyse d'impact relative à la protection des données

(Article 39 du règlement 2018/1725)

Date : 19/02/2021

Numéro de référence : curia-grfc.dginfo.dti.d(2021)1294392

OUTILS DE VISIOCONFÉRENCE

Une analyse d'impact doit contenir une description systématique du traitement et des finalités, une évaluation de la nécessité et de la proportionnalité ainsi qu'une évaluation des risques pour les droits et libertés des personnes concernées et les mesures envisagées pour faire face à ces risques. L'analyse doit en outre documenter la consultation du délégué à la protection des données ainsi que, le cas échéant, des parties concernées ou leurs représentants.

La description du traitement et l'évaluation de la nécessité et de la proportionnalité sont effectuées à l'aide du formulaire pour documenter un traitement. Ce même formulaire identifie également les raisons pour effectuer une analyse d'impact.

Le formulaire pour documenter le traitement, rempli de manière détaillée, fait partie intégrante de l'analyse d'impact et doit être joint en annexe.

Sommaire

L'objet de la présente analyse est l'utilisation de Cisco Webex pour certaines visioconférences, comme notamment des réunions internes qui ne concernent pas des informations sensibles ou confidentielles ou des formations à distance, réunions collaboratives ou webinaires avec des participants externes.

Pour des visioconférences concernant des informations sensibles ou confidentielles, d'autres outils sont à disposition « on-premise ».

I. Description détaillée du traitement et des outils utilisés

Pour les besoins de l'analyse d'impact, il convient de compléter le cas échéant la description du traitement avec d'autres éléments pertinents, dont les flux internes et/ou les outils utilisés.

Description des outils

Cisco offre des solutions pour tenir des visioconférences. Afin d'assurer la continuité du service et assurer le bon fonctionnement de l'institution (notamment dans le cadre de la gestion de crise et la période de travail à domicile obligatoire), la Cour de justice de l'Union européenne (ci-après « Cour ») souhaite acheter différents services de Cisco :

- **Cisco Webex Meetings** est une solution de visioconférence qui fonctionne sur base du Cloud et qui sera également utilisée pour les formations à distance.
- **Cisco Webex Events** permet l'organisation d'événements et webinars en ligne, également dans le Cloud.
- **Cisco Webex Support** permet au Helpdesk interne d'offrir une assistance technique à distance, avec contrôle du bureau à distance.
- **Cisco Video Mesh** est une solution qui permettra l'organisation de visioconférences sur un serveur local de la Cour, en limitant, dans certaines conditions, le transfert de données vers les serveurs de Cisco.

Le service suivant est déjà utilisé par la Cour :

- **Cisco Meeting Server** permet la tenue de visioconférences en interne à l'institution (on-premise), sans transmission de données à Cisco. Cette solution continuera à être utilisé par la Cour pour une grande partie des visioconférences et ne fait pas l'objet de la présente analyse.

L'utilisation de certains services de Cisco (autre que Cisco Meeting Server) nécessite le traitement de données à caractère personnel par Cisco ainsi que, pour l'instant, leur transfert en dehors de l'Union européenne.

Le contrat avec Cisco couvre également l'utilisation de Cisco Unified Communications Manager (CUCM) qui fonctionne « on-premises ». Son utilisation ne fait pas l'objet de la présente analyse d'impact. Les autres outils couverts par le contrat (à savoir Cisco Webex Training, Cisco Webex Teams, Cisco Webex Calling, UCM Cloud Calling ou CUCM Hosted Collaboration Solution) ne seront pas utilisés par la Cour.

Flux des données à caractère personnel

Le flux des données à caractère personnel pour l'utilisation de **Cisco Webex Meetings, Cisco Webex Events** et **Cisco Webex Support** est expliqué dans le « Cisco Webex Meetings data privacy sheet » ainsi que le « Cisco Webex Meetings Data Map » (voir annexes).

L'utilisation de ces outils nécessite la transmission de données à caractère personnel à Cisco afin de vérifier la validité de la licence (données d'identification) et, lorsque la visioconférence a lieu dans le Cloud, la transmission des données à caractère personnel concernant l'organisation et le contenu de la visioconférence.

Un « End-to-end encryption » par défaut (au niveau du paramétrage des outils) avec clé privée non-détenu par Cisco sera testé afin de valider cette mesure de sécurité supplémentaire pour des visioconférences dans le cloud (et donc notamment avec des participants externes).

