ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΕΛΕΓΚΤΙΚΟ ΣΥΝΕΔΡΙΟ
ΥΠΗΡΕΣΙΑ ΕΠΙΤΡΟΠΟΥ
ΣΤΗ ΓΡΑΜΜΑΤΕΙΑ
ΚΛΙΜΑΚΙΟ Ζ΄
Ταχ. Δ/νση: Βουρνάζου 4 &Τσόχα
Τ.Κ.:11521 ΑΘΗΝΑ
Πληροφορίες: Μαρίνα Πέτρου
Τηλέφωνο:213 1309795,783
Fax: 210 6470255
Γραφείο: 2.23, 2ο όροφος
email: klimakio05@elsyn.gr

Αθήνα, 16/03/2021
Αριθμ. Πρωτ.: 8842

ΠΡΟΣ: Κοινωνία της Πληροφορίας
Τμήμα Διαχείρισης Συμβάσεων
κ. Γεώργιος Χριστόπουλος
τηλ. 213 1300839
email: info@ktpae.gr

ΘΕΜΑ : Κοινοποίηση Πράξης Ελεγκτικού Συνεδρίου

Σας κοινοποιούμε αντίγραφο της **109/2021** Πράξης του **Ζ΄ Κλιμακίου** του Ελεγκτικού Συνεδρίου για τις δικές σας ενέργειες, το οποίο πρέπει να κοινοποιήσετε αμελλητί με ηλεκτρονικό ταχυδρομείο σε όλους τους συμμετέχοντες στην ελεγχθείσα διαδικασία ανάδειξης αναδόχου (άρθρο 326 παρ. 2 του ν. 4700/2020, Α΄ 127).

Σας γνωρίζουμε ότι μπορείτε να προβείτε άμεσα στην υπογραφή του ελεγχθέντος σχεδίου σύμβασης, χωρίς να αναμένετε την πάροδο της 15νθήμερης προθεσμίας, δεδομένου ότι, σύμφωνα με τη διάταξη του άρθρου 328 παρ. 1 του ν.4700/2020 (Α΄ 127), κατά της Πράξης αυτής δεν προβλέπεται άσκηση προσφυγής ανάκλησης ενώπιον του Έβδομου Τμήματος του Ελεγκτικού Συνεδρίου.

Η ΓΡΑΜΜΑΤΕΑΣ ΤΟΥ Ζ΄ ΚΛΙΜΑΚΙΟΥ

ΜΑΡΙΝΑ ΠΕΤΡΟΥ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΤΟ ΕΛΕΓΚΤΙΚΟ ΣΥΝΕΔΡΙΟ

Ζ΄ ΚΛΙΜΑΚΙΟ

ΠΡΑΞΗ 109 /2021

Αποτελούμενο από τον Πρόεδρο του Κλιμακίου Σταμάτιο Πουλή, Σύμβουλο, και τα μέλη Θεόδωρο Μαυροβουνιώτη και Αθανασία – Μυροφόρα Σιδηροπούλου, Παρέδρους.

Συνήλθε σε τηλεδιάσκεψη στις 8 Μαρτίου 2021, κατ' εφαρμογή του άρθρου 295 παρ. 2, σε συνδυασμό με τα άρθρα 336 παρ. 1 και 357 του ν. 4700/2020 (Α' 127), προκειμένου να ελέγξει τη νομιμότητα έξι (6) σχεδίων τροποποίησης των αντίστοιχων 1453.1.2, 1453.1.3, 1453.1.4, 1453.1.5, 1453.1.6/10.12.2020 και 1453.2.1/7.12.2020 εκτελεστικών συμβάσεων των 1453.1/4.7.2019 και 1453.2/5.7.2019 επιμέρους συμβάσεων της 1453/2019 συμφωνίας - πλαίσιο για την ανάθεση, από την «ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ Α.Ε.», του Έργου «ΣΥΖΕΥΞΙΣ ΙΙ – Υποδομές ασφάλειας/τηλεφωνίας/τηλεδιάσκεψης/καλωδίωσης», Υποέργων «ΣΥΖΕΥΞΙΣ ΙΙ – Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης – Νησίδων 1, 2, 3, 4, 5, 6 – Προμήθεια Υποδομών Φορέων / Υ-2.1, Υ-2.2, Υ-2.3, Υ-2.4, Υ-2.5, Υ-2.6», συμβατικού ποσού α) 16.407.795,00 ευρώ πλέον Φ.Π.Α., β) 11.435.953,00 ευρώ πλέον Φ.Π.Α., γ) 14.814.620,00 ευρώ πλέον Φ.Π.Α., δ) 16.930.289,00 ευρώ πλέον Φ.Π.Α., ε) 21.990.222,50 ευρώ πλέον Φ.Π.Α. και στ) 19.068.343,00 ευρώ πλέον Φ.Π.Α. αντιστοίχως. Ο φάκελος με τα στοιχεία της υπόθεσης υποβλήθηκε στο Ελεγκτικό Συνέδριο στις 23.2.2021 (αρ. πρωτ. Ελ.Σ. 8842), με το 2395/19.2.2021 έγγραφο του Γενικού Διευθυντή Λειτουργίας της ανώνυμης εταιρείας «ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ Α.Ε.».

Άκουσε την εισήγηση της Παρέδρου Αθανασίας – Μυροφόρας Σιδηροπούλου.

Σκέφθηκε κατά το νόμο

Και αποφάσισε τα ακόλουθα:

1. Το άρθρο 324 του ν. 4700/2020 ορίζει ότι: «1. Στις συμβάσεις (...) υπηρεσιών (...) που συνάπτονται από το Δημόσιο (...), τα λοιπά νομικά πρόσωπα δημοσίου δικαίου και τις δημόσιες επιχειρήσεις ή οργανισμούς, η προϋπολογιζόμενη δαπάνη των οποίων υπερβαίνει το ποσό του ενός εκατομμυρίου (1.000.000,00) ευρώ, μη συμπεριλαμβανομένου του φόρου προστιθέμενης αξίας, διενεργείται υποχρεωτικά έλεγχος νομιμότητας, πριν από τη σύναψή τους από Κλιμάκιο του Ελεγκτικού Συνεδρίου (...). 3. Ειδικά για τις συμβάσεις των παρ. 1 (...), που συγχρηματοδοτούνται από ενωσιακούς πόρους, διενεργείται υποχρεωτικά έλεγχος νομιμότητας πριν από τη σύναψή τους από Κλιμάκια του Ελεγκτικού Συνεδρίου, εφόσον η προϋπολογιζόμενη δαπάνη, μη συμπεριλαμβανομένου του φόρου προστιθέμενης αξίας, υπερβαίνει το ποσό των πέντε εκατομμυρίων (5.000.000,00) ευρώ. 4. Στον έλεγχο των παρ. 1 έως 3 συμπεριλαμβάνονται: (...) (γ) οι συμφωνίες πλαίσιο και οι εκτελεστικές αυτών συμβάσεις, σύμφωνα με την παρ. 9 του άρθρου 39 και την παρ. 3 του άρθρου 273 του ν. 4412/2016 (...). 5. Σε προσυμβατικό έλεγχο υπάγονται οι τροποποιήσεις των συμβάσεων των παρ. 1 έως και 4 όταν: α) η αρχική σύμβαση υποβλήθηκε σε έλεγχο, εφόσον η τροποποίηση είναι ουσιώδης (...)». Στην αιτιολογική έκθεση του νόμου αναφέρεται ότι με την παρ. 5 θεσπίζεται οριζόντιας εφαρμογής ρύθμιση για τις τροποποιητικές συμβάσεις, με βάση τις κατευθύνσεις των ήδη ισχυουσών διατάξεων των άρθρων 132 παρ. 6 και 337 παρ. 6 του ν. 4412/2016 (Α' 147), όπως οι τελευταίες τροποποιήθηκαν, ύστερα, μάλιστα, από θετική γνωμοδότηση του Δικαστηρίου (Πρακτικά 16ης Γεν. Συν./12.12.2018 Ολ. Ελ.Σ., Θέμα Β'), με το ν. 4605/2019 (Α' 52). Συνεπώς, στην έννοια της ανωτέρω «ουσιώδους» τροποποίησης, η οποία μετά την ισχύ της παρ. 5 περ. α' του άρθρου 324 του ν. 4700/2020 συνιστά αυτοτελή δικονομική έννοια, με το περιεχόμενό της να φωτίζεται απλώς ερμηνευτικά από τις «κατευθύνσεις» των διατάξεων της παρ. 6 του άρθρου 132 και των αποτελουσών συστηματική ενότητα με αυτή διατάξεων των παρ. 1α', 2 και 4, υπάγονται, μεταξύ άλλων, οι περιπτώσεις συμβάσεων, το αντικείμενο των οποίων περιλαμβάνει τροποποίηση ουσιωδών όρων της αρχικής σύμβασης, η δε μεταβολή τους δύναται να υπαχθεί σε κάποια από τις προβλεπόμενες στην παρ. 4 του άρθρου 132 του ν. 4412/2016 περιπτώσεις.

2. Κατόπιν τούτων, τα σχέδια τροποποίησης των έξι (6) εκτελεστικών συμβάσεων μεταξύ το μεν της εταιρείας «ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ Α.Ε.» («ΚτΠ Α.Ε.»), το δε της ένωσης εταιρειών «ΟΤΕ Α.Ε. – SPACE HELLAS Α.Ε. – UNISYSTEMS Α.Ε.», καθώς και της εταιρείας «LOGICOM SOLUTIONS LIMITED», με αντικείμενο την εκτέλεση του Υποέργου «ΣΥΖΕΥΞΙΣ ΙΙ – Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης» του Έργου «ΔΙΚΤΥΟ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ "ΣΥΖΕΥΞΙΣ ΙΙ"», συνολικής προϋπολογιζόμενης δαπάνης 134.813.145,33 ευρώ πλέον Φ.Π.Α., το οποίο χρηματοδοτείται από το Επιχειρησιακό Πρόγραμμα «Μεταρρύθμιση Δημόσιου Τομέα 2014 - 2020» με Κωδικό Ο.Π.Σ. 5041737, παραδεκτώς εισάγονται για έλεγχο ενώπιον του παρόντος Κλιμακίου, αφενός διότι η σύναψη της κύριας συμφωνίας – πλαίσιο και των εκτελεστικών αυτής συμβάσεων έχουν εγκριθεί με τις 210/2019 και 400/2020 Πράξεις του παρόντος Κλιμακίου αντιστοίχως και αφετέρου διότι οι ελεγχόμενες τροποποιήσεις παρίστανται «ουσιώδεις» (άρθρο 324 παρ. 5α' του ν. 4700/2020), καθώς εντοπίζονται σε ουσιώδεις όρους των αντίστοιχων εκτελεστικών συμβάσεων, οι οποίοι καθορίζουν το αντικείμενο των παρεχόμενων από τους αναδόχους υπηρεσιών, γεγονός που δεν αποκλείει εκ των προτέρων την εφαρμογή της διάταξης του άρθρου 132 παρ. 4 του ν. 4412/2014, αλλά επιβάλλει τον έλεγχο του κατά πόσον στην προκειμένη περίπτωση οι τροποποιήσεις αυτές είναι ουσιώδεις και κατά το ουσιαστικό δίκαιο (Ελ.Σ. Ζ' Κλιμ. 99/2021, πρβλ. Ζ' Κλιμ. 707/2019).

3. Ο ν. 4412/2016 «Δημόσιες Συμβάσεις Έργων, Προμηθειών και Υπηρεσιών (προσαρμογή στις Οδηγίες 2014/24/ΕΕ και 2014/25/ΕΕ)» (Α΄ 147), οι διατάξεις του οποίου περιλαμβάνονται μεταξύ των επικαλούμενων από την αναθέτουσα Αρχή ως εφαρμοστέων κατά την ελεγχόμενη διαδικασία (βλ. και Ζ' Κλιμ. 400/2020), ορίζει στο άρθρο 132 ότι: «1. Οι συμβάσεις (...) μπορούν να τροποποιούνται χωρίς νέα διαδικασία σύναψης σύμβασης, σε οποιαδήποτε από τις ακόλουθες περιπτώσεις: α) (...) ε) όταν οι τροποποιήσεις, ανεξαρτήτως της αξίας τους, δεν είναι ουσιώδεις κατά την έννοια της παραγράφου 4(...). 4. Η τροποποίηση σύμβασης (...) κατά τη διάρκειά της θεωρείται ουσιώδης κατά την έννοια της περίπτωσης ε' της παραγράφου 1, εφόσον καθιστά τη σύμβαση (...) ουσιωδώς διαφορετική, ως προς το χαρακτήρα, από την αρχικώς συναφθείσα. Σε κάθε περίπτωση, με την επιφύλαξη των παραγράφων 1 και 2, μία τροποποίηση θεωρείται ουσιώδης όταν πληροί μία ή

περισσότερες από τις ακόλουθες προϋποθέσεις: α) η τροποποίηση εισάγει όρους οι οποίοι, εάν είχαν αποτελέσει μέρος της αρχικής διαδικασίας σύναψης σύμβασης, θα είχαν επιτρέψει τη συμμετοχή διαφορετικών υποψηφίων από αυτούς που επιλέχθηκαν αρχικώς ή στην αποδοχή άλλης προσφοράς από εκείνη που επελέγη αρχικώς ή θα προσέλκυαν και άλλους συμμετέχοντες στη διαδικασία σύναψης σύμβασης, β) η τροποποίηση αλλάζει την οικονομική ισορροπία της σύμβασης ή της συμφωνίας-πλαίσιο υπέρ του αναδόχου, κατά τρόπο που δεν προβλεπόταν στην αρχική σύμβαση ή συμφωνία-πλαίσιο, γ) η τροποποίηση επεκτείνει σημαντικά το αντικείμενο της σύμβασης ή της συμφωνίας-πλαίσιο (...). 5. Απαιτείται νέα διαδικασία σύναψης σύμβασης (...) για τροποποιήσεις των διατάξεων μίας δημόσιας σύμβασης ή μιας συμφωνίας-πλαίσιο κατά τη διάρκειά τους, που είναι διαφορετικές από τις προβλεπόμενες στις παραγράφους 1 και 2 (...)».

4. Από τις ανωτέρω διατάξεις συνάγεται ότι η σύναψη τροποποιητικής σύμβασης με τον ανάδοχο ήδη εκτελούμενης σύμβασης, συμπεριλαμβανομένων των περιπτώσεων υλοποίησης εκτελεστικών συμβάσεων συμφωνιών – πλαίσιο, επιτρέπεται μόνο στις περιοριστικά αναφερόμενες στο άρθρο 132 περιπτώσεις, καθώς η δυνατότητα αυτή συνιστά παρέκκλιση από τις αρχές της διαφάνειας, της ισότητας συμμετοχής στις διαδικασίες κατάρτισης δημόσιων συμβάσεων και της διασφάλισης του ελεύθερου ανταγωνισμού. Επιτρεπτή περίπτωση τροποποίησης συναφθείσας σύμβασης αποτελεί, μεταξύ άλλων, η μη ουσιώδης τροποποίησή της, ανεξαρτήτως της αξίας του αντικειμένου της. Η έννοια της ουσιώδους τροποποίησης, η συνδρομή της οποίας επιτάσσει την εκκίνηση νέας διαδικασίας σύναψης σύμβασης εκ μέρους της αναθέτουσας Αρχής και, συνακόλουθα, καθιστά μη επιτρεπτή τη σύναψη τροποποιητικής, όπως έχει διαμορφωθεί νομολογιακά από το Δικαστήριο της Ε.Ε. και έχει διατυπωθεί στις διατάξεις της Οδηγίας 2014/25/ΕΕ, αποτυπώνεται στην παράγραφο 4 του άρθρου 132 του ν. 4412/2016. Ουσιώδης δε τροποποίηση σύμβασης είναι εκείνη, συνεπεία της οποίας μεταβάλλεται ιδίως το εύρος και το περιεχόμενο των αμοιβαίων δικαιωμάτων και υποχρεώσεων των συμβαλλόμενων, υποδηλώνοντας τη βούληση των τελευταίων να επαναδιαπραγματευθούν ουσιώδεις όρους της σύμβασης (βλ. αιτιολογική σκέψη 113 της Οδηγίας 2014/25/ΕΕ, πρβλ. Δ.Ε.Ε. C-454/06 Pressetext Nachrichtenagentur GmbH, σκ. 34-37, C-549/14 Finn Frogne A/S, σκ. 28-30, C-526/17, Επιτροπή κατά

Ιταλίας, σκ. 58 - 59). Στο πλαίσιο αυτό, καθορίζονται στην προαναφερόμενη διάταξη συγκεκριμένα κριτήρια, η συνδρομή έστω και ενός εκ των οποίων, στοιχειοθετεί ουσιώδη τροποποίηση της αρχικής σύμβασης. Ειδικότερα, συντρέχει περίπτωση ουσιώδους τροποποίησης όταν, μεταξύ άλλων: α) οι τροποποιήσεις είναι ικανές να θέσουν εν αμφιβόλω την ανάθεση της σύμβασης στον ήδη ανάδοχο, υπό την έννοια ότι εάν είχαν συμπεριληφθεί στα έγγραφα της διαδικασίας ανάθεσης της αρχικής σύμβασης (διακήρυξη κ.λπ.), θα είχαν επηρεάσει την πορεία της είτε προσελκύοντας και άλλους συμμετέχοντες στη διαδικασία σύναψης της σύμβασης είτε κάνοντας δεκτή άλλη προσφορά από εκείνη που επιλέχθηκε είτε επιτρέποντας τη συμμετοχή διαφορετικών οικονομικών φορέων από αυτούς που επιλέχθηκαν αρχικά, β) η τροποποίηση αλλάζει την οικονομική ισορροπία της σύμβασης υπέρ του αναδόχου, κατά τρόπο που δεν προβλεπόταν στην αρχική σύμβαση ή συμφωνία-πλαίσιο, γ) με την τροποποίηση διευρύνεται σημαντικά το αντικείμενο της σύμβασης περιλαμβάνοντας υπηρεσίες που δεν είχαν αρχικώς προβλεφθεί. Η επέκταση του αντικειμένου της αρχικής σύμβασης αποτελεί συνθήκη που κρίνεται ad hoc λαμβανομένων υπόψη των εκάστοτε πραγματικών περιστατικών για το χαρακτηρισμό της ως σημαντικής (πρβλ. Ελ.Σ VI Τμ. 1340/2018).

5. Στην υπό κρίση υπόθεση, από το σύνολο των στοιχείων του φακέλου προκύπτουν τα εξής:

Α. Με τις 1453.1/4.7.2019 και 1453.2/5.7.2019 επιμέρους συμβάσεις της 1453/2019 συμφωνίας - πλαίσιο μεταξύ αφενός της ανώνυμης εταιρείας «ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ Α.Ε.» και αφετέρου της ένωσης εταιρειών «ΟΤΕ Α.Ε. – SPACE HELLAS A.E. – UNISYSTEMS A.E.» (1453.1/2019 σύμβαση), καθώς και της εταιρείας «LOGICOM SOLUTIONS LTD» (1453.2/2019 σύμβαση), η υπογραφή της οποίας κρίθηκε ότι δεν κωλύεται με την 210/2019 Πράξη του παρόντος Κλιμακίου, συμφωνήθηκε η εκτέλεση του Έργου «ΣΥΖΕΥΞΙΣ ΙΙ – Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης», στο αντικείμενο του οποίου περιλαμβάνονται: α) υπηρεσίες πρόσβασης/ασφάλειας, που περιλαμβάνουν την προμήθεια, εγκατάσταση, παραμετροποίηση και λειτουργία εξοπλισμού πρόσβασης/ασφάλειας των φορέων του ΣΥΖΕΥΞΙΣ ΙΙ, καθώς και την απαραίτητη υποδομή ασφαλείας για την προστασία των κεντρικών υποδομών του ΣΥΖΕΥΞΙΣ ΙΙ, β)

υπηρεσία τηλεφωνίας, που περιλαμβάνει την προμήθεια και λειτουργία υποδομών τηλεφωνίας για τους φορείς των οκτώ (8) Νησίδων του έργου ΣΥΖΕΥΞΙΣ ΙΙ, γ) θέσεις εργασίας δομημένης καλωδίωσης, που περιλαμβάνουν την προμήθεια και λειτουργία υποδομών IP τηλεφωνίας και παθητικών και ενεργών στοιχείων δομημένης καλωδίωσης σε επιλεγμένους φορείς των Νησίδων, δ) υποδομές (εξοπλισμός – λογισμικό) τηλεδιάσκεψης που περιλαμβάνουν την προμήθεια και λειτουργία συστημάτων τηλεδιάσκεψης σε επιλεγμένους φορείς των Νησίδων και ε) συστήματα τηλεπαρουσίας (tele presence), που περιλαμβάνουν την παροχή και λειτουργία συστημάτων τηλεπαρουσίας σε επιλεγμένους φορείς των Νησίδων. Η κατά τα ανωτέρω υλοποίηση του Υποέργου περιλαμβάνει τις φάσεις: α) Φάση 1 «Ανάλυση Απαιτήσεων – Μελέτη Εφαρμογής», β) Φάση 2 «Εγκατάσταση και παραμετροποίηση εξοπλισμού στους φορείς», γ) Φάση 3.1. «Εγκατάσταση κεντρικών υποδομών ασφάλειας και τηλεφωνίας», δ) Φάση 3.2. «Ανάπτυξη και παραμετροποίηση κεντρικών υποδομών ασφάλειας και τηλεφωνίας» ε) Φάση 4 «Πιλοτική Λειτουργία» και στ) Φάση 5 «Δοκιμαστική Λειτουργία». Η συνολική προϋπολογισθείσα δαπάνη των εν λόγω υπηρεσιών, συμπεριλαμβανομένου του δικαιώματος προαίρεσης της αναθέτουσας Αρχής για αύξηση του φυσικού αντικειμένου του Έργου σε ποσοστό έως 25% του προϋπολογισμού του, ανήλθε σε 134.813.145,33 ευρώ πλέον Φ.Π.Α. Η διάρκεια της συμφωνίας - πλαίσιο ορίσθηκε στους σαράντα οκτώ (48) μήνες, ενώ η διάρκεια των εκτελεστικών συμβάσεων αυτής στους σαράντα δύο (42) μήνες.

Β. Εν συνεχεία, εκδόθηκαν από την αναθέτουσα Αρχή οι 3211/28.4.2020, 3238/29.4.2020, 3240/29.4.2020, 3351, 3352 και 3353/4.5.2020 αποφάσεις Πρόσκλησης Υποβολής Εξατομικευμένων Προσφορών, με κριτήριο ανάθεσης τη χαμηλότερη τιμή, για τη σύναψη αντίστοιχων εκτελεστικών συμβάσεων με τα μέλη – αντισυμβαλλόμενους της συμφωνίας – πλαίσιο για τα Υποέργα «ΣΥΖΕΥΞΙΣ ΙΙ – Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης – Νησίδα 1 – Προμήθεια Υποδομών Φορέων / Υ-2.1», «ΣΥΖΕΥΞΙΣ ΙΙ – Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης – Νησίδα 2 – Προμήθεια Υποδομών Φορέων / Υ-2.2», «ΣΥΖΕΥΞΙΣ ΙΙ – Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης – Νησίδα 3 – Προμήθεια Υποδομών Φορέων / Υ-2.3», «ΣΥΖΕΥΞΙΣ ΙΙ – Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης –

Νησίδα 4 – Προμήθεια Υποδομών Φορέων / Υ-2.4», «ΣΥΖΕΥΞΙΣ ΙΙ – Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης – Νησίδα 5 – Προμήθεια Υποδομών Φορέων / Υ-2.5» και «ΣΥΖΕΥΞΙΣ ΙΙ – Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης – Νησίδα 6 – Προμήθεια Υποδομών Φορέων / Υ-2.6» αντιστοίχως.

Γ. Κατόπιν ολοκλήρωσης της διαδικασίας αξιολόγησης των προσφορών για καθεμία εκ των εκτελεστικών συμβάσεων και έγκρισης των αντίστοιχων Πρακτικών τόσο από το Δ.Σ. της «ΚτΠ Α.Ε.», όσο και από την αρμόδια, συσταθείσα και συγκροτηθείσα με την Π1/384/21.12.2012 Κοινή Υπουργική Απόφαση, Διακομματική Επιτροπή και σε συμφωνία με την 400/2020 θετική Πράξη του παρόντος Κλιμακίου, υπεγράφησαν οι οικείες εκτελεστικές συμβάσεις: α) για τα Υποέργα «ΣΥΖΕΥΞΙΣ ΙΙ – Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης – Νησίδα 1 – Προμήθεια Υποδομών Φορέων / Υ-2.1», «ΣΥΖΕΥΞΙΣ ΙΙ – Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης – Νησίδα 2 – Προμήθεια Υποδομών Φορέων / Υ-2.2», «ΣΥΖΕΥΞΙΣ ΙΙ – Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης – Νησίδα 3 – Προμήθεια Υποδομών Φορέων / Υ-2.3», «ΣΥΖΕΥΞΙΣ ΙΙ –Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης – Νησίδα 4 – Προμήθεια Υποδομών Φορέων / Υ-2.4» και «ΣΥΖΕΥΞΙΣ ΙΙ – Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης – Νησίδα 5 – Προμήθεια Υποδομών Φορέων / Υ-2.5», με την ένωση εταιρειών «ΟΡΓΑΝΙΣΜΟΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΤΗΣ ΕΛΛΑΔΟΣ Α.Ε., SPACE HELLAS ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΥΠΗΡΕΣΙΕΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ, ΠΛΗΡΟΦΟΡΙΚΗΣ, ΑΣΦΑΛΕΙΑΣ - ΙΔΙΩΤΙΚΗ ΕΠΙΧΕΙΡΗΣΗ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΑΣΦΑΛΕΙΑΣ και UNISYSTEMS ΣΥΣΤΗΜΑΤΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΜΟΝΟΠΡΟΣΩΠΗ ΑΝΩΝΥΜΗ ΕΜΠΟΡΙΚΗ ΕΤΑΙΡΕΙΑ», έναντι συμβατικού ποσού i) 16.407.807,00 ευρώ πλέον Φ.Π.Α., ii) 11.435.954,00 ευρώ πλέον Φ.Π.Α., iii) 14.814.625,00 ευρώ πλέον Φ.Π.Α., iv) 16.930.296,00 ευρώ πλέον Φ.Π.Α. και v) 21.990.227,50 ευρώ πλέον Φ.Π.Α. αντιστοίχως και β) για το Υποέργο «ΣΥΖΕΥΞΙΣ ΙΙ – Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης – Νησίδα 6 – Προμήθεια Υποδομών Φορέων / Υ-2.6», με την εταιρεία «LOGICOM SOLUTIONS LIMITED» έναντι συμβατικού ποσού 19.068.343,00 ευρώ πλέον Φ.Π.Α.

6. Μετά την υπογραφή των ανωτέρω, απεστάλη προς την «ΚτΠ Α.Ε.» η

5260/28.12.2020 επιστολή του Διευθυντή του Γραφείου του Υπουργού Ψηφιακής Διακυβέρνησης, στην οποία αναφέρεται ότι: «(...) Ενόψει των περιοριστικών μέτρων που έχουν ληφθεί πρόσφατα στην εκπαίδευση εξαιτίας της πανδημίας COVID-19, είναι απαραίτητο όπως η υπηρεσία τηλε-μαθημάτων παρασχεθεί το συντομότερο δυνατό στο σύνολο της εκπαιδευτικής κοινότητας της χώρας. Για το σκοπό αυτό, παρακαλώ όπως προχωρήσετε άμεσα στην υλοποίηση της παραπάνω υπηρεσίας μέσω της υπηρεσίας τηλεδιάσκεψης που παρέχεται στο πλαίσιο του έργου "ΣΥΖΕΥΞΙΣ ΙΙ", την ευθύνη υλοποίησης του οποίου έχει η υπηρεσία σας. Η προαναφερθείσα υπηρεσία τηλε-μαθημάτων θα πρέπει να καλύπτει κατά προτεραιότητα το σύνολο των 154.000 εκπαιδευτικών μονάδων της χώρας για διάστημα ενός (1) έτους, έναντι των προβλεπόμενων στις συμβάσεις του ΣΥΖΕΥΞΙΣ ΙΙ υπηρεσιών τηλεδιάσκεψης για τους φορείς της Δημόσιας Διοίκησης, διάρκειας 36 μηνών (...)».

7. Στη με ίδια ημερομηνία (28.12.2020) επιστολή της ένωσης εταιρειών «ΟΤΕ Α.Ε. – SPACE HELLAS A.E. – UNISYSTEMS A.E.» προς την «ΚτΠ Α.Ε.» αναφέρονται τα εξής: «Σε συνέχεια της υπογραφής των συμβάσεων του έργου «ΣΥΖΕΥΞΙΣ ΙΙ – Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης» (συμβάσεις 1453.1.2, 1453.1.3, 1453.1.4, 1453.1.5, 1453.1.6), προτείνεται (...) η αντικατάσταση του Λογισμικού Τηλεδιάσκεψης HUAWEI TE Desktopμε προϊόντα τηλεδιάσκεψης του κατασκευαστή Cisco, σύμφωνα με την συνημμένη ανάλυση (....)» και, πιο συγκεκριμένα: «(...) Η τεχνική λύση της Ένωσης Εταιρειών ΟΤΕ- Unisystems-Space Hellas περιλάμβανε το Λογισμικό Τηλεδιάσκεψης HUAWEI TE Desktop που προβλεπόταν να εγκατασταθεί σε υπολογιστές Φορέων του ΣΥΖΕΥΞΙΣ ΙΙ. Η Ένωση, με βάση το πλήθος των Εκτελεστικών τις οποίες έχει αναλάβει, έχει υποχρέωση παροχής της συγκεκριμένης υπηρεσίας σε έως 33.280 υπολογιστές των Εκτελεστικών Συμβάσεων 1-5. Το συγκεκριμένο προϊόν δεν είναι πλέον διαθέσιμο από τον κατασκευαστή, ενώ δεν έχει αντικατασταθεί από κάποιο παρεμφερές του ίδιου κατασκευαστή που να ανταποκρίνεται στις απαιτήσεις του Έργου. Συνεπώς, καθίσταται επιβεβλημένη η αναζήτηση νέας λύσης, ώστε να προσφερθεί η ζητούμενη λειτουργικότητα. Η διερεύνηση για την προτεινόμενη λύση (...) βασίστηκε στις παρακάτω γενικές αρχές: - Να καλύπτει τις λειτουργικές προδιαγραφές της υπηρεσίας τηλεδιάσκεψης με αποδοτικό τρόπο. – Να ανήκει σε

κάποιον εγκεκριμένο κατασκευαστικό οίκο που ιδανικά αποτελεί μέρος της συνολικής λύσης. – Να αποτελεί ένα σύγχρονο και ευρέως διαδεδομένο εργαλείο με το οποίο είναι εξοικειωμένοι οι χρήστες. – Να προσφέρει ευελιξία στη χρήση και δυνατότητα αύξησης των χρηστών σύμφωνα με τις απαιτήσεις του έργου. - Να καλύπτει τρέχουσες ανάγκες της Δημόσιας Διοίκησης, ανταποκρινόμενη στις νέες συνθήκες που δημιουργεί η τηλε-εκπαίδευση και τηλε-εργασία. Λαμβάνοντας υπόψη τα παραπάνω, προτείνεται ο συνδυασμός δύο λύσεων για την κάλυψη του Λογισμικού Τηλεδιάσκεψης, που ανήκουν στη σουΐτα προϊόντων τηλεδιάσκεψης της Cisco, όπως και οι υπόλοιπες λύσεις τηλεδιάσκεψης που έχουν προταθεί στο έργο και μπορούν να παραγγελθούν, ανάλογα με τις ανάγκες της ΚτΠ. Η 1η λύση περιλαμβάνει το λογισμικό Webex Meetings for Education (...), το οποίο είναι το πιο διαδεδομένο προϊόν σε παγκόσμιο επίπεδο στην κατηγορία Meeting Solutions. Η συγκεκριμένη λύση απευθύνεται αποκλειστικά σε χρήστες της εκπαιδευτικής κοινότητας. Το Webex Meetings έχει αναδειχθεί στην πλέον δημοφιλή πλατφόρμα τηλεδιάσκεψης με τα νέα δεδομένα που διαμορφώνει η πανδημία covid-19 και η τηλε-εργασία. Τα βασικά πλεονεκτήματα της λύσης συνοψίζονται στη συνέχεια: - Δοκιμασμένη λύση με διευρυμένη χρήση σε όλες τις βαθμίδες εκπαίδευσης. - Δυνατότητα λειτουργίας σε προσωπικούς σταθερούς ή φορητούς υπολογιστές ή σε έξυπνα τηλέφωνα. – Φιλοξενία στο Cloud και χρήση τεχνολογιών Web για εξασφαλισμένη διαλειτουργικότητα, χωρίς την ανάγκη κεντρικών υποδομών. – Δυνατότητα επιλογής χρήσης video ή μόνο audio. -Υψηλής ευκρίνειας (High Definition) video και ήχος. – Ατομικές διασκέψεις ή πολυδιασκέψεις χωρίς χρήση MCU. – Δυνατότητα διαμοιρασμού σε πραγματικό χρόνο (Screen, application, file, and browser) και Multimedia sharing. – Δυνατότητα μεταφοράς αρχείων. Για τις ανάγκες του, η προτεινόμενη λύση προσφέρεται με τα παρακάτω χαρακτηριστικά: - Δυνατότητα χρήσης αποκλειστικά εντός της εκπαιδευτικής κοινότητας (Α' βάθμια και Β' βάθμια εκπαίδευση). – Χρονική διάρκεια κάλυψης: 12 μήνες. – Μέγιστο πλήθος προσφερόμενων αδειών: 113.892. Η 2η λύση περιλαμβάνει το λογισμικό Cisco Jabber (...). Το συγκεκριμένο προϊόν αποτελεί μια δυναμική πλατφόρμα που προσφέρει πληθώρα λειτουργιών μέσα από ένα ενοποιημένο περιβάλλον και έναν κοινό client. Τα βασικά πλεονεκτήματα της λύσης συνοψίζονται στη συνέχεια: - Πλήρης συμμόρφωση με τις αρχικές προδιαγραφές. – Διαδεδομένη λύση σε όλες τις

λύσεις Unified Communications της Cisco. – Δυνατότητα λειτουργίας σε προσωπικούς σταθερούς ή φορητούς υπολογιστές ή σε έξυπνα τηλέφωνα. – Instant messaging, desktop sharing, audio, video, και web conferencing. – Δυνατότητα επιλογής χρήσης video ή μόνο audio. - Υψηλής ευκρίνειας (High Definition) video και ήχος. Για τις ανάγκες του, η προτεινόμενη λύση προσφέρεται με τα παρακάτω χαρακτηριστικά: - Δυνατότητα χρήσης από όλους τους χρήστες της Δημόσιας Διοίκησης. – Χρονική διάρκεια κάλυψης: 36 μήνες. – Μέγιστο πλήθος προσφερόμενων αδειών: 5.306. Ο συνδυασμός των δύο λύσεων με το μέγιστο πλήθος αδειών ανά προϊόν δεν προκαλεί ουσιαστική αλλαγή του μέγιστου τιμήματος για την ΚτΠ στην κατηγορία του Λογισμικού Τηλεδιάσκεψης, όπως φαίνεται στον πίνακα που ακολουθεί (...)». Σύμφωνα δε με το συνημμένο σχετικό Πίνακα, το Συνολικό Κόστος της Προσφοράς το έτος 2014 του Είδους HUAWEI TE Desktop με διάρκεια χρήσης 36 μηνών για αριθμό μονάδων 33.280,κόστους ανά μονάδα 57,00 ευρώ πλέον Φ.Π.Α. ανερχόταν σε 1.896.960,00 ευρώ πλέον Φ.Π.Α., ενώ το Συνολικό Κόστος της Προσφοράς του έτους 2020 των Ειδών Webex Meetings for Education και Cisco Jabberμε διάρκεια χρήσης 12 μηνών και 36 μηνών αντιστοίχως, για αριθμό μονάδων 113.892 και 5.306, κόστους ανά μονάδα 14,00 ευρώ πλέον Φ.Π.Α. και 57,00 ευρώ πλέον Φ.Π.Α. αντιστοίχως, ανέρχεται σε (1.594.488,00 + 302.442,00 =) 1.896.930,00 ευρώ πλέον Φ.Π.Α. Το έγγραφο καταλήγει: «Το ισοδύναμο της λύσης προκύπτει και από τη διαστασιολόγηση του νέου φυσικού οικονομικού αντικειμένου, αφού οι συνολικοί προσφερόμενοι μήνες αδειών των λογισμικών ανέρχονται σε 1.557.720, έναντι των 1.198.080 που προβλέπονται στις Εκτελεστικές Συμβάσεις».

8. Ομοίως με τα ανωτέρω, όπως προκύπτει από την από 24.12.2020 επιστολή της έτερης αναδόχου εταιρείας «LOGICOM SOLUTIONS LIMITED» και στο πλαίσιο υλοποίησης της εκτελεστικής σύμβασης 1453.2.1, προτείνεται η τροποποίηση της πλατφόρμας Λογισμικού Τηλεδιάσκεψης, όπου μέρος των αδειών του προσφερόμενου λογισμικού Cisco Jabber αντικαθίσταται με το λογισμικό Cisco Webex Meetings, για να καλυφθούν οι ανάγκες της τηλεκπαίδευσης. Πιο συγκεκριμένα, από τις αρχικώς προσφερόμενες 11.720 άδειες χρήσης λογισμικού Cisco Jabber προσφέρονται 1.869 άδειες χρήσης, τριετούς διάρκειας υποστήριξης. Επιπλέον, προσφέρονται 40.108 άδειες χρήσης λογισμικού τηλεδιάσκεψης /

τηλεκπαίδευσης Cisco Webex, οι οποίες καλύπτουν τους προσφερόμενους χρήστες με συνδρομή διάρκειας 12 μηνών, με συνολικό ετήσιο κόστος 668.045,00 ευρώ πλέον Φ.Π.Α. έναντι του ήδη συμφωνηθέντος 668.045,00 ευρώ πλέον Φ.Π.Α. Δηλώνεται, τέλος, ότι λόγω της διαφοράς που προκύπτει στο συνολικό κόστος των προσφερόμενων αδειών λογισμικού της τάξης των 5,00 ευρώ, η διαφορά απορροφάται από τον ανάδοχο, ώστε το συνολικό κόστος που προκύπτει να είναι ίσο με της αρχικής εκτελεστικής σύμβασης.

9. Κατόπιν τούτων, με το από 30.12.2020 Πρακτικό η Επιτροπή Παρακολούθησης και Παραλαβής του Έργου προέβη στις ακόλουθες διαπιστώσεις: α) δεν είναι δυνατή η κάλυψη της απαίτησης του Υπουργείου Ψηφιακής Διακυβέρνησης από τον πίνακα προσφερόμενων λογισμικών των υφιστάμενων εκτελεστικών συμβάσεων, όμως καλύπτεται πλήρως από τις προσφερόμενες στα αιτήματα τροποποίησης των αναδόχων πλατφόρμες λογισμικού τηλεδιάσκεψης, β) στις υφιστάμενες εκτελεστικές συμβάσεις προβλέπεται η απόκτηση 45.000 αδειών χρήσης λογισμικού τηλεδιάσκεψης για τρία (3) έτη, το οποίο αντιστοιχεί σε 1.620.000 μήνες παροχής της υπηρεσίας. Τα αιτήματα τροποποίησης των αναδόχων περιλαμβάνουν την προμήθεια συνολικά 7.175 αδειών χρήσης λογισμικού Cisco Jabber για τρία (3) έτη και 154.000 αδειών Cisco Webex για τηλεδιασκέψεις / τηλεκπαίδευση για ένα (1) έτος που αντιστοιχούν συνολικά σε 2.106.300 μήνες (258.300 μήνες για τις 7.175 άδειες Jabber και 1.848.000 μήνες για τις 154.000 άδειες Webex) παροχής της υπηρεσίας τηλεδιάσκεψης. Η δυνατότητα του κεντρικού συστήματος διαχείρισης του προσφερόμενου client τηλεδιάσκεψης ανταλλαγής δεδομένων με το κεντρικό σύστημα υποστήριξης τηλεδιασκέψεων του υποέργου του SIX (MCU), ώστε να είναι δυνατή η συμμετοχή χρηστών της client εφαρμογής σε πολυδιασκέψεις, σύμφωνα με τις αναφερόμενες δυνατότητες στην κεντρική MCU του Υποέργου 4 του SIX – Data Center, που αποτελεί προδιαγραφή της διακήρυξης του Έργου, παρέχεται πλήρως από το μέρος της λύσης που αντιστοιχεί στο λογισμικό Cisco Jabber. Το λογισμικό Cisco Webex παρέχει τη λειτουργία πολυδιάσκεψης εγγενώς, χωρίς την δυνατότητα ανταλλαγής δεδομένων με την MCU. Όμως, δεδομένου ότι το προσφερόμενο λογισμικό Cisco Webex θα εξυπηρετήσει την τηλεκπαίδευση, δεν απαιτείται ανταλλαγή δεδομένων με το κεντρικό σύστημα υποστήριξης τηλεδιασκέψεων του υποέργου του SIX (MCU), γ) το

νέο αντικείμενο είναι ισοδύναμο τεχνικά και οικονομικά με το προβλεπόμενο στις εκτελεστικές συμβάσεις και δ) Οι προτεινόμενες τροποποιήσεις κρίνονται, αφενός, αναγκαίες για την τεχνική επικαιροποίηση του λογισμικού τηλεδιάσκεψης και, αφετέρου, απαραίτητες για να εξυπηρετήσουν το δημόσιο συμφέρον, ήτοι για την κάλυψη αναγκών που ανακύπτουν λόγω της πανδημίας.

10. Για τους λόγους αυτούς η Επιτροπή, με το ως άνω Πρακτικό, αποφάσισε αφενός την έγκριση των αιτημάτων τροποποίησης του λογισμικού τηλεδιάσκεψης για τις προαναφερόμενες εκτελεστικές συμβάσεις, όπως αυτά υποβλήθηκαν στην «ΚτΠ Α.Ε.» από τους αντισυμβαλλόμενους αναδόχους, με τη διευκρίνιση που διαλαμβάνεται στο Πρακτικό σχετικά με το χρόνο κατανάλωσης των αδειών χρήσης και β) την τροποποίηση του φυσικού αντικειμένου των συμβάσεων ως εξής: **1.** Αναφορικά με την εκτελεστική σύμβαση 1453.1.2: Η Προσφορά 16 του Είδους HUAWEI TE Desktop με διάρκεια χρήσης 36 μηνών με αριθμό μονάδων 6.493, κόστους ανά μονάδα 57,00 ευρώ πλέον Φ.Π.Α. και συνολικού κόστους 370.101,00 ευρώ πλέον Φ.Π.Α. αντικαθίσταται με τις Προσφορές 16.1 του Είδους Webex Meetings for Education διάρκειας χρήσης 12 μηνών με αριθμό μονάδων 22.221, κόστους ανά μονάδα 14,00 ευρώ πλέον Φ.Π.Α. και συνολικού κόστους 311.094,00 ευρώ πλέον Φ.Π.Α. και 16.2 του Είδους Cisco Jabber διάρκειας χρήσης 36 μηνών με αριθμό μονάδων 1.035, κόστους ανά μονάδα 57,00 ευρώ πλέον Φ.Π.Α. και συνολικού κόστους 58.995,00 ευρώ πλέον Φ.Π.Α., ήτοι συνολικού κόστους (των Προσφορών 16.1 και 16.2) ύψους 370.089,00 ευρώ πλέον Φ.Π.Α. **2.** Αναφορικά με την εκτελεστική σύμβαση 1453.1.3: Η Προσφορά 16 του Είδους HUAWEI TE Desktop με διάρκεια χρήσης 36 μηνών με αριθμό μονάδων 4.531, κόστους ανά μονάδα 57,00 ευρώ πλέον Φ.Π.Α. και συνολικού κόστους 258.267,00ευρώ πλέον Φ.Π.Α. αντικαθίσταται με τις Προσφορές 16.1 του Είδους Webex Meetings for Education διάρκειας χρήσης 12 μηνών με αριθμό μονάδων 15.508, κόστους ανά μονάδα 14,00 ευρώ πλέον Φ.Π.Α. και συνολικού κόστους 217.112,00 ευρώ πλέον Φ.Π.Α. και 16.2 του Είδους Cisco Jabber διάρκειας χρήσης 36 μηνών με αριθμό μονάδων 722, κόστους ανά μονάδα 57,00 ευρώ πλέον Φ.Π.Α. και συνολικού κόστους 41.154,00 ευρώ πλέον Φ.Π.Α., ήτοι συνολικού κόστους (των Προσφορών 16.1 και 16.2) ύψους 258.266,00ευρώ πλέον Φ.Π.Α. **3.** Αναφορικά με την εκτελεστική σύμβαση 1453.1.4: Η Προσφορά 16 του Είδους HUAWEI TE Desktop με διάρκεια χρήσης 36 μηνών με

αριθμό μονάδων 5.086, κόστους ανά μονάδα 57,00 ευρώ πλέον Φ.Π.Α. και συνολικού κόστους 289.902,00ευρώ πλέον Φ.Π.Α. αντικαθίσταται με τις Προσφορές 16.1 του Είδους Webex Meetings for Education διάρκειας χρήσης 12 μηνών με αριθμό μονάδων 17.405, κόστους ανά μονάδα 14,00 ευρώ πλέον Φ.Π.Α. και συνολικού κόστους 243.670,00 ευρώ πλέον Φ.Π.Α. και 16.2 του Είδους Cisco Jabber διάρκειας χρήσης 36 μηνών με αριθμό μονάδων 811, κόστους ανά μονάδα 57,00 ευρώ πλέον Φ.Π.Α. και συνολικού κόστους 46.227,00 ευρώ πλέον Φ.Π.Α., ήτοι συνολικού κόστους (των Προσφορών 16.1 και 16.2) ύψους 289.897,00 ευρώ πλέον Φ.Π.Α. **4.** Αναφορικά με την εκτελεστική σύμβαση 1453.1.5: Η Προσφορά 16 του Είδους HUAWEI TE Desktop με διάρκεια χρήσης 36 μηνών με αριθμό μονάδων 5.538, κόστους ανά μονάδα 57,00 ευρώ πλέον Φ.Π.Α. και συνολικού κόστους 315.666,00ευρώ πλέον Φ.Π.Α. αντικαθίσταται με τις Προσφορές 16.1 του Είδους Webex Meetings for Education διάρκειας χρήσης 12 μηνών με αριθμό μονάδων 18.952, κόστους ανά μονάδα 14,00 ευρώ πλέον Φ.Π.Α. και συνολικού κόστους 265.328,00 ευρώ πλέον Φ.Π.Α. και 16.2 του Είδους Cisco Jabber διάρκειας χρήσης 36 μηνών με αριθμό μονάδων 833 κόστους ανά μονάδα 57,00 ευρώ πλέον Φ.Π.Α. και συνολικού κόστους 50.331,00 ευρώ πλέον Φ.Π.Α., ήτοι συνολικού κόστους (των Προσφορών 16.1 και 16.2) ύψους 315.659,00ευρώ πλέον Φ.Π.Α. **5.** Αναφορικά με την εκτελεστική σύμβαση 1453.1.6: Η Προσφορά 16 του Είδους HUAWEI TE Desktop με διάρκεια χρήσης 36 μηνών με αριθμό μονάδων 11.632, κόστους ανά μονάδα 57,00 ευρώ πλέον Φ.Π.Α. και συνολικού κόστους 663.024,00ευρώ πλέον Φ.Π.Α. αντικαθίσταται με τις Προσφορές 16.1 του Είδους Webex Meetings for Education διάρκειας χρήσης 12 μηνών με αριθμό μονάδων 39.806, κόστους ανά μονάδα 14,00 ευρώ πλέον Φ.Π.Α. και συνολικού κόστους 557.284,00 ευρώ πλέον Φ.Π.Α. και 16.2 του Είδους Cisco Jabber διάρκειας χρήσης 36 μηνών με αριθμό μονάδων 1.855 κόστους ανά μονάδα 57,00 ευρώ πλέον Φ.Π.Α. και συνολικού κόστους 105.735,00 ευρώ πλέον Φ.Π.Α., ήτοι συνολικού κόστους (των Προσφορών 16.1 και 16.2) ύψους 663.019,00ευρώ πλέον Φ.Π.Α. Και **6.** Αναφορικά με την εκτελεστική σύμβαση 1453.2.1: Η Προσφορά 16 του Είδους Desktop Conf. Clients με αριθμό μονάδων 11.720, κόστους ανά μονάδα 57,00 ευρώ πλέον Φ.Π.Α. και συνολικού κόστους 668.040,00ευρώ πλέον Φ.Π.Α. αντικαθίσταται με τις Προσφορές 16.1 του Είδους Cisco Jabber με αριθμό μονάδων 1.869, κόστους ανά μονάδα 57,00 ευρώ πλέον

Φ.Π.Α. και συνολικού κόστους 106.533,00ευρώ πλέον Φ.Π.Α. και 16.2 του Είδους Cisco Webex με αριθμό μονάδων 40.108, κόστους ανά μονάδα 14,00 ευρώ πλέον Φ.Π.Α. και συνολικού κόστους 561.512,00ευρώ πλέον Φ.Π.Α., ήτοι συνολικού κόστους (των Προσφορών 16.1 και 16.2) ύψους (668.045,00 - 5,00 ευρώ =) 668.040,00ευρώ πλέον Φ.Π.Α. Το εν λόγω Πρακτικό εγκρίθηκε με την 41/4.1.2021 (ορθή επανάληψη στις 15.2.2021) απόφαση του, ενεργούντος κατ' εξουσιοδότηση του Δ.Σ., Διευθύνοντος Συμβούλου της «ΚτΠ Α.Ε.».

11. Περαιτέρω, μετά την αποστολή αιτημάτων εκ μέρους των αναδόχων προς την «ΚτΠ Α.Ε.» περί παράτασης της Φάσης 1 υλοποίησης του Έργου («Ανάλυση Απαιτήσεων – Μελέτη Εφαρμογής») χωρίς αύξηση του οικονομικού αντικειμένου, η Επιτροπή Παρακολούθησης και Παραλαβής του Έργου, με το από 28.1.2021 Πρακτικό, εξέτασε τα συγκεκριμένα αιτήματα, ενώ συνεκτίμησε, μεταξύ άλλων, τις συνθήκες που έχουν διαμορφωθεί από τα μέτρα κατά της πανδημίας covid-19 που επηρεάζουν τόσο την επικοινωνία των αναδόχων με τους φορείς (π.χ. τηλεργασία), όσο και τις επιτόπου επισκέψεις των ομάδων έργου των αναδόχων (π.χ. περιορισμοί μετακινήσεων), με άμεση επίπτωση στη διαδικασία της επικαιροποίησης των στοιχείων των φορέων (site surveys), η οποία αποτελεί σημαντικό δεδομένο του σχεδιασμού της λύσης, ως μέρους του παραδοτέου της Μελέτης Εφαρμογής. Ακολούθως, πρότεινε την έγκριση των αιτημάτων τροποποίησης του χρονοδιαγράμματος για τις εκτελεστικές συμβάσεις, με την παράταση της Φάσης 1 «Ανάλυση Απαιτήσεων – Μελέτη Εφαρμογής» κατά δύο (2) μήνες, στους τέσσερις (4) συνολικά και τη συνεπακόλουθη επιμήκυνση του συνολικού χρονοδιαγράμματος κατά δύο (2) μήνες, στους σαράντα τέσσερις (44) συνολικά. Το τελευταίο αυτό Πρακτικό εγκρίθηκε με την 1971/9.2.2021 απόφαση του, ενεργούντος κατ' εξουσιοδότηση του Δ.Σ., Διευθύνοντος Συμβούλου της «ΚτΠ Α.Ε.».

12. Με δεδομένα αυτά και σύμφωνα με όσα έγιναν δεκτά ανωτέρω, το Κλιμάκιο κρίνει ότι οι επίμαχες τροποποιήσεις δεν συνεπάγονται ουσιώδη τροποποίηση, κατά την έννοια του άρθρου 132 παρ. 4 του ν. 4412/2016, των εκτελεστικών συμβάσεων των Υποέργων «ΣΥΖΕΥΞΙΣ ΙΙ – Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης – Νησίδων 1, 2, 3, 4, 5, 6 – Προμήθεια Υποδομών Φορέων / Υ-2.1, Υ-2.2, Υ-2.3, Υ-2.4, Υ-2.5, Υ-2.6». Ειδικότερα, η

αντικατάσταση του Λογισμικού Τηλεδιάσκεψης HUAWEI TE Desktop, με το συνδυασμό προϊόντων τηλεδιάσκεψης του κατασκευαστή Cisco, λόγω έλλειψης διαθεσιμότητας του αρχικού προϊόντος, δεν επεκτείνει σημαντικά και δεν μεταβάλλει ουσιωδώς το κύριο αντικείμενο της συμφωνίας – πλαίσιο και των εκτελεστικών αυτής συμβάσεων, στο οποίο περιλαμβάνεται, μεταξύ άλλων, η λειτουργία συστημάτων τηλεδιάσκεψης και τηλεπαρουσίας, ενώ επιπλέον, όπως ως ανωτέρω προκύπτει, δεν επιφέρει κατ' ουσίαν μεταβολή του οικονομικού αντικειμένου των ήδη υπογραφεισών συμβάσεων. Αντιθέτως, η εξεύρεση και εφαρμογή λύσεων για την υποστήριξη της υπηρεσίας τηλεδιάσκεψης / τηλεμαθημάτων για την εκπαιδευτική κοινότητα από την υπηρεσία τηλεδιάσκεψης του Έργου «ΣΥΖΕΥΞΙΣ ΙΙ», η οποία υπαγορεύτηκε και από την απαίτηση για κάλυψη των σχετικών αναγκών κατά τη διάρκεια ισχύος των περιοριστικών μέτρων που επέβαλε η πανδημία covid-19 στο σύνολο της Επικράτειας, δικαιολογείται από αντικειμενικούς λόγους, οι οποίοι σχετίζονται με το αίτημα για τεχνική επικαιροποίηση της προσφερόμενης πλατφόρμας λογισμικού τηλεδιάσκεψης. Δεν υποδηλώνεται δε με αυτόν τον τρόπο βούληση των συμβαλλόμενων μερών για επαναδιαπραγμάτευση ουσιωδών όρων των τροποποιούμενων εκτελεστικών συμβάσεων, με στόχο τη νόθευση, στο στάδιο εκτέλεσης, του ελεύθερου ανταγωνισμού, ενόψει και των προϋποθέσεων διεξαγωγής της οικείας διαγωνιστικής διαδικασίας, καθώς και του γεγονότος ότι ο συγκεκριμένος διαγωνισμός απευθύνθηκε εξαρχής σε εξειδικευμένους τεχνικά ενδιαφερόμενους φορείς. Συνεπώς, οι επίμαχες τροποποιήσεις παρίστανται σύμφωνες με τη διάταξη της παρ. 4 του άρθρου 132 του ν. 4412/2016, αφού δεν προκύπτει ότι οι σχετικές συμβάσεις εισάγουν όρους οι οποίοι, εάν είχαν αποτελέσει μέρος της αρχικής διαδικασίας σύναψης, θα είχαν επιτρέψει τη συμμετοχή διαφορετικών υποψηφίων από αυτούς που επελέγησαν αρχικώς ή στην αποδοχή άλλων προσφορών από εκείνες που προκρίθηκαν αρχικώς ή θα προσέλκυαν και άλλους συμμετέχοντες στη διαδικασία σύναψης των εν λόγω συμβάσεων.

13. Κατ' ακολουθία των ανωτέρω και λαμβάνοντας υπόψη ότι και οι λοιποί όροι περί τροποποίησης του χρονοδιαγράμματος υλοποίησης του Έργου συνέχονται με τις προμνησθείσες αλλαγές του φυσικού αντικειμένου των εκτελεστικών συμβάσεων, το Κλιμάκιο κρίνει ότι δεν συντρέχουν ουσιώδεις νομικές πλημμέλειες

που να κωλύουν την υπογραφή των ελεγχόμενων σχεδίων, αντίγραφα των οποίων τηρούνται σε ηλεκτρονική μορφή στη Γραμματεία του παρόντος Κλιμακίου.

Για τους λόγους αυτούς

Δεν κωλύεται η υπογραφή των έξι (6) σχεδίων τροποποίησης των αντίστοιχων 1453.1.2, 1453.1.3, 1453.1.4, 1453.1.5, 1453.1.6 και 1453.2.1 εκτελεστικών συμβάσεων των 1453.1/4.7.2019 και 1453.2/5.7.2019 επιμέρους συμβάσεων της 1453/2019 συμφωνίας - πλαίσιο για την ανάθεση, από την «ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ Α.Ε.», του Έργου «ΣΥΖΕΥΞΙΣ ΙΙ – Υποδομές ασφάλειας/τηλεφωνίας/τηλεδιάσκεψης/καλωδίωσης», μεταξύ αφενός της ανώνυμης εταιρείας «ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ Α.Ε.» και αφετέρου της ένωσης εταιρειών «ΟΡΓΑΝΙΣΜΟΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΤΗΣ ΕΛΛΑΔΟΣ Α.Ε., SPACE HELLAS ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΥΠΗΡΕΣΙΕΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ, ΠΛΗΡΟΦΟΡΙΚΗΣ, ΑΣΦΑΛΕΙΑΣ - ΙΔΙΩΤΙΚΗ ΕΠΙΧΕΙΡΗΣΗ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΑΣΦΑΛΕΙΑΣ και UNISYSTEMS ΣΥΣΤΗΜΑΤΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΜΟΝΟΠΡΟΣΩΠΗ ΑΝΩΝΥΜΗ ΕΜΠΟΡΙΚΗ ΕΤΑΙΡΕΙΑ» (για τις εκτελεστικές συμβάσεις 1453.1.2, 1453.1.3, 1453.1.4, 1453.1.5, 1453.1.6), καθώς και της εταιρείας περιορισμένης ευθύνης «LOGICOM SOLUTIONS LIMITED» (για την εκτελεστική σύμβαση 1453.2.1).

Ο ΠΡΟΕΔΡΟΣ **Η ΕΙΣΗΓΗΤΡΙΑ ΠΑΡΕΔΡΟΣ**

ΣΤΑΜΑΤΙΟΣ ΠΟΥΛΗΣ **ΑΘΑΝΑΣΙΑ ΜΥΡΟΦΟΡΑ ΣΙΔΗΡΟΠΟΥΛΟΥ**

Για την ακρίβεια
Αθήνα 16/03/21
Η Γραμματέας
ΕΥΣΕΤ & Σ' ΚΛΙΜΑΚΙΩΝ
ΜΑΡΙΝΑ ΠΕΤΡΟΥ

ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ Α.Ε.

Χανδρή 3, 183 46 - Μοσχάτο (Αττική) • Τηλ.: 213 1300 700 • Fax: 213 1300 800-1

http://www.ktpae.gr • e-mail: info@ktpae.gr

ΝΠΙΔ Μη Κερδοσκοπικό • Αρ. ΓΕΜΗ: 004261201000

Διεύθυνση Οικονομικής Διαχείρισης (ΟΔ)
Τμήμα Διαχείρισης Συμβάσεων (Contract Management)
Πληροφορίες : Κουρτερίδου Αθανασία
Τηλέφωνο : 213 - 1300 744
Fax : 213 - 1300 800-1
e-mail : nkourt@ktpae.gr

ΟΡΘΗ ΕΠΑΝΑΛΗΨΗ 15-02-2021
Αρ.Πρωτ.: 41/04-01-2021

Προς : Ως Πίνακας Αποδεκτών

Α Π Ο Φ Α Σ Η

ΘΕΜΑ: Τροποποίηση των υπ'αρ.**1453.1.2, 1453.1.3, 1453.1.4, 1453.1.5, 1453.1.6/10-12-2020** και **1453.2.1/7-12-2020 Εκτελεστικών Συμβάσεων** της Συμφωνίας Πλαίσιο για το έργο: «ΣΥΖΕΥΞΙΣ ΙΙ - Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης» για τα Υποέργα «ΣΥΖΕΥΞΙΣ ΙΙ – Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης– Νησίδων 1,2,3,4,5,6– Προμήθεια Υποδομών Φορέων/ Υ-2.1,Υ-2.2, Υ-2.3,Υ-2.4,Υ-2.5, Υ-2.6» του ΕΠ «Μεταρρύθμιση Δημοσίου Τομέα», με Κωδ. ΟΠΣ: 5041737.

Έχοντας υπόψη:

1. Την με αρ. C(2014) 7801_final/29-10-2014 Απόφαση της Επιτροπής των ΕΚ για την έγκριση ορισμένων στοιχείων του Συμφώνου Εταιρικής Σχέσης με την Ελλάδα.
2. Την με αρ. C(2014) 3542_final/23-05-2014 απόφαση της Ε.Ε. για την έγκριση ορισμένων στοιχείων του Συμφώνου Εταιρικής Σχέσης με την Ελλάδα και την εκτελεστική απόφαση C(2014)6582 – 24/09/2014 σχετικά με την διόρθωσή της (Κωδικός CCI 2014GR16M8PA001).
3. Την Εκτελεστική Απόφαση της Ευρωπαϊκής Επιτροπής της 17-12-2014 με αριθμό C(2014) 10138 final/17-12-2014 για την έγκριση ορισμένων στοιχείων του Επιχειρησιακού Προγράμματος (ΕΠ) «Μεταρρύθμιση Δημοσίου Τομέα» για στήριξη από το Ευρωπαϊκό Κοινωνικό Ταμείο και το Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης στο πλαίσιο του στόχου «Επενδύσεις στην ανάπτυξη και την απασχόληση» στην Ελλάδα.
4. Τον Ν. 4314/2014 «Α) Για τη διαχείριση, τον έλεγχο και την εφαρμογή αναπτυξιακών παρεμβάσεων για την προγραμματική περίοδο 2014 - 2020, Β) Ενσωμάτωση της Οδηγίας 2012/17 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Ιουνίου 2012 (ΕΕ L 156/16.6.2012) στο ελληνικό δίκαιο, τροποποίηση του ν. 3419/2005 (Α 297) και άλλες διατάξεις» (ΦΕΚ 265/Α/23-12-2014), όπως έχει τροποποιηθεί και ισχύει.
5. Την Αριθμ. 126829/ΕΥΘΥ/1217/8-12-2015 Κοινή Απόφαση των Υπουργών Οικονομίας, Ανάπτυξης και Τουρισμού - Οικονομικών "Σύστημα δημοσιονομικών διορθώσεων και διαδικασίες ανάκτησης αχρεωστήτως ή παρανόμως καταβληθέντων ποσών από πόρους του κρατικού προϋπολογισμού ΕΣΠΑ 2014 - 2020" (ΦΕΚ 2784/Β/21-12-2015).

6. Την Αριθμ. 137675/ΕΥΘΥ1016 Απόφαση του Υφυπουργού Οικονομίας & Ανάπτυξης "Αντικατάσταση της υπ' αριθμ. 110427/ΕΥΘΥ/1020/20.10.2016 (ΦΕΚ Β' 3521) υπουργικής απόφασης με τίτλο «Τροποποίηση και αντικατάσταση της υπ' αριθμ. 81986/ΕΥΘΥ712/31.7.2015 (ΦΕΚ Β' 1822) υπουργικής απόφασης "Εθνικοί κανόνες επιλεξιμότητας δαπανών για τα προγράμματα του ΕΣΠΑ 2014 - 2020 - Έλεγχοι νομιμότητας δημοσίων συμβάσεων συγχρηματοδοτούμενων πράξεων ΕΣΠΑ 2014 - 2020 από Αρχές Διαχείρισης και Ενδιάμεσους Φορείς - Διαδικασία ενστάσεων επί των αποτελεσμάτων αξιολόγησης πράξεων" (ΦΕΚ 5968/Β/31-12-2018).
7. Το Εγχειρίδιο Διαδικασιών ΣΔΕ ΕΣΠΑ 2014 - 2020.
8. Το Άρθρο Πρώτο Παρ. Ζ, Ν.4152/2013 "Επείγοντα μέτρα εφαρμογής των νόμων 4046/2012, 4093/2012 και 4127/2013" (ΦΕΚ 107/Α/09-05-2013)".
9. Το Π.Δ. 80/2016 «Ανάληψη υποχρεώσεων από τους Διατάκτες» (ΦΕΚ 145/Α/05-08-2016).
10. Τα άρθρα 74 έως 83 – «ΚΕΦΑΛΑΙΟ ΙΑ'/ΨΗΦΙΑΚΗ ΔΙΑΦΑΝΕΙΑ - ΠΡΟΓΡΑΜΜΑ ΔΙΑΥΓΕΙΑ» του Ν. 4727/23-09-2020 (ΦΕΚ/Α/184/23.09.2020) - Ψηφιακή Διακυβέρνηση (Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972) και άλλες διατάξεις.
11. Τον Ν. 4250/2014 "Διοικητικές Απλουστεύσεις - Καταργήσεις, Συγχωνεύσεις Νομικών Προσώπων και Υπηρεσιών του Δημοσίου Τομέα - Τροποποίηση Διατάξεων του π.δ. 318/1992 (Α' 161) και λοιπές ρυθμίσεις." (ΦΕΚ 74/Α/26-03-2014).
12. Τον Ν. 4412/2016 «Δημόσιες Συμβάσεις Έργων, Προμηθειών και Υπηρεσιών (προσαρμογή στις Οδηγίες 2014/24/ΕΕ και 2014/25/ΕΕ)» (ΦΕΚ 147/Α/08-08-2016), όπως τροποποιήθηκε και ισχύει.
13. Το Π.Δ. 60/2007 «Προσαρμογή της Ελληνικής Νομοθεσίας στα διατάξεις της Οδηγίας 2004/18/ΕΚ «περί συντονισμού των διαδικασιών σύναψης των δημοσίων συμβάσεων έργων, προμηθειών και υπηρεσιών», όπως τροποποιήθηκε με την οδηγία 2005/51/ΕΚ της Επιτροπής και την Οδηγία 2005/75/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 16ης Νοεμβρίου 2005.» (ΦΕΚ 64/Α/16-03-2007).
14. Τον Ν. 3614/2007 «Διαχείριση, έλεγχος και εφαρμογή αναπτυξιακών παρεμβάσεων για την προγραμματική περίοδο 2007 - 2013» (ΦΕΚ 267/Α/03-12-2007), όπως τροποποιήθηκε με τον Ν. 3840/2010 «Αποκέντρωση, απλοποίηση και ενίσχυση της αποτελεσματικότητας των διαδικασιών του Εθνικού Πλαισίου Αναφοράς (ΕΣΠΑ) 2007-2013 και άλλες διατάξεις» (ΦΕΚ 53/Α/31-03-2010) και ισχύει.
15. Την υπ' αρ. 263/24-04-2002 Κοινή Απόφαση των Υπουργών Οικονομίας και Οικονομικών και Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης «Κύρωση του Κανονισμού Προμηθειών της Εταιρείας «Κοινωνία της Πληροφορίας Α.Ε.» (ΦΕΚ 528/Β/29-04-2002)
16. Το Α.24 του Ν. 2860/2000 «Διαχείριση, παρακολούθηση και έλεγχος του κοινοτικού πλαισίου στήριξης και άλλες διατάξεις» (ΦΕΚ 251/Α/14-11-2000), όπως τροποποιήθηκε με το Α.32 του Ν. 3614/2007 «Διαχείριση, έλεγχος και εφαρμογή αναπτυξιακών παρεμβάσεων για την προγραμματική περίοδο 2007 - 2013» (ΦΕΚ 267/Α/03-12-2007), συμπληρώθηκε με το Α.59, παρ. 17 του Ν. 4314/2014 «Α) Για τη διαχείριση, τον έλεγχο και την εφαρμογή αναπτυξιακών παρεμβάσεων για την προγραμματική περίοδο 2014 - 2020, Β) Ενσωμάτωση της Οδηγίας 2012/17 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Ιουνίου 2012 (ΕΕ L 156/16.6.2012) στο ελληνικό δίκαιο, τροποποίηση του ν. 3419/2005 (Α 297) και άλλες διατάξεις» (ΦΕΚ 265/Α/23-12-2014) και ισχύει.
17. Τον Ν. 3429/2005 «Δημόσιες Επιχειρήσεις και Οργανισμοί (Δ.Ε.Κ.Ο.).» ΦΕΚ (314/Α/27-12-2005), όπως τροποποιήθηκε από Α.31, Κεφ. Β, Ν. 4465/2017 (ΦΕΚ 47/Α/04-04-2017) και «Αριθμ. 30422/ΕΓΔΕΚΟ 342 «Εξαίρεση από το πεδίο εφαρμογής του άρθρου 3 του ν.

3429/2005 της Ανώνυμης Εταιρείας «Κοινωνία της Πληροφορίας Α.Ε.» ΦΕΚ (967/Β/21-07-2006).

18. Το Α.39 του Ν. 4578 «Μείωση ασφαλιστικών εισφορών και άλλες διατάξεις» (ΦΕΚ 200/Α/03-12-2018).

19. Την υπ' αρ. 33864 ΕΞ 2020 Απόφαση του Υπουργού Επικρατείας «Τροποποίηση του καταστατικού της ανώνυμης εταιρείας "Κοινωνία της Πληροφορίας Α.Ε." και κωδικοποίηση αυτού» (ΦΕΚ Β' 5386/07-12-2020).

20. Την υπ' αρ. 252/ΓΔΟΔΥ/ΔΔΥ/2020 Απόφαση του Υπουργού Επικρατείας «Έγκριση του Κανονισμού της Ανώνυμης Εταιρείας «Κοινωνία της Πληροφορίας Α.Ε.», με κατάργηση της υπ' αριθμ. ΔΙΔΚ/ΚτΠ/οικ. 21588/04-11-2011 (Β' 2541) υπουργική απόφαση «Κανονισμός της Ανώνυμης Εταιρείας "Κοινωνία της Πληροφορίας Α.Ε."», όπως τροποποιήθηκε με την υπ' αριθμ. ΔΙΔΚ/οικ 35181/11-11-2015 (Β' 2532) κοινή υπουργική απόφαση «Τροποποίηση άρθρων του Κανονισμού της Ανώνυμης Εταιρείας "Κοινωνία της Πληροφορίας Α.Ε."» (ΦΕΚ 164/Β/29-01-2020).

21. Το Α.1, παρ. 2.1 του ΠΔ 81 "Σύσταση, συγχώνευση, μετονομασία και κατάργηση Υπουργείων και καθορισμός των αρμοδιοτήτων τους - Μεταφορά υπηρεσιών και αρμοδιοτήτων μεταξύ Υπουργείων." (ΦΕΚ 119/Α/08-07-2019).

22. Την υπ' αρ. 146 Απόφαση του Υπουργού Επικρατείας «Ορισμός του Προέδρου και των Μελών του Διοικητικού Συμβουλίου της Ανώνυμης Εταιρείας "Κοινωνία της Πληροφορίας Α.Ε."» (ΦΕΚ ΥΟΔΔ' 474/25-07-2019), σε συνέχεια της υπ' αριθμ. 90/2020/ΓΔΟΔΥ/ΔΔΥ απόφασης (ΦΕΚ ΥΟΔΔ' 60/30-01-2020), όπως τροποποιήθηκε με την αριθμ. 32273 ΕΞ 2020 «Τροποποίηση της αριθμ. 146/25-07-2019 απόφασης του Υπουργού Επικρατείας "Ορισμός του Προέδρου και των Μελών του Διοικητικού Συμβουλίου της Ανώνυμης Εταιρείας "Κοινωνία της Πληροφορίας Α.Ε." (Υ.Ο.Δ.Δ. 474)» (ΦΕΚ ΥΟΔΔ' 977/20-11-2020).

23. Την Απόφαση του ΔΣ της ΚτΠ Α.Ε. κατά την υπ' αρ. 688/30-07-2019 Συνεδρίασή του, με θέμα Εκλογή Διευθύνοντος Συμβούλου (Θέμα 1).

24. Τις υπ' αρ. **1453.1.2, 1453.1.3, 1453.1.4, 1453.1.5,1453.1.6/10-12-2020** Εκτελεστικές Συμβάσεις της Συμφωνίας Πλαίσιο για το έργο: «ΣΥΖΕΥΞΙΣ ΙΙ - Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης» για τα Υποέργα «ΣΥΖΕΥΞΙΣ ΙΙ – Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης– **Νησίδων 1,2,3,4,5**– Προμήθεια Υποδομών Φορέων/ **Υ-2.1,Υ-2.2, Υ-2.3,Υ-2.4,Υ-2.5,** μεταξύ της ένωσης εταιρειών **«ΟΤΕ Α.Ε - SPACE HELLAS A.E - UNISYSTEMS ΜΑΕ»** και της ΚτΠ Α.Ε.

25. Την υπ' αρ. **1453.2.1/7-12-2020** Εκτελεστική Σύμβαση της Συμφωνίας Πλαίσιο για το έργο: «ΣΥΖΕΥΞΙΣ ΙΙ - Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης» για το Υποέργο «ΣΥΖΕΥΞΙΣ ΙΙ – Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης– **Νησίδα 6**– Προμήθεια Υποδομών Φορέων/ **Υ-2.6**» μεταξύ της εταιρείας **«Logicom Solutions** LTD» και της ΚτΠ Α.Ε.

26. Την υπ' αρ. 12491/21-12-2020 Απόφαση της ΚτΠ Α.Ε. με θέμα: Σύσταση και συγκρότηση Επιτροπής Παρακολούθησης & Παραλαβής Έργου (ΕΠΠΕ) των υπ'αρ.1453.1.2, 1453.1.3, 1453.1.4, 1453.1.5, 1453.1.6/10-12-2020 και 1453.2.1/7-12-2020 Εκτελεστικών Συμβάσεων της Συμφωνίας Πλαίσιο για το έργο: «ΣΥΖΕΥΞΙΣ ΙΙ - Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης» για τα Υποέργα «ΣΥΖΕΥΞΙΣ ΙΙ – Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης– Νησίδων 1,2,3,4,5,6– Προμήθεια Υποδομών Φορέων/ Υ-2.1,Υ-2.2, Υ-2.3,Υ-2.4,Υ-2.5, Υ-2.6» του ΕΠ «Μεταρρύθμιση Δημοσίου Τομέα», με Κωδ. ΟΠΣ: 5041737.

27. Το υπ'αρ. 1/30-12-2020 (αρ. πρωτ. ΚτΠ ΑΕ: 13065/30-12-2020) πρακτικό της Επιτροπής Παραλαβής Έργου (ΕΠΕ).

28. Την υπ'αρ.41/4-1-2021 απόφαση της ΚτΠ Α.Ε. με θέμα: "Τροποποίηση των υπ'αρ.1453.1.2, 1453.1.3, 1453.1.4, 1453.1.5, 1453.1.6/10-12-2020 και 1453.2.1/7-12-2020 Εκτελεστικών Συμβάσεων της Συμφωνίας Πλαίσιο για το έργο: «ΣΥΖΕΥΞΙΣ ΙΙ - Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης» για τα Υποέργα «ΣΥΖΕΥΞΙΣ ΙΙ – Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης– Νησίδων 1,2,3,4,5,6– Προμήθεια Υποδομών Φορέων/ Υ-2.1,Υ-2.2, Υ-2.3,Υ-2.4,Υ-2.5, Υ-2.6» του ΕΠ «Μεταρρύθμιση Δημοσίου Τομέα», με Κωδ. ΟΠΣ: 5041737".
29. Το από 12-2-2021 (Α/Α 330284 Docutracks) ορθή επανάληψη του Ενημερωτικού Σημειώματος από το Τμήμα Δικτύου Δημόσιου Τομέα.
30. Την Απόφαση του ΔΣ της ΚτΠ Α.Ε. κατά την υπ' αρ. 713ης/5-2-2020 (Θέμα 7.3) Συνεδρίασή του.

Α π ο φ α σ ί ζ ο υ μ ε

Τροποποίηση των υπ'αρ.**1453.1.2, 1453.1.3, 1453.1.4, 1453.1.5, 1453.1.6/10-12-2020** και **1453.2.1/7-12-2020 Εκτελεστικών Συμβάσεων** της Συμφωνίας Πλαίσιο για το έργο: «ΣΥΖΕΥΞΙΣ ΙΙ - Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης» για τα Υποέργα «ΣΥΖΕΥΞΙΣ ΙΙ – Υποδομές ασφάλειας / τηλεφωνίας / τηλεδιάσκεψης / καλωδίωσης– Νησίδων 1,2,3,4,5,6– Προμήθεια Υποδομών Φορέων/ Υ-2.1,Υ-2.2, Υ-2.3,Υ-2.4,Υ-2.5, Υ-2.6» του ΕΠ «Μεταρρύθμιση Δημοσίου Τομέα», με Κωδ. ΟΠΣ: 5041737, σύμφωνα με το υπ'αρ.1/30-12-2020 πρακτικό της ΕΠΠΕ, ως ακολούθως:

1. Την έγκριση των αιτημάτων τροποποίησης του λογισμικού τηλεδιάσκεψης για τις εκτελεστικές συμβάσεις 1453.1.2, 1453.1.3, 1453.1.4, 1453.1.5, 1453.1.6, 1453.2.1, όπως αυτά υποβλήθηκαν στην ΚτΠ Α.Ε., από τους αντισυμβαλλόμενους Αναδόχους, με τη διευκρίνηση ότι οι άδειες χρήσης Cisco Webex, δύναται να καταναλωθούν είτε όλες μαζί σε ένα (1) έτος ή τμηματικά στη διάρκεια των τριών (3) ετών του έργου, εφόσον η Αναθέτουσα Αρχή το κρίνει απαραίτητο.