L'utilisation du **Cisco Video Mesh** nécessite également le traitement des données d'identification et d'authentification par Cisco afin de vérifier la validité de la licence. Le contenu de la visioconférence n'est pas traité par Cisco, à condition que l'ensemble des participants soient internes à l'institution[1] et que le serveur interne n'est pas surchargé.

Le Video Mesh permet toutefois de bloquer éventuellement l'utilisation du Cloud pour une visioconférence avec des participants internes.

En outre, Cisco mettra prochainement à disposition une option (« Private meeting ») qui permettra à l'organisateur de la visioconférence avec des participants internes de choisir si la visioconférence peut se tenir dans le Cloud ou pas. Cette dernière option n'est toutefois pas à disposition à ce stade.

---

[1] La notion de participants internes désigne les personnes qui sont connectées au réseau de la Cour avec un ordinateur fourni par la Cour. La connexion peut se faire à partir du bureau ou en mode télétravail. Dans ce cas, la connexion est établie par un réseau VPN.

Une visioconférence avec une personne externe nécessite le traitement des données sur la visioconférence par Cisco. Le contenu de la visioconférence peut dans ce cas être protégé par un « end-to-end encryption » (voir supra).

Vu qu'une vidéoconférence peut donc également avoir lieu sur le Cloud, le Video Mesh n'offre pas une protection absolue. Son utilisation réduit toutefois le nombre de visioconférences sur le Cloud et permet notamment de suivre l'utilisation de Webex.

Lors d'une visioconférence avec **Cisco Meeting Server**, l'ensemble des données est traité en local sur le serveur de la Cour. L'utilisation de cette solution nécessite par contre l'intervention d'un technicien de la Cour pour organiser la visioconférence.

Dans le cadre du support et l'offre d'assistance technique **Cisco Technical Assistance,** Cisco doit, le cas échéant, traiter des données à caractère personnel afin de traiter la demande et analyser le problème. Les données sont dans ce cas transmis dans le cadre de la demande d'assistance.

A priori, les données suivantes sont traitées par Cisco et ses sous-traitants des outils Webex :

Data Privacy Sheet (Version 4.5, janvier 2021)	
User information	• Name[2] • Email Address[3] • Password • IP Address • Browser • Phone Number (Optional) • Mailing Address (Optional) • Geographic region • Avatar (Optional) • User information included in the Customer's Active Directory (if synched) • • Unique User ID (UUID)
Host and usage information	• IP Address • User Agent Identifier • Hardware Type • Operating System Type and Version • Client Version

[2] Remplacé par un pseudonyme
[3] Remplacé par un pseudonyme

	• IP Addresses Along the Network Path
	• MAC Address of Your Client (As Applicable)
	• Service Version
	• Actions Taken
	• Geographic Region
	• Meeting Session Information (e.g., date and time, frequency, average and actual duration, quantity, quality, network activity, and network connectivity)
	• Number of Meetings
	• Number of Screen-Sharing and NonScreen-Sharing Sessions
	• Number of Participants
	• Screen resolution
	• Join Method
	• Performance, Troubleshooting and Diagnostics information
	• Meeting Host Information*
	  ○ Host Name[4] and ID
	  ○ Meeting Site URL
	  ○ Meeting Start/End Time
	• Meeting title
	• Call attendee information, including email addresses[5], IP address, username[6], phone numbers, room device information
	* Used for billing purpose

User generated information	• Meeting Recordings • Transcriptions of Call Recordings (optional, only applicable if enabled) • Uploaded Files (for Webex Events and Training only)

[4] Remplacé par un pseudonyme
[5] Remplacé par un pseudonyme pour les utilisateurs de la Cour
[6] Remplacé par un pseudonyme pour les utilisateurs de la Cour

Cisco Technical Assistance (TAC) Service Delivery (version 1.3, 25 septembre 2020)	
TAC Support information	• Name • Email Address • Phone Number of the Employee Appointed to Open the Service Request • Authentication Information (exclusive of passwords) • Information About the Condition of the System • Registry Data About Software Installations and Hardware Configurations • Error-Tracking File
Customer Case Attachment	Cisco TAC does not intentionally collect or process personal data via Customer Case Attachments. We instruct customers to provide the least amount of personal data possible. However, unsolicited personal data may be contained in the files provided by customers. For illustrative purposes only, the list below includes the types of data that may be processed for Customer Case Attachments for the purpose of providing support: • Device Configuration (e.g., running • config and startup config, SNMP • Strings (masked); Interface • description • Command Line Interface (CLI) (i.e., • Show Commands, such as Show • Version) • Product Identification Numbers • Serial Numbers • Host Names • Sysdescription (has device location) • IP Addresses • Operating System (OS) Feature Sets • OS Software Versions

	• Hardware Versions • Installed Memory • Installed Flash • Boot Versions • Chassis Series • Slot IDs • Card Types • Card Families • Firmware Versions • MAC Address • • SNMP MIBs (ACLs, CDP)
Other	
Billing information	Meeting Host Information User information

Il y a toutefois lieu de relever également que l'appendix aux clauses contractuelles relatives aux transferts des données à caractère personnel conclu entre la Cour et Cisco ne contient pas les données suivantes en tant que données qui peuvent être transférées en dehors de l'UE/EEE :

Registration Information (or user information)	• Geographic region • User information included in the Customer's Active Directory (if synched) • • Unique User ID (UUID) • Phone number (Optional) • Mailing address (Optional) • Avatar (Optional)
Host and usage information	• Geographic Region • Call attendee information, including email addresses[7], IP address, username[8], phone numbers, room device information
User generated information	• Transcriptions of Call Recordings

[7] Remplacé par un pseudonyme pour le personnel de la Cour
[8] Remplacé par un pseudonyme pour le personnel de la Cour

Il s'ensuit notamment que le contrat conclu avec Cisco ne permettra pas que les données des participants tiers (autre que le personnel de la Cour) soient transférées (notamment l'adresse courriel et le nom). Ces données peuvent toutefois être traitées par Cisco[9] au sein de l'UE/EEE et le Royaume-Uni (pendant la période de 4 +2 mois prévu dans l'accord de commerce et de coopération entre l'Union européenne et la Communauté européenne de l'énergie atomique, d'une part, et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, d'autre part).

En ce qui concerne l'assistance technique, il convient de préciser que les demandes d'assistance passent d'abord par le Helpdesk interne de la Cour. Le Helpdesk de la Cour évaluera le besoin de contacter Cisco et veillera dans ce cadre à limiter la transmission des données à caractère personnel au strict nécessaire pour régler le problème.

Sous réserve de ces précisions, le traitement des données par les différentes solutions se présente ainsi :

Solution	Cisco Webex Meetings, Events et Training	Cisco Webex avec Video Mesh ('on premises')	Cisco Webex avec Video Mesh (avec utilisateur externe)	Cisco Meeting Server
Registration Information	✓	✓	✓	×
Host and usage information	✓	✓	✓	×
User generated information	✓	×	Selon le cas[10]	×
Billing information	✓	✓	✓	×

[9] Voir l'article 11.2 sous a, point ii, du contrat : « External participants supply their information at time of logging in into the system with their desired name, potentially providing personal data ».

[10] La Cour va tester la mise en place par défaut d'un « end-to-end-encryption ». Cette option est également disponible aux utilisateurs qui peuvent l'activer manuellement afin de rendre le contenu de la visioconférence inaccessible à Cisco.

Transferts des données effectués par Cisco

Les pays dans lesquels les données peuvent être traitées dans le cadre des services cloud sont ceux où Cisco ou son sous-traitant dispose d'un Data Center, à savoir :

- États-Unis (Cisco et sous-traitant Amazon Web Services)
- Royaume-Uni
- Inde
- Singapore (Cisco et sous-traitant Amazon Web Services)
- Australie
- Pays-Bas (UE)
- Allemagne (UE – sous-traitant Amazon Web Services)
- Japon (décision d'adéquation)
- Canada (décision d'adéquation)

Toutefois, Cisco offre certaines mesures pour limiter les transferts. Ainsi, il est indiqué dans le Data Privacy Sheet que les « User generated information » soient stockées dans le centre de données le plus proche de l'endroit où se trouve le client ou comme prévu lors du processus de commande.

Pour la Cour, les serveurs aux Pays-Bas et l'Allemagne seront donc utilisés pour traiter le « User generated information ». Cette précision est reprise explicitement dans le contrat.