2. Την τροποποίηση του Φυσικού Αντικειμένου και Οικονομικού Αντικειμένου των παραπάνω Εκτελεστικών Συμβάσεων ως εξής:

a. <u>Εκτελεστική σύμβαση 1453.1.2</u>

Προσφορά	Είδος	ΔΙΑΡΚΕΙΑ ΧΡΗΣΗΣ	ΑΡΙΘΜΟΣ ΜΟΝΑΔΩΝ	ΚΟΣΤΟΣ ΑΝΑ ΜΟΝΑΔΑ ΧΩΡΙΣ ΦΠΑ (€)	ΣΥΝΟΛΙΚΟ ΚΟΣΤΟΣ ΧΩΡΙΣ ΦΠΑ (€)
16	HUAWEI TE Desktop	36 μήνες	6.493	57	**€ 370.101,00**
			αντικαθίσταται με		
16.1	Webex Meetings for Education	12 μήνες	22.221	14	€ 311.094,00
16.2	Cisco Jabber	36 μήνες	1.035	57	€ 58.995,00
			Σύνολο		**€ 370.089,00**

b. Εκτελεστική σύμβαση 1453.1.3

Προσφορά	Είδος	ΔΙΑΡΚΕΙΑ ΧΡΗΣΗΣ	ΑΡΙΘΜΟΣ ΜΟΝΑΔΩΝ	ΚΟΣΤΟΣ ΑΝΑ ΜΟΝΑΔΑ ΧΩΡΙΣ ΦΠΑ (€)	ΣΥΝΟΛΙΚΟ ΚΟΣΤΟΣ ΧΩΡΙΣ ΦΠΑ (€)
16	HUAWEI TE Desktop	36 μήνες	4.531	57	**€ 258.267,00**
			αντικαθίσταται με		
16.1	Webex Meetings for Education	12 μήνες	15.508	14	€ 217.112,00
16.2	Cisco Jabber	36 μήνες	722	57	€ 41.154,00
			Σύνολο		**€ 258.266,00**

c. Εκτελεστική σύμβαση 1453.1.4

Προσφορά	Είδος	ΔΙΑΡΚΕΙΑ ΧΡΗΣΗΣ	ΑΡΙΘΜΟΣ ΜΟΝΑΔΩΝ	ΚΟΣΤΟΣ ΑΝΑ ΜΟΝΑΔΑ ΧΩΡΙΣ ΦΠΑ (€)	ΣΥΝΟΛΙΚΟ ΚΟΣΤΟΣ ΧΩΡΙΣ ΦΠΑ (€)
16	HUAWEI TE Desktop	36 μήνες	5.086	57	**€ 289.902,00**
			αντικαθίσταται με		
16.1	Webex Meetings for Education	12 μήνες	17.405	14	€ 243.670,00
16.2	Cisco Jabber	36 μήνες	811	57	€ 46.227,00
			Σύνολο		**€ 289.897,00**

d. Εκτελεστική σύμβαση 1453.1.5

Προσφορά	Είδος	ΔΙΑΡΚΕΙΑ ΧΡΗΣΗΣ	ΑΡΙΘΜΟΣ ΜΟΝΑΔΩΝ	ΚΟΣΤΟΣ ΑΝΑ ΜΟΝΑΔΑ ΧΩΡΙΣ ΦΠΑ (€)	ΣΥΝΟΛΙΚΟ ΚΟΣΤΟΣ ΧΩΡΙΣ ΦΠΑ (€)
16	HUAWEI TE Desktop	36 μήνες	5.538	57	**€ 315.666,00**
			αντικαθίσταται με		
16.1	Webex Meetings for Education	12 μήνες	18.952	14	€ 265.328,00
16.2	Cisco Jabber	36 μήνες	883	57	€ 50.331,00
			Σύνολο		**€ 315.659,00**

e. Εκτελεστική σύμβαση 1453.1.6

Προσφορά	Είδος	ΔΙΑΡΚΕΙΑ ΧΡΗΣΗΣ	ΑΡΙΘΜΟΣ ΜΟΝΑΔΩΝ	ΚΟΣΤΟΣ ΑΝΑ ΜΟΝΑΔΑ ΧΩΡΙΣ ΦΠΑ (€)	ΣΥΝΟΛΙΚΟ ΚΟΣΤΟΣ ΧΩΡΙΣ ΦΠΑ (€)
16	HUAWEI TE Desktop	36 μήνες	11.632	57	**€ 663.024,00**
		αντικαθίσταται με			
16.1	Webex Meetings for Education	12 μήνες	39.806	14	€ 557.284,00
16.2	Cisco Jabber	36 μήνες	1.855	57	€ 105.735,00
		Σύνολο			**€ 663.019,00**

f. Εκτελεστική σύμβαση 1453.2.1

	Α	*Β*	*Γ*	*Δ*	*Ε*	
i	*Είδος [1]*	*ΜΕΓΙΣΤΗ ΕΠΙΤΡΕΠΟΜΕΝΗ ΤΙΜΗ ΧΩΡΙΣ ΦΠΑ (€)*	*ΑΡΙΘΜΟΣ ΜΟΝΑΔΩΝ (*)*	*ΚΟΣΤΟΣ ΑΝΑ ΜΟΝΑΔΑ ΧΩΡΙΣ ΦΠΑ (€) Δ≤Β*	*ΣΥΝΟΛΙΚΟ ΚΟΣΤΟΣ ΧΩΡΙΣ ΦΠΑ (€) Γ*Δ*	
16	***Desktop Conf Clients***	***57,72 €***	***11.720***	***57,00 €***	***668.040,00 €***	
		αντικαθίσταται με				
16.1	*Cisco Jabber*		***1.869***	***57,00 €***	***106.533,00 €***	
16.2	*Cisco Webex*		***40.108***	***14,00 € (ανά χρήστη – ανά έτος)***	***561.512,00 €***	
	ΣΥΝΟΛΟ				***668.045,00€***	
	ΤΕΛΙΚΟ ΣΥΝΟΛΙΚΟ ΚΟΣΤΟΣ				***668.040,00€ (-5,00€)***	

3. Την απομείωση του συμβατικού τιμήματος των κάτωθι εκτελεστικών συμβάσεων και την διαμόρφωση του ως ακολούθως:
   - Υπ'αρ. 1453.1.2: € 20.345.665,80
   - Υπ'αρ. 1453.1.3: € 14.180.581,72
   - Υπ'αρ. 1453.1.4 : € 18.370.128,80
   - Υπ'αρ. 1453.1.5: € 20.933.558,36
   - Υπ'αρ. 1453.1.6: € 27.267.875,90

Κατ' εξουσιοδότηση του Διοικητικού Συμβουλίου

Ο Διευθύνων Σύμβουλος

Σταύρος Ασθενίδης

Συνημμένα:
Υπ᾽αρ. 41/4-1-2021 απόφαση της ΚτΠ Α.Ε.
Κοινοποίηση:
- Γραφείο Υπουργού Ψηφιακής Διακυβέρνησης
- Γραφείο Γενικού Γραμματέα Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης
- Γραφείο Υφυπουργού Οικονομικών, αρμόδιου για τη Δημοσιονομική Πολιτική
- Γραφείο Γενικού Γραμματέα Δημοσίων Επενδύσεων ΕΣΠΑ
- Γραφείο Προϊσταμένου ΕΥΔΕ -ΤΠΕ
- Ενδιαφερόμενους (Μέλη ΕΠΠΕ)

Εσωτερική Διανομή:
- Γραμματεία Προέδρου ΔΣ
- Γραμματεία Διευθύνοντος Συμβούλου
- Διεύθυνση Διοίκησης & Οικονομικής Διαχείρισης
- Δ/νση Υποστήριξης Υποδομών (ΥΥ) /(Υπ. Τομέα, Υπεύθυνο Έργου Β.Θωμόπουλος)

ΠΙΝΑΚΑΣ ΑΠΟΔΕΚΤΩΝ ΤΗΣ ΑΝΩΤΕΡΩ ΑΠΟΦΑΣΗΣ ΤΗΣ ΚτΠ Α.Ε

Α/Α	ΕΤΑΙΡΕΙΑ / ΕΝΩΣΗ ΕΤΑΙΡΕΙΩΝ	ΑΝΤΙΚΛΗΤΟΣ	ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ
1.	LOGICOM SOLUTIONS LTD	ΜΙΧΑΗΛ ΠΑΠΑΝΤΩΝΙΟΥ ΜΑΡΙΟΣ ΒΑΣΙΛΕΙΟΥ	**Δ/ΝΣΗ:** Λ. ΚΕΝΕΝΤΥ 50, ΛΕΥΚΩΣΙΑ 1076 ΤΗΛ: 0035722551210150-53 ΦΑΞ: 0035722660969 E-MAIL: m.papantoniou@logicom.net m.vassiliou@logicom.net
2.	OTE A.E. - SPACE HELLAS A.E. - UNISYSTEMS A.E.	ΛΥΚΟΥΡΓΟΣ ΑΝΤΩΝΟΠΟΥΛΟΣ	**Δ/ΝΣΗ:** Λ. Κηφισίας, 99 Μαρούσι 151 24 ΤΗΛ: 210 6115365 ΦΑΞ: 2106117739 E-MAIL: lantonopoulos@ote.gr

CISCO

Ministry of Education and Religious Affairs of Greece
Andrea Papandreou st., 37
15180 Marousi (Athens)
Greece

Subject: Letter of Agreement regarding the applicability of certain additional data protection terms to the EUIFs and the EA Program Terms entered into between Cisco and the Ministry of Education and Religious Affairs of Greece

Dear Sir/Madam,

Whereas:

A. **Cisco Hellas S.A** (**"Cisco"**) and the **Ministry of Education and Religious Affairs of Greece** (the "**Ministry**") previously entered into:
   i) A Master Data Protection Agreement dated 13th March 2020 with Cisco ref. #152385 (the **"MDPA"**), attached hereto, which includes:
      a) An Annex entitled "Privacy Data Sheet - Cisco Webex Meetings"; and
      b) An Annex entitled "Clarification Appendix",
   ii) An Agreement for the Free Trial of the Cisco Webex teleconferencing platform for the realization of modern distance learning in the educational system dated 9th November 2020 with Cisco ref. #155930 (the "**Free Trial Agreement**"), as amended by the Parties under the Amendment to the Free Trial Agreement dated 4th December 2020 with Cisco ref. #158293, which includes a Section 2 (Protection of Personal Data) reiterating the duties and responsibilities undertaken by the parties in
      a) the above MDPA, and in
      b) the Free Trial Agreement entered between the Ministry and Cisco Hellas S.A., dated 13th March 2020, and the Free Trial Agreement entered between the Ministry and Cisco Hellas S.A., dated 11th September 2020, attached hereto.

B. The Ministry has signed:
   i) The End User Information Form For End Users of the Cisco Flex Plans and Cisco Collaboration Flex Plan Education (2 **EUIFs**) dated 7th January 2021 and
   ii) the corresponding Cisco Enterprise Agreement Program Terms and Conditions for End Users (**EA Program Terms**) dated 7th January 2021.

C. Following a public procurement process for the procurement of teleconferencing software and relevant contracts, the entity of the Ministry of Digital Governance operating under the name "Society of Information SA" issued a Decision No. 41 dated 4-JAN-2021, according to which, among others, the following number of WEBEX MEETINGS FOR EDUCATION LICENCES were allocated to the Ministry of Education and Religious Affairs of Greece:

	No. of Licences
1.	22.221
2.	15.508
3.	17.405
4.	18.952
5.	39.806
6.	40.108
TOTAL	154.000

Cisco and the Ministry, who confirms acceptance by countersigning this letter (the "**Letter of Agreement**"), now hereby agree to apply the data protection terms referenced above to the EUIFs and the EA Program Terms referenced above on the basis of the following terms agreed herein:

1. This Letter of Agreement is valid from 11th January 2021 (the "**Effective Date**") until the end of the term of the EUIFs and EA Program Terms (the "**Term**").

2. This Letter of Agreement shall be governed by the terms of the EUIFs and EA Program Terms.

3. Unless the context determines otherwise, any defined terms used in this Letter of Agreement but not defined herein shall have the meanings given in the EUIFs and EA Program Terms, the MDPA or the Free Trial Agreement. In the event of a conflict between this Letter of Agreement and the EUIFs and EA Program Terms, this Letter of Agreement shall prevail but only with regards the subject matter herein. Subject to the terms of this Letter of Agreement, all other terms and conditions the EUIFs and EA Program Terms remain unchanged and in full force and effect.

4. Cisco agrees that, from the Effective Date, the terms of the following documents executed by the Parties shall apply to the EUIFs and EA Program Terms:
   i) Master Data Protection Agreement dated 13th March 2020 (the "**MDPA**") stipulated under A.i) above.
   ii) Section 2 (Protection of Personal Data) of the Agreement for the Free Trial of the Cisco Webex teleconferencing platform for the realization of modern distance learning in the educational system dated 9th November 2020 (the "**Free Trial Agreement**"), as amended by the Parties under the Amendment to the Free Trial Agreement dated 4th December 2020 stipulated under under A.ii) above.

5. This Letter of Agreement constitutes the entire agreement between the parties concerning the subject matter of this Letter of Agreement and replaces any prior oral or written communications between the parties, all of which are excluded. There are no conditions, understandings, agreements, representations or warranties, expressed or implied, that are not specified herein. This Letter of Agreement may be modified only by a written document executed by the parties hereto.

6. The parties have caused this Letter of Agreement to be duly executed. Each party represents that its respective signatories whose signatures appear below have been and are on the date of signature duly authorized to execute this Letter of Agreement.

7. This Letter of Agreement may be executed in two or more counterparts, each of which shall be deemed an original and together which shall constitute one and the same instrument. A validly executed counterpart that is delivered by one party to the other via electronic transmission (a "**Counterpart Image**") shall be valid and binding to the same extent as one delivered physically, provided that the valid signature is clearly visible in the Counterpart Image.

8. The validity, interpretation, and performance of this Letter of Agreement shall be controlled by and construed under the laws of Greece and the Courts of Athens, Greece shall have exclusive jurisdiction over any claim arising under this letter.

AGREED by the parties through their authorized signatories.

Signed for and on behalf of
Cisco International Limited:

Signature: _____

Name (Printed): **James Glenister**
DIRECTOR.MGMT-FINANCE

Title: _____

Date: 01 February 2021

APPROVED BY LEGAL

CISCO
Cisco International Limited
9-11 New Square Park
Bedfont Lakes, Feltham
Middlesex, TW14 8HA
United Kingdom

Signed for and on behalf of the
Ministry of Education and Religious Affairs of Greece:

Signature: _____

Name (Printed): ΝΙΚΗ ΚΕΡΑΜΕΩΣ

Title: Minister of Education and Religious Affairs

Date: 1/2/2021

Η συνημμένη στην ελληνική γλώσσα μετάφραση αφορά το παρόν στην αγγλική γλώσσα έγγραφο.

Αθήνα, 1/2/2021

Η μεταφράσασα δικηγόρος

ΕΙΡΗΝΗ Γ. ΚΑΠΕΛΛΑΚΗ
ΔΙΚΗΓΟΡΟΣ - ΑΜ ΔΣΑ 31124
ΠΕΝΤΕΛΗΣ 58 - ΚΗΦΙΣΙΑ 145 62
ΤΗΛ: 210 6013843 - 6945087480
e-mail: ekapellaki@gmail.com
ΑΦΜ: 103603599 - ΔΟΥ ΚΑΘΕΝΤΡΩΝ

ΕΙΡΗΝΗΝ Γ.
ΔΙΚΗΓΟΡΟΣ
ΠΕΝΤΕΛΗΣ 5
ΤΗΛ: 210 60
e-mail: ekap
ΑΦΜ: 103603

CISCO

Υπουργείο Παιδείας και Θρησκευμάτων
Ανδρέα Παπανδρέου 37
15180 Μαρούσι (Αθήνα)
Ελλάδα

Θέμα: Επιστολή Συμφωνίας σχετικά με την εφαρμογή συγκεκριμένων επιπλέον όρων για την προστασία των προσωπικών δεδομένων επιπλέον εκείνων που περιέχονται στα Ενημερωτικά Έντυπα Τελικού Χρήστη (EUIFs) και στους Όρους και Προϋποθέσεις για Τελικούς Χρήστες του Προγράμματος Cisco Enterprise Agreement (EA PROGRAM TERMS) μεταξύ της Cisco και του Υπουργείου Παιδείας και Θρησκευμάτων της Ελλάδας

Αγαπητέ/η κύριε/κυρία,

Λαμβάνοντας υπόψιν ότι:

Α. Η Cisco Ελλάς Α.Ε. («Cisco») και το Υπουργείο Παιδείας και Θρησκευμάτων («το Υπουργείο») έχουν προγενέστερα συνάψει:

i) Την από 13.03.2020 Σύμβαση Πλαίσιο για την Προστασία των Προσωπικών Δεδομένων με αριθμό αναφοράς Cisco #152385 (Master Data Protection Agreement – «MDPA»), που επισυνάπτεται στην παρούσα, η οποία περιλαμβάνει:

α) το Παράρτημα με τίτλο « Φύλλο Προστασίας Προσωπικών Δεδομένων για το Cisco Webex Meetings» («Privacy Data Sheet Cisco Webex Meetings») και

β) το Παράρτημα με τίτλο «Διευκρινιστικό Παράρτημα» («Clarification Appendix»),

ii) Την από 09.11.2020 Σύμβαση Δωρεάν Παραχώρησης της πλατφόρμας τηλεδιασκέψεων Cisco Webex για την πραγματοποίηση σύγχρονης εξ αποστάσεως διδασκαλίας στο εκπαιδευτικό σύστημα με αριθμό αναφοράς Cisco #155930 (η «Σύμβαση Δωρεάν Παραχώρησης»), όπως τροποποιήθηκε από τα συμβαλλόμενα μέρη με την από 04.12.2020 Τροποποιητική Πράξη της Σύμβασης Δωρεάν Παραχώρησης με αριθμό αναφοράς Cisco #158293, η οποία περιλαμβάνει το Άρθρο 2 (Προστασία Προσωπικών Δεδομένων), στην οποία επαναλαμβάνονται τα καθήκοντα και οι υποχρεώσεις που ανέλαβαν τα μέρη σύμφωνα με:

α) την προαναφερθείσα από 13.02.2020 Σύμβαση Πλαίσιο για την Προστασία των Προσωπικών Δεδομένων (Master Data Protection Agreement – «MDPA»), και

β) τη Σύμβαση Δωρεάν Παραχώρησης που υπεγράφη μεταξύ του Υπουργείου και της Cisco Ελλάς Α.Ε. στις 13.03.2020 και τη Σύμβαση Δωρεάν Παραχώρησης που υπεγράφη μεταξύ του Υπουργείου και της Cisco Ελλάς Α.Ε. στις 11.09.2020, οι οποίες επισυνάπτονται στο παρόν.

Β. Το Υπουργείο έχει υπογράψει:

i) Το Ενημερωτικό Έντυπο Τελικού Χρήστη (End User Information Form) για τους Τελικούς Χρήστες των Προγραμμάτων Flex και Collaboration Flex Plan Education της Cisco με ημερομηνία 7 Ιανουαρίου 2021 και

ii) τους αντίστοιχους Όρους και Προϋποθέσεις για Τελικούς Χρήστες του Προγράμματος Cisco Enterprise Agreement με ημερομηνία 7 Ιανουαρίου 2021.

Γ. Μετά τη διεξαγωγή δημόσιου διαγωνισμού για την προμήθεια λογισμικού τηλεδιασκέψεων και συναφών αντικειμένων, ο εποπτευόμενος από το Υπουργείο Ψηφιακής Διακυβέρνησης φορέας με την επωνυμία «Κοινωνία της Πληροφορίας Α.Ε.» εξέδωσε την υπ' αριθμόν 41/04.01.2021 Απόφαση, με την οποία αποφασίστηκε, μεταξύ άλλων, η διάθεση στο Υπουργείο Παιδείας και Θρησκευμάτων των παρακάτω αδειών χρήσης του προγράμματος WEBEX MEETINGS FOR EDUCATION:

ΔΙΚΗΓΟΡΟΣ
ΠΕΝΤΕΛΗΣ 56
ΤΗΛ: 210 601
e-mail: ekap

	Αριθμός Αδειών Χρήσης
1.	22.221
2.	15.508
3.	17.405
4.	18.952
5.	39.806
6.	40.108
ΣΥΝΟΛΟ	154.000

Η Cisco και το Υπουργείο, το οποίο επιβεβαιώνει την αποδοχή της παρούσας επιστολής συμφωνίας με την προσυπογραφή της (η «Επιστολή Συμφωνίας»), συμφωνούν την εφαρμογή των προαναφερθέντων όρων για την προστασία των προσωπικών δεδομένων στα Ενημερωτικά Έντυπα Τελικού Χρήστη (EUIFs) και στους Όρους και Προϋποθέσεις για Τελικούς Χρήστες του Προγράμματος Cisco Enterprise Agreement (EA PROGRAM TERMS), σύμφωνα με τους παρακάτω όρους που συμφωνούνται στο παρόν:

1. Η παρούσα Επιστολή Συμφωνίας ισχύει από τις 11 Ιανουαρίου 2021 (η «Ημερομηνία Έναρξης Ισχύος») μέχρι τη λήξη της διάρκειας των Ενημερωτικών Εντύπων Τελικού Χρήστη (EUIFs) και των Όρων και Προϋποθέσεων για Τελικούς Χρήστες του Προγράμματος Cisco Enterprise Agreement (EA PROGRAM TERMS) (η «Διάρκεια Ισχύος»).

2. Η παρούσα Επιστολή Συμφωνίας διέπεται από τους όρους των Ενημερωτικών Εντύπων Τελικού Χρήστη (EUIFs) και των Όρων και Προϋποθέσεων για Τελικούς Χρήστες του Προγράμματος Cisco Enterprise Agreement (EA PROGRAM TERMS).

3. Εκτός εάν το περιεχόμενο της παρούσας καθορίζει διαφορετικά, τυχόν ορισμοί που χρησιμοποιούνται στην παρούσα αλλά δεν ορίζονται σε αυτήν έχουν τις έννοιες που προσδιορίσθηκαν στα Ενημερωτικά Έντυπα Τελικού Χρήστη (EUIFs) και στους Όρους και Προϋποθέσεις για Τελικούς Χρήστες του Προγράμματος Cisco Enterprise Agreement (EA PROGRAM TERMS), στη Σύμβαση Πλαίσιο για την Προστασία των Προσωπικών Δεδομένων (Master Data Protection Agreement – «MDPA») και στη Σύμβαση Δωρεάν Παραχώρησης. Σε περίπτωση σύγκρουσης μεταξύ της παρούσας και των όρων των Ενημερωτικών Εντύπων Τελικού Χρήστη και των Όρων και Προϋποθέσεων για Τελικούς Χρήστες του Προγράμματος Cisco Enterprise Agreement, η παρούσα επιστολή συμφωνίας υπερισχύει αλλά μόνο όσον αφορά το αντικείμενο της. Με την επιφύλαξη των όρων της παρούσας επιστολής συμφωνίας, όλοι οι άλλοι όροι και προϋποθέσεις των Ενημερωτικών Εντύπων Τελικού Χρήστη και των Όρων και Προϋποθέσεων για Τελικούς Χρήστες του Προγράμματος Cisco Enterprise Agreement δεν επηρεάζονται και παραμένουν σε πλήρη ισχύ.

4. Η Cisco συμφωνεί ότι από την Ημερομηνία Έναρξης Ισχύος, οι όροι των παρακάτω εγγράφων που έχουν υπογραφεί από τα συμβαλλόμενα μέρη θα εφαρμόζονται στα Ενημερωτικά Έντυπα Τελικού Χρήστη (EUIFs) και στους Όρους και Προϋποθέσεις για Τελικούς Χρήστες του Προγράμματος Cisco Enterprise Agreement (EA PROGRAM TERMS):

i) Της από από 13.03.2020 Σύμβασης Πλαίσιο για την Προστασία των Προσωπικών Δεδομένων (Master Data Protection Agreement – «MDPA») που αναφέρεται ανωτέρω στην παράγραφο A.i) της παρούσας.

ii) Του Άρθρου 2 (Προστασία Προσωπικών Δεδομένων) της από 09.11.2020 Σύμβασης για την Δωρεάν Παραχώρηση της πλατφόρμας τηλεδιασκέψεων Cisco Webex για την πραγματοποίηση της σύγχρονης εξ αποστάσεως διδασκαλίας στο εκπαιδευτικό σύστημα (η «Σύμβαση Δωρεάν Παραχώρησης»), όπως τροποποιήθηκε από τα συμβαλλόμενα μέρη με την από 04.12.2020 Τροποποίηση της Σύμβασης Δωρεάν Παραχώρησης, η οποία αναφέρεται ανωτέρω παράγραφο A.ii) της παρούσας.

ΚΑΠΕΛΛΑΚΗ
- ΑΜ ΔΣΑ 31124
- ΚΗΦΙΣΙΑ 145 62
3843 - 6945087480
ekapellaki@gmail.com
99 - ΔΟΥ: ΚΗΦΙΣΙΑΣ

5. Η παρούσα επιστολή συμφωνίας αποτελεί τη συνολική συμφωνία μεταξύ των συμβαλλομένων μερών αναφορικά με το αντικείμενο της παρούσας επιστολή συμφωνίας και αντικαθιστά οποιεσδήποτε προγενέστερες προφορικές ή γραπτές επικοινωνίες / συμφωνίες μεταξύ των συμβαλλομένων μερών, οι οποίες δεν ισχύουν. Δεν ισχύουν όροι, συνεννοήσεις, συμφωνίες, δηλώσεις ή εγγυήσεις, ρητές ή σιωπηρές, που δεν καθορίζονται στην παρούσα Η παρούσα επιστολή συμφωνίας δύναται να τροποποιηθεί με έγγραφο που θα υπογράφεται από τα συμβαλλόμενα στο παρόν μέρη.

6. Τα συμβαλλόμενα μέρη υπέγραψαν την παρούσα επιστολή συμφωνίας προσηκόντως. Κάθε συμβαλλόμενο μέρος δηλώνει ότι οι αντίστοιχοι υπογράφοντες, των οποίων οι υπογραφές εμφανίζονται παρακάτω έχουν (εξουσιοδοτηθεί) και είναι κατά την ημερομηνία υπογραφής αρμοδίως εξουσιοδοτημένοι να υπογράψουν την παρούσα επιστολή συμφωνίας.

7. Η παρούσα επιστολή συμφωνίας δύναται να υπογραφεί σε δύο ή περισσότερα αντίτυπα, καθένα εκ των οποίων θεωρείται πρωτότυπο και από κοινού αποτελούν το ίδιο ένα έγγραφο. Ένα εγκύρως υπογεγραμμένο αντίτυπο που παραδίδεται από το ένα συμβαλλόμενο μέρος στο άλλο μέσω ηλεκτρονικής διαβίβασης («Εικόνα Αντιτύπου») είναι έγκυρο και έχει την ίδια δεσμευτική ισχύ όπως ένα αντίτυπο που παραδίδεται με φυσικό τρόπο, υπό την προϋπόθεση ότι η έγκυρη υπογραφή είναι εμφανώς ορατή στην Εικόνα Αντιτύπου.

8. Η εγκυρότητα, ερμηνεία και εκτέλεση της παρούσας επιστολής συμφωνίας διέπεται και ερμηνεύεται σύμφωνα με την Ελληνική νομοθεσία και τα Δικαστήρια της Αθήνας έχουν αποκλειστική δικαιοδοσία επί οποιασδήποτε διαφοράς τυχόν ανακύψει σχετικά με την παρούσα.

Συμφωνήθηκε από τα συμβαλλόμενα μέρη με την υπογραφή των εξουσιοδοτημένων υπογραφόντων προσώπων.

Υπεγράφη από και για λογαριασμό της Cisco International Limited
Υπογραφή: (υπογραφή)
Ονοματεπώνυμο: James Glenister
Ιδιότητα: Διευθυντής Διοίκησης Οικονομικού
Ημερομηνία: 01 Φεβρουαρίου 2021
(Εγκρίθηκε από τη νομική υπηρεσία της Cisco International Limited)

Υπεγράφη από και για λογαριασμό του Υπουργείου Παιδείας και Θρησκευμάτων
Υπογραφή: (υπογραφή)
Ονοματεπώνυμο: Νίκη Κεραμέως
Ιδιότητα: Υπουργός Παιδείας και Θρησκευμάτων
Ημερομηνία: 01 Φεβρουαρίου 2021
(σφραγίδα Υπουργείου Παιδείας και Θρησκευμάτων)

Η παρούσα μετάφραση στην Ελληνική γλώσσα αφορά
το συνημμένο στην Αγγλική γλώσσα έγγραφο.
Αθήνα, 01.02.2021
Η μεταφράσασα δικηγόρος

ΕΙΡΗΝΗ Ε. ΚΑΠΕΛΛΑΚΗ
ΔΙΚΗΓΟΡΟΣ ΑΜ ΔΣΑ 31124
ΠΕΝΤΕΛΗΣ 58 - ΚΗΦΙΣΙΑ 145 62
ΤΗΛ: 210 8013843 - 6945087480
e-mail: ekapellaki@gmail.com
ΑΦΜ 106403699 - ΔΟΥ ΚΗΦΙΣΙΑΣ

Σύμβαση δωρεάν παραχώρησης της πλατφόρμας τηλεδιασκέψεων WEBEX για την πραγματοποίηση σύγχρονης εξ αποστάσεως διδασκαλίας στο εκπαιδευτικό σύστημα. – Τροποποιητική Πράξη

Στον τόπο και κατά το χρόνο που αναφέρονται παρακάτω, οι εδώ συμβαλλόμενοι:

ΑΦ' ΕΝΟΣ

Το Ελληνικό Δημόσιο, όπως νομίμως εκπροσωπείται από την Υπουργό Παιδείας και Θρησκευμάτων (το «πρώτο Συμβαλλόμενο Μέρος»),

ΑΦ' ΕΤΕΡΟΥ

Η εταιρεία με την επωνυμία «CISCO HELLAS A.E.», η οποία εδρεύει στην Αθήνα (Λεωφόρος Κηφισίας 44, Μαρούσι) όπως νομίμως εκπροσωπείται από το Γενικό Διευθυντή Αντώνη Τσιμπούκη (το «δεύτερο Συμβαλλόμενο Μέρος»),

συλλογικά αναφερόμενοι ως «**Συμβαλλόμενα Μέρη**» και μεμονωμένα ως «**Συμβαλλόμενο Μέρος**».

συμφωνούν αμοιβαίως την τροποποίηση του άρθρου υπ' αρ. 2 «**Προστασία Προσωπικών Δεδομένων**» της από 09/11/2020 μεταξύ τους Σύμβασης με αντικείμενο τη δωρεάν παραχώρηση της πλατφόρμας τηλεδιασκέψεων WEBEX για την πραγματοποίηση σύγχρονης εξ αποστάσεως διδασκαλίας κατά το σχολικό έτος 2020-2021 ως εξής:

«2.1. Στο δεύτερο Συμβαλλόμενο Μέρος θα καταστούν διαθέσιμα προσωπικά δεδομένα για λογαριασμό του πρώτου Συμβαλλόμενου Μέρους από το νομικό πρόσωπο ιδιωτικού δικαίου μη κερδοσκοπικού χαρακτήρα με την επωνυμία «Ινστιτούτο Τεχνολογίας Υπολογιστών και Εκδόσεων "Διόφαντος" (Ι.Τ.Υ.Ε.)», το οποίο επιτελεί, εν προκειμένω, ρόλο «Εκτελούντος την Επεξεργασία», σύμφωνα με το άρ. 4 περ. 8 του Γενικού Κανονισμού για την Προστασία Δεδομένων ((ΕΕ) 2016/679, εφεξής «ΓΚΠΔ»). Περαιτέρω, το δεύτερο Συμβαλλόμενο Μέρος θα επεξεργαστεί για λογαριασμό του πρώτου Συμβαλλόμενου Μέρους δεδομένα προσωπικού χαρακτήρα, τα οποία είτε θα καταστούν διαθέσιμα στο δεύτερο Συμβαλλόμενο Μέρος από το ως άνω Ινστιτούτο «Διόφαντος», είτε θα εισαχθούν από τους ίδιους τους χρήστες στην πλατφόρμα WEBEX, είτε θα προκύψουν ως αποτέλεσμα συνδυασμού/συσχέτισης κατά τη λειτουργία της εν λόγω πλατφόρμας, είτε θα διαβιβαστούν με οποιονδήποτε τρόπο στο δεύτερο Συμβαλλόμενο Μέρος αποκλειστικά προς εκπλήρωση του σκοπού της παρούσας Σύμβασης, όπως ανωτέρω περιγράφηκε.

2.2. Το δεύτερο Συμβαλλόμενο Μέρος δεν επιτρέπεται να προβεί σε οποιαδήποτε χρήση των προσωπικών δεδομένων που θα επεξεργαστεί για την εκτέλεση της παρούσας Σύμβασης για σκοπούς εκτός του αντικειμένου αυτής, όπως ανωτέρω περιγράφηκε. Ιδιαίτερα, οφείλει να απέχει από κάθε χρήση των προσωπικών δεδομένων που θα διαβιβαστούν / τύχουν επεξεργασίας στο πλαίσιο της παρούσας Σύμβασης (π.χ. διευθύνσεις ηλεκτρονικού ταχυδρομείου) για προωθητικές ή άλλες εμπορικές ενέργειες που δεν συνδέονται με τον σκοπό της παρούσας Σύμβασης. Επιπλέον, το δεύτερο Συμβαλλόμενο Μέρος δεσμεύεται να τηρεί τα προβλεπόμενα στον ΓΚΠΔ και τον Ν. 4624/2019 σε σχέση με τα προσωπικά δεδομένα που θα επεξεργαστεί για λογαριασμό του πρώτου Συμβαλλόμενου Μέρους.

2.3. Το δεύτερο Συμβαλλόμενο Μέρος υποχρεούται, μόλις εκπληρωθεί ο σκοπός της παρούσας Σύμβασης, να προβεί αμελλητί, κατόπιν σχετικού αιτήματος του πρώτου Συμβαλλόμενου Μέρους, σε διαγραφή των προσωπικών δεδομένων που θα έχει επεξεργαστεί για λογαριασμό του πρώτου Συμβαλλόμενου Μέρους, εκτός αν άλλως απαιτείται εκ του νόμου..

2.4. Σε περίπτωση που το δεύτερο Συμβαλλόμενο Μέρος αποφασίσει να προσλάβει άλλον Εκτελούντα την Επεξεργασία (Υπεργολάβο) οφείλει να ενημερώσει το πρώτο Συμβαλλόμενο Μέρος. Εφ' όσον δεν υπάρξει εναντίωση εκ μέρους του πρώτου Συμβαλλόμενου Μέρους, το δεύτερο Συμβαλλόμενο Μέρος οφείλει περαιτέρω να εξασφαλίσει ότι ο Υπεργολάβος θα τηρεί ουσιαστικά όμοιους όρους με τους όρους της παρούσας Σύμβασης και τις διατάξεις της ισχύουσας νομοθεσίας για την προστασία των προσωπικών δεδομένων. Ο κατάλογος των Υπεργολάβων που ήδη έχουν προσληφθεί και θα διενεργήσουν/διενεργούν επεξεργασία για λογαριασμό του πρώτου Συμβαλλόμενου Μέρους προσαρτάται ως Παράρτημα Α στην παρούσα Σύμβαση και καθίσταται αναπόσπαστο τμήμα αυτής. Έναντι του πρώτου Συμβαλλόμενου Μέρους, το δεύτερο Συμβαλλόμενο Μέρος θα ευθύνεται εις ολόκληρον για οποιαδήποτε παράβαση των όρων της παρούσας Σύμβασης ή/και της νομοθεσίας για την προστασία των προσωπικών δεδομένων από τους Υπεργολάβους που τυχόν θα χρησιμοποιήσει.

2.5. Τα δεδομένα που υποβάλλονται σε επεξεργασία για λογαριασμό του πρώτου Συμβαλλόμενου Μέρους δε θα διαβιβαστούν εκτός ΕΕ/ΕΟΧ δίχως το δεύτερο Συμβαλλόμενο Μέρος να έχει προηγουμένως ενημερώσει το πρώτο Συμβαλλόμενο Μέρος. Σε περίπτωση που λάβει χώρα διαβίβαση δεδομένων εκτός ΕΕ/ΕΟΧ, αυτή θα πραγματοποιηθεί μόνον υπό τις προϋποθέσεις που θεσπίζονται στο Κεφάλαιο V του ΓΚΠΔ. Το δεύτερο Συμβαλλόμενο Μέρος οφείλει να ενημερώσει εκ των προτέρων το πρώτο Συμβαλλόμενο Μέρος και να παράσχει επαρκείς πληροφορίες και αποδείξεις που θα τεκμηριώνουν ότι πληρούνται οι ως άνω προϋποθέσεις του ΓΚΠΔ.

2.6. Το δεύτερο Συμβαλλόμενο Μέρος υποχρεούται να λαμβάνει κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας των προσωπικών δεδομένων που θα επεξεργαστεί για λογαριασμό του πρώτου Συμβαλλόμενου Μέρους, τα οποία περιγράφονται εκτενώς α) στην από 13/3/2020 Σύμβαση- Πλαίσιο περί προστασίας προσωπικών δεδομένων με τίτλο «MASTER DATA PROTECTION AGREEMENT», β) στο από 13/3/2020 Παράρτημα με τίτλο «Privacy Data Sheet - Cisco Webex Meetings», γ) στο από 13/3/2020 Παράρτημα με τίτλο «**CLARIFICATION APPENDIX**», που προσαρτώνται στην παρούσα Σύμβαση ως Παραρτήματα Β, Γ και Δ, αντίστοιχα, (εφεξής «τα Παραρτήματα Προστασίας Προσωπικών Δεδομένων») και καθίστανται αναπόσπαστο τμήμα αυτής. Εφόσον υπάρξουν νέες απαιτήσεις της νομοθεσίας περί προστασίας προσωπικών δεδομένων (συμπεριλαμβανομένων τυχόν σχετικών Αποφάσεων, Οδηγιών, Γνωμοδοτήσεων και Κατευθυντηρίων Γραμμών της ΑΠΔΠΧ), το δεύτερο Συμβαλλόμενο Μέρος αναλαμβάνει την υποχρέωση να προβαίνει αζημίως σε κάθε αναγκαία προσαρμογή των εφαρμοζόμενων μέτρων προστασίας των προσωπικών δεδομένων, κατόπιν γραπτής συμφωνίας με το πρώτο Συμβαλλόμενο Μέρος η οποία θα προσαρτάται στην παρούσα Σύμβαση.

2.7 Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, σύμφωνα με το άρ. 4 περ. 12 ΓΚΠΔ, ή ακόμη και σε ενδεχόμενο φερόμενης παραβίασης, το δεύτερο Συμβαλλόμενο Μέρος, λαμβάνοντας υπ' όψιν τη φύση των υπό επεξεργασία προσωπικών δεδομένων και τις προθεσμίες που θέτει ο ΓΚΠΔ, θα επικοινωνεί αμελλητί με τον Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ)

του πρώτου Συμβαλλόμενου Μέρους μέσω της ηλεκτρονικής διεύθυνσης: «dpo@minedu.gov.gr».

2.8. Κατά τα λοιπά, εφόσον δεν ορίζεται διαφορετικά στην παρούσα, ισχύουν τα διαλαμβανόμενα στα Παραρτήματα Προστασίας Προσωπικών Δεδομένων.»

Κατά τα λοιπά θα ισχύουν όλοι οι όροι της από 09/11/2020 Σύμβασης των Συμβαλλόμενων Μερών.

Αφού διαβάστηκε και βεβαιώθηκε το κείμενο της παρούσης τροποποιητικής πράξης από τα Συμβαλλόμενα Μέρη, υπογράφεται στον τόπο και κατά το χρόνο που αναφέρονται κατωτέρω.

Αθήνα, 4 Δεκεμβρίου 2020

Για το Ελληνικό Δημόσιο

Νίκη Κεραμέως

Για την CISCO HELLAS S.A.

CISCO ΣΥΣΤΗΜΑΤΑ ΔΙΑΔΙΚΤΥΩΣΗΣ ΕΛΛΑΣ Α.Ε.
ΕΡ. ΚΑΤ. ΑΝΑΠ. ΠΩΛ. ΕΜΠ. ΔΙΑΝ. & ΤΕΧΝ.
ΥΠΟΣ/ΞΗ ΠΡΟΪΟΝΤΩΝ ΔΙΑΔ/ΣΗΣ
ΚΗΦΙΣΙΑΣ 44 - ΚΤΙΡΙΟ Γ' - ΜΑΡΟΥΣΙ 151 25
Α.Φ.Μ.: 094497464 - Δ.Ο.Υ.: ΦΑΕ ΑΘΗΝΩΝ
Α.Φ.Σ.: 572687 - ΑΡ. Μ.Α.Ε.: 38099/01/Β/97/241

Αντώνης Τσιμπούκης

Γενικός Διευθυντής

Ελλάδα, Πορτογαλία, Κύπρο, Μάλτα.

Σύμβαση δωρεάν παραχώρησης της πλατφόρμας τηλεδιασκέψεων WEBEX για την πραγματοποίηση σύγχρονης εξ αποστάσεως διδασκαλίας στο εκπαιδευτικό σύστημα.

μεταξύ

Του Ελληνικού Δημοσίου, όπως νομίμως εκπροσωπείται από την Υπουργό Παιδείας και Θρησκευμάτων.

και

την εταιρεία με την επωνυμία «CISCO HELLAS A.E.», η οποία εδρεύει στην Αθήνα (Λεωφόρος Κηφισίας 44, Μαρούσι) όπως νομίμως εκπροσωπείται από το Γενικό Διευθυντή Αντώνη Τσιμπούκη.

συλλογικά αναφερόμενων ως «**Συμβαλλόμενα Μέρη**» και μεμονωμένα ως «**Συμβαλλόμενο Μέρος**».

Η παρούσα Συμφωνία καθορίζει τον σκοπό, το περιεχόμενο, τη διάρκεια και τις εν γένει υποχρεώσεις των Συμβαλλομένων Μερών. Πιο συγκεκριμένα, τα Συμβαλλόμενα Μέρη συμφωνούν αμοιβαία τα εξής:

1. Αντικείμενο, σκοπός και διάρκεια της Σύμβασης

Η παρούσα Συμφωνία για τη δωρεάν παραχώρηση της πλατφόρμας Cisco Webex («η Συμφωνία» ή «η Σύμβαση») υπόκειται (1) στη Συμφωνία Universal Could της Cisco, διαθέσιμη στο ακόλουθο σύνδεσμο: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/universal-cloud-agreement.html, (2) στην από 13/3/2020 Σύμβαση-Πλαίσιο περί προστασίας προσωπικών δεδομένων με τίτλο «MASTER DATA PROTECTION AGREEMENT» μεταξύ των Συμβαλλομένων Μερών (συμπεριλαμβανομένων όλων των συνημμένων), και (3) περιορίζεται σε 30.000 ταυτόχρονες συναντήσεις ή 700.000 συμμετέχοντες. Η τυπική εγγύηση της Cisco δεν ισχύει για τέτοιες δοκιμές και, στο βαθμό που επιτρέπεται από το νόμο, η Cisco αποποιείται ρητά όλες τις εγγυήσεις, ρητές ή σιωπηρές (συμπεριλαμβανομένων, χωρίς περιορισμό, ικανοποιητικής ποιότητας, καταλληλόλητας για σκοπού ή ως προς την εύλογη ικανότητα και φροντίδα).