Conformément au contrat, les serveurs au Royaume-Uni peuvent également être utilisés, en respectant les conditions[11] de l'accord de commerce et de

[11] Cet accord prévoit que les parties « s'abstiennent d'imposer, en ce qui concerne les flux de données transfrontières entre elles, des restrictions telles que : [...] l'exigence que les données soient localisées sur le territoire de la Partie à des fins de stockage ou de traitement ; [ou] l'interdiction de stocker ou de traiter les données sur le territoire de l'autre Partie » (voir l'article DIGIT.6 Flux de données transfrontières de l'accord dans le chapitre sur le commerce numérique).
En outre, pendant une période de 6 mois (4 mois + 2 mois de prolongation en absence d'opposition) la transmission de données à caractère personnel de l'Union au Royaume-Uni n'est pas considérée comme un transfert vers un pays tiers en vertu du droit de l'Union (sous réserve que le droit du Royaume-Uni ne soit pas modifié de manière inappropriée) (voir Article FINPROV.10A : Disposition provisoire concernant la transmission de données à caractère personnel au Royaume-Uni).
Ensuite, il est attendu que la Commission adoptera une décision d'adéquation qui autorisera donc le transfert des données à caractère personnel vers le Royaume-Uni. En absence d'une décision d'adéquation, le transfert de données pourra néanmoins avoir lieu sur base de garanties appropriées qui devront être convenues.

coopération entre l'Union européenne et la Communauté européenne de l'énergie atomique, d'une part, et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, d'autre part. Après la période de transition spécifique, le transfert doit notamment être couvert par une décision d'adéquation ou des garanties appropriées.

Pour le « Billing information », il est indiqué explicitement que les données sont transférées vers les États-Unis. Les données utilisées pour le Webex Analytics Platform sont également transférées vers les États-Unis. Il s'agit de « Host and usage information ».

Le transfert vers les États-Unis sera maintenu jusqu'au 31 décembre 2021, afin de permettre à Cisco de prendre les mesures nécessaires pour mettre fin à ce transfert.

Ce délai peut être prolongé par les parties au contrat.

Le cas échéant, la Cour peut terminer le contrat lorsque Cisco ne respecte pas son engagement d'arrêter le transfert vers les États-Unis.

Finalement, les clauses contractuelles spécifiques aux transferts limitent les données qui sont transférées par Cisco en dehors de l'UE/EEE (voir supra).

Dans le cadre du support, un transfert de certaines données peut également avoir lieu vers les États-Unis ou d'autres pays. Il s'agit notamment de coordonnées de contact et éventuellement des données pour décrire le cas. Ces données seront toutefois limitées à ceux qui sont strictement nécessaires pour résoudre le cas. Leur pertinence et les éventuels risques doivent être évalués au cas par cas. Avant qu'une demande d'assistance soit ouverte auprès de Cisco, la Cour fait également appel à son propre sous-traitant pour la fourniture d'une assistance technique sur les produits Cisco.

Pseudonymisation du nom et adresse courriel

Le nom de l'utilisateur et son adresse courriel sont remplacés par un pseudonyme lors de l'activation de la licence par la Cour.

La pseudonymisation est mise en place en créant une adresse « alias » dans Outlook avec un nom générique. Ces données sont transmises dans l'annuaire Cisco dans le Cloud, par une synchronisation de l'Active Directory limitée à ces données :

Nom : xxxxxxx

Adresse E-mail : xxxxxxx@curia.europa.eu

L'enregistrement au service avec l'initialisation du mot de passe est effectué par l'utilisateur, qui reçoit dans sa boite officielle de la Cour le message en

provenance de Cisco et à destination du compte pseudonymisé xxxxxxx@curia.europa.eu

Pour utiliser le service, à la première utilisation, l'utilisateur doit s'authentifier avec son compte xxxxxxx@curia.europa.eu sur son poste de la Cour dans l'application Webex Meeting (productivity tools) et/ou Jabber.

L'Add-in WebEx Meeting dans Outlook va être utilisé pour générer le lien de l'invitation en utilisant le compte générique xxxxxxx@curia.europa.eu renseigné dans les productivity tools de Webex Meeting.

L'invitation est envoyée aux participants depuis Outlook avec l'adresse officielle de l'expéditeur, avec comme destinataires les adresses officielles des participants. L'invitation contient le lien pour joindre la réunion, lien qui a donc été généré avec le compte générique xxxxxxx@curia.europa.eu.

Toutefois, afin de respecter la pseudonymisation l'accès web aux services Webex Meeting via l'URL https://curia.webex.com ne devra pas être utilisé pour organiser des réunions. Il existe à cet égard la possibilité de bloquer les utilisateurs Webex anonymisés de changer leur nom et prénom sur le portail https://curia.webex.com ou même de leur bloquer l'accès au portail pour les forcer à utiliser le plug-in Webex Productivity Tool installé sur le poste de travail de la Cour.

Durée de conservation

La durée de conservation des données est précisée dans le Data Privacy Sheet de Cisco. Cette durée concerne également le traitement de données fait ultérieurement par Cisco aux fins de ses propres obligations de contrôle financier et d'audit.

La Cour conserve les données que pendant la durée nécessaire pour la gestion des licences. Un éventuel enregistrement d'une visioconférence relèvera de la responsabilité de l'organisateur qui devra prendre dans ce cas les mesures nécessaires pour respecter les obligations en matière de protection des données à caractère personnel. Un enregistrement n'est toutefois pas possible avec un « End-to-end encryption ».

Lignes directrices et information aux utilisateurs

Des lignes directrices pour les utilisateurs seront établies afin de les guider dans le choix de l'outil de visioconférence : Cisco Webex, Cisco Meeting Server ou Jabber (Soft Phone avec option vidéo « one to one » « on-premises »).

Il convient notamment d'attirer l'attention à la nécessité d'utiliser Cisco Meeting Server ou l'outil Jabber pour des discussions d'informations confidentielles ou personnelles. Une grande partie des réunions internes à la Cour devraient se dérouler avec ces outils Les lignes directrices devront contenir également une

explication sur le traitement de données à caractère personnel réalisé par Cisco, les droits des personnes ainsi que les mesures à prendre afin de respecter les droits d'autres personnes qui peuvent le cas échéant participer à une visioconférence organisée par la Cour.

Autres éléments

Cisco est également soumis à des règles d'entreprises contraignantes, approuvées par l'autorité de contrôle des Pays-Bas sous la directive 95/46/CE.

Les autres normes appliquées par Cisco sont reprises dans le Data Privacy Sheet.

II. Nécessité et proportionnalité

Évaluez la nécessité et la proportionnalité des opérations de traitement.

Afin d'assurer la continuité du service et assurer le bon fonctionnement de l'institution (notamment dans le cadre de la gestion de crise et la période de travail à domicile obligatoire), la Cour a besoin de disposer d'un outil de visioconférence qui répond à ces besoins.

Cisco offre des services de visioconférences de qualité et dans un environnement sécurisé. Les outils Cisco sont en outre intégrés dans l'environnement de travail de la Cour (intégration avec Outlook et Jabber).

L'utilisation d'un service Cloud pour les visioconférences nécessite la transmission de données d'identification et d'authentification afin d'assurer le bon déroulement de la visioconférence et d'en assurer la sécurité.

Dans certains cas, le contenu de la visioconférence doit également être transmis via le service Cloud, notamment lorsqu'un utilisateur externe y participe ou lorsque les serveurs de la Cour ne peuvent pas répondre à l'ensemble des demandes. L'utilisation du Cloud est dans ces cas nécessaire afin de pouvoir offrir l'ensemble des services de visioconférences aux utilisateurs de la Cour.

Lorsque des sujets confidentiels ou sensibles doivent être traités en visioconférence (y compris des informations personnelles), la Cour préconise l'utilisation de Cisco Meeting Server, afin d'éviter le traitement de ces informations dans le Cloud. Cette solution nécessite toutefois une réservation d'un créneau et l'intervention d'un technicien et ne peut donc pas être mise en place pour répondre à l'ensemble des demandes de visioconférence.

Afin de réduire le besoin d'organiser des visioconférences pour discuter des sujets sensibles, la Cour mettra également en place un système de « Soft Phone » qui permettra de contacter d'autres personnes au sein de la Cour par l'ordinateur de travail (en audio avec plusieurs personnes ou en vidéo « one to one » « on premises »).

La transmission de certaines données à caractère personnel à Cisco est également limitée à des données pseudonymisées et ne permettent donc pas à Cisco d'identifier directement la personne concernée.

Eu égard à, d'une part, l'importance pour la Cour de disposer d'un outil de visioconférence performant et, d'autre part, les mesures prises pour limiter le transfert de données à caractère personnel et ainsi les risques y relatives, le traitement est proportionnel.

III. Consultation

Indiquez les personnes et entités consultées ainsi que la date de consultation. Le délégué à la protection des données doit être consulté dans le cadre de l'analyse d'impact. Le cas échéant, l'avis des personnes concernées ou de leurs représentants est également demandé.

Un groupe de personnes de différents services ont participé aux tests de l'outil afin de confirmer que l'outil correspond à leurs besoins.

Le délégué à la protection des données et le Conseiller juridique ont été consultés avant la conclusion du contrat.

Les clauses contractuelles concernant le transfert doivent être soumises pour autorisation au CEPD. L'ensemble du contrat ainsi que la présente analyse sont également transmis au CEPD afin de fournir une information utile sur les mesures supplémentaires mises en œuvre pour assurer une protection appropriée des données à caractère personnel. Les services « Cloud » ne seront activés qu'après l'autorisation du CEPD pour l'utilisation des garanties appropriées pour encadrer les transferts.