1.1. Το δεύτερο των Συμβαλλόμενων Μερών θα προβεί στη δωρεάν παραχώρηση της πλατφόρμας τηλεδιασκέψεων WEBEX, προς χρήση εκ μέρους των υπαγόμενων στο ή εποπτευόμενων από το Υπουργείο Παιδείας και Θρησκευμάτων σχολικών μονάδων Πρωτοβάθμιας και Δευτεροβάθμιας Εκπαίδευσης, καθώς και δομών Επαγγελματικής Εκπαίδευσης και Κατάρτισης, των στελεχών και διοικητικών υπαλλήλων τους, των εκπαιδευτικών λειτουργών και λοιπού διδακτικού και διοικητικού προσωπικού, καθώς και των εν γένει μαθητών και σπουδαστών των ανωτέρω εκπαιδευτικών δομών.

1.2. Σκοπός της Σύμβασης είναι να καταστεί δυνατή, μέσω της πλατφόρμας τηλεδιασκέψεων WEBEX, η σύγχρονη εξ αποστάσεως διδασκαλία για το σχολικό έτος 2020-2021 όλως εξαιρετικώς λόγω των έκτακτων επιδημιολογικών συνθηκών που

δημιούργησε η πανδημία κορωνοϊού COVID-19, και για τη χρονική διάρκεια μέχρι τις 11 Ιανουαρίου 2021.

1.3. Μετά την παρέλευση του ως άνω χρονικού διαστήματος, οι προαναφερόμενοι χρήστες της πλατφόρμας, ενεργούντες ατομικώς ή συλλογικώς, καθώς και το Υπουργείο Παιδείας και Θρησκευμάτων και εν γένει το Ελληνικό Δημόσιο, θα αποδεσμευθούν από τη χρήση της πλατφόρμας, χωρίς από τη συντελεσθείσα χρήση να απορρέει οποιαδήποτε, οικονομικής ή άλλης φύσεως, υποχρέωση σε βάρος τους και ιδίως χωρίς να θεμελιώνεται δέσμευση χρήσης της εν λόγω πλατφόρμας ή άλλου παρεχόμενου από το δεύτερο των Συμβαλλομένων Μερών αγαθού ή υπηρεσίας στο μέλλον. Επιπλέον συμφωνείται ότι εναπόκειται στο Υπουργείο Παιδείας και Θρησκευμάτων και στους υπαγόμενους ή εποπτευόμενους από αυτό φορείς και δομές το εάν και σε ποια έκταση θα κάνουν χρήση της πλατφόρμας αυτής, χωρίς να δεσμεύονται προς τούτο.

2. Προστασία Προσωπικών Δεδομένων

2.1. Στο δεύτερο των Συμβαλλομένων Μερών θα διατεθούν προσωπικά δεδομένα για λογαριασμό του πρώτου εξ αυτών από το νομικό πρόσωπο ιδιωτικού δικαίου μη κερδοσκοπικού χαρακτήρα με την επωνυμία «Ινστιτούτο Τεχνολογίας Υπολογιστών και Εκδόσεων "Διόφαντος" (Ι.Τ.Υ.Ε.)» («Εκτελών την Επεξεργασία»). Το δεύτερο των Συμβαλλομένων Μερών δεν επιτρέπεται να προβεί σε οποιαδήποτε χρήση των προσωπικών δεδομένων που θα διατεθούν για την υλοποίηση της παρούσας Σύμβασης που να εκφεύγει του σκοπού αυτής, όπως ανωτέρω περιγράφηκε. Ιδιαίτερα, οφείλει να μην κάνει χρήση των προσωπικών δεδομένων που θα διατεθούν (π.χ. διευθύνσεις ηλεκτρονικού ταχυδρομείου) για προωθητικές ή άλλες εμπορικές ενέργειες. Επιπλέον, το δεύτερο των Συμβαλλομένων Μερών δεσμεύεται να τηρεί τα προβλεπόμενα στον Κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων ή EU GDPR), σε σχέση με τα προσωπικά δεδομένα που θα του χορηγηθούν από το πρώτο των Συμβαλλομένων Μερών.

2.2. Το δεύτερο των Συμβαλλομένων Μερών υποχρεούται, μόλις εκπληρωθεί ο σκοπός της παρούσας Σύμβασης, να προβεί αμελλητί σε διαγραφή των προσωπικών δεδομένων που θα διατεθούν από το πρώτο των Συμβαλλομένων Μερών για την υλοποίησή της.

2.3. Σε περίπτωση που το δεύτερο των Συμβαλλομένων Μερών χρησιμοποιήσει υπεργολάβους επεξεργασίας και διαβιβάσει σε αυτούς τα προσωπικά δεδομένα που του έχουν τυχόν διατεθεί από το πρώτο των Συμβαλλομένων Μερών, οφείλει να εξασφαλίσει ότι οι υπεργολάβοι επεξεργασίας θα τηρούν τους όρους της παρούσας σύμβασης και τα προβλεπόμενα από την ισχύουσα νομοθεσία για την προστασία των προσωπικών δεδομένων. Έναντι του πρώτου των Συμβαλλομένων Μερών, το δεύτερο των Συμβαλλομένων Μερών θα ευθύγεται αλληλεγγύως και εις ολόκληρον για οποιαδήποτε παράβαση της παρούσας σύμβασης ή/και της νομοθεσίας για την προστασία των προσωπικών δεδομένων από τους υπεργολάβους επεξεργασίας που τυχόν θα χρησιμοποιήσει.

2.4. Η διαβίβαση Προσωπικών Δεδομένων εκτός ΕΕ/ΕΟΧ από τον Εκτελούντα την Επεξεργασία και τους Υπεργολάβους Επεξεργασίας γίνεται σύμφωνα με την από 13/3/2020 Σύμβαση-Πλαίσιο περί προστασίας προσωπικών δεδομένων με τίτλο «MASTER DATA PROTECTION AGREEMENT μεταξύ των Συμβαλλομένων Μερών.

2.5. Το δεύτερο των Συμβαλλόμενων Μερών υποχρεούται να λαμβάνει κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας των προσωπικών δεδομένων που θα διατεθούν από το πρώτο των Συμβαλλόμενων Μερών, τα οποία περιγράφονται εκτενώς α) στην από 13/3/2020 Σύμβαση- Πλαίσιο περί προστασίας προσωπικών δεδομένων με τίτλο «MASTER DATA PROTECTION AGREEMENT», β) στο από 13/3/2020 Παράρτημα με τίτλο «Privacy Data Sheet - Cisco Webex Meetings», γ) στο από 13/3/2020 Παράρτημα με τίτλο «**CLARIFICATION APPENDIX**», που προσαρτώνται στην παρούσα Σύμβαση ως Παραρτήματα Α, Β και Γ, αντίστοιχα, (εφεξής «τα Παραρτήματα Προστασίας Προσωπικών Δεδομένων») και καθίστανται αναπόσπαστο τμήμα αυτής. Κατόπιν γραπτής συμφωνίας των Συμβαλλομένων Μερών η οποία θα προσαρτάται στην παρούσα Σύμβαση ως Παράρτημα Δ, το δεύτερο των Συμβαλλόμενων Μερών θα προβαίνει αζημίως σε κάθε αναγκαία ενέργεια προκειμένου να διασφαλίζεται η συμμόρφωση των εφαρμοζόμενων μέτρων προστασίας των προσωπικών δεδομένων προς το Γενικό Κανονισμό για την Προστασία Δεδομένων (EU GDPR) και τις οδηγίες της ελληνικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, και θα λαμβάνει υπόψη τις Αποφάσεις, Οδηγίες, Γνωμοδοτήσεις και Κατευθυντήριες Γραμμές της ελληνικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

2.6. Κατά τα λοιπά, εφόσον δεν ορίζεται διαφορετικά στην παρούσα, ισχύουν τα διαλαμβανόμενα στα Παραρτήματα Προστασίας Προσωπικών Δεδομένων.

3. Λοιπές διατάξεις

3.1. Οι όροι της παρούσας Συμφωνίας υπόκεινται στη Συμφωνία Universal Cloud της Cisco, όπως αναφέρθηκε στην παρ.1 της παρούσας. Σε περίπτωση σύγκρουσης μεταξύ της παρούσας και προγενέστερων συμφωνιών, η παρούσα υπερισχύει αλλά μόνο όσον αφορά το αντικείμενο της παρούσας.

Η Συμφωνία αυτή αποτελεί την πλήρη συμφωνία μεταξύ των συμβαλλομένων μερών και υπερισχύει όλων των προγενέστερων έγγραφων ή προφορικών συμφωνιών, δηλώσεων και εγγυήσεων των συμβαλλομένων μερών σχετικά με το αντικείμενο της παρούσας.

Κάθε διαφορά ή αξίωση που προκύπτει από ή σε σχέση με την παρούσα Συμφωνία, συμπεριλαμβανομένων (1) της προαναφερόμενης Συμφωνίας Universal Cloud και (2) της Σύμβασης-Πλαίσιο περί προστασίας προσωπικών δεδομένων με τίτλο «MASTER DATA PROTECTION AGREEMENT», θα επιλύεται από τα δικαστήρια της Αθήνας (Ελλάδας) και θα διέπεται από το Ελληνικό δίκαιο.

3.2. Η παρούσα Σύμβαση καταρτίστηκε σε 2 (δύο) πρωτότυπα έγγραφα; και το κάθε μέρος έλαβε από ένα.

Αθήνα, 9 Νοεμβρίου 2020

Για το Ελληνικό Δημόσιο

Νίκη Κεραμέως

Για την CISCO HELLAS S.A.

CISCO ΣΥΣΤΗΜΑΤΑ ΔΙΑΔΙΚΤΥΩΣΗΣ ΕΛΛΑΣ Α.
ΕΡ. ΚΑΤ. ΑΝΑΠ. ΠΩΛ. ΕΜΠ. ΔΙΑΝ. & ΤΕΧ.
ΥΠΟΣΞΗ ΠΡΟΪΟΝΤΩΝ ΔΙΑΔΙΣΗ
ΚΗΦΙΣΙΑΣ 44 - ΚΤΙΡΙΟ Γ' - ΜΑΡΟΥΣΙ 151 2
Α.Φ.Μ.: 094497464 - Δ.Ο.Υ.: ΦΑΕ ΑΘΗΝΩ
Α.Φ.: 672687 - ΑΡ. Μ.Α.Ε.: 38099/01/Β/97/

Αντώνης Τσιμπούκης

Γενικός Διευθυντής

Ελλάδα, Πορτογαλία, Κύπρο, Μάλτα.

Σύμβαση δωρεάν παραχώρησης της πλατφόρμας τηλεδιασκέψεων WEBEX για την πραγματοποίηση σύγχρονης εξ αποστάσεως διδασκαλίας στο εκπαιδευτικό σύστημα.

μεταξύ

Του Ελληνικού Δημοσίου, όπως νομίμως εκπροσωπείται από την Υπουργό Παιδείας και Θρησκευμάτων,

και

την εταιρεία με την επωνυμία «CISCO HELLAS A.E.», η οποία εδρεύει στην Αθήνα (Λεωφόρος Κηφισίας 44, Μαρούσι) όπως νομίμως εκπροσωπείται από το Γενικό Διευθυντή Αντώνη Τσιμπούκη.

συλλογικά αναφερόμενων ως «**Συμβαλλόμενα Μέρη**» και μεμονωμένα ως «**Συμβαλλόμενο Μέρος**».

Η παρούσα σύμβαση καθορίζει το σκοπό, το περιεχόμενο, τη διάρκεια και τις εν γένει υποχρεώσεις των Συμβαλλομένων Μερών. Πιο συγκεκριμένα, τα Συμβαλλόμενα Μέρη συμφωνούν αμοιβαία τα εξής:

1. Αντικείμενο, σκοπός και διάρκεια της Σύμβασης

Η παρούσα Συμφωνία για τη δωρεάν παραχώρηση της πλατφόρμας Cisco Webex («Η Συμφωνία») υπόκειται σε (1) Συμφωνία Universal Could της Cisco, διαθέσιμη στο ακόλουθο σύνδεσμο: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/universal-cloud-agreement.html, (2) από 13/3/2020 Σύμβαση-Πλαίσιο περί προστασίας προσωπικών δεδομένων με τίτλο «MASTER DATA PROTECTION AGREEMENT μεταξύ των Συμβαλλομένων Μερών (συμπεριλαμβανομένων όλων των συνημμένων), και (3) περιορίζεται σε 16.000 ταυτόχρονες συναντήσεις με 400.000 συμμετέχοντες. Η τυπική εγγύηση της Cisco δεν ισχύει για τέτοιες δοκιμές και, στο βαθμό που επιτρέπεται από το νόμο, η Cisco αποποιείται ρητά όλες τις εγγυήσεις, ρητές ή σιωπηρές (συμπεριλαμβανομένων, χωρίς περιορισμό, ικανοποιητικής ποιότητας, καταλληλότητας για σκοπούς ή ως προς την εύλογη ικανότητα και φροντίδα).

1.1. Το δεύτερο των Συμβαλλόμενων Μερών θα προβεί στη δωρεάν παραχώρηση της πλατφόρμας τηλεδιασκέψεων WEBEX, προς χρήση εκ μέρους των υπαγόμενων ή εποπτευόμενων από το Υπουργείο Παιδείας και Θρησκευμάτων σχολικών μονάδων Πρωτοβάθμιας και Δευτεροβάθμιας Εκπαίδευσης, καθώς και δομών Επαγγελματικής Εκπαίδευσης και Κατάρτισης (Σχολεία Δεύτερης Ευκαιρίας, Μαθητεία, δημόσια Ινστιτούτα Επαγγελματικής Κατάρτισης), των στελεχών και διοικητικών υπαλλήλων τους, των εκπαιδευτικών λειτουργών και λοιπού διδακτικού και διοικητικού προσωπικού, καθώς και των εν γένει μαθητών και σπουδαστών των ανωτέρω εκπαιδευτικών δομών.

1.2. Σκοπός της Σύμβασης είναι να καταστεί δυνατή, μέσω της πλατφόρμας τηλεδιασκέψεων WEBEX, η σύγχρονη εξ αποστάσεως διδασκαλία για το σχολικό έτος 2020-2021 όλως εξαιρετικώς λόγω των έκτακτων επιδημιολογικών συνθηκών που δημιούργησε η πανδημία κορωνοϊού COVID-19, και όχι περισσότερο από τέσσερις (4) μήνες από την υπογραφή της παρούσης.

1.3. Μετά την παρέλευση του ως άνω χρονικού διαστήματος, οι προαναφερόμενοι χρήστες της πλατφόρμας, ενεργούντες ατομικώς ή συλλογικώς, καθώς και το Υπουργείο Παιδείας και Θρησκευμάτων και εν γένει το Ελληνικό Δημόσιο, θα αποδεσμευθούν από τη χρήση της

πλατφόρμας, χωρίς από τη συντελεσθείσα χρήση να απορρέει οποιαδήποτε, οικονομικής ή άλλης φύσεως, υποχρέωση σε βάρος τους και ιδίως χωρίς να θεμελιώνεται δέσμευση χρήσης της εν λόγω πλατφόρμας ή άλλου παρεχόμενου από το δεύτερο των Συμβαλλομένων Μερών αγαθού ή υπηρεσίας στο μέλλον. Επιπλέον συμφωνείται ότι εναπόκειται στο Υπουργείο Παιδείας και Θρησκευμάτων και στους υπαγόμενους ή εποπτευόμενους από αυτό φορείς και δομές το εάν και σε ποια έκταση θα κάνουν χρήση της πλατφόρμας αυτής, χωρίς να δεσμεύονται προς τούτο.

2. Προστασία Προσωπικών Δεδομένων

2.1. Στο δεύτερο των Συμβαλλομένων Μερών θα διατεθούν προσωπικά δεδομένα για λογαριασμό του πρώτου εξ αυτών από το νομικό πρόσωπο ιδιωτικού δικαίου μη κερδοσκοπικού χαρακτήρα με την επωνυμία «Ινστιτούτο Τεχνολογίας Υπολογιστών και Εκδόσεων "Διόφαντος" (Ι.Τ.Υ.Ε.)» («Εκτελών την Επεξεργασία»). Το δεύτερο των Συμβαλλομένων Μερών δεν επιτρέπεται να προβεί σε οποιαδήποτε χρήση των προσωπικών δεδομένων που θα διατεθούν για την υλοποίηση της παρούσας Σύμβασης που να εκφεύγει του σκοπού αυτής, όπως ανωτέρω περιγράφηκε. Ιδιαίτερα, οφείλει να μην κάνει χρήση των προσωπικών δεδομένων που θα διατεθούν (π.χ. διευθύνσεις ηλεκτρονικού ταχυδρομείου) για προωθητικές ή άλλες εμπορικές ενέργειες. Επιπλέον, το δεύτερο των Συμβαλλομένων Μερών δεσμεύεται να τηρεί τα προβλεπόμενα στον Κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων ή EU GDPR), σε σχέση με τα προσωπικά δεδομένα που θα του χορηγηθούν από το πρώτο των Συμβαλλομένων Μερών.

2.2. Το δεύτερο των Συμβαλλομένων Μερών υποχρεούται, μόλις εκπληρωθεί ο σκοπός της παρούσας Σύμβασης, να προβεί αμελλητί σε διαγραφή των προσωπικών δεδομένων που θα διατεθούν από το πρώτο των Συμβαλλομένων Μερών για την υλοποίησή της.

2.3. Σε περίπτωση που το δεύτερο των Συμβαλλομένων Μερών χρησιμοποιήσει υπεργολάβους επεξεργασίας και διαβιβάσει σε αυτούς τα προσωπικά δεδομένα που του έχουν τυχόν διατεθεί από το πρώτο των Συμβαλλομένων Μερών, οφείλει να εξασφαλίσει ότι οι υπεργολάβοι επεξεργασίας θα τηρούν τους όρους της παρούσας σύμβασης και τα προβλεπόμενα από την ισχύουσα νομοθεσία για την προστασία των προσωπικών δεδομένων. Έναντι του πρώτου των Συμβαλλομένων Μερών, το δεύτερο των Συμβαλλομένων Μερών θα ευθύνεται εις ολόκληρον για οποιαδήποτε παράβαση της παρούσας σύμβασης ή/και της νομοθεσίας για την προστασία των προσωπικών δεδομένων από τους υπεργολάβους επεξεργασίας που τυχόν θα χρησιμοποιήσει.

2.4. Η διαβίβαση Προσωπικών Δεδομένων εκτός ΕΕ/ΕΟΧ από τον Εκτελών την Επεξεργασία και τους Υπεργολάβους Επεξεργασίας γίνεται σύμφωνα με την από 13/3/2020 Σύμβαση-Πλαίσιο περί προστασίας προσωπικών δεδομένων με τίτλο «MASTER DATA PROTECTION AGREEMENT μεταξύ των Συμβαλλομένων Μερών.

2.5. Το δεύτερο των Συμβαλλόμενων Μερών υποχρεούται να λαμβάνει κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας των προσωπικών δεδομένων που θα διατεθούν από το πρώτο των Συμβαλλόμενων Μερών, τα οποία περιγράφονται εκτενώς α) στην από 13/3/2020 Σύμβαση- Πλαίσιο περί προστασίας προσωπικών δεδομένων με τίτλο «MASTER DATA PROTECTION AGREEMENT», β) στο από 13/3/2020 Παράρτημα με τίτλο «Privacy Data Sheet - Cisco Webex Meetings», γ) στο από 13/3/2020 Παράρτημα με τίτλο «**CLARIFICATION APPENDIX**», που προσαρτώνται στην παρούσα Σύμβαση ως Παραρτήματα Β, Γ και Δ, αντίστοιχα, (εφεξής «τα Παραρτήματα Προστασίας Προσωπικών

Δεδομένων») και καθίστανται αναπόσπαστο τμήμα αυτής. Κατόπιν γραπτής συμφωνίας των Συμβαλλομένων Μερών η οποία θα προσαρτάται στην παρούσα Σύμβαση ως Παράρτημα Ε, το δεύτερο των Συμβαλλόμενων Μερών θα προβαίνει αζημίως σε κάθε αναγκαία ενέργεια προκειμένου να διασφαλίζεται η συμμόρφωση των εφαρμοζόμενων μέτρων προστασίας των προσωπικών δεδομένων προς το Γενικό Κανονισμό για την Προστασία Δεδομένων (EU GDPR) και τις οδηγίες της ελληνικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, και θα λαμβάνει υπόψη τις Αποφάσεις, Οδηγίες, Γνωμοδοτήσεις και Κατευθυντήριες Γραμμές της ελληνικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

2.6. Κατά τα λοιπά, εφόσον δεν ορίζεται διαφορετικά στην παρούσα, ισχύουν τα διαλαμβανόμενα στα Παραρτήματα Προστασίας Προσωπικών Δεδομένων.

3. Λοιπές διατάξεις

3.1. Οι όροι αυτής της παρούσας υπόκεινται στη Συμφωνία Universal Cloud της Cisco, όπως αναφέρθηκε στην παρ.1 της παρούσας. Σε περίπτωση σύγκρουσης μεταξύ της παρούσας και μεταγενέστερων συμφωνιών, η παρούσα υπερισχύει αλλά μόνο όσον αφορά το αντικείμενο της παρούσας.

Κάθε διαφορά ή αξίωση που προκύπτει από ή σε σχέση με την παρούσα Σύμβαση, συμπεριλαμβανομένων (1) της προαναφερόμενης Συμφωνίας Universal Cloud και (2) της Σύμβαση-Πλαίσιο περί προστασίας προσωπικών δεδομένων με τίτλο «MASTER DATA PROTECTION AGREEMENT», θα επιλύεται από τα δικαστήρια της Αθήνας (Ελλάδας) και θα διέπεται από το Ελληνικό δίκαιο.

3.2. Η παρούσα Σύμβαση καταρτίστηκε σε 2 (δύο) πρωτότυπα έγγραφα, και το κάθε μέρος έλαβε από ένα.

Αθήνα, 11 Σεπτεμβρίου 2020

Για το Ελληνικό Δημόσιο

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ

Νίκη Κεραμέως

Για την CISCO HELLAS S.A.

CISCO ΣΥΣΤΗΜΑΤΑ ΔΙΑΔΙΚΤΥΩΣΗΣ ΕΛΛΑΣ Α.Ε.
ΕΡ. ΚΑΤ. ΑΝΑΠ. ΠΩΛ. ΕΜΠ. ΔΙΑΝ. & ΤΕΧΝ.
ΥΠΟΣΤΗΡΙΞΗ ΠΡΟΪΟΝΤΩΝ ΔΙΑΔΙΚΤΥΩΣΗΣ
ΚΗΦΙΣΙΑΣ 44 - ΚΤΙΡΙΟ Γ' - ΜΑΡΟΥΣΙ 151 25
Α.Φ.Μ.: 094497464 - Δ.Ο.Υ.: ΦΑΕΕ ΑΘΗΝΩΝ

Αντώνης Τσιμπούκης
Γενικός Διευθυντής

Ελλάδα, Πορτογαλία, Κύπρο, Μάλτα.

Σύμβαση δωρεάν παραχώρησης της πλατφόρμας τηλεδιασκέψεων WEBEX για την πραγματοποίηση σύγχρονης εξ αποστάσεως διδασκαλίας στο εκπαιδευτικό σύστημα.

μεταξύ

Του Ελληνικού Δημοσίου, όπως νομίμως εκπροσωπείται από την Υπουργό Παιδείας και Θρησκευμάτων.

και

την εταιρεία με την επωνυμία «CISCO HELLAS A.E.», η οποία εδρεύει στην Αθήνα, όπως νομίμως εκπροσωπείται.

συλλογικά αναφερόμενων ως «**Συμβαλλόμενα Μέρη**» και μεμονωμένα ως «**Συμβαλλόμενο Μέρος**».

Η παρούσα σύμβαση καθορίζει το σκοπό, το περιεχόμενο, τη διάρκεια και τις εν γένει υποχρεώσεις των Συμβαλλομένων Μερών. Πιο συγκεκριμένα, τα Συμβαλλόμενα Μέρη συμφωνούν αμοιβαία τα εξής:

1. Αντικείμενο, σκοπός και διάρκεια της Σύμβασης

1.1. Το δεύτερο των Συμβαλλόμενων Μερών θα προβεί στη δωρεάν παραχώρηση της πλατφόρμας τηλεδιασκέψεων WEBEX, προς χρήση εκ μέρους των υπαγόμενων ή εποπτευόμενων από το Υπουργείο Παιδείας και Θρησκευμάτων δομών της εκπαίδευσης, των στελεχών και διοικητικών υπαλλήλων τους, των εκπαιδευτικών λειτουργών και λοιπού διδακτικού και διοικητικού προσωπικού καθώς και των εν γένει μαθητών, σπουδαστών και φοιτητών όλων των τύπων και βαθμίδων της εκπαίδευσης.

1.2. Σκοπός της Σύμβασης είναι να καταστεί δυνατή, μέσω της πλατφόρμας τηλεδιασκέψεων WEBEX, η σύγχρονη εξ αποστάσεως διδασκαλία για όσο χρονικό διάστημα ισχύει η απαγόρευση λειτουργίας των εκπαιδευτικών δομών λόγω του κορωνοϊού COVID-19 και όχι περισσότερο από τέσσερις (4) μήνες από την υπογραφή της παρούσης.

1.3. Μετά την παρέλευση του ως άνω χρονικού διαστήματος, οι προαναφερόμενοι χρήστες της πλατφόρμας, ενεργούντες ατομικώς ή συλλογικώς, καθώς και το Υπουργείο Παιδείας και Θρησκευμάτων και εν γένει το Ελληνικό Δημόσιο, θα απαδεσμευθούν από τη χρήση της πλατφόρμας, χωρίς από τη συντελεσθείσα χρήση να απορρέει οιαδήποτε, οικονομικής ή άλλης φύσεως, υποχρέωση σε βάρος τους και ιδίως χωρίς να θεμελιώνεται δέσμευση χρήσης της εν λόγω πλατφορμας ή άλλου παρεχόμενου από το δεύτερο των Συμβαλλομένων Μερών αγαθού ή υπηρεσίας στο μέλλον. Επιπλέον συμφωνείται οτι εναπόκειται στο Υπουργείο Παιδείας και Θρησκευμάτων και στους υπαγόμενους ή εποπτευόμενους από αυτό φορείς και δομές το εάν και σε ποια έκταση θα κάνουν χρήση της πλατφόρμας αυτής, χωρίς να δεσμεύονται προς τούτο.

2. Προστασία Προσωπικών Δεδομένων

2.1. Το δεύτερο των Συμβαλλομένων Μερών δεν επιτρέπεται να προβεί σε οποιαδήποτε χρήση των προσωπικών δεδομένων που θα διατεθούν για την υλοποίηση της παρούσας Σύμβασης που να εκφεύγει του σκοπού αυτής, όπως ανωτέρω

περιγράφηκε. Ιδιαίτερα, οφείλει να μην κάνει χρήση των προσωπικών δεδομένων που τυχόν διατεθούν (π.χ. e-mail) για προωθητικές ή άλλες εμπορικές ενέργειες. Επιπλέον, το δεύτερο των Συμβαλλομένων Μερών δεσμεύεται να τηρεί τα προβλεπόμενα στη νομοθεσία για την προστασία των προσωπικών δεδομένων, σε σχέση με τα προσωπικά δεδομένα που τυχόν του χορηγηθούν από το πρώτο των Συμβαλλομένων Μερών.

2.2. Το δεύτερο των Συμβαλλομένων Μερών υποχρεούται, μόλις εκπληρωθεί ο σκοπός της παρούσας Σύμβασης, να προβεί αμελλητί σε διαγραφή των προσωπικών δεδομένων που θα διατεθούν από το πρώτο των Συμβαλλομένων Μερών για την υλοποίησή της.

2.3. Σε περίπτωση που το δεύτερο των Συμβαλλομένων Μερών χρησιμοποιήσει υπεργολάβους επεξεργασίας και διαβιβάσει σε αυτούς τα προσωπικά δεδομένα που του έχουν τυχόν διαβιβαστεί από το πρώτο των Συμβαλλομένων Μερών, οφείλει να εξασφαλίσει ότι οι υπεργολάβοι επεξεργασίας θα τηρούν τους όρους της παρούσας σύμβασης και τα προβλεπόμενα από την ισχύουσα νομοθεσία για την προστασία των προσωπικών δεδομένων. Έναντι του πρώτου των Συμβαλλομένων Μερών, το δεύτερο των Συμβαλλομένων Μερών θα ευθύνεται εις ολόκληρον για οποιαδήποτε παράβαση της παρούσας σύμβασης ή/και της νομοθεσίας για την προστασία των προσωπικών δεδομένων από τους υπεργολάβους επεξεργασίας που τυχόν θα χρησιμοποιήσει.

2.4. Ο Εκτελών την Επεξεργασία και οι Υπεργολάβοι Επεξεργασίας δεν επιτρέπεται να διαβιβάζουν Προσωπικά Δεδομένα εκτός ΕΕ/ΕΟΧ, χωρίς την προηγούμενη γραπτή συγκατάθεση του πρώτου των Συμβαλλομένων Μερών . Σε περίπτωση χορήγησης τέτοιας συγκατάθεσης, ο Εκτελών την Επεξεργασία και/ή οι Υπεργολάβοι Επεξεργασίας πρέπει να συμμορφώνονται με τυχόν απαιτήσεις που έχουν θεσπιστεί από οποιαδήποτε αρχή προστασίας δεδομένων ή οποιαδήποτε άλλη κυβερνητική αρχή που είναι αναγκαίες για τη χορήγηση συγκατάθεσης από τις εν λόγω αρχές για τη διαβίβαση προσωπικών δεδομένων εκτός ΕΕ/ΕΟΧ, συμπεριλαμβανομένης της συμμόρφωσης με τις τυποποιημένες συμβατικές ρήτρες της Επιτροπής.

2.5. Κατά τα λοιπά, εφόσον δεν ορίζεται διαφορετικά στην παρούσα, ισχύουν τα διαλαμβανόμενα στα Παραρτήματα α) με τίτλο «MASTER DATA PROTECTION AGREEMENT», β) με τίτλο «Privacy Data Sheet - Cisco Webex Meetings», γ) με τίτλο «CLARIFICATION APPENDIX» τα οποία αποτελούν αναπόσπαστο τμήμα της παρούσας Σύμβασης.

3. Λοιπές διατάξεις

3.1. Κάθε διαφορά ή αξίωση που προκύπτει από ή σε σχέση με την παρούσα Σύμβαση θα επιλύεται από τα δικαστήρια της Αθήνας (Ελλάδας) και θα διέπεται από το Ελληνικό δίκαιο.

3.2. Η παρούσα Σύμβαση καταρτίστηκε σε 2 (δύο) πρωτότυπα έγγραφα, και το κάθε μέρος έλαβε από ένα.

Αθήνα, 13 Μαρτίου 2020

Για το Ελληνικό Δημόσιο

Νίκη Κεραμέως

Για την CISCO HELLAS S.A.

CISCO ΣΥΣΤΗΜΑΤΑ ΔΙΑΔΙΚΤΥΑΚΗΣ ΕΛΛΑΣ Α.Ε.
ΕΡ. ΚΑΤ/ΝΑΛΩ. ΠΩΛ. ΕΜΠ. ΔΙΑΝ. & ΤΕΧΝ.
ΥΠΟΣΤΗΡ. ΠΡΟΪΟΝΤΩΝ ΔΙΑΔΙΣΗΣ
ΚΗΦΙΣΙΑΣ 34 - ΚΤΙΡΙΟ Γ' - ΜΑΡΟΥΣΙ 151 25
Α.Φ.Μ.: 094027484 - Α.Ο.Υ.: ΦΑΕΕ ΑΘΗΝΩΝ
ΑΡ. Μ.Α.Ε.: 38099/01/Β/97/241

Αντώνης Τσιμπούκης

Γενικός Διευθυντής

Ελλάδα, Πορτογαλία, Κύπρο, Μάλτα.

MASTER DATA PROTECTION AGREEMENT

This MDPA has effective date 13.3.2020

This **MASTER DATA PROTECTION AGREEMENT ("MDPA")** is entered in to by and between **Cisco International Limited** having a principal place of business at 9-11 New Square Park, Bedfont Lakes, Feltham, England TW14 8HA, United Kingdom and its Affiliates **("Cisco")**, and the **Ministry of National Education and Religious Affairs of Greece**, having its principal seat at Andrea Papandreou st., 37, 15180 Marousi, Athens **("Customer")**, (together "Parties").

This MDPA is governed by the terms of the applicable agreement entered into by and between the Parties for the supply of Products and/or Services by Cisco to Customer dated 13/3/2020 ("the Agreement"). In the event of a conflict between this MDPA, including any attachments herein, and the Agreement, the provisions of this MDPA will control but only with respect to the subject matter hereof.

In consideration of the mutual promises and covenants hereinafter contained and of other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree as follows:

SCOPE OF AGREEMENT. This MDPA is comprised of the following Attachments A-E attached herein, which are incorporated by reference:

1. Attachment A INFORMATION SECURITY EXHIBIT
2. Attachment B DATA PROTECTION EXHIBIT
3. Attachment C CISCO WEBEX MEETINGS PRIVACY DATA SHEET
4. Attachment D STANDARD CONTRACTUAL CLAUSES
5. Attachment E GLOSSARY

This MDPA is the complete agreement between the Parties concerning the subject matter of this MDPA and replaces any prior oral or written communications between the Parties. This MDPA is subject to the terms and conditions of the Agreement, including, but not limited to any limitations or exclusions of liability set forth in the Agreement. There are no conditions, understandings, agreements, representations, or warranties expressed or implied, that are not specified herein. This MDPA may only be modified by a written document executed by the Parties hereto. The Parties, by signing below, confirm that they have read, understood, and expressly approve of the terms and conditions of this MDPA. Cisco's obligations under this MDPA will terminate when Cisco no longer holds, Processes, or otherwise has access to Protected Data.

The Parties have caused this MDPA to be duly executed. Each Party warrants and represents that its respective signatories whose signatures appear below are on the date of signature authorized to execute this MDPA.

("Customer")	**("Cisco")**
Authorized Signature	Auth
Name	Nam DIRECTOR MGMT FINANCE
Date: 13.3.2020	Date:

CISCO
Cisco International Limited
9-11 New Square Park
Bedfont Lakes, Feltham
Middlesex, TW14 8HA
United Kingdom

ATTACHMENT A

INFORMATION SECURITY EXHIBIT

1. Scope

This Information Security Exhibit ("ISE") applies to the extent that Cisco Processes or has access to Protected Data in the Performance of its obligations to the Customer. This ISE outlines the information security requirements between Customer and Cisco and describes the technical and organizational security measures that shall be implemented by Cisco to secure Protected Data prior to the Performance of any Processing under the Agreement.

Unless otherwise stated, in the event of a conflict between the Agreement and this ISE, the terms of this ISE will control as it relates to the Processing of Protected Data.

All capitalized terms not defined in the Glossary have the meanings set forth in the Agreement.

2. General Security Practices

Cisco has implemented and shall maintain appropriate technical and organizational measures designed to protect Protected Data against accidental loss, destruction or alteration, unauthorized disclosure or access, or unlawful destruction, including the policies, procedures, and internal controls set forth in this ISE for its personnel, equipment, and facilities at Cisco's locations involved in Performing any part of the Agreement.

3. General Compliance

i. **Compliance**. Cisco shall document and implement processes and procedures to avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security or other security requirements. Such processes and procedures shall be designed to provide appropriate security to protect Protected Data given the risk posed by the nature of the data Processed by Cisco. Cisco shall implement and operate information security in accordance with Cisco's own policies and procedures, which shall be no less strict than the information security requirements set forth in this ISE.

ii. **Protection of records**. Cisco shall implement appropriate procedures designed to protect records from loss, destruction, falsification, unauthorized access, and unauthorized release, in accordance with legislative, regulatory, and contractual requirements.

iii. **Review of information security.** Cisco's approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures) shall be reviewed at planned intervals or when significant changes occur by appropriate internal or external assessors.

iv. **Compliance with security policies and standards.** Cisco's management shall regularly review the compliance of information processing and procedures with the appropriate applicable security policies and standards.

v. **Technical compliance review.** Cisco shall regularly review information systems for compliance with Cisco's information security policies and standards.

vi. **Information Risk Management ("IRM").** Cisco shall implement and utilize an appropriate information risk management process to frame, assess, respond and monitor risk, consistent with

applicable contractual and legal obligations. Cisco is required to have a risk management framework and conduct periodic (i.e., at least annual) risk assessments of its environment and systems to understand the risks and apply appropriate controls to manage and mitigate such risks. Threat and vulnerability assessment must be periodically reviewed and prompt remediation actions taken where material weaknesses are found. Cisco will provide Customer with relevant summary reports and analysis upon written request, provided the disclosure of which would not violate Cisco's own information security policies, or mandatory applicable law.

4. Technical and Organizational Measures for Security

a. Organization of Information Security

i. **Security Ownership.** Cisco shall appoint one or more security officers responsible for coordinating and monitoring the security requirements and procedures. Such officers shall have the knowledge, experience, and authority to serve as the owner(s) of, with responsibility and accountability for, information security within the organization.

ii. **Security Roles and Responsibilities.** Cisco shall define and allocate information security responsibilities in accordance with Cisco's approved policies for information security. Such policies (or summaries thereof) shall be published and communicated to employees and relevant external parties required to comply with such policies.

iii. **Project Management.** Cisco shall address information security in project management to identify and appropriately address information security risks.

iv. **Risk Management.** Cisco shall have a risk management framework and conduct periodic (i.e., at least annual) risk assessment of its environment and systems to understand its risks and apply appropriate controls to manage and mitigate risks before Processing Protected Data.

b Human Resources Security

i. **General.** Cisco shall ensure that its personnel are under a confidentiality agreement that includes the protection of Protected Data and shall provide adequate training about relevant privacy and security policies and procedures. Cisco shall further inform its personnel of possible consequences of breaching Cisco's security policies and procedures, which must include disciplinary action, including possible termination of employment for Cisco's employees and termination of contract or assignment for Representatives and temporary personnel.

ii. **Training.** Cisco personnel with access to Protected Data shall receive appropriate, annual periodic education and training regarding privacy and security procedures for services to aid in the prevention of unauthorized use (or inadvertent disclosure) of Protected Data and training regarding how to effectively respond to security incidents. Training shall be provided before Cisco personnel are granted access to Protected Data or begin providing services. Training shall be regularly reinforced through refresher training courses, emails, posters, notice boards, and other training and awareness materials.

iii. **Background Checks.** In addition to any other terms in the Agreement related to this subject matter, Cisco shall conduct criminal and other relevant background checks for its personnel in compliance with or mandatory applicable law and Cisco's policies.

c. Personnel Access Controls

i. Access.

A. Limited Use. Cisco understands and acknowledges that Customer may be granting Cisco access to sensitive and proprietary information and computer systems in order for Cisco to Perf-

orm its obligations to the Customer. Cisco will not (i) access the Protected Data or computer systems for any purpose other than as necessary to Perform its obligations to Customer; or (ii) use any system access information or log-in credentials to gain unauthorized access to Protected Data or Customer's systems, or to exceed the scope of any authorized access.

B. Authorization. Cisco shall restrict access to Protected Data and systems at all times solely to those Representatives whose access is necessary to Performing Cisco's obligations to the Customer.

C. Suspension or Termination of Access Rights. At Customer's reasonable request, Cisco shall promptly and without undue delay suspend or terminate the access rights to Protected Data and systems for any Cisco's personnel or its Representatives reasonably suspected of breaching any of the provisions of this ISE; and Cisco shall remove access rights of all employees and external party users upon suspension or termination of their employment, or engagement.