IV. Évaluation des risques

Indiquez dans le tableau les différents risques identifiés, l'origine du risque et ses conséquences pour la personne concernée. Procédez à l'évaluation de chaque risque sans que des mesures soient prises. Indiquez ensuite les mesures envisagées et procédez à une nouvelle évaluation du risque résiduel.

	Identification du risque			Évaluation[12]				Risque résiduel		
N°	Événement	Cause	Conséquences potentielles	Probabilité	Impact pour la personne concernée	Risque	Réponse au risque	Probabilité résiduelle	Impact pour la personne concernée résiduel	Risque résiduel
1	Transferts des données à caractère personnel vers les États-Unis (dans le cadre des services Cloud)	Des données d'identification sont transférées par Cisco aux États-Unis pour réaliser la facturation du service et offrir des outils d'analyse.	Volume important de données (ensemble du personnel de la Cour) – Perte de contrôle sur les données – Accès non autorisés aux données par une autorité d'un pays tiers – Absence de droits et de recours effectifs en	3	3	↗	• Les données permettant l'identification directe de la personne sont pseudonymisées par la Cour, avant leur transmission à Cisco (uniquement pour le	3	1	→

[12] Critères d'évaluation du risque :

			Impact		
			1	2	3
			Pas significatif	Modéré	Important
Probabilité	3	Il est fort probable que la menace survienne	Moyen	Élevé	Élevé
	2	Il est probable que la menace survienne	Bas	Moyen	Élevé
	1	Il est peu probable que la menace survienne	Bas	Bas	Moyen

			cas d'un accès par les autorités américaines aux données sur base du FISA 702 et EO 12333				• personnel de la Cour). • Le contrat n'autorise pas à Cisco de transférer des données d'identification des participants aux visioconférences (notamment pour les participants externes à la Cour). • Le contrat prévoit des obligations pour Cisco afin de contester de telles demandes d'accès et de fournir une information dans la mesure du possible. • Le contrat contient une clause spécifique sur le dédommagement. • Cisco s'engage à arrêter le transfert des données vers les États-Unis			
2	Transferts des données à caractère personnel vers les États-Unis et en dehors de l'UE/EEE dans le cadre des services de support	Des données d'identification de la personne qui ouvre la demande d'assistance et des données liées au problème sont transférées vers les États-Unis et, le cas échéant, des centres d'aides de Cisco dans d'autres pays tiers.	Perte de contrôle sur les données – Accès non autorisés aux données par une autorité d'un pays tiers – Absence de droits et de recours effectifs en cas d'un accès par les autorités américaines aux données sur base du FISA 702 et EO 12333	1	2	→	• Limitation des données décrivant le cas au strict nécessaire et, le cas échéant, après anonymisation (si possible) ou pseudonymisation	1	1	↘
3	Accès aux données transmis à un serveur localisé dans l'UE/EEE par une autorité d'un pays tiers (données d'identification)	Les autorités américaines peuvent adresser une demande contraignante à Cisco afin d'accéder aux données détenues	Perte de contrôle sur les données – Absence de droits et de recours effectifs en cas d'un accès par les autorités américaines aux	1	3	→	• Les données permettant l'identification directe de la personne sont pseudonymisées par la	1	2	↘

		par elle sur base du FISA 702, EO 12333 ou le Cloud Act.	données sur base du FISA 702 et EO 12334 – Accès aux données sans intervention des autorités judiciaires de l'UE dans le cas d'une demande au titre du Cloud Act.				Cour, avant leur transmission à Cisco (uniquement pour le personnel de la Cour). • Une information sera fournie aux participants externes afin de les informer des éventuels risques et les mesures qu'ils peuvent prendre. • Le contrat prévoit des obligations pour Cisco afin de contester de telles demandes d'accès et de fournir une information dans la mesure du possible. • Le contrat contient une clause spécifique sur le dédommagement.			
4	Accès aux données transmis à un serveur localisé dans l'UE/EEE par une autorité d'un pays tiers (données de contenu)	Les autorités américaines peuvent adresser une demande contraignante à Cisco afin d'accéder aux données détenues par elle sur base du FISA 702, EO 12333 ou le Cloud Act.	Perte de confidentialité de données (éventuellement protégées par le secret professionnel) – Perte de contrôle sur les données – Absence de droits et de recours effectifs en cas d'un accès par les autorités américaines aux données sur base du FISA 702 et EO 12334 – Accès aux données sans intervention des autorités judiciaires de l'UE dans le cas d'une demande au titre du Cloud Act.	1	3	→	• Pour les réunions lors desquelles des données à caractère personnel sensibles ou autrement confidentielles doivent être discutées, le Cisco Meeting Server (« on-premise ») ou le « Soft Phone » doit être utilisé. • Le contrat contient une clause spécifique sur le dédommagement. • Le contenu de la visioconférence peut faire	1	1	↘