D. Information Classification. Cisco shall classify, categorize, and/or tag Protected Data to help identify it and to allow for access and use to be appropriately restricted.

ii. **Access Policy.** Cisco shall determine appropriate access control rules, rights, and restrictions for each specific user's roles towards their assets. Cisco shall maintain a record of security privileges of its personnel that have access to Protected Data; and control their access, networks, and network services as set out in Section 4. of the Cisco Webex Meetings Privacy Data Sheet. Cisco shall restrict and tightly control the use of utility programs that might be capable of overriding system and application controls.

d. **Access Authorization.**

i. Cisco shall have user account creation and deletion procedures, with appropriate approvals, for granting and revoking access to Customer's systems and networks. Cisco shall use an enterprise access control system that requires revalidation of its personnel by managers at regular intervals based on the principle of "least privilege" and need-to-know criteria based on job role.

ii. Cisco shall maintain and update a record of personnel authorized to access systems that contain Protected Data and Cisco shall review users' access rights at regular intervals.

iii. For systems that process Protected Data, Cisco shall revalidate (or where appropriate, deactivate) access of users who change reporting structure and deactivate authentication credentials that have not been used for a period of time not to exceed four (4) months.

iv. Cisco shall restrict access to program source code and associated items such as software object code, designs, specifications, verification plans, and validation plans, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes.

e. **Network Design.** For systems that process Protected Data, Cisco shall have controls to avoid personnel assuming access rights beyond those that they have been assigned to gain unauthorized access to Protected Data.

f. **Least Privilege.** Cisco shall limit access to Protected Data to that personnel with Performance obligations and, to the extent technical support is needed, its personnel performing such technical support.

g. **Authentication**

i. Cisco shall use industry standard practices to identify and authenticate users who attempt to ac-

ces information systems. Where authentication mechanisms are based on passwords/PINs, Cisco shall require that the passwords/PINs are renewed and changed regularly, at least every 180 days.

ii. Where authentication mechanisms are based on passwords, Cisco shall require the password to conform to strong password control parameters (e.g., length, character complexity, and/or non-repeatability).

iii. Cisco shall ensure that de-activated or expired identifiers and log-in credentials are not granted to other individuals.

iv. Cisco shall monitor repeated failed attempts to exceed privileges or gain access to the information system.

v. Cisco shall maintain industry standard procedures to deactivate log-in credentials that have been corrupted or inadvertently disclosed.

vi. Cisco shall use industry standard log-in credential protection practices, including practices designed to maintain the confidentiality and integrity of log-in credentials when they are assigned and distributed, and during storage (e.g., log-in credentials shall not be stored or shared in plain text). Such practices shall be designed to ensure strong, confidential log-in credentials.

h. **Physical and Environmental Security**

i. **Physical Access to Facilities**

A. Cisco shall limit access to facilities where systems that Process Protected Data are located to authorized individuals.

B. Security perimeters shall be defined and used to protect areas that contain both sensitive or critical information and information processing facilities.

C. Facilities shall be monitored and access-controlled at all times (24x7).

D. Access shall be controlled through key card and/or appropriate sign-in procedures for facilities with systems Processing Protected Data. Cisco must register personnel and require them to carry appropriate identification badges.

ii. **Physical Access to Equipment.** Cisco equipment used to process or store Protected Data shall be protected using industry standard processes to limit access to authorized individuals.

iii. **Protection from Disruptions.** Cisco shall implement appropriate measures designed to protect against loss of data due to power supply failure or line interference.

iv. **Clear Desk.** Cisco shall have policies requiring a "clean desk/clear screen" to prevent inadvertent disclosure of Protected Data.

i. **Operations Security**

i. **Operational Policy.** Cisco shall maintain written policies describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Protected Data and to its systems and networks. Cisco shall communicate its policies and requirements to all persons involved in the Processing of Protected Data. Cisco shall implement the appropriate management structure and control designed to ensure compliance with such policies and with or mandatory applicable law concerning the protection and Processing of Protected Data.

ii. **Security and Processing Controls.**

A. **Areas.** Cisco shall maintain, document, and implement standards and procedures to address the configuration, operation, and management of systems and networks and services that store or Process Protected Data.

B. **Standards and Procedures.** Such standards and procedures shall include: security controls, identification and patching of security vulnerabilities, change control process and procedures, and incident prevention, detection, remediation, and management.

iii. **Logging and Monitoring.** Cisco shall maintain logs of administrator and operator activity and data recovery events related to Protected Data.

j. **Communications Security and Data Transfer**

i. **Networks.** Cisco shall, at a minimum, use the following controls to secure its networks that access or Process Protected Data:

A. Network traffic shall pass through firewalls, which are monitored at all times. Cisco must implement intrusion prevention systems that allow traffic flowing through the firewalls and LAN to be logged and protected at all times.

B. Network devices used for administration must utilize industry standard cryptographic controls when Processing Protected Data.

C. Anti-spoofing filters and controls must be enabled on routers.

D. Network, application, and server authentication passwords are required to meet minimum complexity guidelines (at least 7 characters with at least 3 of the following four classes: upper case, lower case, numeral, special character) and be changed at least every 180 days; or utilize other strong log-in credentials (e.g., biometrics).

E. Initial user passwords are required to be changed at first log-on. Cisco shall have a policy prohibiting the sharing of user IDs, passwords, or other log-in credentials.

F. Firewalls must be deployed to protect the perimeter of Cisco's networks.

ii. **Virtual Private Networks ("VPN").** When remote connectivity to the Customer's or Cisco's network is required for Processing of Protected Data:

A. Connections must be encrypted using industry standard cryptography (i.e., a minimum of 256-bit encryption).

B. Connections shall only be established using VPN servers.

C. The use of multi-factor authentication is required.

iii. **Data Transfer.** Cisco shall have formal transfer policies in place to protect the transfer of information through the use of all types of communication facilities and removable media that adhere to the requirements of this ISE. Such policies shall be designed to protect transferred information from unauthorized interception, copying, modification, corruption, routing and destruction.

k. **System Acquisition, Development, and Maintenance**

i. Security Requirements. Cisco shall adopt security requirements for the purchase, use, or deve-

lopment of information systems, including for application services delivered through public networks.

ii. **Development Requirements.** Cisco shall have policies for secure development, system engineering, and support. Cisco shall conduct appropriate tests for system security as part of acceptance testing processes. Cisco shall supervise and monitor the activity of outsourced system development.

l **Penetration Testing and Vulnerability Scanning & Audit Reports**

i. **Testing.** Cisco will perform periodic penetration tests on its internet perimeter network. Audits will be conducted by Cisco's compliance team using industry recommended network security tools to identify vulnerability information. Upon written request from Customer, Cisco shall provide a Vulnerability & Penetration testing report at the organization level which may include an executive summary of the results and not the details of actual findings.

ii. **Audits.** Cisco shall respond promptly to and cooperate with reasonable requests by Customer for security audit, and testing reports. Customer shall treat the contents of and reports related to Cisco's security and certifications as Protected Data pursuant to the terms contained in this MDPA.

iii. **Remedial Action.** If any audit or penetration testing exercise referred to in Section 4(l)(ii). above reveals any deficiencies, weaknesses, or areas of non-compliance, Cisco shall promptly take such steps as may be required, in Cisco's reasonable discretion, to address material deficiencies, weaknesses, and areas of non-compliance as soon as may be practicable given the circumstances.

iv. **Status of Remedial Action.** Upon request, Cisco shall keep Customer informed of the status of any remedial action that is required to be carried out, including the estimated timetable for completing the same, and shall certify to Customer as soon as may be practicable given the circumstances that all necessary remedial actions have been completed.

m. **Contractor Relationships**

i. **Policies.** Cisco shall have information security policies or procedures for its use of Representatives that impose requirements consistent with this ISE. Such policies shall be reviewed at planned intervals or if significant changes occur. Agreements with Representatives shall include requirements that are consistent with, or analogous to, this MDPA.

ii. **Monitoring.** Cisco shall monitor and audit service delivery by its Representatives and review its Representatives' security practices against the security requirements set forth in Cisco's agreements with such Representatives. Cisco shall manage changes in Representative services that may have an impact on security.

n. **Management of Information Security Incidents and Improvements**

i. **Responsibilities and Procedures.** Cisco shall establish procedures to ensure a quick, effective, and orderly response to Information Security Incidents.

ii. **Reporting Information Security Incident.** Cisco shall implement procedures for Information Security Incidents to be reported through appropriate management channels as quickly as reasonably possible. All employees and Representatives should be made aware of their responsibility to report Information Security Incidents as quickly as reasonably possible.

iii. **Reporting Information Security Weaknesses.** Cisco, employees, and Representatives are required to note and report any observed or suspected information security weaknesses in systems or services.

iv. **Assessment of and Decision on Information Security Events.** Cisco shall have an incident classification scale in place in order to decide whether a security event should be classified as an Information Security Incident. The classification scale should be based on the impact and extent of an incident.

v. **Response Process.** Cisco shall maintain a record of Information Security Incidents with a description of the incident which may include the categories of personal data affected to the extent the Information Security Incidents affects Personal Data, the effect of the incident, the name of the reporter and to whom the incident was reported, the procedure for rectifying the incident, and the remedial action taken to prevent future security incidents; such record to be available to the Customer upon request.

o. **Information Security Aspects of Business Continuity Management**

i. **Planning.** Cisco shall maintain emergency and contingency plans for the facilities where Cisco information systems that process Protected Data are located. Cisco shall verify the established and implemented information security continuity controls at regular intervals.

ii. **Data Recovery.** Cisco shall design redundant storage and procedures for recovering data in a manner sufficient to reconstruct Protected Data in its original state as found on the last recorded backup provided by the Customer.

5. **Notification and Communication Obligations**

a. **Notification.** Cisco shall notify Customer without undue delay and where feasible within 24 hours, but in any event within no later than 48 hours from confirmation.

Notification to Customer shall be sent to:

if any of the following events occur:

i. any unmitigated, material security vulnerability, or weakness of which Cisco has actual knowledge in (i) Customer's systems, or networks, or (ii) Cisco's systems or networks, that has compromised Protected Data;

ii. an Information Security Incident that compromises or is likely to compromise the security of Protected Data and weaken or impair business operations of the Customer;

iii. an Information Security Incident that negatively impacts the confidentiality, integrity, and availability of Protected Data that is Processed, stored, and transmitted using a computer; or

iv. known and willful failure or inability to maintain material compliance with requirements of this ISE and Applicable Laws.

b. **Cooperation**

Cisco shall: (i) respond promptly to any Customer reasonable requests for information, cooperation, and assistance, including to a Customer designated response center.

c. **Information Security Communication**

Except as required by mandatory applicable law or by existing applicable contractual obligations,

Cisco agrees that it will not inform any third party of any of the events described above in this Section referencing, or identifying the Customer, without Customer's prior written consent. Cisco shall fully cooperate with Customer and law enforcement authorities concerning any unauthorized access to Customer's systems or networks, or Protected Data. Such co-operation shall include the retention of all information and data within Cisco's possession, custody, or control that is directly related to any Information Security Incident. If disclosure is required by law, Cisco will work with Customer regarding the timing, content, and recipients of such disclosure. To the extent Cisco was at fault, Cisco will bear the cost of reproduction or any other remedial steps necessary to address the incident or compromise. If disclosure is not permitted by law, Cisco will take any necessary action to seek legal remedies in accordance with Greek legislation regarding secrecy of communications before disclosing information or protected data.

d. **Post-Incident**

Cisco shall reasonably cooperate with Customer in any post-incident investigation, remediation, and communication efforts.

e. **Availability of Procedural Manuals, Policy Handbooks and Audits**

Cisco shall make available to Customer such information as is reasonably necessary to demonstrate Cisco's compliance with the obligations of Data Processors under applicable law, and allow for and contribute to information security audits by Customer (or another auditor mandated by the Customer) at Customer's expense, for this purpose, subject to the Customer a. no more than once annually and by giving Cisco at least 6 weeks' prior written notice of such information audit being required by Customer; b. ensuring that all information obtained or generated by the Customer or its auditor(s) in connection with such information security audit is kept strictly confidential (save for disclosure to a supervisory authority or as otherwise required by law); and c. before the commencement of any such information security audit, Cisco and Customer shall mutually agree upon the scope, timing, and duration of the information security audit.

ATTACHMENT B

DATA PROTECTION EXHIBIT

1. SCOPE

This Data Protection Exhibit ("DPE") outlines the terms and conditions with which the Parties must comply with respect to Processing Personal Data and applies to the extent that Cisco Processes or has access to Protected Data in the Performance of its obligations to the Customer.

2. DEFAULT STANDARDS

a. To the extent that Cisco Processes Special Categories of Data, the security measures referred to in this DPE shall also include, at a minimum (i) routine risk assessments of Cisco's information security program, (ii) regular testing and monitoring to measure and confirm the effectiveness of the information security program's key controls, systems, and procedures, and (iii) encryption of Special Categories of Data while during transmission (whether sent by e-mail, fax, or otherwise) and storage (including when stored on mobile devices, such as a portable computer, flash drive, PDA, or cellular telephone). If encryption is not feasible, Cisco shall not store Special Categories of Data on any unencrypted devices unless compensating controls are implemented. Cisco shall protect all Special Categories of Data stored on electronic databases, servers, or other forms of non-mobile devices against all reasonably anticipated forms of compromise by use of the safeguards contained in Attachment A (Information Security Exhibit).

b. In addition to the foregoing, to the extent Cisco receives, processes, transmits or stores any Cardholder Data for or on behalf of Customer, Cisco represents and warrants that information security procedures, processes, and systems will at all times meet or exceed all applicable information security laws, standards, rules, and requirements related to the collection, storage, Processing, and transmission of payment card information, including those established by applicable governmental regulatory agencies, the Payment Card Industry (the "PCI"), all applicable networks, and any written standards provided by Customer's information security group to Cisco from time to time (all the foregoing collectively the "PCI Compliance Standards").

c. If any of the Applicable Laws are superseded by new or modified mandatory applicable law (including any decisions or interpretations by a relevant court or governmental authority relating thereto), the new or modified mandatory applicable law shall be deemed to be incorporated into this DPE, and Cisco will promptly begin complying with such mandatory applicable law.

d. If this DPE does not specifically address a particular data security or privacy standard or obligation, Cisco will use appropriate, Generally Accepted Practices to protect the confidentiality, security, privacy, integrity, availability, and accuracy of Personal Data.

e. Cisco agrees that, in the event of a breach of this DPE, whether Customer has an adequate remedy in damages, Customer may be entitled to seek injunctive or equitable relief to immediately cease or prevent the use, Processing, or disclosure of Personal Data not contemplated by Cisco's obligations to the Customer and/or this MDPA and to enforce the terms of this DPE or enforce compliance with all mandatory applicable law.

f. Any ambiguity in this DPE shall be resolved to permit Customer to comply with all mandatory applicable law. In the event and to the extent that the mandatory applicable law impose stricter obligations on Cisco than under this DPE, the mandatory applicable law shall prevail.

3. CERTIFICATIONS

a. Cisco must maintain the certifications listed in an applicable agreement between the Parties, if any, and Cisco shall recertify such certifications as reasonably required. If there is a material change in the requirements of a required certification or the nature of the Performance Cisco is providing, such that Cisco no longer wishes to maintain such certifications, the Parties will discuss alternatives and compensating controls in good faith.

b. Prior to Processing Personal Data and at Customer's request, Cisco will provide Customer with copies of any certifications it maintains (along with relevant supporting documentation) that apply to the systems, policies, and procedures that govern the Processing of Personal Data. Cisco will notify Customer if Cisco has failed or no longer intends to adhere to such certifications or successor frameworks. This notification may be provided by posting or publication on Cisco's public website.

4. DATA PROTECTION AND PRIVACY

a. The Parties agree that, for the Personal Data, Customer shall be the Data Controller and Cisco shall be the Data Processor, as these terms are defined in the GDPR.

b. Customer shall:

i. in its use of the Products and/or Services, comply with mandatory applicable law, including maintaining all relevant regulatory registrations and notifications as required under mandatory applicable law;

ii. ensure all instructions given by it to Cisco in respect of Personal Data shall at all times be in accordance with mandatory applicable law;

iii. have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data, including providing any required notices to, and obtaining any necessary consent from, its employees, agents or third parties to whom it extends the benefits of the Products and/or Services; and

iv. keep the amount of Personal Data provided to Cisco to the minimum necessary for the performance of the Products and/or Services.

c. If Cisco has access to or otherwise Processes Personal Data, then Cisco shall:

i. implement and maintain commercially reasonable and appropriate physical, technical, and organizational security measures described in this DPE (including any appendices or attachments or referenced certifications) designed to protect Personal Data against accidental or unlawful destruction; accidental loss, alteration, unauthorized disclosure or access; all other unlawful forms of Processing; and any Information Security Incident;

ii. take reasonable steps designed to ensure the reliability of its staff and that they are subject to a binding written contractual obligation with Cisco to keep the Personal Data confidential (except where disclosure is required in accordance with mandatory applicable laws, in which case Cisco shall, where practicable and not prohibited by mandatory applicable law, notify Customer of any such requirement before such disclosure) and any other person acting under its supervision who may come into contact with, or otherwise have access to and Process Personal Data; and require that such personnel are aware of their responsibilities under this DPE and any mandatory applicable law (or Cisco's own written binding policies that are at least as restrictive as this DPE);

iii. appoint a data protection officer (a Privacy Officer based in the EU). Upon request, Cisco will provide the contact details of the appointed person; who shall undertake the duties and obligations defined in GDPR (Section 4).

iv. assist Customer as reasonably needed to respond to requests from supervisory authorities, data subjects, customers, or others to provide information (including details of the Services provided by Cisco) related to Cisco's Processing of Personal Data;

v. not transfer Personal Data from the EEA or Switzerland to a jurisdiction which is not an Approved Jurisdiction, unless it first provides Customer advance notice and an opportunity to object; if Customer reasonably objects to the proposed cross border transfer the applicable Performance that is the subject matter of the objection shall terminate.

Where Cisco Processes Personal Data from the EEA or Switzerland on behalf of Customer, Cisco shall perform such Processing in a manner consistent with the Privacy Shield Principles (see www.commerce.gov/privacyshield) or its successor framework(s) to the extent the Principles are applicable to Cisco's Processing of such data. If Cisco is unable to provide the same level of protection as required by the Principles, Cisco shall promptly notify Customer and cease Processing. In such event, Customer may terminate the applicable Performance of such Processing by written notice within thirty (30) days.

vi. for jurisdictions other than the EEA or Switzerland, not transfer Personal Data outside of the jurisdiction where the Personal Data is obtained unless permitted under mandatory applicable law and it first provides Customer advance notice and an opportunity to object; if Customer reasonably objects to the proposed cross border transfer the applicable Performance that is the subject matter of the objection shall terminate.

d. In addition, if Cisco Processes Personal Data in the course of Performance of its obligations to the Customer, then Cisco shall also:

i. only Process the Personal Data in accordance with Customer's documented instructions, Appendix 1 of Attachment C and this DPE, but only to the extent that such instructions are consistent with mandatory applicable laws. If Cisco reasonably believes that Customer's instructions are inconsistent with mandatory applicable law, Cisco will promptly notify Customer of such;

ii. if required by mandatory applicable law, court order, warrant, subpoena, or other legal or judicial process to process Personal Data other than in accordance with Customer's instructions, notify Customer of any such requirement before Processing the Personal Data (unless mandatory applicable law prohibits such information on important grounds of public interest);

iii. only process or use Personal Data on its systems or facilities to the extent necessary to Perform its obligations solely on behalf of Customer and only for the purposes contemplated by the Parties;

iv. where applicable, act as a subprocessor of such Personal Data;

v. maintain reasonably accurate records of the Processing of any Personal Data received from Customer under the Agreement;

vi. make reasonable efforts to ensure that Personal Data is accurate and up to date at all times while in its custody or under its control, to the extent Cisco has the ability to do so;

vii. not lease, sell, distribute, or otherwise encumber Personal Data unless mutually agreed to

by separate signed, written agreement;

viii. provide reasonable cooperation and assistance to Customer in allowing the persons to whom Personal Data relate to have access to their data and to delete or correct such Personal Data if they are demonstrably incorrect (or, if Customer or Customer's customer does not agree that they are incorrect, to have recorded the fact that the relevant person considers the data to be incorrect);

ix. provide such assistance as Customer reasonably requests (either on its own behalf or on behalf of its customers), and Cisco or a Representative is reasonably able to provide, with a view to meeting any applicable filing, approval or similar requirements in relation to mandatory applicable law;

x. promptly notify Customer of any investigation, litigation, arbitrated matter, or other dispute relating to Cisco's information security or privacy practices as it relates to Cisco's Performance of its obligations to Customer;

xi. provide such reasonable information and assistance as Customer reasonably requires (taking into account the nature of Processing and the information available to Cisco) to Customer in ensuring compliance with Customer's obligations under mandatory applicable law with respect to:

A. security of Processing;

B. data protection impact assessments as such term is defined in GDPR;

C. prior consultation with a supervisory authority regarding high risk Processing; and

D. notifications to the supervisory authority and/or communications to Data Subjects by Customer in response to any Information Security Incident; and,

xii. on termination of the MDPA for whatever reason, or upon written request at any time during the Term, Cisco shall cease to Process any Personal Data received from Customer, and within a reasonable period will, at the request of Customer: 1) return all Personal Data; or 2) securely and completely destroy or erase (e.g. using a standard such as US Department of Defense 5220.22-M, NIST 800-53, or British HMG InfoSec Standard 5, Enhanced Standard) all Personal Data in its possession or control unless such return or destruction is not feasible or continued retention and Processing is required by mandatory applicable law. At Customer's request, Cisco shall give Customer a certificate signed by one of its senior managers, confirming that it has fully complied with this Clause.

5. STANDARD CONTRACTUAL CLAUSES FOR THE PROCESSING OF PERSONAL DATA

If, and only with Customer's prior consent, Cisco Processes Personal Data from the EEA or Switzerland in a jurisdiction that is not an Approved Jurisdiction, the Parties shall confirm there is a legally approved mechanism in place to allow for the international data transfer.

If Cisco intends to rely on Standard Contractual Clauses (rather than another permissible transfer mechanism), the following additional terms will apply to Cisco and Cisco's subprocessors and/or Affiliates who may be Performing on behalf of Cisco:

a. The Standard Contractual Clauses set forth in Attachment D will apply. If such Standard Contractual Clauses are superseded by new or modified Standard Contractual Clauses, the Parties shall promptly enter into the new or modified Standard Contractual Clauses, as necessary.

b. If Cisco subcontracts any Processing of Personal Data (only as expressly allowed by an applicable agreement between the Parties and mandatory applicable law), Cisco will:

i. Notify Customer in advance of such Processing and provide Customer an opportunity to object prior to Processing; and

ii. Require that Cisco's subprocessors have entered into written agreements with Cisco in which the subprocessors agree to abide by terms consistent with the applicable portions of the Standard Contractual Clauses with respect to such Personal Data.

c. If necessary to comply with mandatory applicable law, and where reasonably requested by Customer on behalf of its customers, Cisco shall enter into the Standard Contractual Clauses directly with Customer's customers.

6. **SUBPROCESSING**

a. Cisco shall have a documented security program and policies that provide (i) guidance to its subprocessors with respect to ensuring the security, confidentiality, integrity, and availability of personal data and systems maintained or processed by Cisco; and (ii) express instructions regarding the steps to take in the event of a compromise or other anomalous event.

b. Cisco shall not subcontract its obligations under this DPE to another person or entity, in whole or in part, without providing Customer with advance notice and an opportunity to object; if Customer reasonably objects to the proposed subcontracting, the applicable Performance that is the subject matter of the objection shall terminate.

c. Cisco will execute a written agreement with such approved subprocessors containing terms at least as protective as this DPE and the applicable Exhibits (provided that Cisco shall not be entitled to permit the subprocessor to further subcontract or otherwise delegate all or any part of the subprocessor's Processing without Cisco's prior notice and opportunity to object) and designating Customer as a third party beneficiary with rights to enforce such terms either by contract or operation of law. Further, if privity of contract is required by mandatory applicable law, Cisco shall procure that any such subprocessors cooperates and enters into any necessary additional agreements directly with Customer.

d. Cisco shall be liable and accountable for the acts or omissions of Representatives to the same extent it is liable and accountable for its own actions or omissions under this DPE.

e. Customer acknowledges and expressly agrees that Cisco's Affiliates may be retained as subprocessors, and (b) Cisco and Cisco's Affiliates respectively may engage third-party subprocessors in the course of Performance. Cisco shall make available to Customer a current list of subprocessors for the respective Services with the identities of those subprocessors ("Subprocessor List") upon Customer's reasonable request.

7. **RIGHTS OF DATA SUBJECTS**

a. **Data Subject Requests.** Cisco shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject for access to, correction, portability, or deletion of such Data Subject's Personal Data. Unless required by mandatory applicable law, Cisco shall not respond to any such Data Subject request without Customer's prior written consent except to confirm that the request relates to Customer. In addition Cisco shall provide such information and cooperation and take such action as the Customer reasonably requests in relation to a Data Subject request.

b. **Complaints or Notices related to Personal Data.** In the event Cisco receives any official complaint, notice, or communication that relates to Cisco's Processing of Personal Data or either Party's compliance with mandatory applicable law in connection with Personal Data, to the extent legally permitted, Cisco shall promptly notify Customer and, to the extent applicable, Cisco shall provide Customer with commercially reasonable cooperation and assistance in relation to any such complaint, notice, or communication.

8. **PERMITTED USE AND DISCLOSURE**

Notwithstanding anything to the contrary in this MDPA, (i) Cisco may disclose Telemetry Data and Support Data to third parties, provided such data has been aggregated and/or appropriately de-identified to reasonably prevent the identification of any individual natural person or legal entity; (ii) Cisco may use such de-identified Telemetry Data and Support Data for its own business purposes without attribution or compensation to Customer; and (iii) Cisco may use Administrative Data for its own internal business purposes or to fulfill its obligations to Customer under an applicable agreement. Cisco shall not be required to return or destroy Protected Data that constitutes Administrative Data, Telemetry Data or Support Data and shall continue to be permitted to use and disclose such Administrative Data, Telemetry Data, and Support Data, only in de-identified form, as set forth in this Section 8 (Permitted Use and Disclosure) following the termination or expiration of this MDPA.

ATTACHMENT C

All the detailed information about the Processing of Personal Data by Cisco Webex Meetings can be found in the following Privacy Data Sheet:

cisco-webex-meeting
s-privacy-data-sheet (

The processing details included in this Attachment C may be subject to change provided such change does not materially reduce Cisco's protection of personal data. For an up to date description of the processing activities please see the Privacy Data Sheet for Webex Meetings on Cisco's Trust Center at https://www.cisco.com/c/en/us/about/trust-center/solutions-privacy-data-sheets.html.

ATTACHMENT D

Standard Contractual Clauses

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection (These can be located in their original text on the European Commission website here: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm).

Cisco will use Standard Contractual Clauses as these are from time to time proposed and approved by the European Data Protection Board ("EDPB").

APPENDIX 1 TO ATTACHMENT C
THE STANDARD CONTRACTUAL CLAUSES
CISCO WEBEX MEETINGS

This Appendix 1 to Attachment C the Standard Contractual Clauses "Cisco Webex Meetings" forms part of the Standard Contractual Clauses.

Cisco Webex Meetings is referred to as "Service" or "Webex Meetings" in this Appendix 1.

Data exporter
The data exporter is Company, acting as data exporter on behalf of itself or a customer where applicable. Activities relevant to the transfer include the performance of services for Company and its customer(s).

Data importer
The data importer is Cisco. Activities relevant to the transfer include the performance of services for Company and customers.

Data subjects
The personal data transferred may concern the following categories of data subjects: Company or customer employees.

Webex Meetings, Webex Events, Webex Support, and Webex Training

Personal data category	Types of personal data	Purpose of processing
Registration Information	• Name • Email Address • Password • Public IP Address • Browser • Phone Number (Optional) • Mailing Address (Optional) • Avatar (Optional) • Billing Information	• Enroll customer in Service • Display customer user avatar identity to other users • Provide support
Host and Usage Information	• IP Address • User Agent Identifier • Hardware Type • Operating System Type and Version • Client Version • IP Addresses Along the Network Path • MAC Address of endpoint (as Applicable) • Service Version • Actions Taken • Meeting Session Information (title, date and time, frequency, average and actual duration, quantity, quality, network activity, and network connectivity)	• Understand how the Service is used • Diagnose technical issues • Conduct analytics and statistical analysis in aggregate form to improve the Service • Respond to Customer support requests

	• Number of Meetings • Number of Screen-Sharing and Non-Screen-Sharing Sessions • Number of Participants • Host Name • Screen Resolution • Join Method • Performance, Troubleshooting, and Diagnostics Information	
User-Generated Information* *Optional: only applicable if these features are enabled.	• Meeting and Call Recordings • Uploaded Files	Provide the Service, optional components which include recording meetings and file sharing

Technical Support Assistance (TAC)

Personal data category	Types of personal data	Purpose of processing
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 Files	• Provide support • Review quality of the support service • Perform analysis of the service solution

Categories of data
The personal data transferred may concern the following categories of data:

1. Registration information (as set out in the tables above)
2. Host and usage information (as set out in the tables above)
3. User-generated information (as set out in the tables above*) (***Optional: only applicable if this feature is enabled).**
4. TAC Support information (as set out in the tables above)

Special categories of data
The personal data transferred may concern the following special categories of data: only if revealed by a Data Subject

Processing operations
Cisco Webex Meetings is a cloud-based web and video conferencing solution made available by Cisco to Customer who purchase it for use by their authorized users. Cisco Webex Meetings enables global employees and virtual teams to collaborate in real time from anywhere, anytime, on any mobile device or video system as though they were working in the same room. Solutions include meetings, events, training, and support services.

Cisco Webex Meetings allows users to instantly connect in a way that is as personal as a face-to-face meeting. The meeting host has the option to record meetings and all users have the option to upload and preserve files shared during and outside of meetings. If the meeting host opts not to preserve the meeting content, it disappears from the Cisco Webex platform immediately after the meeting concludes*. (***Optional: only applicable if this feature is enabled).**

Similarly, if users participate in meetings hosted by users in other companies, the meeting host will control any meeting recordings or files shared during the meeting* (***Optional: only applicable if this feature is enabled**), which will be subject to the host's corporate policies regarding access, use, monitoring, deletion, preservation, and export of information. Cisco has no control over, and is not responsible or liable for the privacy of any information that Customer have shared with others. Even after Customer removes information from the Webex platform, there exists a minor possibility that copies of that information remain viewable elsewhere to the extent it has been shared with others.

Data Deletion & Retention

Customers have the ability to set organization-wide retention periods for recordings using APIs. After the Service is terminated or expires, User-Generated Information is deleted from the Cisco Webex platform within 60 days.

Customers can request deletion of other personal data retained on the Cisco Webex platform by sending a request to privacy@cisco.com or opening a TAC service request, and unless the personal data is required to be retained for Cisco's legitimate business purposes, Cisco endeavors to delete the requested data from its systems within 30 days. The table below describes the retention period and the business reasons that Cisco retains the personal data. Users seeking deletion of other personal data retained on the Cisco Webex platform must request deletion from their employer's site administrator.

Personal Data Category	Retention Period	Reason and Criteria for Retention
Registration Information	7 years from when the Service is terminated	Data collected as part of registration, including information provided by customers as part of Cisco's financial due diligence, constitute Cisco business records and are kept to comply with Cisco financial and audit policies, as well as tax requirements. **This applies only to those users who have created a Webex profile under the Customer's account.**
TAC Support Information	Until Customer (i) requests deletion via email to privacy@cisco.com or (ii) by opening a TAC service request	TAC Support Information is retained to ensure efficient support in case of recurring issues and to comply with Cisco audit policies related to business records of services provided to Customer.
User-Generated Information	Active Subscriptions: At Customer's or user's discretion Terminated Service: Deleted within 60 days by **Cisco or earlier by Customer**	User-Generated Information is not retained on the Cisco Webex platform when Customer or user deletes this data.
Host and Usage Information	7 years from when the Service is terminated	Information generated by instrumentation and logging systems created through the use and operation of the Service is kept as part of Cisco's record of Service delivery. Usage information

		used to conduct analytics and measure statistical performance is retained but pseudonymized.

The processing details included in this Appendix 1 may be subject to change provided such change does not materially reduce Cisco's protection of personal data below the requirements of applicable mandatory laws. For an up-to date description of the processing activities please see the applicable Privacy Data Sheet on Cisco's Trust Center at [illegible] about/legal-data-privacy-sheets.html.

DATA EXPORTER

Name

Authorised Signature

DATA IMPORTER

Name

Authorised Signature

APPENDIX 2 TO ATTACHMENT D
THE STANDARD CONTRACTUAL CLAUSES

Appendix 2 to Attachment D, the Standard Contractual Clauses, is the Information Security Exhibit ("ISE") located at *Attachment A*

ATTACHMENT E
GLOSSARY OF TERMS

All capitalized terms not defined in this Glossary have the meanings set forth elsewhere in the MDPA.

a. **"Administrative Data"** means data related to employees or representatives of Customer that is collected and used by Cisco in order to administer or manage Cisco's Performance, or the Customer's account, for Cisco's own business purposes. Administrative Data may include Personal Data and information about the contractual commitments between Customer and Cisco, whether collected at the time of the initial registration or thereafter in connection with the delivery, management or Performance. Administrative Data is Protected Data.

b. **"Affiliates"** means any entity that directly or indirectly controls, is controlled by, or is under common control with, another entity, for so long as such control exists. In the case of companies and corporations, "control" and "controlled" mean beneficial ownership of more than fifty percent (50%) of the voting stock, shares, interest or equity in an entity. In the case of any other legal entity, "control" and "controlled" mean the ability to directly or indirectly control the management and/or business of the legal entity.

c. Not applicable.

d. Not applicable.

e. **"Approved Jurisdiction"** means a member state of the European Economic Area, or other jurisdiction as may be approved as having adequate legal protections for data by the European Commission currently found here: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

f. **"Business Associate Agreement"** means the specific terms and conditions that would be added as Attachment C and would apply when Cisco Processes Protected Health Information

g. Not applicable.

h. **"Confidential Information"** means any confidential information or materials relating to the business, products, customers or employees of the Customer and includes, without limitation, trade secrets, know-how, inventions, techniques, processes, programs, schematics, software source documents, data, customer lists, financial information, pricing, product development, sales and marketing plans or information that Cisco knows or has reason to know is confidential, proprietary or trade secret information obtained by Cisco from the Customer or at the request or direction of the Customer in the course of Performing: (i) that has been marked as confidential; (ii) whose confidential nature has been made known by the Customer to Cisco; or (iii) that due to their character and nature, a reasonable person under like circumstances would treat as confidential.

i. **"Customer Data"** means all data (including text, audio, video, or image files) that is either provided by a customer in connection with the customer's use of products or services, or data developed at the specific request of a customer pursuant to a statement of work or contract. Customer Data does not include Administrative Data, Financing Data, Support Data or Telemetry Data.

j. **"Data Subject"** means the individual to whom Personal Data relates.

k. **"Customer"** means that party making available Protected Data (whether confidential or not) to the other party.

l. **"EEA"** or **"European Economic Area"** means those countries that are members of European Free Trade Association ("EFTA"), and the then-current, post-accession member states of the European Union.

m. Not applicable.

n. Not applicable.

o. **"Generally Accepted Practices"** refer to the levels of accuracy, quality, care, prudence, completeness, timeliness, responsiveness, resource efficiency, productivity, and proactive monitoring of service performance that are at least equal to the then-current accepted industry standards of first-tier providers of the tasks contemplated in Performance of the Agreement.

p. **"Information Security Incident"** means a successful or imminent threat of unauthorized access, use, disclosure, breach, modification, theft, loss, corruption, or destruction of information; interference with information technology operations; or interference with system operations.

q. **"Performance"** means any acts by either Party in the course of completing obligations contemplated under the Agreement, including the performance of services, providing deliverables and work product, access to Personal Data, or providing Software as a Service ("SaaS"), cloud platforms or hosted services. **"Perform," "Performs,"** and **"Performing"** shall be construed accordingly.

r. **"Personal Data"** means any information as per art. 4(1) GDPR. Personal Data shall be considered Confidential Information regardless of the source. Personal Data is Protected Data.

s. **"Process"** as per 4(2) GDPR.

t. **"Product"** means Cisco-branded hardware and software products that are made generally available.

u. **"Protected Data"** means Administrative Data, Confidential Information, Customer Data, Financing Data, Cardholder Data, Support Data, Telemetry Data, and all Personal Data.

v. Not applicable.

w. **"Cisco"** means the Party receiving Protected Data.

x. **"Representatives"** means either Party and its Affiliates' officers, directors, employees, agents, contractors, temporary personnel, subcontractors and consultants.

y. **"Sensitive Personal Data"** or **"Special Categories of Data"** means personal information that requires an extra level of protection and a higher duty of care. These categories are defined by mandatory applicable law and include: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, or information related to offenses or criminal convictions. Sensitive Personal Data and Special Categories of Data are each a category of Personal Data that are particularly sensitive and pose greater risk. Customer may require additional privacy responsibilities when dealing with such Personal Data, which will be appended to the Agreement or a statement of work, as applicable.

z. **"Service"** means a Cisco-branded service offering described in an applicable service or offer description, statement of work, or purchase order listed selected by Customer.

aa. **"Support Data"** means information that Cisco collects when Customer submits a request for support services or other troubleshooting, including information about hardware, software and other details related to the support incident, such as authentication information, information about the condition of the product, system and registry data about software installations and hardware configurations, and error-tracking files. Support Data is Protected Data.

bb. **"Telemetry Data"** means information generated by instrumentation and logging systems created through the use and operation of the products and/or services. Telemetry Data is Protected Data.

Cisco Webex Meetings

This Privacy Data Sheet describes the processing of personal data (or personal identifiable information) by Cisco Webex Meetings.

1. Overview of Cisco Webex Meetings Capabilities

Cisco Webex Meetings (the "Service" or "Webex Meetings") is a cloud-based web and video conferencing solution made available by Cisco to companies or persons ("Customers," "you," or "your") who purchase it for use by their authorized users (each, a "user"). The Service enables global employees and virtual teams to collaborate in real time from anywhere, anytime, on any mobile device or video system as though they were working in the same room. Solutions include meetings, events, training, and support services. For more information regarding the People Insights feature for Cisco Webex Meetings, please see Addendum One below. For a detailed overview of the Service, please visit the Cisco Web Conferencing [illegible].

Because the Service enables collaboration among its users, you may be asked to provide your personal data in order to use the Service. The following paragraphs describe Cisco's processing of personal data in connection with the delivery of the Service, the location and transfers of that data, and how it is secured in accordance with privacy principles, laws, and regulations. If you choose to purchase the Service, you will need to disclose personal data to Cisco in order to use it. Cisco will use your personal data consistent with this Privacy Data Sheet. Note that this Privacy Data Sheet is a supplement to the [illegible].

2. Personal Data Processing

The Service allows users to instantly connect in a way that is as personal as a face-to-face meeting. The meeting host has the option to record meetings and all users have the option to upload and preserve files shared during and outside of meetings, which may be discoverable in a legal matter. The meeting host should inform all meeting attendees prior to recording if the meeting host intends to record the meeting. If the meeting host opts not to preserve the meeting content, it disappears from the Webex Meetings platform immediately after the meeting concludes. If you are a user and your employer is the Customer that purchased the Service, all of the information described in this Privacy Data Sheet is accessible by your employer and is subject to your employer's policies regarding access, use, monitoring, deletion, preservation, and export of information associated with the Service.

Similarly, if users participate in meetings hosted by users in other companies, the meeting host will control any meeting recordings or files shared during the meeting, which will be subject to the host's corporate policies regarding access, use, monitoring, deletion, preservation, and export of information. Note, Cisco has no control over, and is not responsible or liable for the privacy of any information that you have shared with others. Even after you remove information from the Webex Meetings platform, copies of that information may remain viewable elsewhere to the extent it has been shared with others.

This Privacy Data Sheet covers the Cisco Webex Meetings Suite, Cisco Webex Events, and Cisco Webex Training. If you use the Service together with Cisco Webex Teams, see the see the Cisco Webex Teams Privacy Data Sheet (available on [illegible]) for descriptions of the data that may be collected and processed in connection with those services. The table below list the categories of personal data used by the Service and describe why we process such data.