							l'objet d'un « end-to-end encryption »				
5	Information pas claire sur le traitement des données à caractère personnel effectué	Les documents contractuels ne sont pas clairs ou contradictoires. Les documents contiennent des références vers des documents accessibles sur internet qui peuvent être modifiés par Cisco.	Perte de contrôle sur les données – Difficulté d'exercer ses droits – Information incomplète ou erronée sur le traitement	3	1	→	• Les documents applicables sont joints au contrat. Le contrat précise que les dispositions du contrat valent en cas d'indications contradictoires dans les autres documents. • Une information sur le traitement et le transfert des données sera fournie dans le cadre du guide d'utilisation. • Une information doit également être fournie aux participants externes à la Cour. • Une documentation est établie et la présente analyse d'impact rendu accessible au sein de la	2	1	↘

							Cour.			
6	Transferts de données à caractère personnel vers le Royaume-Uni	Des données d'identification et de contenues sont transférées par Cisco au Royaume-Uni pour offrir les services de visioconférence lorsque le serveur situé au Royaume-Uni est utilisé comme un des serveurs les plus proches de Luxembourg, siège de la Cour.	Perte de contrôle sur les données	3	1	→	Les conditions de l'accord de commerce et de coopération entre l'Union européenne et la Communauté européenne de l'énergie atomique, d'une part, et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, d'autre part, sont prises en compte et seront respectées.	1	1	↘
7	Intrusion d'un tiers dans une visioconférence qui obtient accès aux informations discutés	Mesures de sécurité insuffisantes pour protéger l'accès (mot de passe, numéro d'identification de la réunion, lien)	Perte de confidentialité de données (éventuellement protégées par le secret professionnel) – Perte de contrôle sur les données – Accès non autorisés aux informations discutées, y compris les données à caractère personnel d'un tiers	2	3	↗	• Mise en place des mesures de sécurité appropriées par Cisco • Information aux utilisateurs sur le choix de l'outil à utiliser et les bonnes pratiques en matière de sécurité (protection des accès, utilisation d'une salle d'attente). • Utilisation de la visioconférence « on-premise » ou « Soft Phone » lorsqu'il s'agit d'une discussion confidentielle.	1	1	↘
8	Manque de précision sur la localisation des données et transfert vers un autre pays tiers (autre qu'US ou UK)	Absence d'adaptation du fonctionnement de Cisco à l'arrêt Schrems II	Perte de contrôle sur les données – Un transfert des données à caractère personnel peut avoir lieu sans mécanisme approprié et sans protection adéquate des données à caractère personnel.	3	2	↗	• Les données permettant l'identification directe de la personne sont pseudonymisées par la Cour, avant leur transmission à Cisco	1	1	↘

							(uniquement pour le personnel de la Cour). • Les clauses contractuelles précisent la localisation des données • Dans le cadre du support, seulement les données nécessaires pour la résolution du cas seront transmises			
9	Profilage ou vente des données réalisée par Cisco	Cisco utilise les données à caractère personnel transmis afin de réaliser un profilage des utilisateurs ou pour les revendre à un tiers	Perte de contrôle sur les données – Absence d'information sur le traitement	2	2	→	• Les données peuvent uniquement être traitées sur base des instructions du responsable du traitement. • Cisco précise qu'elle n'utilise pas les données afin de fournir des publicités (voir Data Privacy Sheet). • Cisco s'engage dans le contrat de ne pas revendre les données.	1	1	↘
10	Transmission non prévue de données vers Cisco, permettant notamment l'identification des utilisateurs par Cisco	À cause d'une erreur humaine, des données (sans pseudonyme) sont transmises	Identification des utilisateurs qui enlève la protection offerte par la pseudonymisation	2	2	→	• Une procédure appropriée sera mise en place par la DTI (avec synchronisation automatisée des données pseudonymisées) • Cisco s'engage à respecter la pseudonymisation.	1	2	↘
11	Non-respect de la pseudonymisation à l'aide d'autres données éventuellement traitées.	À l'aide d'autres données, une personne peut éventuellement être identifiée, malgré la pseudonymisation.	Identification des utilisateurs qui enlève la protection offerte par la pseudonymisation	2	2	→	Cisco s'engage à respecter la pseudonymisation.	1	2	↘