Table 1 Webex Meetings, Webex Events, and Webex Training

Personal Data Category	Types of Personal Data	Purpose of Processing
Registration Information	• Name • Email Address • Password • Public IP Address • Browser • Phone Number (Optional) • Mailing Address (Optional) • Avatar (Optional) • Billing Information • User information included in the Customer's Active Directory (if synched)	We use Registration Information to: • Enroll you in the Service • Display your user avatar identity to other users • Make improvements to the Service and other Cisco products and services • Provide you support • Notify you about features and updates • Send you Cisco marketing communications • Authenticate and authorize access to your account • Bill you for the Service • Display directory information to other Webex users

Host and Usage Information	• IP Address
	• User Agent Identifier
	• Hardware Type
	• Operating System Type and Version
	• Client Version
	• IP Addresses Along the Network Path
	• MAC Address of Your Client (As Applicable)
	• Service Version
	• Actions Taken
	• Meeting Session Information (title, 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
	• Meeting Host Information*
	  • Host Name
	  • Meeting Site URL
	  • Meeting Start/End Time
	• Subscription Type
	• Meeting Attendee Information*
	  • Username of attendees
	  • Meeting Start/End time
	  • Subscription info
	• Screen Resolution
	• Join Method
	• Performance, Troubleshooting, and Diagnostics Information
	• Call participant information, including email addresses, IP address, username, phone numbers, room device information
	
	* Used for billing purpose
		We use Host and Usage Information to:
		• Understand how the Service is used
		• Diagnose technical issues
		• Conduct analytics and statistical analysis in aggregate form to improve the technical performance of the Service
		• Respond to Customer support requests
		• Bill you for the Service

User-Generated Information	• Meeting and Call Recordings • Transcriptions of Call Recordings • Uploaded Files (for Webex Events and Training only)	We use User-Generated Information to: • Provide the Service, optional components which include recording meetings

Technical Support Assistance

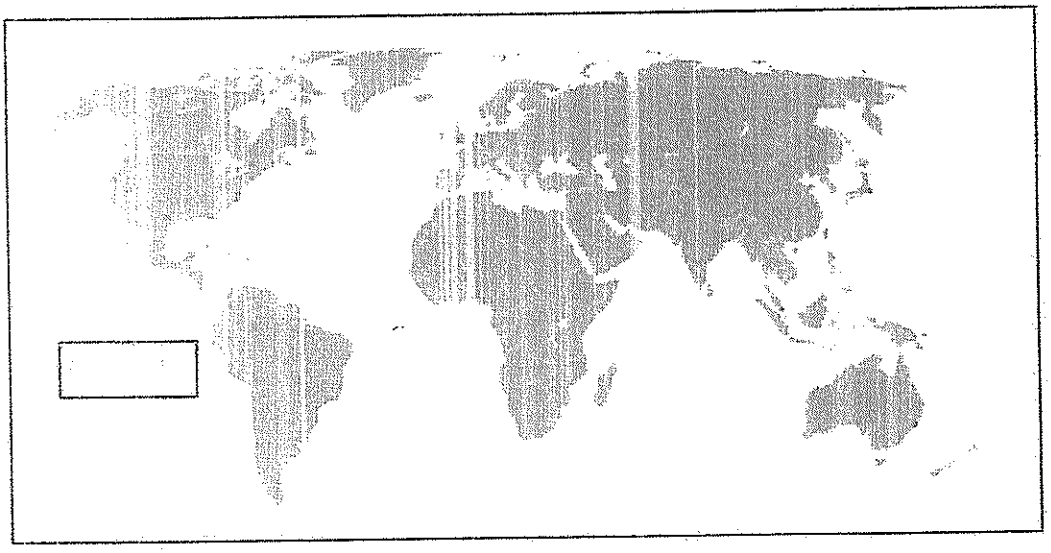
If a Customer reaches out to Cisco Technical Assistance Center (TAC) for problem diagnosis and resolution, Cisco TAC may receive and process personal data from the Service. [illegible] Privacy Data Sheet describes Cisco's processing of such data.

Webex Analytics Platform

Cisco Webex Control Hub Analytics provides usage trends and valuable insights that can be used to help with strategies to promote and optimize adoption across teams. The Webex Analytics Platform utilizes Registration, Host and Usage information to provide advanced analytics capabilities and reports.

3. Cross-Border Transfers

The Service leverages its own data centers to deliver the Service globally. If you join a meeting using Cisco Webex Teams, please see the Cisco Webex Teams Privacy Data Sheet for applicable privacy information, including data center locations. The Webex Meetings data centers are currently located in the following countries (data center locations may change from time to time and this Privacy Data Sheet will be updated to reflect those changes):



Cisco Data Center Locations:	Internet Point of Presence (IPOP) Locations:
Amsterdam, Netherlands	Amsterdam, Netherlands
Bangalore, India	California, USA
California, USA	Hong Kong, China
London, UK	Illinois, USA
New York, USA	New Jersey, USA
North Carolina, USA*	Sydney, Australia
Singapore, Singapore	Texas, USA
Sydney, Australia	
Texas, USA*	
Tokyo, Japan	
Toronto, Canada	
Virginia, USA	

User-Generated Information is stored in the data center closest to a Customer's location as provided during the ordering process. However, billing data is stored in Texas, USA and North Carolina, USA. Webex Analytics data is stored in California, USA and Texas, USA.

An Internet Point of Presence (IPOP) is used to route traffic geographically from nearby areas to a Cisco Data Center Location. It is intended to route Webex Meeting traffic through Cisco's infrastructure and improve performance. Data routed through these internet point of presence points is not decrypted and not stored at these locations.

Cisco has invested in a number of transfer mechanisms to enable the lawful use of data across jurisdictions. In particular:

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

4. Access Control

Customers and Cisco can access personal data on the Service as described in the table below.

Personal Data Category	Who has access	Purpose of the access
Registration Information	User through the My Webex Page	Modify, control, and delete information
	Customer through the Site Admin Page or Webex Control Hub	Modify, control, and delete in accordance with Customer's personal data policy
	Cisco	Support the Service in accordance with Cisco's data access and security controls process
Host and Usage Information	Host through the My Webex Page	View meeting session information
	Customer may view this information through the Site Admin Page, Webex Control Hub, or may be otherwise provided by Cisco	View usage, meeting session and configuration information
	Cisco	Support and improvement of the Service by the Cisco Webex Meetings Support and Development Team
User Generated Information	User through the My Webex Page	Modify, control, and delete based on user's preference
	Customer using APIs provided with the Service or through the Site Admin Page or Webex Control Hub	Modify, control, and delete in accordance with Customer's personal data policy
	Cisco	While Cisco operates the Service, Cisco will not access this data unless it is shared with Cisco by Customer, and will only access in accordance with Cisco's data access and security controls process.
	Other Customers and users (when shared during a meeting)	Content you choose to share during a meeting may be accessed by users in the meeting, wherever they are located. Even after you remove information from the Service, copies of that content may remain viewable elsewhere to the extent it has been shared with others.

5. Data Portability

The Service allows Customers and users to export all User-Generated Information. A Customer's administrator may do so using APIs provided with the Service (recordings only) or through the Site Admin Page; while individual users may do so through the My Webex Page. Meeting recordings are available in proprietary ARF and standard mp4 formats depending on the account type. Cisco offers a free ARF player to convert ARF files to mp4 format.

Customers are permitted to export personal data collected about their users on the Webex Meetings platform using APIs or via the Site Admin Configuration. There is no time restriction on exporting this data

6. Data Deletion & Retention

Subject only to their employer's corporate retention policies, users with an active subscription have complete control over how long their User-Generated Information (e.g., recordings and files they initiate or upload) is stored on the Webex Meetings platform and can delete such User-Generated Information from their account through the My Webex Page at any time during the term of their subscription. Enterprise Customers have the ability to set organization-wide retention periods for recordings using APIs. After the Service is terminated or expires, User-Generated Information is deleted from the Webex Meetings platform within 60 days.

Customers can request deletion of other personal data retained on the Webex Meetings platform by sending a request to [illegible] or opening a TAC service request, and unless the personal data is required to be retained for Cisco's legitimate business purposes, Cisco endeavors to delete the requested data from its systems within 30 days. The table below describes the retention period and the business reasons that Cisco retains the personal data. Users seeking deletion of other personal data retained on the Webex Meetings platform must request deletion from their employer's site administrator.

Personal Data Category	Retention period	Reason and Criteria for Retention
Registration Information	7 years from when the Service is terminated	Data collected as part of registration, including information provided by Customers as part of Cisco's financial due diligence, constitute Cisco business records and are kept to comply with Cisco financial and audit policies, as well as tax requirements.
User Generated Information	Active Subscriptions: • At Customer's or user's discretion Terminated Service: • Deleted within 60 days	User-Generated Information is not retained on the Webex Meetings platform when Customer or user deletes this data.
Host and Usage Information	7 years from when the Service is terminated	Information generated by instrumentation and logging systems created through the use and operation of the Service is kept as part of Cisco's record of Service delivery. Usage information used to conduct analytics and measure statistical performance is retained but pseudonymized.

7. Personal Data Security

The Service adopts technical and organizational security measures to protect your personal data from unauthorized access use or disclosure as required by law. Additional information about our encryption architecture is summarized in the table and paragraphs below.

Personal Data Category	Type of Encryption
Registration Information (excluding Passwords, discussed below)	Encrypted in transit, but not at rest
Passwords	Encrypted and hashed in transit and at rest
Host and Usage Information	Encrypted in transit, but not at rest
User Generated Information	Beginning in May 2018, Cisco released encryption of recordings at rest. Any new recordings created on your site after the enablement of this feature will be automatically encrypted in transit and at rest. Recordings created in the Webex Meetings FedRAMP-Authorized are encrypted in transit, but not at rest.

Protecting Data at Rest

The Service encrypts sensitive data at rest. Any data not encrypted at rest is protected by highly-secure data center protection mechanisms and operational procedures. Webex Meetings data centers feature communication infrastructure with industry-leading performance, integration, flexibility, scalability, and availability.

Encryption at Run Time

All communications on the Webex Meetings platform occur over encrypted channels. After a session is established, all media streams (audio, VOIP, video, screen share, and document share) are encrypted. The Service then re-encrypts the media stream before sending it to other users. Note that if a Customer allows attendees to join its meetings using third-party video end points, those attendees may be sending your meeting data unencrypted on the Internet. Media streams flowing from a user to Cisco Webex Meetings servers are decrypted after they cross the Cisco firewalls. This enables Cisco to provide network-based recording and SIP-based call support for video end points.

End-to-End Encryption (Optional)

For businesses requiring a higher level of security, the Service also provides end-to-end encryption. With this option, the Service does not decrypt the media streams. In this model, traffic cannot be deciphered by the Cisco Webex Meetings server. The end-to-end encryption option is available for Webex Meetings and Webex Support. Note that when end-to-end encryption is enabled, the following features are not supported:

- Network-based recordings
- Join Before Host
- Cisco Webex Video Platform (formerly known as Collaboration Meeting Rooms Cloud)

8. Third Party Service Providers (Sub-processors)

We may share Registration Information, Host Information, and/or Usage Information with service providers, contractors or other third parties to assist in providing and improving the Service. The data shared may include aggregate statistics or pseudonymized data. All sharing of information is carried out consistent with the Cisco Privacy Statement and we contract with third-party service providers that can provide the same level of data protection and information security that you can expect from Cisco. We do not rent or sell your information.

If a Customer purchases the Service through a Cisco partner, we may share any or all of the information described in this Data Sheet with the partner. Customers have the option of disabling this information-sharing with Cisco partners.

9. Information Security Incident Management

Breach and Incident Notification Processes

The Data Protection & Privacy team within Cisco's Security & Trust Organization coordinates the Data Incident Response Process and manages the enterprise-wide response to data-centric incidents. The Incident Commander directs and coordinates Cisco's response, leveraging diverse teams including the Cisco Product Security Incident Response Team (PSIRT), the Cisco Security Incident Response Team (CSIRT), and the Advanced Security Initiatives Group (ASIG).

PSIRT manages the receipt, investigation, and public reporting of security vulnerabilities related to Cisco products and networks. The team works with Customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security issues with Cisco products and networks. The Cisco Security Center details the process for reporting security incidents.

The Cisco Notification Service allows Customers to subscribe and receive important Cisco product and technology information, including Cisco security advisories for critical and high severity security vulnerabilities. This service allows Customers to choose the timing of notifications, and the notification delivery method (email message or RSS feed). The level of access is determined by the subscriber's relationship with Cisco. If you have questions or concerns about any product or security notifications, contact your Cisco sales representative.

10. Certifications and Compliance with Privacy Laws

The Security and Trust Organization and Cisco Legal provide risk and compliance management and consultation services to help drive security and regulatory compliance into the design of Cisco products and services. The Service and its underlying processes are designed to meet Cisco's obligations under the EU General Data Protection Regulation and other privacy laws around the world.

Cisco leverages the following privacy transfer mechanisms related to the lawful use of data across jurisdictions:

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

In addition to complying with our stringent internal standards, Cisco also continually maintains third-party validations to demonstrate our commitment to information security. The Service has received the following certifications:

- ISO 27001 + 27017
- SOC 2 Type II Attestation + C5
- FedRAMP

11. General Information and GDPR FAQ

For more information related to technical and operational security features of the Service, please see the [illegible] Security White Paper.

For more general information and FAQs related to Cisco's Security Compliance Program and Cisco's GDPR readiness please visit [illegible]

Spectrum One: People Insights feature for Cisco Webex (Optional)

This Privacy Data Sheet describes the processing of personal data (or personal identifiable information) by the People Insights feature for Cisco Webex Meetings and Cisco Webex Teams.

1. Overview of People Insights Capabilities

The People Insights feature ("People Insights" or the "Feature") provides Cisco Webex users with comprehensive, publicly available business and professional information for meeting participants giving users context and increased insight about the people with whom they collaborate.

Only the Customer's site administrator has the ability to enable the Feature for their organization and users. Individual users cannot opt-in to use People Insights independently of their site administrator. Users at an enabled organization can opt-out of People Insights by suppressing their profile from other meeting participants' view. This is accomplished in two ways:

1. Entering a meeting and selecting the "Hide Profile" link,
2. Signing into people.webex.com and clicking on "Hide Profile"

2. Personal Data Processing

People Insights compiles business and professional profiles for meeting participants using publicly available and legitimately sourced information, published authored works, news articles, search engine results, via APIs and through content supplied by the profile owner.

The tables below list the personal data used by People Insights and describes why we process that data.

Personal Data Category	Types of Personal Data	Purpose of Processing
Publicly Available Business and Professional Biographical Data	• Profile Photos • News • Tweets • Authored Works • Bios • Employment History • Education History • Web Links for a specific person	• To source the People Insights profile and to enable search within the feature.
Account & Usage Information	• User Level Account Details (including email, name, and web interactions and platform usage)	• To provide support and improvement of the Feature • Product analytics (e.g. frequency of profile edits, # of successful profile loads in a meeting, etc.)
Directory Data	• If the Active Directory option is enabled by the site administrator, professional information including the following may be collected from the internal company directory (as selected by the site administrator): ◦ Title ◦ Phone Number ◦ Location ◦ Organization ◦ Department ◦ Photo ◦ Role ◦ Reporting Structure	• To augment the user's People Insights profile by providing company specific context to meeting participants who belong to the same organization. This data will only be visible to participants within the user's organization.

Personal Data Category	Types of Personal Data	Purpose of Processing
User Generated Information	• Information that the user adds in their People Insights profile.	• Augment the user's own People Insights profile (visible to Insights users)

3. Cross-Border Transfers

People Insights data is stored on third party servers provided by Amazon Web Services ("AWS") and Algolia. AWS servers are located in Oregon, Ohio and Virginia. Algolia servers are located in California.

Cisco has invested in a number of transfer mechanisms to enable the lawful use of data across jurisdictions, as fully described in the Cisco Webex Meetings or Teams Privacy Data Sheets.

4. Access Control

Personal Data Category	Who has access	Purpose of the access
Publicly Available Business and Professional Biographical Data	Customer Cisco People Insight users within the Customer's organization	To provide the Feature
Account Information	Cisco	Registration Support Correlate users with correct profiles Analytics to improve service Feature enablement/disablement.
Customer Directory Data	Customer Customer (Admin) People Insight users within the Customer's organization Cisco	Directory data is provided and maintained by customer administrator to allow integration into People Insights profile. Directory data is imported and integrated with customer profile data to support profile development
User-Generated Information	User	Users may access their own User-Generated Information to edit or delete content.

5. Data Portability

Individuals can receive a copy of their own People Insights profile, including their self-generated information, by contacting

privacy@cisco.com

6. Data Deletion & Retention

Type of Personal Data	Retention Period	Criteria for retention
Publicly Available Business & Professional Data	Obtained from public websites: Indefinite Obtained through third-party APIs: In accordance with contractual requirements	Publicly Available Business & Professional Data is derived from public sources. It is retained indefinitely by default. Upon request, publication and links to source data can be suppressed and restricted from view and publication. As publicly available data originates from outside of Cisco WebEx, any permanent changes or deletions must be addressed and requested with the primary source. At the request of users, the data can be archived in order to not appear. This allows for the data to remain permanently hidden rather than re-appearing with a new search after being previously purged.
[redacted]	ctive Subscriptions: Customer's or user's discretion ctivated Accounts: leted within thirty (30) days	Users can request to remove their Account Information by opening a TAC service request. Cisco will respond to such requests within 30 days.
Directory Data	Active Subscriptions: At Customer's or user's discretion ctivated Accounts: eted within thirty (30) days	Administrators can disable Active Directory feature while still enabling People Insights. Directory data will be hard deleted in this case of deactivation. Non-directory data will remain, with the exception of name and email for users who had only directory data in their profile before the deactivation. Users can delete User-Generated Information from their profile at any time.
[redacted]	ive Subscriptions: At Customer's or user's discretion Deactivated Accounts: Deleted within thirty (30) days	

7. Personal Data Security

Personal Data Category	Type of Encryption
Publicly Available Business & Professional Data	Encrypted in transit, AES 256 for storage, Keys managed through AWS KMS
[redacted]	Encrypted in transit, AES 256 for storage, Keys managed through AWS KMS
Directory Data	Encrypted in transit, AES 256 for storage, Keys managed through AWS KMS
User-Generated Information	Encrypted in transit, AES 256 for storage, Keys managed through AWS KMS

8. Third Party Service Providers (Sub-processors)

Cisco partners with service providers who contract to provide the same level of data protection and information security that you can expect from Cisco. A current list of sub-processors for People Insights is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
Amazon Web Services	• Publicly Available Business & Professional Data • Host & Usage Information • Directory Data • User-Generated Information	Cloud Storage	Oregon Ohio Virginia
Algolia	• Publicly Available Business and Professional Biographical Data	Full Text Search	California
Amplitude	• Host & Usage Information	User Analytics	California

Addendum Two: Facial Recognition feature for Cisco Webex Meetings (Optional)

This addendum to the Webex Meetings Privacy Data Sheet describes the processing of personal data (or personally identifiable information) by the Facial Recognition feature for Cisco Webex Meetings.

1. Overview of Facial Recognition Capabilities

Cisco introduced the facial recognition feature ("Facial Recognition" or the "Feature") to provide Webex Meetings users with the ability to identify and recognize registered Webex meeting participants (i.e., associate participant names with their positions in a Webex meeting video), giving users increased connection to meeting participants. The Feature recognizes a face by converting it to an abstracted facial vector. A facial vector is a list of numbers that characterize salient facial features of a user that is then used to identify who is in the meeting. This level of abstraction allows the system to recognize the same face even when things like lighting and position change.

Facial Recognition is disabled by default, and requires affirmative action by both the customer and the user to enable. First, the administrator for the customer may enable Facial Recognition using Webex Control Hub. However, the feature will not be available on the user's account until the user opt-ins at https://settings.webex.com. Because the Feature is based on facial vectors derived from profile images, the user must have a picture taken at the time of enablement.

2. Personal Data Processing

If the user opts-in to the Facial Recognition feature, the web page uses the camera of the user's device to take a profile picture. This picture is sent to the Webex cloud where the Feature algorithm generates a facial vector from the picture so that it can be used for matching as further described below. Both the picture and the facial vector are encrypted and stored securely. The picture may be used to generate a new facial vector in the event Cisco updates or modifies the algorithm by which facial vectors are generated. In the event a customer or user reaches out to Cisco for support with the Feature, Cisco may also use the picture during the troubleshooting process. During each meeting, a second facial vector is generated, then matched in the Webex cloud against the stored facial vector. This second facial vector is not retained.

The tables below list the personal data used by the Feature and describes why we process that data.

Personal Data Category	Types of Personal Data	Purpose of Processing
Registration	• Name (First, Last) • Email • User ID	• To display name of recognized user • Enroll you in the Feature and enable opt-in
Biometrics	• User facial image • Facial vector mapping	• To create facial vector mapping and provide the facial recognition feature • To generate a new facial vector in case of a modification or update to the Feature algorithm • To provide the Facial Recognition feature
Host & Usage Information	• Information regarding accuracy of product, including: ○ Successful and unsuccessful facial vector matching ○ User feedback	• To provide support and product analytics
Location	• Meeting Room Proximity data	• Proximity data is used to improve Facial Recognition to assure facial vectors are matched to the correct users in the correct locations
Calendar	• Meeting Room Calendar information	• Calendar information is used to improve Facial Recognition to assure facial vectors are matched to the correct users in the correct locations

3. Access Control

Personal Data Category	Who has access	Purpose of the access
Registration	Cisco	• To display name of recognized user • Enroll you in the Feature and enable opt-in
	Customer Users through https://settings.webex.com/	• View user facial recognition registration status • View and modify facial recognition registration details
Biometrics	Cisco	• To provide the Facial Recognition feature • Algorithm improvement • To troubleshoot issues in the event a customer or user requests support • To provide the Facial Recognition feature
Host & Usage Information	Cisco	• To provide support and product analytics
Location	Cisco	• Proximity data is used to improve Facial Recognition to assure facial vectors are matched to the correct users in the correct locations
Calendar	Cisco	• Calendar information is used to improve Facial Recognition to assure facial vectors are matched to the correct users in the correct locations

5. Data Portability

While Webex Meetings allows Customers and users to export data as described in Section 5 of the Webex Meetings Data Privacy Sheet, it does not support the automatic export of Facial Recognition data.

6. Data Deletion & Retention

Type of Personal Data	Retention Period	Reason and Criteria for Retention
Registration	User ID is maintained for all active Webex Meetings users. Once a user is deleted from a Customer's account, the User ID is also deleted from the Facial Recognition service. All other registration information is not stored or retained by the Facial Recognition service as this information is already stored by Webex Meetings.	UserID is used to track your enrollment in the Feature Names are displayed upon a match in the facial recognition feature.
Biometrics	Images: Users control their image retention. The image is retained as long as the feature is enabled and the user leaves the image associated with their profile. The image can be deleted at any time by user. Images for all users are deleted upon customer's discontinuation of the service. Facial vectors are retained as long as the facial images, but are stored separately. Facial vectors are deleted upon discontinuation of the service.	The image is used to provide the Facial Recognition feature, update the facial vector in case of an update to the algorithm, and to troubleshoot issues when requested by a customer or user. The facial vectors are used to provide the facial recognition feature.
Host & Usage Information	2 Weeks	To provide support and product analytics
Location	2 days	Proximity data is used to improve facial recognition to assure images are assigned to the correct users in the correct locations.
Calendar	Facial Recognition does not store or retain this information separately than already maintained by Webex Meetings.	Calendar data is used to improve facial recognition to assure images are assigned to the correct users in the correct locations.

7. Personal Data Security

The table below summarizes encryption architecture of data stored specifically for the Facial Recognition feature.

Personal Data Category	Type of Encryption
Registration	Encrypted in transit, AES 256 for storage
Images	Encrypted in transit, AES 256 for storage
Biometrics	Encrypted in transit, AES 256 for storage
Host & Usage Information	Encrypted in transit, AES 256 for storage
Location	Encrypted in transit, AES 256 for storage

CLARIFICATION APPENDIX to Attachment C
Cisco Webex Meetings Privacy Data Sheet v. 4.1

This Clarification Appendix has effective date 13.3.2020

Following the MASTER DATA PROTECTION AGREEMENT ("MDPA") entered in to by and between **Cisco International Limited** having a principal place of business at 9-11 New Square Park, Bedfont Lakes, Feltham, England TW14 8HA, United Kingdom and its Affiliates ("Cisco"), and the **Ministry of National Education and Religious Affairs of Greece**, having its principal seat at Andrea Papandreou st., 37, 15180 Marousi, Athens ("Customer"), (together "Parties") and regarding the Cisco Webex Meetings Privacy Data Sheet v. 4.1 ("PDS") attached therein, the parties agree that the following individual arrangements shall prevail in relation to the said Privacy Data Sheet:

1. **[PDS art. 2 - Table]** **Email address.** It is a data necessary to activate the service, but users may insert a "dummy" email address.

2. **[PDS art. 2]** **Webex analytics platform:** This refers only to anonymized communication data.

3. **[PDS art. 3]** **Data map.** It is understood between the Parties that this trial of Webex Meetings and any figures are for demonstration purposes only and, in any case, cross-border transfer of data will be done according to terms and conditions of the MDPA.

4. **[PDS art. 3]** **Cross-Border Transfers.** Cisco hereby clarifies that its closest datacenter is in Amsterdam. The user generated data (conference metadata) will therefore stay within the EU. In the event of a major network malfunction incident on the data center, the user generated data may however be rerouted to another data center specified in the data sheet or data map.

5. **[PDS art. 3]** **Transfer Mechanisms:** The MDPA and this Clarification Appendix shall prevail.

6. **[PDS art. 4]** **Access Control.** As per Attachment A "INFORMATION SECURITY EXHIBIT" to the MDPA.

7. **[PDS art. 5]** **Data Portability.** Since, during the trial, the recordings feature is disabled, this right shall not apply. Customers or Users may, however, submit a data portability request only for User-Generated Information. In such case, Cisco will make the User-Generated Information available to the Customer in a format that is suitable for the Customer and Users and allow for the export of the corresponding API.

8. **[PDS art. 6]** **Deletion of 60 days.** When the Service is terminated, Customer, however, has the option to delete the User-Generated Information, if applicable, earlier.

9.	[PDS art. 8]	**Third parties.** This is limited only to "Limited Host & Usage Information, meeting media traffic", i.e. communication information and media traffic data, not personal data Such list to be provided upon request.
10.	[PDS art. 11]	**How to Exercise Your Data Subject Rights.** Such rights only to be exercised by individuals.
11.	[PDS art. 11]	Communication only with the **EMEAR Privacy Officer based in EU /Netherlands.**
12.	[PDS Addendum One]	**People Insights feature:** Not applicable (N/A).
13.	[PDS Addendum Two]	**Facial Recognition.** Not applicable (N/A).

("Customer")	**("Cisco")**
Authorized Signature	Authorized Sig
Name	Name
Date: 13.3.2020	Date:

Η συνημμένη στην ελληνική γλώσσα μετάφραση αφορά το παρόν στην αγγλική γλώσσα έγγραφο.

Αθήνα, 9/11/2020

Η μεταφράσασα δικηγόρος

ΕΙΡΗΝΗ Τ. ΚΑΠΕΛΛΑΚΗ
ΔΙΚΗΓΟΡΟΣ - ΑΜ ΔΣΑ 31124
ΠΕΝΤΕΛΗΣ 56 - ΚΗΦΙΣΙΑ 145 62
ΤΗΛ: 210 6013843 - 6945087480
e-mail: ekapellaki@gmail.com
ΑΦΜ: 103403699 - ΔΟΥ: ΚΗΦΙΣΙΑΣ

ΚΑΝΕΛΛΑΚΗ
- ΑΜ ΔΣΑ 31124
- ΚΗΦΙΣΙΑ 145 62
3843 - 6945087480
sllaki@gmail.com
09 - ΔΟΥ: ΚΗΦΙΣΙΑΣ

ΣΥΜΒΑΣΗ ΠΛΑΙΣΙΟ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Αυτή η Σύμβαση Πλαίσιο Προστασίας Δεδομένων (ΣΠΠΔ) έχει ημερομηνία έναρξης ισχύος την 13η/03/2020

Η ΣΥΜΒΑΣΗ ΠΛΑΙΣΙΟ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ("ΣΠΠΔ") συνάπτεται μεταξύ της **Cisco International Limited** με έδρα στο Ηνωμένο Βασίλειο, Αγγλία, 9-11 New Square Park, Bedfont Lakes, Feltham, TW14 8HA και των συνδεδεμένων της εταιρειών ("**Cisco**") και του Υπουργείου Παιδείας και Θρησκευμάτων της Ελλάδος, με έδρα στην οδό Ανδρέα Παπανδρέου αρ. 37, 15180 Μαρούσι, Αθήνα (ο "**Πελάτης**"), (από κοινού τα "**Μέρη**").

Η παρούσα ΣΠΠΔ διέπεται από τους όρους της ισχύουσας σύμβασης που έχει συναφθεί μεταξύ των Μερών για την προμήθεια Προϊόντων ή/και Υπηρεσιών από την Cisco στον Πελάτη με ημερομηνία 13/3/2020 (η "Σύμβαση"). Σε περίπτωση σύγκρουσης μεταξύ της παρούσας ΣΠΠΔ, συμπεριλαμβανομένων τυχόν συνημμένων στην παρούσα, και της Σύμβασης, οι διατάξεις της παρούσας ΣΠΠΔ θα υπερισχύουν, αλλά μόνο αναφορικά με το αντικείμενο της παρούσας.

Λαμβάνοντας υπόψη τις αμοιβαίες υποσχέσεις και συμφωνίες που περιέχονται στην παρούσα, καθώς και του καλού και πολύτιμου αντιτίμματος, η είσπραξη και η επάρκεια του οποίου αναγνωρίζεται με την παρούσα, τα Μέρη συμφωνούν ως εξής:

ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΣΥΜΒΑΣΗΣ: Η παρούσα ΣΠΠΔ αποτελείται από τα ακόλουθα Συνημμένα Α-Ε που επισυνάπτονται στην παρούσα, τα οποία ενσωματώνονται ως εξής:

1. Συνημμένο Α ΠΑΡΑΡΤΗΜΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ
2. Συνημμένο Β ΠΑΡΑΡΤΗΜΑ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
3. Συνημμένο Γ ΦΥΛΛΟ ΑΠΟΡΡΗΤΟΥ ΔΕΔΟΜΕΝΩΝ ΤΩΝ CISCO WEBEX ΣΥΝΕΔΡΙΑΣΕΩΝ
4. Συνημμένο Δ ΠΡΟΚΑΘΟΡΙΣΜΕΝΟΙ ΣΥΜΒΑΤΙΚΟΙ ΟΡΟΙ
5. Συνημμένο Ε ΓΛΩΣΣΑΡΙΟ

Η παρούσα ΣΠΠΔ αποτελεί την πλήρη συμφωνία μεταξύ των Μερών σχετικά με το αντικείμενο της παρούσας ΣΠΠΔ και αντικαθιστά κάθε προηγούμενη προφορική ή γραπτή επικοινωνία μεταξύ των Μερών. Η παρούσα ΣΠΠΔ υπόκειται στους όρους και τις προϋποθέσεις της Σύμβασης, συμπεριλαμβανομένων ενδεικτικά οποιωνδήποτε περιορισμών ή αποκλεισμών ευθύνης που ορίζονται στη Σύμβαση. Δεν υπάρχουν όροι, συμφωνίες, συμβάσεις, υποσχέσεις ή εγγυήσεις, είτε ρητές είτε σιωπηρές, οι οποίες δεν προβλέπονται στην παρούσα. Η παρούσα ΣΠΠΔ μπορεί να τροποποιηθεί μόνο με έγγραφο τύπο που υπογράφεται από τα Μέρη της παρούσας. Τα Μέρη, υπογράφοντας παρακάτω, επιβεβαιώνουν ότι έχουν διαβάσει, κατανοήσει και εγκρίνει ρητά τους όρους και τις προϋποθέσεις της παρούσας ΣΠΠΔ. Οι υποχρεώσεις της Cisco βάσει της παρούσας ΣΠΠΔ θα ολοκληρωθούν όταν η Cisco δεν θα κατέχει πλέον, δεν θα Επεξεργάζεται ή δεν θα έχει με άλλο τρόπο πρόσβαση σε Προστατευμένα Δεδομένα.

Τα Μέρη έχουν προβεί στη νόμιμη υπογραφή της παρούσας ΣΠΠΔ. Κάθε Μέρος εγγυάται και δηλώνει ότι οι αντίστοιχοι υπογράφοντες των οποίων οι υπογραφές εμφανίζονται παρακάτω έχουν, κατά την ημερομηνία υπογραφής, την εξουσία να υπογράψουν την παρούσα ΣΠΠΔ.

_____	_____
("**Πελάτης**")	("**Cisco**")

Εξουσιοδοτημένη Υπογραφή Εξουσιοδοτημένη Υπογραφή

Όνομα Όνομα

Julia O'Shea

Διευθύντρια Οικονομικής Διεύθυνσης

Ημερομηνία 13.3.2020 Ημερομηνία:

[ΕΓΚΡΙΘΗΚΕ ΑΠΟ ΝΟΜΙΚΟ ΤΜΗΜΑ]

Έκδοση: Ιανουάριος 2019

ΣΥΝΗΜΜΕΝΟ Α

ΠΑΡΑΡΤΗΜΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

1. Πεδίο εφαρμογής

Το παρόν Παράρτημα Ασφάλειας Πληροφοριών ("ΠΑΠ") ισχύει στο βαθμό που η Cisco Επεξεργάζεται ή έχει πρόσβαση σε Προστατευμένα Δεδομένα κατά την Εκτέλεση των υποχρεώσεών της προς τον Πελάτη. Το παρόν ΠΑΠ περιγράφει τις απαιτήσεις ασφάλειας πληροφοριών μεταξύ του Πελάτη και της Cisco και περιγράφει τα τεχνικά και οργανωτικά μέτρα ασφαλείας που θα εφαρμοστούν από την Cisco για την ασφάλεια των Προστατευόμενων Δεδομένων πριν από την Εκτέλεση οποιασδήποτε Επεξεργασίας βάσει της Σύμβασης.

Εκτός εάν ορίζεται διαφορετικά, σε περίπτωση σύγκρουσης μεταξύ της Σύμβασης και του παρόντος Παραρτήματος, οι όροι του παρόντος ΠΑΠ θα υπερισχύουν καθόσον αφορούν την Επεξεργασία των Προστατευόμενων Δεδομένων.

Όλοι οι όροι με κεφαλαία που δεν ορίζονται στο Γλωσσάριο έχουν τις έννοιες που τους αποδίνονται στη Σύμβαση.

2. Γενικές πρακτικές ασφαλείας

Η Cisco έχει εφαρμόσει και διατηρεί τα κατάλληλα τεχνικά και οργανωτικά μέτρα που αποσκοπούν στην προστασία των Προστατευόμενων Δεδομένων από τυχαία απώλεια, καταστροφή ή αλλοίωση, παράνομη αποκάλυψη ή πρόσβαση, ή παράνομη καταστροφή, συμπεριλαμβανομένων των πολιτικών, των διαδικασιών και των εσωτερικών ελέγχων που ορίζονται στο παρόν ΠΑΠ για το προσωπικό της, τον εξοπλισμό και τις εγκαταστάσεις στις τοποθεσίες της Cisco που εμπλέκονται στην Εκτέλεση οποιουδήποτε μέρους της Σύμβασης.

3. Γενική Συμμόρφωση

i. **Συμμόρφωση**. Η Cisco τεκμηριώνει και εφαρμόζει επεξεργασίες και διαδικασίες για την αποφυγή παραβιάσεων νομικών, κανονιστικών, κανονιστικών ή συμβατικών υποχρεώσεων που σχετίζονται με την ασφάλεια των πληροφοριών ή άλλες απαιτήσεις ασφαλείας. Οι εν λόγω επεξεργασίες και διαδικασίες σχεδιάζονται έτσι ώστε να παρέχουν ασφάλεια για την προστασία των Προστατευόμενων Δεδομένων, δεδομένων των κινδύνων που ενέχει η φύση των δεδομένων που Επεξεργάζεται η Cisco. Η Cisco εφαρμόζει και λειτουργεί την ασφάλεια των πληροφοριών σύμφωνα με τις πολιτικές και τις διαδικασίες της, οι οποίες δεν θα είναι λιγότερο αυστηρές από τις απαιτήσεις ασφάλειας πληροφοριών που ορίζονται στο παρόν ΠΑΠ.

ii. **Προστασία των αρχείων**. Η Cisco εφαρμόζει κατάλληλες διαδικασίες που έχουν σχεδιαστεί για την προστασία των αρχείων από απώλεια, καταστροφή, παραποίηση, παράνομη πρόσβαση και παράνομη κυκλοφορία, σύμφωνα με τις νομοθετικές, κανονιστικές και συμβατικές απαιτήσεις.

iii. **Επανεξέταση της ασφάλειας των πληροφοριών.** Η προσέγγιση της Cisco για τη διαχείριση της ασφάλειας των πληροφοριών και την εφαρμογή της (π.χ. στόχοι ελέγχου, έλεγχοι, πολιτικές, επεξεργασίες και διαδικασίες) θα επανεξετάζονται σε προγραμματισμένα χρονικά διαστήματα ή όταν πραγματοποιούνται σημαντικές αλλαγές από κατάλληλους εσωτερικούς ή εξωτερικούς αξιολογητές.

iv. **Συμμόρφωση με πολιτικές και πρότυπα ασφαλείας**. Η διοίκηση της Cisco θα επανεξετάζει τακτικά τη συμμόρφωση της επεξεργασίας πληροφοριών και των διαδικασιών με τις κατάλληλες ισχύουσες πολιτικές και πρότυπα.

v. **Επανεξέταση της τεχνικής συμμόρφωσης.** Η Cisco θα εξετάζει τακτικά τα συστήματα πληροφοριών με σκοπό τη συμμόρφωση με τις πολιτικές και τα πρότυπα ασφάλειας των πληροφοριών.

vi. **Διαχείριση κινδύνων πληροφοριών ("IRM").** Η Cisco εφαρμόζει και χρησιμοποιεί την κατάλληλη διαδικασία διαχείρισης κινδύνου στο πλαίσιο της αξιολόγησης, ανταπόκρισης και της παρακολούθησης του κινδύνου, σύμφωνα με τις ισχύουσες συμβατικές και νομικές υποχρεώσεις. Η Cisco υποχρεούται να έχει ένα πλαίσιο διαχείρισης κινδύνου και να διενεργεί περιοδικές (π.χ. τουλάχιστον ετήσιες) εκτιμήσεις κινδύνου του περιβάλλοντος και των συστημάτων της για την κατανόηση των κινδύνων και την εφαρμογή κατάλληλων ελέγχων για τη διαχείριση και τον μετριασμό των κινδύνων αυτών. Η αξιολόγηση της απειλής και της ευπάθειας πρέπει να επανεξετάζεται περιοδικά και να λαμβάνονται άμεσα μέτρα αποκατάστασης όταν εντοπίζονται ουσιώδεις αδυναμίες. Η Cisco θα παρέχει στον Πελάτη σχετικές συνοπτικές εκθέσεις και αναλύσεις κατόπιν γραπτού αιτήματος, υπό την προϋπόθεση ότι η αποκάλυψη των οποίων δεν θα παραβίαζε τις πολιτικές ασφάλειας πληροφοριών της Cisco ή τους ισχύοντες νόμους.

4.<u>Τεχνικά και οργανωτικά μέτρα για την ασφάλεια</u>

α. Οργάνωση Ασφάλειας Πληροφοριών

i. **Ασφάλεια ιδιοκτησίας.** Η Cisco θα διορίζει έναν ή περισσότερους υπαλλήλους ασφαλείας υπεύθυνους για το συντονισμό και την παρακολούθηση των απαιτήσεων και των διαδικασιών ασφαλείας. Οι εν λόγω υπάλληλοι πρέπει να έχουν τη γνώση, την εμπειρία και την εξουσία να λειτουργούν ως ιδιοκτήτης(-ες), με υπευθυνότητα και λογοδοσία για την ασφάλεια των πληροφοριών εντός του οργανισμού.

ii. **Ρόλοι Προστασίας και Αρμοδιότητες.** Η Cisco καθορίζει και κατανέμει τις αρμοδιότητες ασφάλειας πληροφοριών σύμφωνα με τις εγκεκριμένες πολιτικές της για την ασφάλεια των πληροφοριών. Οι εν λόγω πολιτικές (ή περιλήψεις τους) δημοσιεύονται και κοινοποιούνται στους υπαλλήλους και σχετικοί εξωτερικοί συνεργάτες απαιτείται να συμμορφωθούν με τις εν λόγω πολιτικές.

iii. **Διαχείριση Έργου.** Η Cisco αντιμετωπίζει την ασφάλεια των πληροφοριών στη διαχείριση του έργου για τον εντοπισμό και την κατάλληλη αντιμετώπιση των κινδύνων ασφάλειας πληροφοριών.

iv. **Διαχείριση κινδύνων.** Η Cisco θα διαθέτει ένα πλαίσιο διαχείρισης κινδύνων και θα διενεργεί περιοδική (π.χ. τουλάχιστον ετήσια) αξιολόγηση κινδύνου του περιβάλλοντος και των συστημάτων της για την κατανόηση των κινδύνων και την εφαρμογή κατάλληλων ελέγχων για τη διαχείριση και τον μετριασμό των κινδύνων πριν από την Επεξεργασία των Προστατευόμενων Δεδομένων.

β. **Ασφάλεια Ανθρώπινου Δυναμικού**

i.Γενικά. Η Cisco θα διασφαλίζει ότι το προσωπικό του θα δεσμεύεται από σύμβαση εμπιστευτικότητας που θα περιλαμβάνει την προστασία των Προστατευόμενων Δεδομένων και θα παρέχει επαρκή εκπαίδευση σχετικά με τις σχετικές πολιτικές και διαδικασίες προστασίας και ασφάλειας προσωπικών δεδομένων. Η Cisco θα ενημερώνει περαιτέρω το προσωπικό της για πιθανές συνέπειες παραβίασης των πολιτικών και των διαδικασιών ασφαλείας της, οι οποίες πρέπει να περιλαμβάνουν πειθαρχικά μέτρα, συμπεριλαμβανομένης της πιθανής καταγγελίας της απασχόλησης των υπαλλήλων της Cisco και της καταγγελίας της σύμβασης ή της ανάθεσης για τους Αντιπροσώπους και του προσωρινού προσώπου.

ii.**Κατάρτιση.** Το προσωπικό της Cisco με πρόσβαση σε Προστατευμένα Δεδομένα θα λαμβάνει κατάλληλη, ετήσια περιοδική εκπαίδευση και κατάρτιση σχετικά με τις διαδικασίες προστασίας της ιδιωτικής ζωής και ασφάλειας για τις υπηρεσίες που βοηθούν στην πρόληψη της μη εξουσιοδοτημένης χρήσης (ή ακούσιας αποκάλυψης) των Προστατευόμενων Δεδομένων και στο βαθμό που η εκπαίδευση ανταποκρίνεται αποτελεσματικά στην αντιμετώπιση συμβάντων ασφαλείας. Η εκπαίδευση παρέχεται πριν από την πρόσβαση του προσωπικού της Cisco σε Προστατευμένα Δεδομένα ή την έναρξη παροχής υπηρεσιών. Η κατάρτιση ενισχύεται τακτικά μέσω μαθημάτων επανεκπαίδευσης, μηνυμάτων ηλεκτρονικού ταχυδρομείου, αφισών, πινάκων ανακοινώσεων και άλλου υλικού κατάρτισης και ευαισθητοποίησης.

iii. **Έλεγχοι ιστορικού**. Εκτός από τους άλλους όρους της Σύμβασης που σχετίζονται με το θέμα αυτό, η Cisco θα διενεργεί ποινικούς και άλλους σχετικούς ελέγχους ιστορικού για το προσωπικό της σύμφωνα με τους αναγκαστικούς ισχύοντες νόμους και τις πολιτικές της.

Γ. Έλεγχοι πρόσβασης προσωπικού

i.Πρόσβαση.

Α. Περιορισμένη χρήση. Η Cisco κατανοεί και αναγνωρίζει ότι ο Πελάτης μπορεί να παρέχει πρόσβαση στη Cisco σε ευαίσθητες και ιδιόκτητες πληροφορίες και συστήματα υπολογιστών, προκειμένου η Cisco να εκπληρώσει τις υποχρεώσεις της στον Πελάτη. Η Cisco δεν i) θα έχει πρόσβαση στα Προστατευμένα Δεδομένα ή τα συστήματα υπολογιστών για οποιονδήποτε άλλο σκοπό εκτός από τον απαραίτητο για την εκπλήρωση των υποχρεώσεών της προς τον Πελάτη ή (ii) δεν θα χρησιμοποιήσει οποιαδήποτε διαπιστευτήρια πληροφοριών πρόσβασης συστήματος ή σύνδεσης για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε Προστατευμένα Δεδομένα ή συστήματα του Πελάτη, ή να υπερβεί το πεδίο εφαρμογής οποιασδήποτε εξουσιοδοτημένης πρόσβασης.

Β. Άδεια. Η Cisco θα περιορίζει την πρόσβαση σε Προστατευμένα Δεδομένα και συστήματα ανά πάσα στιγμή μόνο στους Αντιπροσώπους των οποίων η πρόσβαση είναι απαραίτητη για την εκτέλεση των υποχρεώσεων της Cisco προς τον Πελάτη.

Γ. Αναστολή ή τερματισμός των Δικαιωμάτων Πρόσβασης. Κατόπιν εύλογου αιτήματος του Πελάτη, η Cisco αμέσως και χωρίς αδικαιολόγητες καθυστερήσεις θα αναστέλλει ή τερματίζει τα δικαιώματα πρόσβασης σε Προστατευμένα Δεδομένα και συστήματα για το προσωπικό της Cisco ή τους Αντιπροσώπους της που είναι εύλογα ύποπτοι για παραβίαση οποιασδήποτε από τις διατάξεις του παρόντος ΠΑΠ και η Cisco θα καταργεί τα δικαιώματα πρόσβασης όλων των εργαζομένων και των εξωτερικών χρηστών μερών μετά την αναστολή ή τη λήξη της εργασίας τους ή της απασχόλησής τους.

Δ. Ταξινόμηση Πληροφοριών. Η Cisco ταξινομεί, κατηγοριοποιεί ή/και καθυστερεί τα Προστατευμένα Δεδομένα για να βοηθήσει στην αναγνώρισή τους και να επιτρέψει την κατάλληλο περιορισμό της πρόσβασης και της χρήσης τους.

ii. **Πολιτική πρόσβασης**. Η Cisco θα καθορίζει κατάλληλους κανόνες ελέγχου πρόσβασης, δικαιωμάτων και περιορισμούς για τους ρόλους κάθε συγκεκριμένου χρήστη έναντι των περιουσιακών του στοιχείων. Η Cisco τηρεί αρχείο των προνομίων ασφαλείας του προσωπικού της που έχει πρόσβαση σε προστατευμένα δεδομένα και ελέγχει την πρόσβασή τους, το δίκτυο και τα συστήματα του δικτύου όπως παρατίθενται στο 4° Μέρος του Φύλλου Απορρήτου Δεδομένων των Cisco Webex Συνεδριάσεων. Η Cisco περιορίζει και ελέγχει αυστηρά τη χρήση των συστημάτων λειτουργίας, τα οποία είναι ικανά να παρακάμπτουν το σύστημα και τους ελέγχους εφαρμογής.

δ. Άδεια Πρόσβασης

i. Η Cisco θα έχει διαδικασίες δημιουργίας και διαγραφής λογαριασμού χρήστη, με τις κατάλληλες διαδικασίες αποδοχής, για τη χορήγηση και ανάκληση πρόσβασης στα συστήματα και τα δίκτυα του Πελάτη. Η Cisco χρησιμοποιεί σύστημα ελέγχου πρόσβασης των επιχειρήσεων που απαιτεί εκ νέου επικύρωση του προσωπικού της από τους υπευθύνους σε τακτά χρονικά διαστήματα με βάση την αρχή του "ελάχιστου προνομίου" και των κριτηρίων αναγκαίων γνώσεων βάσει των υποχρεώσεων απόδοσης.

ii. Η Cisco θα διατηρεί και ενημερώνει αρχείο του προσωπικού που θα είναι εξουσιοδοτημένο να έχει πρόσβαση στα συστήματα τα οποία περιλαμβάνουν τα Προστατευμένα Δεδομένα και η Cisco θα επανεξετάζει τα δικαιώματα πρόσβασης των χρηστών σε τακτά διαστήματα.

iii. Για συστήματα που επεξεργάζονται Προστατευμένα Δεδομένα, η Cisco θα επαληθεύει εκ νέου (ή, κατά περίπτωση, απενεργοποιεί) την πρόσβαση των χρηστών που αλλάζουν δομή αναφοράς και απενεργοποιούν τα συστήματα ελέγχου ταυτότητας που δεν έχουν χρησιμοποιηθεί για χρονικό διάστημα που δεν υπερβαίνει τους τέσσερις (4) μήνες.

iv. Η Cisco περιορίζει την πρόσβαση στον πηγαίο κώδικα του προγράμματος και σε συναφή στοιχεία, όπως ο κώδικας αντικειμένου λογισμικού, τα σχέδια, οι προδιαγραφές, τα σχέδια επαλήθευσης και τα σχέδια επικύρωσης, προκειμένου να αποτραπεί η εισαγωγή μη εξουσιοδοτημένης λειτουργικότητας και να αποφευχθούν ακούσιες αλλαγές.

ε. **Σχεδιασμός Δικτύου**. Για συστήματα που επεξεργάζονται Προστατευμένα Δεδομένα, η Cisco διαθέτει ελέγχους για να αποφύγει την αξίωση δικαιωμάτων πρόσβασης από το προσωπικό πέραν εκείνων που τους έχουν ανατεθεί για να αποκτήσουν πρόσβαση σε Προστατευμένα Δεδομένα.

ΑΚΗ
Α 31124
ΑΑ 145 62
6945087480
aki@gmail.com
ΔΟΥ: ΚΗΦΙΣΙΑ

στ. **Ελάχιστο Προνόμιο.** Η Cisco περιορίζει την πρόσβαση στα Προστατευμένα Δεδομένα μόνο στο προσωπικό που έχει υποχρεώσεις Εκτέλεσης και στην έκταση που είναι απαραίτητη η τεχνική υποστήριξη, στο προσωπικό της που εκτελεί πράξεις τεχνικής υποστήριξης.

ζ. **Ταυτοποίηση**

i.Η Cisco θα χρησιμοποιεί τις πρότυπες πρακτικές του κλάδου για να αναγνωρίσει και να ταυτοποιήσει τους χρήστες που προσπαθούν να εισέλθουν στο σύστημα πληροφοριών. Όπου οι μηχανισμοί ελέγχου ταυτότητας βασίζονται σε κωδικούς πρόσβασης, η Cisco θα απαιτεί οι κωδικοί πρόσβασης να ανανεώνονται και να αλλάζουν τακτικά, τουλάχιστον κάθε 180 μέρες.

ii. Όπου οι μηχανισμοί ελέγχου ταυτότητας βασίζονται σε κωδικούς πρόσβασης, η Cisco απαιτεί ο κωδικός πρόσβασης να ανταποκρίνεται σε ισχυρές παραμέτρους ελέγχου του κωδικού πρόσβασης (π.χ. μήκος, πολυπλοκότητα χαρακτήρων ή/και μη επαναληψιμότητα).

iii. Η Cisco θα εξασφαλίζει ότι τα απενεργοποιημένα ή ληγμένα αναγνωριστικά και τα διαπιστευτήρια σύνδεσης δεν χορηγούνται σε άλλα άτομα.

iv. Η Cisco θα εποπτεύει τις επανειλημμένες αποτυχημένες προσπάθειες απόκτησης προνομίων ή για να αποκτήσουν πρόσβαση στο σύστημα πληροφοριών.

v. Η Cisco θα διατηρεί τις πρότυπες διαδικασίες του κλάδου για την απενεργοποίηση των διαπιστευτηρίων σύνδεσης που έχουν διαφθαρεί ή αποκαλυφθεί ακούσια.

vi. Η Cisco θα χρησιμοποιεί τις πρότυπες πρακτικές του κλάδου για πρακτικές ασφαλείας των διαπιστευτηρίων σύνδεσης, συμπεριλαμβανομένων των πρακτικών που αποσκοπούν στη διατήρηση της εμπιστευτικότητας και της ακεραιότητας των διαπιστευτηρίων σύνδεσης όταν εκχωρούνται και διανέμονται, και κατά τη διάρκεια της αποθήκευσης (π.χ. τα διαπιστευτήρια σύνδεσης δεν αποθηκεύονται ή κοινοποιούνται σε απλό κείμενο). Οι πρακτικές αυτές σχεδιάζονται έτσι ώστε να εξασφαλίζουν ισχυρά και εμπιστευτικά διαπιστευτήρια σύνδεσης.

η. **Φυσική και Περιβαλλοντική ασφάλεια**

i. Φυσική πρόσβαση στις Εγκαταστάσεις

Α. Η Cisco θα περιορίζει την πρόσβαση σε εγκαταστάσεις όπου βρίσκονται συστήματα που επεξεργάζονται Προστατευμένα Δεδομένα σε εξουσιοδοτημένα άτομα.

Β. Οι περίμετροι ασφαλείας θα καθορίζονται και χρησιμοποιούνται για την προστασία περιοχών που περιέχουν τόσο ευαίσθητες όσο και κρίσιμες πληροφορίες σχετικά με τις εγκαταστάσεις επεξεργασίας.

Γ. Οι εγκαταστάσεις θα παρακολουθούνται και θα ελέγχεται η πρόσβαση ανά πάσα στιγμή (24x7).

Δ. Η πρόσβαση θα ελέγχεται μέσω κάρτας-κλειδιού ή/και κατάλληλων διαδικασιών εισόδου για εγκαταστάσεις με συστήματα επεξεργασίας Προστατευόμενων Δεδομένων. Η Cisco πρέπει να καταχωρεί το προσωπικό και να απαιτεί από αυτό να φέρει τα κατάλληλα σήματα ταυτοποίησης.

ii. **Φυσική πρόσβαση στον εξοπλισμό**. Ο εξοπλισμός της Cisco που χρησιμοποιήθηκε για την επεξεργασία ή την αποθήκευση Προστατευόμενων Δεδομένων πρέπει να είναι

προστατευμένος με τη χρήση πρότυπων διαδικασιών του κλάδου για τον περιορισμό της πρόσβασης σε εξουσιοδοτημένα άτομα.

iii. **Προστασία από επιπλοκές**. Η Cisco θα εφαρμόζει τα κατάλληλα μέτρα που έχουν σχεδιαστεί για την προστασία από την απώλεια δεδομένων λόγω βλάβης της παροχής ηλεκτρικού ρεύματος ή παρεμβολής γραμμής.

iv. **Πολιτική «Ασφαλούς Γραφείου» («Clear Desk»)**. Η Cisco θα διαθέτει πολιτικές που απαιτούν ένα "ασφαλές γραφείο / ασφαλή οθόνη" για να αποτρέψει ακούσια αποκάλυψη των Προστατευόμενων Δεδομένων.

θ. Ασφάλεια Λειτουργιών

i. **Επιχειρησιακή πολιτική**. Η Cisco θα τηρεί γραπτές πολιτικές που περιγράφουν τα μέτρα ασφαλείας της και τις σχετικές διαδικασίες και ευθύνες του προσωπικού της που έχει πρόσβαση σε Προστατευόμενα Δεδομένα και στα συστήματα και δίκτυά της. Η Cisco κοινοποιεί τις πολιτικές και τις απαιτήσεις της σε όλα τα πρόσωπα που εμπλέκονται στην Επεξεργασία Προστατευόμενων Δεδομένων. Η Cisco θα εφαρμόζει την κατάλληλη δομή διαχείρισης και ελέγχου που έχει σχεδιαστεί για τη διασφάλιση της συμμόρφωσης με τις εν λόγω πολιτικές και με τους αναγκαστικούς ισχύοντες νόμους σχετικά με την προστασία και επεξεργασία των Προστατευόμενων Δεδομένων.

ii. Έλεγχοι Ασφαλείας και Επεξεργασίας.

Α. **Τομείς**. Η Cisco θα διατηρεί, τεκμηριώνει και εφαρμόζει πρότυπα και διαδικασίες για τη διαχείριση της διαμόρφωσης, λειτουργίας και διαχείρισης συστημάτων και δικτύων και υπηρεσιών που αποθηκεύουν ή επεξεργάζονται Προστατευμένα Δεδομένα.

Β. **Πρότυπα και Διαδικασίες**. Αυτά τα πρότυπα και οι διαδικασίες περιλαμβάνουν: τους ελέγχους ασφάλειας, τον προσδιορισμό και την επιδιόρθωση των τρωτών σημείων ασφάλειας, την αλλαγή διαδικασίας ελέγχου και τις διαδικασίες και την πρόληψη περιστατικών, την ανίχνευση, την αποκατάσταση, και διαχείριση.

iii. **Καταγραφή και Παρακολούθηση**. Η Cisco θα διατηρεί αρχεία καταγραφής της δραστηριότητας διαχειριστή και συμβάντα ανάκτησης δεδομένων που σχετίζονται με τα Προστατευόμενα Δεδομένα.

ι. Ασφάλεια Επικοινωνιών και Μεταφορά δεδομένων

i. **Δίκτυα**. Η Cisco θα χρησιμοποιεί, κατ' ελάχιστο τα ακόλουθα στοιχεία ελέγχου για την ασφάλεια των δικτύων της που έχουν πρόσβαση ή επεξεργάζονται προστατευμένα δεδομένα:

Α. Η κυκλοφορία του δικτύου διέρχεται από προγράμματα προστασίας, τα οποία παρακολουθούνται ανά πάσα στιγμή. Η Cisco πρέπει να εφαρμόσει συστήματα πρόληψης εισβολών που επιτρέπουν την καταγραφή και προστασία της κυκλοφορίας μέσω των ελέγχων προστασίας και του LAN ανά πάσα στιγμή.

Β. Οι συσκευές δικτύου που χρησιμοποιούνται για τη διαχείριση πρέπει να χρησιμοποιούν τους πρότυπους κρυπτογραφικούς ελέγχους του κλάδου κατά την επεξεργασία των Προστατευόμενων Δεδομένων.

Γ. Προστατευμένα φίλτρα και έλεγχοι πρέπει να είναι ενεργοποιημένα στους δρομολογητές.

Δ. Οι κωδικοί πρόσβασης ελέγχου ταυτότητας της του δικτύου, της εφαρμογής και του διακομιστή απαιτούνται για την τήρηση των κατευθυντήριων γραμμών πολυπλοκότητας (τουλάχιστον 7 χαρακτήρες με τουλάχιστον 3 από τις ακόλουθες τέσσερις κλάσεις: κεφαλαία, πεζά, αριθμητικά, ειδικά χαρακτηριστικά) και να αλλάζουν τουλάχιστον κάθε 180 ημέρες· ή να χρησιμοποιεί άλλα ισχυρά διαπιστευτήρια σύνδεσης (π.χ. βιομετρικά στοιχεία).

Ε. Οι αρχικοί κωδικοί πρόσβασης χρήστη πρέπει να αλλάξουν κατά την πρώτη σύνδεση. Η Cisco θα έχει μια πολιτική που θα απαγορεύει την κοινή χρήση αναγνωριστικών χρηστών, κωδικών πρόσβασης ή άλλων διαπιστευτηρίων σύνδεσης.

ΣΤ. Προγράμματα προστασίας πρέπεια να αναπτυχθούν για την προστασία της περιμέτρου των δικτύων της Cisco.

ii. **Ψηφιακά ιδιωτικά δίκτυα ("VPN")** Όταν απαιτείται απομακρυσμένη σύνδεση με το δίκτυο του Πελάτη ή της Cisco για την επεξεργασία των προστατευόμενων δεδομένων:

Α. Η σύνδεση πρέπει να κρυπτογραφηθεί χρησιμοποιώντας κρυπτογράφηση προτύπων του κλάδου (δηλαδή τουλάχιστον κρυπτογράφηση 256-bit).

Β. Η σύνδεση θα δημιουργείται μόνο με τη χρήση διακομιστών VPN.

Γ. Η χρήση ελέγχου ταυτότητας πολλαπλών παραγόντων απαιτείται.

iii. **Μεταφορά δεδομένων**. Η Cisco θα έχει σε εφαρμογή επίσημες πολιτικές μεταφοράς για την προστασία της μεταφοράς πληροφοριών μέσω της χρήσης όλων των τύπων μέσων επικοινωνίας που συμμορφώνονται με τις απαιτήσεις του παρόντος ΠΑΠ. Οι πολιτικές αυτές πρέπει να σχεδιάζονται για την προστασία των μεταφερόμενων πληροφοριών από μη εγκεκριμένες απαιτήσεις παρακολούθησης, αντιγραφής, τροποποίησης, διαφθοράς, δρομολόγησης και καταστροφής.

κ. **Απόκτηση, Ανάπτυξη και Συντήρηση Συστήματος.**

i. **Απαιτήσεις Ασφαλείας.** Η Cisco υιοθετεί τις απαιτήσεις ασφάλειας για την αγορά, τη χρήση ή την ανάπτυξη των συστημάτων πληροφοριών, συμπεριλαμβανομένων των υπηρεσιών εφαρμογής που παραδίδονται μέσω του δημόσιου δικτύου.

ii. **Απαιτήσεις Ανάπτυξης**. Η Cisco διαθέτει πολιτικές για την ασφαλή ανάπτυξη, τη μηχανική συστημάτων, και την υποστήριξη. Η Cisco διεξάγει τις κατάλληλες δοκιμές για την ασφάλεια του συστήματος στο πλαίσιο των διαδικασιών ελέγχου αποδοχής. Η Cisco εποπτεύει και παρακολουθεί τη δραστηριότητα της ανάπτυξης συστημάτων εκτός προέλευσης.

λ. **Δοκιμές Διείσδυσης και Ευπάθειας Σάρωσης & Εκθέσεις Ελέγχου.**

i. **Δοκιμή**. Η Cisco θα πραγματοποιεί περιοδικές δοκιμές διείσδυσης στο δίκτυο περιμέτρου διαδικτύου της. Οι έλεγχοι θα διενεργούνται με τα συνιστώμενα εργαλεία ασφάλειας του κλάδου για τον εντοπισμό πληροφοριών ευαλωτότητας. Κατόπιν γραπτού αιτήματος του Πελάτη, η Cisco παρέχει μια έκθεση δοκιμών ευαλωτότητας και διείσδυσης σε επίπεδο οργανισμού, η οποία μπορεί να περιλαμβάνει μια συνοπτική παρουσίαση των αποτελεσμάτων και όχι των λεπτομερειών των πραγματικών ευρημάτων.

ii. **Έλεγχοι**. Η Cisco θα ανταποκρίνεται άμεσα και συνεργάζεται με εύλογα αιτήματα από τον Πελάτη για ελέγχους ασφαλείας και δοκιμές. Ο Πελάτης θα αντιμετωπίζει το περιεχόμενο των εκθέσεων που σχετίζονται με την ασφάλεια και επαλήθευση της Cisco ως Προστατευόμενα Δεδομένα σύμφωνα με τους όρους που περιέχονται στο παρόν MDPA.

iii. **Διορθωτικά μέτρα.** Εάν οποιαδήποτε άσκηση ελέγχου ή δοκιμής διείσδυσης που αναφέρεται στο τμήμα 4(I) σημείο ii), ανωτέρω, αποκαλύψει τυχόν ελλείψεις, αδυναμίες ή τομείς μη συμμόρφωσης, η Cisco θα λάβει αμέσως τα μέτρα που απαιτούνται, κατά την εύλογη διακριτική ευχέρεια της, για την αντιμετώπιση αυτών των ελλείψεων, αδυναμιών και τομέων μη συμμόρφωσης το συντομότερο δυνατόν, δεδομένων των περιστάσεων.

iv. **Κατάσταση των Διορθωτικών Μέτρων**. Κατόπιν αιτήματος, η Cisco θα ενημερώνει τον Πελάτη για την κατάσταση τυχόν διορθωτικών μέτρων που απαιτούνται για την εκτέλεση, συμπεριλαμβανομένου του εκτιμώμενου χρονοδιαγράμματος για την ολοκλήρωση της ίδιας, και πιστοποιεί στον Πελάτη το συντομότερο δυνατόν, δεδομένων των περιστάσεων ότι έχουν ολοκληρωθεί όλες οι απαραίτητες διορθωτικές ενέργειες.

μ. **Σχέσεις με Ανάδοχο**

i. **Πολιτικές**. Η Cisco θα διαθέτει πολιτικές ή διαδικασίες ασφάλειας πληροφοριών για τη χρήση των Αντιπροσώπων που επιβάλλουν απαιτήσεις σύμφωνες με τον παρόν ΠΑΠ. Οι πολιτικές αυτές επανεξετάζονται σε προγραμματισμένα χρονικά διαστήματα ή σε περίπτωση σημαντικών αλλαγών. Οι συμβάσεις με Αντιπροσώπους θα περιλαμβάνουν απαιτήσεις που συνάδουν ή είναι ανάλογες με την παρούσα ΣΠΠΔ.

ii. **Παρακολούθηση**. Η Cisco θα παρακολουθεί και ελέγχει την παροχή υπηρεσιών από τους Αντιπροσώπους της και επανεξετάζει τις πρακτικές ασφαλείας των αντιπροσώπων της σε εφαρμογή των απαιτήσεων ασφαλείας που ορίζονται στο συμφωνητικό της Cisco με τους εν λόγω Αντιπροσώπους. Η Cisco θα διαχειρίζεται τις αλλαγές στις υπηρεσίες των Αντιπροσώπων της που μπορεί να έχουν αντίκτυπο στην ασφάλεια.

ν. **Διαχείριση Περιστατικών και Βελτιώσεων της Ασφάλειας των Πληροφοριών.**

i. **Υποχρεώσεις και Διαδικασίες.** Η Cisco θα θεσπίζει διαδικασίες για να εξασφαλίσει μια γρήγορη, αποτελεσματική και ομαλή απάντηση σε περιστατικά ασφάλειας πληροφοριών.

ii. **Αναφορά συμβάντος ασφάλειας πληροφοριών.** Η Cisco θα εφαρμόζει διαδικασίες για Συμβάντα Ασφάλειας Πληροφοριών που πρέπει να αναφέρονται μέσω κατάλληλων διαύλων διαχείρισης όσο το δυνατόν γρηγορότερα. Όλοι οι υπάλληλοι και Αντιπρόσωποι θα πρέπει να ενημερώνονται για την ευθύνη τους να αναφέρουν τα περιστατικά ασφάλειας πληροφοριών το συντομότερο δυνατό.

iii. **Υποβολή εκθέσεων για τις αδυναμίες της ασφάλειας των πληροφοριών. .**Η Cisco, οι υπάλληλοι και οι Αντιπρόσωποι υποχρεούνται να σημειώνουν και να αναφέρουν τυχόν παρατηρούμενες ή ύποπτες αδυναμίες ασφάλειας πληροφοριών σε συστήματα ή υπηρεσίες.

iv **Αξιολόγηση και Απόφαση σχετικά με συμβάντα ασφάλειας πληροφοριών.** Η Cisco θα έχει μια κλίμακα ταξινόμησης περιστατικών σε ισχύ προκειμένου να αποφασιστεί εάν ένα γεγονός ασφάλειας πρέπει να χαρακτηριστεί ως περιστατικό Ασφάλειας Πληροφοριών. Η κλίμακα ταξινόμησης θα πρέπει να βασίζεται στην επίδραση και την έκταση ενός περιστατικού.

ν.**Διαδικασία Απόκρισης.** Η Cisco θα διατηρεί αρχείο των περιστατικών Ασφάλειας Πληροφοριών με την περιγραφή του συμβάντος που μπορεί να περιλαμβάνει τις κατηγορίες δεδομένων προσωπικού χαρακτήρα που επηρεάζονται στο βαθμό που τα Συμβάντα Ασφάλειας Πληροφοριών επηρεάζουν τα Προσωπικά Δεδομένα, την επίδραση του συμβάντος, το όνομα του προσώπου που κάνει την αναφορά και στον οποίο αναφέρθηκε το

περιστατικό, τη διαδικασία διόρθωσης του συμβάντος και τα διορθωτικά μέτρα που λαμβάνονται για την πρόληψη μελλοντικών συμβάντων ασφαλείας, τα οποία θα είναι διαθέσιμα στον Πελάτη κατόπιν αιτήματος.

ξ. Πτυχές ασφάλειας πληροφοριών της διαχείρισης επιχειρησιακής συνέχειας

i. **Σχεδιασμός.** Η Cisco θα διατηρεί σχέδια έκτακτης ανάγκης για τις εγκαταστάσεις όπου βρίσκονται τα συστήματα πληροφοριών της Cisco που επεξεργάζονται τα Προστατευμένα Δεδομένα. Η Cisco επαληθεύει τους καθιερωμένους και υλοποιητέους ελέγχους συνέχειας ασφάλειας πληροφοριών σε τακτά χρονικά διαστήματα.

ii. **Ανάκτηση Δεδομένων**. Η Cisco σχεδίασε την αποθήκευση και τις διαδικασίες για την ανάκτηση των δεδομένων κατά τρόπο επαρκή για την ανακατασκευή των Προστατευόμενων Δεδομένων στην αρχική τους κατάσταση, όπως διαπιστώθηκε στην τελευταία καταγεγραμμένη δημιουργία αντιγράφων ασφαλείας που παρέχεται από τον Πελάτη.

5. Υποχρεώσεις κοινοποίησης και επικοινωνίας

α. **Κοινοποίηση**. Η Cisco χωρίς αδικαιολόγητη καθυστέρηση θα ενημερώνει τον Πελάτη και όπου είναι εφικτό εντός 24 ωρών, αλλά σε κάθε περίπτωση εντός 48 ωρών από την επιβεβαίωση.

Η κοινοποίηση στον Πελάτη αποστέλλεται:

εάν συμβεί οποιοδήποτε από τα ακόλουθα συμβάντα.

i. οποιαδήποτε απόλυτη, υλική ευαλωτότητα ασφάλειας ή αδυναμία της οποίας η Cisco έχει πραγματική γνώση (i) στα συστήματα του Πελάτη, ή στα δίκτυα, ή (ii) στα συστήματα ή τα δίκτυα της Cisco, που έχει υπονομεύσει τα Προστατευμένα Δεδομένα,
ii. ένα Περιστατικό Ασφάλειας Πληροφοριών που θέτει σε κίνδυνο την ασφάλεια των Προστατευόμενων Δεδομένων και αποδυναμώνει ή μειώνει τις επιχειρηματικές δραστηριότητες του Πελάτη.
iii. ένα Περιστατικό Ασφάλειας Πληροφοριών που επηρεάζει αρνητικά την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των προστατευμένων δεδομένων, που επεξεργάζονται, αποθηκεύονται και μεταδίδονται μέσω υπολογιστή ή
iv. γνωστή και εσκεμμένη αποτυχία ή αδυναμία διατήρησης της ουσιαστικής συμμόρφωσης με τις απαιτήσεις του παρόντος ΠΑΠ και των ισχυόντων νόμων.

β. **Συνεργασία.**

Η Cisco: (i) θα ανταποκρίνεται άμεσα σε τυχόν λογικά αιτήματα του Πελάτη για πληροφορίες, συνεργασία και βοήθεια, συμπεριλαμβανομένου του καθορισμένο κέντρου απόκρισης του Πελάτη.

γ. **Επικοινωνία για την ασφάλεια των πληροφοριών.**

Εκτός εάν απαιτείται από τους αναγκαστικούς ισχύοντες νόμους ή από τις υφιστάμενες ισχύουσες συμβατικές υποχρεώσεις,

Η Cisco συμφωνεί ότι δεν θα ενημερώσει οποιοδήποτε τρίτο μέρος για οποιοδήποτε από τα γεγονότα που περιγράφονται παραπάνω στην παρούσα Ενότητα, ή τον προσδιορισμό του Πελάτη χωρίς τη γραπτή συγκατάθεση του. Η Cisco έχει πλήρως συνεργασία με τον Πελάτη

και τις αρχές επιβολής του νόμου σχετικά με οποιαδήποτε μη εξουσιοδοτημένη πρόσβαση στα συστήματα ή τα δίκτυα του Πελάτη ή στα Προστατευμένα Δεδομένα. Η συνεργασία αυτή περιλαμβάνει τη διατήρηση όλων των πληροφοριών και των δεδομένων εντός της κατοχής, της φύλαξης ή του ελέγχου της Cisco που σχετίζεται άμεσα με οποιοδήποτε Περιστατικό Ασφάλειας Πληροφοριών. Εάν η γνωστοποίηση απαιτείται από το νόμο, η Cisco θα συνεργαστεί με τον Πελάτη σχετικά με το χρονοδιάγραμμα, το περιεχόμενο και τους παραλήπτες της εν λόγω αποκάλυψης. Στο βαθμό που η Cisco ήταν υπεύθυνη, η Cisco θα αναλάβει το κόστος αναπαραγωγής ή οποιαδήποτε άλλα διορθωτικά μέτρα είναι απαραίτητα για την αντιμετώπιση του συμβάντος ή του συμβιβασμού. Εάν η γνωστοποίηση δεν απαιτείται από το νόμο, η Cisco θα λάβει κάθε αναγκαίο μέτρο για να αναζητήσει νόμιμες λύσεις βάσει της ελληνικής νομοθεσίας σχετικά με το απόρρητο των πληροφοριών πριν τη ν αποκάλυψη των πληροφοριών ή των Προστατευμένων Δεδομένων.

δ. **Μετά το Περιστατικό**

Η Cisco θα συνεργάζεται εύλογα με τον Πελάτη σε οποιαδήποτε έρευνα μετά το περιστατικό, αποκατάσταση και προσπάθεια επικοινωνίας.

ε. **Διαθεσιμότητα Διαδικαστικών Εγχειριδίων, Εγχειριδίων Πολιτικής και Ελέγχων**

Η Cisco θα διαθέτει στον πελάτη τις πληροφορίες που είναι εύλογα αναγκαίες για να αποδείξει τη συμμόρφωση της Cisco με τις υποχρεώσεις των Εκτελώντων την Επεξεργασία Δεδομένων σύμφωνα με την ισχύουσα νομοθεσία, και θα επιτρέπει και θα συμβάλλει σε ελέγχους ασφάλειας πληροφοριών από τον πελάτη (ή άλλο ελεγκτή εξουσιοδοτημένο από τον Πελάτη) με έξοδα του πελάτη, για το σκοπό αυτό, με την επιφύλαξη του πελάτη α)όχι περισσότερες από μία φορές ετησίως και με την παροχή στη Cisco τουλάχιστον 6 εβδομάδες πριν από τη γραπτή ειδοποίηση ότι ο εν λόγω έλεγχος πληροφοριών απαιτείται από τον πελάτη β) διασφάλιση ότι όλες οι πληροφορίες που λαμβάνονται ή παράγονται από τον Πελάτη ή τους ελεγκτές του σε σχέση με τον εν λόγω έλεγχο ασφάλειας πληροφοριών διατηρούνται αυστηρά εμπιστευτικές (εκτός από την κοινοποίηση σε εποπτική αρχή ή όπως άλλως απαιτείται από το νόμο) και γ) πριν από την έναρξη οποιουδήποτε τέτοιου ελέγχου ασφάλειας πληροφοριών, η Cisco και ο Πελάτης συμφωνούν αμοιβαία σχετικά με το πεδίο εφαρμογής, το χρονοδιάγραμμα και τη διάρκεια του ελέγχου ασφάλειας των πληροφοριών.

ΣΥΝΗΜΜΕΝΟ Β

ΕΚΘΕΜΑ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

1.ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Το παρόν Παράρτημα Προστασίας Δεδομένων ("ΠΠΔ") περιγράφει τους όρους και τις προϋποθέσεις με τις οποίες τα Μέρη πρέπει να συμμορφώνονται σε σχέση με την Επεξεργασία Προσωπικών Δεδομένων και ισχύει στο βαθμό που η Cisco επεξεργάζεται ή έχει πρόσβαση σε Προστατευμένα Δεδομένα κατά την εκτέλεση των υποχρεώσεών της προς τον Πελάτη.

2. ΠΡΟΕΠΙΛΕΓΜΕΝΑ ΠΡΟΤΥΠΑ

α. Στο βαθμό που η Cisco Επεξεργάζεται Ειδικές Κατηγορίες Δεδομένων, τα μέτρα ασφαλείας που αναφέρονται στο παρόν ΠΠΔ περιλαμβάνουν επίσης, τουλάχιστον (i) τις αξιολογήσεις κινδύνου ρουτίνας του προγράμματος ασφάλειας της Cisco , (ii) τακτικές δοκιμές και παρακολούθηση για τη μέτρηση και επιβεβαίωση της αποτελεσματικότητας των βασικών ελέγχων, συστημάτων και διαδικασιών του προγράμματος ασφάλειας πληροφοριών, και (iii) κρυπτογράφηση Ειδικών Κατηγοριών Δεδομένων κατά τη διάρκεια της μετάδοσης (είτε έχουν σταλεί μέσω ηλεκτρονικού ταχυδρομείου, φαξ ή με κάποιον άλλο τρόπο)και αποθήκευσης (συμπεριλαμβανομένης της αποθήκευσης σε κινητές συσκευές όπως φορητούς υπολογιστές, συσκευές αποθήκευσης Flash, PDA, ή κινητά τηλέφωνα). Εάν η κρυπτογράφηση δεν είναι εφικτή, η Cisco δεν θα αποθηκεύει Ειδικές Κατηγορίες Δεδομένων σε μη κρυπτογραφημένες συσκευές εκτός αν ενεργούνται ελέγχοι αποζημίωσης. Η Cisco προστατεύει όλες τις Ειδικές Κατηγορίες Δεδομένων που είναι αποθηκευμένες σε ηλεκτρονικές βάσεις δεδομένων, διακομιστές ή άλλες μορφές μη κινητών συσκευών από όλες τις εύλογα αναμενόμενες μορφές συμβιβασμού με τη χρήση των διασφαλίσεων που περιέχονται στο Συνημμένο Α (Παράρτημα Ασφάλειας Πληροφοριών).

β. Εκτός από τα ανωτέρω, στο βαθμό που η Cisco λαμβάνει, επεξεργάζεται, διαβιβάζει ή αποθηκεύει οποιαδήποτε Δεδομένα Κατόχου Κάρτας για λογαριασμό του Πελάτη, η Cisco εκπροσωπεί και εγγυάται ότι οι διαδικασίες ασφάλειας πληροφοριών , οι επεξεργασίες και τα συστήματα θα πληρούν ή θα υπερβαίνουν ανά πάσα στιγμή όλους τους ισχύοντες νόμους, πρότυπα, κανόνες και απαιτήσεις που σχετίζονται με τη συλλογή, αποθήκευση, επεξεργασία και διαβίβαση πληροφοριών καρτών πληρωμής, συμπεριλαμβανομένων εκείνων που έχουν θεσπιστεί από κυβερνητικές ρυθμιστικές υπηρεσίες, η Βιομηχανία Καρτών Πληρωμών (το "PCI"), όλα τα δίκτυα εφαρμογών και τυχόν γραπτά πρότυπα που παρέχονται σε τακτά χρονικά διαστήματα από την ομάδα ασφαλείας πληροφοριών του Πελάτη στην Cisco (όλα τα παραπάνω συλλογικά τα "Πρότυπα Συμμόρφωσης PCI").

γ. Εάν κάποιος από τους Ισχύοντες Νόμους αντικατασταθεί από νέους ή τροποποιημένους Αναγκαστικούς Ισχύοντες Νόμους (συμπεριλαμβανομένων οποιωνδήποτε αποφάσεων ή ερμηνειών από σχετικό δικαστήριο ή κυβερνητική αρχή), οι νέοι ή τροποποιημένοι Ισχύοντες

Νόμοι θα θεωρούνται ότι ενσωματώνονται σε αυτό το ΠΠΔ και η Cisco θα ξεκινήσει αμέσως να συμμορφώνεται με τους εν λόγω Ισχύοντες Νόμους.

δ. Εάν το παρόν ΠΠΔ δεν προσδιορίζει ακριβώς ένα συγκεκριμένο σύστημα ασφαλείας ή ή πρότυπα προστασίας προσωπικών δεδομένων ή υποχρεώσεις, η Cisco θα χρησιμοποιεί κατάλληλες Γενικά Αποδεκτές Πρακτικές για να προστατεύσει την εμπιστευτικότητα, ασφάλεια, ιδιωτικότητα, ακεραιότητα, διαθεσιμότητα και ακρίβεια των Προσωπικών Δεδομένων.

ε. Η Cisco συμφωνεί ότι, σε περίπτωση παραβίασης του παρόντος ακόμη κι αν ο Πελάτης έχει λάβει επαρκή αποζημίωση, ο Πελάτης έχει το δικαίωμα να ζητήσει ασφαλιστικά μέτρα ή αποζημίωση λόγω ηθικής βλάβης για να σταματήσει ή να αποτρέψει τη χρήση, επεξεργασία, ή αποκάλυψη των Προσωπικών Δεδομένων που δεν προβλέπεται από τις υποχρεώσεις της Cisco προς τον Πελάτη και / ή την παρούσα ΣΠΠΔ και να επιβάλει τους όρους του παρόντος Εκθέματος ή να επιβάλλει τη συμμόρφωση με όλους τους ισχύοντες νόμους.

στ. Οποιαδήποτε ασάφεια σε αυτό το ΠΠΔ θα επιλύεται για να επιτρέψει στον Πελάτη να συμμορφωθεί με όλους τους αναγκαστικούς ισχύοντες νόμους. Σε περίπτωση και στο βαθμό που οι ισχύοντες νόμοι επιβάλλουν αυστηρότερες υποχρεώσεις στην Cisco απ' ότι το παρόν Έκθεμα, υπερισχύουν οι αναγκαστικοί ισχύοντες νόμοι.