12	Cisco ne respecte pas les immunités et privilèges dont bénéficient les institutions européennes	Cisco demande que le contrat contienne une clause qui l'autorise à transmettre des données aux autorités nationales sans en informer l'institution.	Perte de contrôle sur les données – Toute donnée à caractère personnel discuté lors d'une visioconférence peut être transmise par Cisco à une autorité nationale	1	3	→	• Pour les réunions lors desquelles des données à caractère personnel sensibles ou autrement confidentielles doivent être discutées, le Cisco Meeting Server (on-premise) ou une autre solution doit être utilisé. • Le « end-to-end encryption » peut être utilisé.	1	1	↘

Une analyse conforme à la norme ISO/IEC 270005 de l'ensemble des risques liés à l'utilisation des outils Cisco figure également en annexe.

V. Conclusion sur l'acceptation du risque

Tenant compte des mesures prises ainsi que la nécessité et la proportionnalité du traitement, indiquez si le risque résiduel peut être accepté. Si le risque ne peut être atténué et engendre un risque élevé pour les droits et libertés de personnes, il convient de consulter le Contrôleur européen de la protection des données préalablement au traitement.

Données d'identification

Les risques résiduels concernent notamment les données d'identification.

Les données d'identification font l'objet d'un transfert vers les États-Unis en attendant l'adaptation par Cisco de ces procédures de traitement. Les données d'identification peuvent également faire l'objet d'un transfert vers les autorités des États-Unis en application du FISA 702 ou le Cloud Act. Cisco s'engage toutefois de contester de telles demandes.

La mesure de pseudonymisation pourrait éventuellement être contournée par un croisement de données non prévu ou un traitement de données non prévu (par exemple en adressant un courrier électronique à une personne qui y répond avec son adresse nominative). Cisco s'est toutefois engagé à respecter la pseudonymisation.

Vu qu'il s'agit de simples données d'identification, les risques pour les personnes concernées sont limités. Le risque est donc acceptable.

Données de contenu

L'utilisation du Cloud pour une visioconférence nécessite également la transmission des données vers Cisco. Ces données peuvent également faire l'objet d'un transfert vers les autorités des États-Unis en application du FISA 702 ou le Cloud Act.

Des lignes directrices internes prévoient toutefois que les outils Webex ne seront pas utilisés pour des discussions qui portent sur des éléments confidentiels, sensibles ou personnels.

En outre, un « end-to-end encryption » peut être utilisé pour rendre le contenu de la visioconférence inaccessible à des tiers (dont Cisco). Cette option sera en outre testée afin de le rendre l'option par défaut.

Le risque qu'une visioconférence dans Webex porte néanmoins sur une information confidentielle, sensible ou personnelle est donc réduit et est acceptable.

Autres mesures

Les autres mesures, dont notamment l'engagement de mettre fin au transfert des données vers les États-Unis, permettent également de réduire les risques à un niveau acceptable.

VI. Validation par le responsable du traitement

Ajoutez la fonction, le nom, la date et la signature. Précisez également l'échéance pour la prochaine révision. Il est conseillé de revoir périodiquement l'analyse d'impact. Une révision s'impose au moins quand il se produit une modification du risque (p. ex. : une évolution technologique qui impacte les mesures prises).

Date : 19/02/2021

Nom : Mme Raluca PEICA [redacted]

Fonction : Directeur, Direction des technologies de l'information

Prochaine révision : (a) Lorsque Cisco adaptera ses flux afin d'arrêter le transfert des données vers les États-Unis ou tout autre changement ayant un impact sur le transfert des données ou, (b) au plus tard, dans 2 ans.

VII. Annexes et modifications

La documentation sur le traitement doit être annexée à l'analyse d'impact. Ajoutez également tout autre document qui précise le traitement (guide, notice d'information, formulaires...).

L'analyse d'impact doit être révisée périodiquement. Indiquez également les modifications apportées à l'analyse lors d'une révision.

N°	Annexe	Date
1	Cisco Webex Meetings data privacy sheet	1/2021
2	Cisco Webex Meetings Data Map	18/12/2018
3	Cisco Technical Assistance (TAC) Service Delivery	25/09/2020
4	Analyse des risques conforme à la norme ISO/IEC 270005	20/01/2021

N°	Révision	Date
1	Version initiale	19/02/2021