3.ΠΙΣΤΟΠΟΙΗΣΕΙΣ

α. Η Cisco πρέπει να διατηρεί τις πιστοποιήσεις που αναφέρονται σε μια ισχύουσα συμφωνία μεταξύ των Μερών, εάν υπάρχει, και η Cisco να θεωρεί ί εκ νέου τις πιστοποιήσεις αυτές, όπως εύλογα απαιτείται. Εάν υπάρχει μια ουσιαστική αλλαγή στις απαιτήσεις της απαιτούμενης πιστοποίησης ή τη φύση της Απόδοσης που παρέχει η Cisco, έτσι ώστε η Cisco να μην επιθυμεί πλέον να διατηρήσει τέτοιες πιστοποιήσεις, τα Μέρη θα συζητήσουν εναλλακτικές λύσεις και την αποκατάσταση της ζημίας καλή τη πίστει.

β. Πριν από την επεξεργασία των Προσωπικών Δεδομένων και κατόπιν αιτήματος του Πελάτη, η Cisco θα παρέχει στον Πελάτη αντίγραφα των πιστοποιήσεων που διατηρεί (μαζί με τα σχετικά δικαιολογητικά) που ισχύουν για τα συστήματα, τις πολιτικές και τις διαδικασίες που διέπουν την επεξεργασία των Προσωπικών Δεδομένων. Η Cisco θα ενημερώνει τον Πελάτη σε περίπτωση αποτυχίας ή εάν πλέον δεν προτίθεται να τηρεί τέτοιες πιστοποιήσεις ή εξαρτώμενα πλαίσια. Η παρούσα ειδοποίηση μπορεί να παρέχεται με κοινοποίηση ή δημοσίευση στη δημόσια ιστοσελίδα της Cisco.

4. Προστασία των Δεδομένων και Ιδιωτικότητα

Α. Τα Μέρη συμφωνούν ότι, για τα Προσωπικά Δεδομένα, ο Πελάτης είναι ο Υπεύθυνος Επεξεργασίας Δεδομένων και η Cisco θα είναι ο Εκτελών την Επεξεργασία των Δεδομένων, όπως αυτοί οι όροι έχουν διευκρινιστεί στον Γενικό Κανονισμό για την Προστασία των Δεδομένων (GDPR).

Β Ο Πελάτης :

i. στη χρήση των Προϊόντων ή/και των Υπηρεσιών, συμμορφώνεται με τους Ισχύοντες Νόμους, συμπεριλαμβανομένης της διατήρησης όλων των σχετικών κανονιστικών καταχωρίσεων και ειδοποιήσεων, όπως απαιτείται από την Ισχύουσα Νομοθεσία,

ii. ii. διασφαλίζει ότι όλες τις οδηγίες που παρέχονται από αυτόν στην Cisco σε σχέση με τα Προσωπικά Δεδομένα θα είναι ανά πάσα στιγμή σύμφωνες με τους Ισχύοντες Νόμους,

iii. iii. έχει αποκλειστική ευθύνη για την ακρίβεια, ποιότητα και νομιμότητα των Προσωπικών Δεδομένων και των μέσων με τα οποία ο Πελάτης απέκτησε Προσωπικά Δεδομένα, συμπεριλαμβανομένης της παροχής τυχόν απαιτούμενων ειδοποιήσεων στους υπαλλήλους, τους αντιπροσώπους ή τρίτους στους οποίους επεκτείνονται τα οφέλη των Προϊόντων ή/και των Υπηρεσιών της, και

iv. διατηρεί τον όγκο των Προσωπικών Δεδομένων που παρέχονται στην Cisco στο ελάχιστο αναγκαίο για την εκτέλεση των Προϊόντων ή/και των Υπηρεσιών.

γ. Εάν η Cisco έχει πρόσβαση ή επεξεργάζεται Προσωπικά Δεδομένα τότε η Cisco θα:

i. εφαρμόζει και διατηρεί εμπορικά εύλογα και κατάλληλα φυσικά, τεχνικά και οργανωτικά μέτρα ασφαλείας που περιγράφονται στο παρόν Έκθεμα (συμπεριλαμβανομένων τυχόν παραρτημάτων, προσαρτημάτων ή πιστοποιητικών αναφοράς) με σκοπό την προστασία των Προσωπικών Δεδομένων από τυχαία ή παράνομη καταστροφή. τυχαία απώλεια, αλλοίωση, μη εξουσιοδοτημένη αποκάλυψη ή όλες τις άλλες παράνομες μορφές επεξεργασίας και κάθε περιστατικό ασφάλειας πληροφοριών,

ii. λάβει εύλογα μέτρα που αποσκοπούν στη διασφάλιση της αξιοπιστίας του προσωπικού της και ότι υπόκεινται σε δεσμευτική γραπτή συμβατική υποχρέωση με την Cisco για να διατηρεί εμπιστευτικά τα Προσωπικά Δεδομένα (εκτός εάν απαιτείται γνωστοποίηση σύμφωνα με τους Ισχύοντες Νόμους, οπότε η Cisco, όπου αυτό είναι εφικτό και δεν απαγορεύεται από την Ισχύουσα Νομοθεσία, ενημερώνει τον Πελάτη για οποιαδήποτε τέτοια απαίτηση πριν από την εν λόγω αποκάλυψη) και οποιοδήποτε άλλο πρόσωπο ενεργεί υπό την εποπτεία του, το οποίο μπορεί να έρθει σε επαφή με , ή να έχει με άλλο τρόπο πρόσβαση και επεξεργασία προσωπικών δεδομένων, και απαιτεί από το εν λόγω προσωπικό να γνωρίζει τις ευθύνες του βάσει του παρόντος Εκθέματος και κάθε ισχύοντος νόμου (ή των γραπτών δεσμευτικών πολιτικών της Cisco που είναι τουλάχιστον εξίσου περιοριστικές με το παρόν ΠΠΔ),

iii. διορίζει τον Υπεύθυνο προστασίας δεδομένων (εγκατεστημένος στην Ευρωπαϊκή Ένωση). Κατόπιν αιτήματος, η Cisco θα παρέχει τα στοιχεία επικοινωνίας του διορισμένου ατόμου, που θα αναλάβει τα καθήκοντα και τις υποχρεώσεις που ορίζονται στον Γενικό Κανονισμό για την Προστασία των Δεδομένων (GDPR) (Τμήμα 4).

iv. βοηθήσει τον Πελάτη όπου εύλογα είναι αναγκαίο για να ανταποκριθεί σε αιτήματα από εποπτικές αρχές, υποκείμενα των δεδομένων, πελάτες ή άλλους να παρέχουν πληροφορίες (συμπεριλαμβανομένων των λεπτομερειών των Υπηρεσιών που παρέχονται από την Cisco) σχετικά με την Επεξεργασία Προσωπικών Δεδομένων της Cisco,

ν.δεν θα μεταφέρει Προσωπικά Δεδομένα από τη δικαιοδοσία της ΕΟΧ ή της Ελβετίας που δεν είναι Εγκεκριμένη Δικαιοδοσία, εκτός εάν πρώτα παρέχει στον πελάτη προειδοποίηση και τη δυνατότητα ένστασης, εάν ο πελάτης αντιτίθεται εύλογα στην προτεινόμενη διασυνοριακή μεταφορά, η εφαρμοστέα εκτέλεση που αποτελεί το αντικείμενο της ένστασης θα τερματίσει.

Σε περίπτωση που η Cisco Επεξεργάζεται Προσωπικά Δεδομένα από τον ΕΟΧ ή την Ελβετία για λογαριασμό του Πελάτη, η Cisco εκτελεί την επεξεργασία αυτή κατά τρόπο σύμφωνο με τις αρχές ασφαλούς προστασίας της Ιδιωτικότητας (βλ. www.commerce.gov/privacyshield)

ή στο πλαίσιο των διαδόχων της, στο βαθμό που οι Αρχές ισχύουν για την Επεξεργασία των εν λόγω δεδομένων από την Cisco. Εάν η Cisco δεν είναι σε θέση να παράσχει το ίδιο επίπεδο προστασίας όπως απαιτείται από τις Αρχές, η Cisco οφείλει να το δηλώνει αμέσως στον Πελάτη και να παύσει την Επεξεργασία. Σε αυτή την περίπτωση, ο Πελάτης μπορεί να καταγγείλει την αντίστοιχη Εκτέλεση της εν λόγω Επεξεργασίας με γραπτή ειδοποίηση εντός τριάντα (30) ημερών.

vi.για δικαιοδοσίες εκτός του ΕΟΧ ή της Ελβετίας, να μην μεταβιβάζει Προσωπικά Δεδομένα εκτός της δικαιοδοσίας όπου λαμβάνονται τα Προσωπικά Δεδομένα, εκτός εάν επιτρέπεται βάσει της Ισχύουσας Νομοθεσίας και εφόσον παρέχει πρώτα ειδοποίηση στον Πελάτη και μια ευκαιρία να αντιταχθεί, εάν ο πελάτης αντιτίθεται εύλογα στην προτεινόμενη διασυνοριακή μεταφορά, η αντίστοιχη Εκτέλεση που αποτελεί το αντικείμενο της ένστασης θα καταγγέλεται.

δ. Επιπλέον, εάν η Cisco Επεξεργάζεται Προσωπικά Δεδομένα στο πλαίσιο της Εκτέλεσης των υποχρεώσεών της προς τον Πελάτη, τότε επίσης η Cisco :

i. θα Επεξεργάζεται μόνο Προσωπικά Δεδομένα σύμφωνα με τις οριζόμενες οδηγίες του Πελάτη, στο Τμήμα 1 του Συνημμένου Γ και του παρόντος ΠΠΔ, αλλά μόνο στο βαθμό που αυτές οι οδηγίες είναι σύμφωνες με τους ισχύοντες νόμους. Εάν η Cisco εύλογα θεωρεί ότι οι οδηγίες του Πελάτη δεν συνάδουν με τους ισχύοντες νόμους, η Cisco θα ενημερώνει γι' αυτό αμέσως τον Πελάτη,

ii.εάν απαιτείται από τους Ισχύοντες Νόμους, δικαστική απόφαση, ένταλμα, κλήτευση ή άλλη νομική ή δικαστική διαδικασία για την επεξεργασία προσωπικών δεδομένων άλλων από ό,τι σύμφωνα με τις οδηγίες του Πελάτη, θα ενημερώσει τον Πελάτη για οποιαδήποτε τέτοια απαίτηση πριν από την επεξεργασία των Προσωπικών Δεδομένων (εκτός εάν οι ισχύοντες νόμοι απαγορεύουν αυτές τις πληροφορίες για σημαντικούς λόγους δημοσίου συμφέροντος),

iii.θα επεξεργάζεται μόνο ή θα χρησιμοποιεί δεδομένα προσωπικού χαρακτήρα στα συστήματα ή τις εγκαταστάσεις της στο βαθμό που απαιτείται για την εκπλήρωση των υποχρεώσεών της αποκλειστικά για λογαριασμό του Πελάτη και μόνο για τους σκοπούς που προβλέπονται από τα Μέρη·

iv. κατά περίπτωση, ενεργεί ως υπό-εκτελών την επεξεργασία των εν λόγω Προσωπικών Δεδομένων,

v. θα διατηρεί ακριβή αρχεία της επεξεργασίας οποιωνδήποτε Προσωπικών Δεδομένων που έχει λάβει από τον Πελάτη βάσει της Συμφωνίας·

vi. θα καταβάλλει εύλογες προσπάθειες για να διασφαλίσει ότι τα Προσωπικά Δεδομένα είναι ακριβή και ενημερωμένα ανά πάσα στιγμή κατά τη διάρκεια της φύλαξης ή υπό τον έλεγχό της , στο βαθμό που η Cisco έχει τη δυνατότητα να το πράξει,

vii. δεν θα εκμισθώσει, πωλήσει, διανείμει ή με άλλο τρόπο επιβαρύνει τα Προσωπικά Δεδομένα, εκτός εάν συμφωνηθεί από κοινού με ξεχωριστά υπογεγραμμένη σύμβαση

viii.παρέχει εύλογη συνεργασία και βοήθεια στον Πελάτη επιτρέποντας στα πρόσωπα στων οποίων τα Προσωπικά Δεδομένα έχουν πρόσβαση και να διαγράψουν ή να διορθώσουν τα εν λόγω Προσωπικά Δεδομένα εάν είναι αποδεδειγμένα εσφαλμένα (ή, εάν ο πελάτης ή ο

Πελάτης του Πελάτη δεν συμφωνεί ότι είναι εσφαλμένα, να έχουν καταγράψει το γεγονός ότι το σχετικό πρόσωπο θεωρεί ότι τα δεδομένα είναι εσφαλμένα),

ix.παρέχουν τέτοια βοήθεια όπως απαιτείται από τον Πελάτη (είτε για λογαριασμό του είτε για λογαριασμό των πελατών του) και η Cisco ή ένας Αντιπρόσωπος είναι εύλογα σε θέση να παράσχει, με σκοπό την εκπλήρωση τυχόν εφαρμοστέων καταθέσεων, εγκρίσεων ή παρόμοιων αιτήσεων σε σχέση με το υποχρεωτικό εφαρμοστέο δίκαιο.

x. αμέσως να ενημερώνει τον Πελάτη για οποιαδήποτε έρευνα, δικαστική διαμάχη, ζήτημα διαιτησίας, ή άλλη διαφορά που σχετίζεται με την ασφάλεια ή τις πρακτικές απορρήτου της Cisco καθώς σχετίζεται με την εκτέλεση της Cisco και τις υποχρεώσεις της προς τον Πελάτη,

xi. παρέχει εύλογες πληροφορίες και βοήθεια, όπως απαιτεί ο Πελάτης (λαμβάνοντας υπόψη τη φύση της Επεξεργασίας και τις πληροφορίες που διαθέτει η Cisco) στον Πελάτη διασφαλίζοντας τη συμμόρφωση με τις υποχρεώσεις του Πελάτη σύμφωνα με το εφαρμοστέο δίκαιο σε σχέση με:

Α. την Ασφάλεια της Επεξεργασίας,

Β. τις εκτιμήσεις των επιπτώσεων για την προστασία των δεδομένων (όπως ο όρος αυτός ορίζεται στον Γενικό Κανονισμό για την Προστασία των Δεδομένων (GDPR))·

Γ. προηγούμενη διαβούλευση με εποπτική αρχή σχετικά με την επεξεργασία υψηλού κινδύνου· και

Δ. κοινοποιήσεις προς την εποπτική αρχή ή/και ανακοινώσεις προς τα υποκείμενα των δεδομένων από τον Πελάτη ως απάντηση σε οποιοδήποτε περιστατικό ασφάλειας πληροφοριών, και

xii.με την καταγγελία της ΣΠΠΔ για οποιονδήποτε λόγο, ή κατόπιν γραπτού αιτήματος ανά πάσα στιγμή κατά τη διάρκεια του, η Cisco παύει να επεξεργάζεται οποιαδήποτε Προσωπικά Δεδομένα που λαμβάνονται από τον Πελάτη, και εντός εύλογου χρονικού διαστήματος, κατόπιν αιτήματος της Cisco: 1) θα επιστρέψει όλα τα Προσωπικά Δεδομένα. ή 2) με ασφάλεια θα καταστρέψει πλήρως ή θα διαγράψει (π.χ. χρήση ενός προτύπου όπως το Υπουργείο Άμυνας των ΗΠΑ 5220.22-M, NIST 800-53, ή η Βρετανική HMG InfoSecStandard 5, Ενισχυμένο Πρότυπο) όλα τα Προσωπικά Δεδομένα στην κατοχή ή τον έλεγχό του, εκτός κι αν η επιστροφή ή η καταστροφή δεν είναι εφικτή ή η συνεχής διατήρηση και επεξεργασία τους απαιτείται από το εφαρμοστέο δίκαιο. Κατόπιν αιτήματος του Πελάτη, η Cisco θα δώσει ένα πιστοποιητικό στον Πελάτη με υπογραφή ενός εκ των υπευθύνων, επιβεβαιώνοντας ότι έχει συμμορφωθεί πλήρως με την παρούσα Ρήτρα.

5. ΠΡΟΚΑΘΟΡΙΣΜΕΝΟΙ ΣΥΜΒΑΤΙΚΟΙ ΟΡΟΙ ΓΙΑ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Εάν, μόνο με την προηγούμενη συγκατάθεση του Πελάτη, η Cisco επεξεργάζεται Προσωπικά Δεδομένα από τον ΕΟΧ ή την Ελβετία σε δικαιοδοσία που δεν είναι εγκεκριμένη, τα Μέρη θα επιβεβαιώνουν ότι υπάρχει ένας νομίμως εγκεκριμένος μηχανισμός που επιτρέπει τη διεθνή μεταφορά δεδομένων.

Εάν η Cisco έχει σκοπό να βασιστεί σε Προκαθορισμένους Συμβατικούς Όρους (και όχι σε άλλο αποδεκτό μηχανισμό μεταβίβασης), οι ακόλουθοι πρόσθετοι όροι θα ισχύουν για τη Cisco και τους υπό-εκτελούντες την επεξεργασία και/ή τα συνδεδεμένα μέρη της Cisco που ενδέχεται να Εκτελούν για λογαριασμό της Cisco:

Α.Θα εφαρμόζονται οι Προκαθορισμένοι Συμβατικοί Όροι που ορίζονται στο Συνημμένο Δ. Εάν οι εν λόγω Προκαθορισμένοι Συμβατικοί Όροι θα αντικαθίστανται από νέους ή τροποποιημένους Προκαθορισμένους Συμβατικούς Όρους, τα Μέρη θα συνάπτουν αμέσως νέους ή τροποποιημένους Προκαθορισμένους Συμβατικούς Όρους, όπως απαιτείται.

Β.Εάν η Cisco υπό-αναθέτει οποιαδήποτε επεξεργασία δεδομένων προσωπικού χαρακτήρα (μόνο εφόσον επιτρέπεται αποκλειστικά από αντίστοιχη συμφωνία μεταξύ των Μερών και της Ισχύουσας Νομοθεσίας), η Cisco θα:

i. Ενημερώνει τον Πελάτη εκ των προτέρων για την εν λόγω Επεξεργασία θα παρέχει στον Πελάτη την ευκαιρία να αντιταχθεί πριν από την Επεξεργασία και

ii. Απαιτεί από τους εκτελούντες την επεξεργασία της Cisco να έχουν συνάψει γραπτές συμφωνίες με αυτήν, στις οποίες οι εκτελούντες την επεξεργασία θα συμμορφώνονται με τους όρους που συνάδουν με τα ισχύοντα τμήματα των Τυποποιημένων Συμβατικών Ρητρών σε σχέση με τα εν λόγω Προσωπικά Δεδομένα.

Γ.Εάν είναι απαραίτητο για τη συμμόρφωση με τους Ισχύοντες Νόμους, και όπου ζητηθεί από τον Πελάτη για λογαριασμό των πελατών του, η Cisco συνάπτει τις Τυποποιημένες Συμβατικές Ρήτρες απευθείας με τους πελάτες του Πελάτη της.

6. ΥΠΕΡΓΟΛΑΒΙΑ ΕΠΕΞΕΡΓΑΣΙΑΣ

Α. Η Cisco διαθέτει τεκμηριωμένα πρόγραμμα και πολιτικές ασφαλείας που παρέχουν (i) καθοδήγηση στους εκτελούντες την επεξεργασία της όσον αφορά τη διασφάλιση της ασφάλειας, της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των προσωπικών δεδομένων και συστημάτων που διατηρούνται ή υποβάλλονται σε επεξεργασία από την Cisco και (ii) εκφράζουν οδηγίες σχετικά με τα μέτρα που πρέπει να ληφθούν σε περίπτωση συμβιβασμού ή άλλου ανώμαλου γεγονότος.

Β. Η Cisco δεν θα αναθέσει υπεργολαβικά τις υποχρεώσεις του σύμφωνα με το παρόν Έκθεμα σε πρόσωπο ή οντότητα, εν όλω ή εν μέρει , χωρίς να παρέχει στον Πελάτη προηγούμενη προειδοποίηση και δυνατότητα ένστασης και εάν ο πελάτης αντιτίθεται εύλογα στην προτεινόμενη περαιτέρω επεξεργασία, η αντίστοιχη Εκτέλεση που αποτελεί το αντικείμενο της ένστασης θα καταγγέλεται.

Γ. Η Cisco θα εκτελέσει γραπτή συμφωνία με τους εν λόγω εγκεκριμένους εκτελούντες την επεξεργασία παρέχοντας όρους τουλάχιστον τόσο προστατευτικούς όσο οι αντίστοιχοι αυτού του Εκθέματος και των εφαρμοστέων Εκθεμάτων (υπό την προϋπόθεση ότι η Cisco δεν θα έχει το δικαίωμα να επιτρέψει στον εκτελούντα την επεξεργασία να αναθέσει περαιτέρω επεξεργασία ή με άλλο τρόπο να αναθέσει το σύνολο ή μέρος της Επεξεργασίας του εκτελούντος χωρίς προηγούμενη ειδοποίηση στη Cisco και τη δυνατότητα ένστασης) και να ορίσει τον Πελάτη ως τρίτο μέρος με δικαιώματα επιβολής των εν λόγω όρων είτε μέσω σύμβασης ή επιβολής του νόμου. Η Cisco εξασφαλίζει ότι οι εν λόγω επιμέρους επεξεργαστές συνεργάζονται και συνάπτουν τυχόν αναγκαίες πρόσθετες συμφωνίες απευθείας με τον Πελάτη.

Δ. Η Cisco θα είναι υπεύθυνη και υπόλογη για τις πράξεις ή παραλείψεις των Αντιπροσώπων στον ίδιο βαθμό που είναι υπεύθυνη και υπόλογη για τις δικές της ενέργειες ή παραλείψεις στο πλαίσιο του παρόντος ΠΠΔ.

Ε. Ο Πελάτης αναγνωρίζει και ρητά συμφωνεί ότι τα Συνδεδεμένα Μέρη της Cisco μπορούν να διατηρηθούν ως υπεργολάβοι εκτελούντες την επεξεργασία, και (β) η Cisco και τα Συνδεδεμένα Μέρη της αντίστοιχα μπορούν να προσλαμβάνουν τρίτους υπεργολάβους κατά τη διάρκεια της Εκτέλεσης. Η Cisco καθιστά διαθέσιμη στον Πελάτη την τρέχουσα λίστα εκτελούντων των επεξεργασία για τις αντίστοιχες Υπηρεσίες με τις ταυτότητες των εν λόγω εκτελούντων ("Κατάλογος εκτελούντων την επεξεργασία") κατόπιν εύλογου αιτήματος του Πελάτη.

7. ΔΙΚΑΙΩΜΑΤΑ ΤΩΝ ΥΠΟΚΕΙΜΕΝΩΝ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Α. **Αιτήσεις υποκειμένου δεδομένων**. Η Cisco, στο βαθμό που επιτρέπεται από το νόμο, ενημερώνει αμέσως τον Πελάτη εάν έχει λάβει αίτημα από υποκείμενο δεδομένων για πρόσβαση, διόρθωση, φορητότητα ή διαγραφή των Προσωπικών Δεδομένων του εν λόγω Υποκειμένου των Δεδομένων. Εκτός εάν απαιτείται από τους ισχύοντες νόμους, η Cisco δεν ανταποκρίνεται σε κανένα τέτοιο αίτημα για το Υποκείμενο των Δεδομένων χωρίς την προηγούμενη γραπτή συγκατάθεση του Πελάτη, εκτός από το να επιβεβαιώσει ότι το αίτημα σχετίζεται με τον Πελάτη. Επιπλέον, η Cisco παρέχει αυτές τις πληροφορίες και τη συνεργασία και προβαίνει σε ενέργειες όπως εύλογα απαιτείται από τον Πελάτη σε σχέση με το αίτημα του Υποκειμένου των Δεδομένων.

Β. **Παράπονα ή Ειδοποιήσεις που σχετίζονται με Προσωπικά Δεδομένα**. Σε περίπτωση που η Cisco λάβει οποιοδήποτε επίσημο παράπονο, ειδοποίηση ή επικοινωνία που σχετίζεται με την Επεξεργασία Προσωπικών Δεδομένων από αυτήν ή τη συμμόρφωση οποιουδήποτε Μέρους με τους Ισχύοντες Νόμους σε σχέση με τα Προσωπικά Δεδομένα, η Cisco ενημερώνει αμέσως τον Πελάτη, στο βαθμό που επιτρέπεται νομικά και εφαρμόζεται, ότι η Cisco παρέχει στον Πελάτη εύλογη συνεργασία σε σχέση με οποιαδήποτε τέτοια καταγγελία, ειδοποίηση ή επικοινωνία.

8. ΕΠΙΤΡΕΠΟΜΕΝΗ ΧΡΗΣΗ ΚΑΙ ΑΠΟΚΑΛΥΨΗ

Εκτός εάν άλλως προβλέπεται στην παρούσα ΣΠΠΔ, (i) η Cisco μπορεί να αποκαλύψει δεδομένα τηλεμετρίας και δεδομένα υποστήριξης σε τρίτους, υπό την προϋπόθεση ότι τα δεδομένα αυτά έχουν συγκεντρωθεί ή/και διαγραφεί κατάλληλα ώστε να αποτραπεί εύλογα η ταυτοποίηση οποιουδήποτε μεμονωμένου φυσικού προσώπου ή νομικής οντότητας, (ii) η Cisco μπορεί να χρησιμοποιεί αυτά τα από-προσωποποιημένα δεδομένα τηλεμετρίας και δεδομένα υποστήριξης για δικούς της επιχειρηματικούς σκοπούς χωρίς απόδοση ή αποζημίωση στον πελάτη, και (iii) η Cisco μπορεί να χρησιμοποιήσει τα Διοικητικά δεδομένα για δικούς της επιχειρηματικούς σκοπούς ή για να εκπληρώσει τις υποχρεώσεις της προς τον πελάτη βάσει ισχύουσας συμφωνίας. η Cisco δεν υποχρεούται να επιστρέψει ή να καταστρέψει προστατευμένα δεδομένα που αποτελούν δεδομένα διαχείρισης, δεδομένα παραμυθιού ή δεδομένα υποστήριξης και θα συνεχίσει να επιτρέπεται να χρησιμοποιεί και να αποκαλύπτει τα εν λόγω δεδομένα διαχείρισης, δεδομένα τηλεμετρίας ή δεδομένα υποστήριξης, μόνο σε μη προσδιορισμένη μορφή, όπως ορίζεται στην παρούσα Ενότητα 8 (επιτρεπόμενη χρήση και αποκάλυψη) μετά την καταγγελία ή τη λήξη της παρούσας ΣΠΠΔ.

ΣΥΝΗΜΜΕΝΟ Γ

Όλες οι λεπτομερείς πληροφορίες σχετικά με την Επεξεργασία των Προσωπικών Δεδομένων από τις Συνεδριάσεις Webex της Cisco μπορούν να βρεθούν στο ακόλουθο φύλλο Δεδομένων Απορρήτου:

[ΗΛΕΚΤΡΟΝΙΚΟ ΑΡΧΕΙΟ]

Οι λεπτομέρειες επεξεργασίας που περιλαμβάνονται στο Συνημμένο Γ, μπορούν να υπόκεινται σε τροποποιήσεις, με την προϋπόθεση ότι οι τροποποιήσεις αυτές δεν μειώνουν ουσιωδώς την Προστασία των προσωπικών δεδομένων της Cisco. Για μια ενημερωμένη περιγραφή των δραστηριοτήτων επεξεργασίας, ανατρέξτε στο Φύλλο Δεδομένων Απορρήτου των συνεδριάσεων Webex στο Κέντρο Εξυπηρέτησης της Cisco στη διεύθυνση https://www.cisco.com/c/en/us/about/trust-center/solutions-privacy-data-sheets.html .

ΣΥΝΗΜΜΕΝΟ Δ

ΠΡΟΚΑΘΟΡΙΣΜΕΝΟΙ ΣΥΜΒΑΤΙΚΟΙ ΟΡΟΙ

Για τους σκοπούς του άρθρου 26 παράγραφος 2 της οδηγίας 95/46/ΕΚ για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε εκτελούντες εγκατεστημένους σε τρίτες χώρες οι οποίοι δεν εξασφαλίζουν επαρκές επίπεδο προστασίας των δεδομένων (αυτές μπορεί να είναι διαθέσιμες στο πρωτότυπο κείμενο τους στον δικτυακό τόπο της Ευρωπαϊκής Επιτροπής εδώ: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index/en.htm):

Η Cisco θα χρησιμοποιεί Προκαθορισμένους Συμβατικούς Όρους όπως αυτοί εκάστοτε προτείνονται και εγκρίνονται από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων ("ΕΣΠΔ").

ΠΑΡΑΡΤΗΜΑ 1 ΣΕ ΣΥΝΗΜΜΕΝΟ Γ

ΟΙ ΠΡΟΚΑΘΟΡΙΣΜΕΝΟΙ ΣΥΜΒΑΤΙΚΟΙ ΟΡΟΙ ΤΩΝ ΣΥΝΕΔΡΙΑΣΕΩΝ WEBEX ΤΗΣ CISCO

Το παρόν παράρτημα 1 στο συνημμένο Γ ΟΙ ΠΡΟΚΑΘΟΡΙΣΜΕΝΟΙ ΣΥΜΒΑΤΙΚΟΙ ΟΡΟΙ ΤΩΝ ΣΥΝΕΔΡΙΑΣΕΩΝ WEBEX ΤΗΣ CISCO αποτελεί μέρος των Πρακαθορισμένων Συμβατικών Όρων.

Οι Συνεδριάσεις Cisco Webex θα αναφέρονται ως «Υπηρεσία» ή «Συνεδριάσεις Webex» στο παρόν Παράρτημα 1.

Εξαγωγέας Δεδομένων

Εξαγωγέας δεδομένων είναι η Εταιρεία, η οποία ενεργεί ως εξαγωγέας δεδομένων για λογαριασμό της ή ως πελάτης, κατά περίπτωση. Οι δραστηριότητες που σχετίζονται με τη μεταφορά περιλαμβάνουν την παροχή υπηρεσιών για την Εταιρεία και τους πελάτες της.

Εισαγωγέας δεδομένων

Ο εισαγωγέας δεδομένων είναι η Cisco.Οι δραστηριότητες που σχετίζονται με τη μεταφορά περιλαμβάνουν την παροχή υπηρεσιών για την Εταιρεία και τους πελάτες της.

Υποκείμενα των δεδομένων

Τα δεδομένα προσωπικού χαρακτήρα που διαβιβάζονται μπορεί να αφορούν τις ακόλουθες κατηγορίες υποκειμένων των δεδομένων: Εταιρεία ή υπαλλήλους της Εταιρείας.

Webex Συσκέψεις, Webex Εκδηλώσεις, Webex Υποστήριξη και Webex Εκπαίδευση

Κατηγορίες Προσωπικών Δεδομένων	Είδη Προσωπικών Δεδομένων	Σκοπός Επεξεργασίας
Πληροφορίες Καταχώρισης	• Όνομα • Διεύθυνση ηλεκτρονικού ταχυδρομείου • Κωδικός πρόσβασης • Δημόσια Διεύθυνση IP • Πρόγραμμα περιήγησης • Αριθμός τηλεφώνου (προαιρετικό) • Ταχυδρομική Διεύθυνση (προαιρετικό)	• Εγγραφή πελάτη σε Υπηρεσία • Εμφάνιση ταυτότητας εικονιδίου του χρήστη πελάτη σε άλλους χρήστες • Παροχή υποστήριξης

	• Εικονίδιο (προαιρετικό) • Πληροφορίες Τιμολόγησης	
Πληροφορίες υποδοχής της σύσκεψης και χρήσης	• Διεύθυνση IP • Αναγνωριστικός παράγοντας χρήστη • Τύπος υλικού • Τύπος και έκδοση λειτουργικού συστήματος • Έκδοση προγράμματος πελάτη • Διευθύνσεις IP κατά μήκος της διαδρομής δικτύου • Διεύθυνση mac του τελικού σημείου (ανάλογα με την περίπτωση) • Έκδοση υπηρεσίας • Δράσεις που έχουν αναληφθεί • Πληροφορίες περιόδου λειτουργίας σύσκεψης (τίτλος, ημερομηνία και ώρα, συχνότητα, μέση και πραγματική διάρκεια, ποσότητα, ποιότητα, δραστηριότητα δικτύου και συνδεσιμότητα δικτύου) • Αριθμός συσκέψεων • Αριθμός περιόδων λειτουργίας κοινής χρήσης οθόνης και κοινής χρήσης εκτός οθόνης • Αριθμός συμμετεχόντων • Όνομα οικοδεσπότη σύσκεψης • Ανάλυση οθόνης	• Κατανόηση του τρόπου με τον οποίο χρησιμοποιείται η υπηρεσία • Διάγνωση τεχνικών ζητημάτων • Ανάλυση και στατιστική ανάλυση σε συγκεντρωτική μορφή για τη βελτίωση της • Απάντηση σε αιτήματα υποστήριξης πελατών

	• Μέθοδος συνδέσμου • Πληροφορίες εκτέλεσης, αντιμετώπισης προβλημάτων και διαγνωστικών	
Πληροφορίες που δημιουργούνται από το χρήστη* *Προαιρετικά: μόνο με δυνατότητα ενεργοποίησης εάν αυτή η δυνατότητα είναι ενεργοποιημένη	• Εγγραφές συσκέψεων και κλήσεων • Μεταφορτωμένα αρχεία	Παρέχουν την Υπηρεσία, προαιρετικά στοιχεία που περιλαμβάνουν την καταγραφή συσκέψεων και την κοινή χρήση αρχείων

Βοήθεια Τεχνικής Υποστήριξης

Κατηγορίες Προσωπικών Δεδομένων	Είδη Προσωπικών Δεδομένων	Σκοπός Επεξεργασίας
Πληροφορίες Τεχνικής Υποστήριξης	• Όνομα • Διεύθυνση ηλεκτρονικού ταχυδρομείου • Αριθμός τηλεφώνου του Υπαλλήλου που διορίζεται για να ανοίξει το αίτημα εξυπηρέτησης • Πληροφορίες ελέγχου ταυτότητας (χωρίς κωδικούς πρόσβασης) • Πληροφορίες σχετικά με την κατάσταση του συστήματος • Δεδομένα μητρώου σχετικά με τις ρυθμίσεις παραμέτρων λογισμικού • Αρχεία παρακολούθησης σφαλμάτων	• Παροχή υποστήριξης • Αναθεώρηση της ποιότητας της υπηρεσίας υποστήριξης • Εκτέλεση ανάλυσης της λύσης της υπηρεσίας

Κατηγορίες Δεδομένων

Τα δεδομένα προσωπικού χαρακτήρα που διαβιβάζονται μπορεί να αφορούν τις ακόλουθες κατηγορίες δεδομένων:

1. Πληροφορίες Εγγραφής (όπως ορίζεται στους ανωτέρω πίνακες)

2. Πληροφορίες κεντρικού υπολογιστή και χρήσης (όπως ορίζεται στους ανωτέρω πίνακες)
3. Πληροφορίες που δημιουργούνται από το χρήστη (όπως ορίζεται στους ανωτέρω πίνακες) (***προαιρετικά: εφαρμόζεται μόνο εάν αυτή η λειτουργία είναι ενεργοποιημένη)**
4. Τεχνική Υποστήριξη και Βοήθεια (όπως ορίζεται στους ανωτέρω πίνακες)

Ειδικές κατηγορίες δεδομένων

Τα δεδομένα προσωπικού χαρακτήρα που διαβιβάζονται μπορεί να αφορούν τις ακόλουθες ειδικές κατηγορίες δεδομένων: μόνο εάν αποκαλυφθεί από το Υποκείμενο των Δεδομένων.

Διαδικασίες Επεξεργασίας

Οι Cisco Webex Συνεδριάσεις είναι μία λύση διαδικτυακής και βίντεο τηλεδιάσκεψης που διατίθενται από την Cisco στον Πελάτη που το αγόρασε για χρήση από τους εξουσιοδοτημένους του χρήστες. Οι Συνεδριάσεις Cisco Webex επιτρέπουν σε υπαλλήλους ανά τον κόσμο και εικονικές ομάδες να συνεργάζονται σε πραγματικό χρόνο από οπουδήποτε, σε οποιαδήποτε κινητή συσκευή ή σύστημα βίντεο σαν να εργάζονταν στο ίδιο δωμάτιο. Οι λύσεις περιλαμβάνουν συναντήσεις, εκδηλώσεις, υπηρεσίες κατάρτισης και υποστήριξης.

Οι Συνεδριάσεις Cisco Webex Meetings επιτρέπουν στους χρήστες να συνδέονται άμεσα με τρόπο που είναι σχεδόν τόσο προσωπικός όσο μια συνάντηση πρόσωπο με πρόσωπο. Ο οικοδεσπότης της σύσκεψης έχει την επιλογή να καταγράψει την σύσκεψη και όλοι οι χρήστες έχουν την επιλογή να το μεταφορτώσουν και να διατηρήσουν τα αρχεία κοινής χρήσης κατά τη διάρκεια και μετά τη λήξη της σύσκεψης. Εάν ο οικοδεσπότης της σύσκεψης δεν επιθυμεί να διατηρήσει το περιεχόμενο της σύσκεψης, αυτό εξαφανίζεται από την πλατφόρμα της Webex Meetings αμέσως μετά τη λήξη της σύσκεψης.*(Προαιρετικό : εφαρμόζεται μόνο εάν έχει ενεργοποιηθεί αυτή η δυνατότητα)

Ομοίως, εάν οι χρήστες συμμετέχουν σε συσκέψεις που φιλοξενούνται από χρήστες σε άλλες εταιρείες, ο οικοδεσπότης της σύσκεψης θα ελέγχει οποιαδήποτε εγγραφή συσκέψεως ή αρχεία που έχουν κοινοποιηθεί κατά τη διάρκεια της σύσκεψης,* (Προαιρετικό : εφαρμόζεται μόνο εάν έχει ενεργοποιηθεί αυτή η δυνατότητα), τα οποία θα υπόκεινται στις εταιρικές πολιτικές του οικοδεσπότη όσον αφορά την πρόσβαση, τη χρήση, παρακολούθηση, διαγραφή, διατήρηση και εξαγωγή πληροφοριών. Η Cisco δεν έχει κανέναν έλεγχο και δεν είναι υπεύθυνη ή υπόλογη για το απόρρητο των πληροφοριών που ο Πελάτης έχει μοιραστεί με άλλους. Ακόμα και μετά την κατάργηση από τον Πελάτη των πληροφοριών από την πλατφόρμα συσκέψεων Webex, αντίγραφα αυτών των πληροφοριών ενδέχεται να παραμείνουν ορατά αλλού στο βαθμό που έχουν μοιραστεί με άλλους.

Διαγραφή και διατήρηση Δεδομένων

Οι Πελάτες έχουν τη δυνατότητα να ορίσουν περιόδους μαζικής διατήρησης σε επίπεδο για τις εγγραφές χρησιμοποιώντας APIs. Μετά τον τερματισμό ή τη λήξη της Υπηρεσίας. Τα δεδομένα που δημιουργήθηκαν από τον Χρήστη διαγράφονται από την πλατφόρμα της Cisco Webex εντός 60 ημερών.

Οι Πελάτες μπορούν να ζητήσουν τη διαγραφή άλλων προσωπικών δεδομένων που διατηρούνται στην πλατφόρμα συσκέψεων της Cisco Webex στέλνοντας ένα αίτημα στη διεύθυνση privacy@cisco.com ή με το άνοιγμα αιτήματος της υπηρεσίας TAC, και εκτός εάν τα δεδομένα προσωπικού χαρακτήρα απαιτείται να διατηρηθούν για νόμιμους επιχειρηματικούς σκοπούς της Cisco, η Cisco προσπαθεί να διαγράψει τα δεδομένα που ζητήθηκαν από τα συστήματά της εντός 30 ημερών. Ο παρακάτω πίνακας περιγράφει την περίοδο διατήρησης και τους επιχειρηματικούς λόγους που η Cisco διατηρεί τα δεδομένα προσωπικού χαρακτήρα. Οι Χρήστες που ζητούν διαγραφή άλλων προσωπικών δεδομένων που διατηρούνται στην πλατφόρμα συσκέψεων της Cisco Webex πρέπει να ζητήσουν διαγραφή από το διαχειριστή της ιστοσελίδας του εργοδότη τους.

Κατηγορία Προσωπικών Δεδομένων	Περίοδος Διατήρησης	Λόγος και Κριτήρια Διατήρησης
Πληροφορίες Καταχώρισης	7 χρόνια από τότε που η Υπηρεσία τερματίστηκε	Τα δεδομένα που συλλέγονται ως μέρος της εγγραφής, συμπεριλαμβανομένων των πληροφοριών που παρέχονται από τους πελάτες, ως μέρος της οικονομικής δέουσας επιμέλειας της Cisco, αποτελούν επιχειρηματικά αρχεία της Cisco και τηρούνται για τη συμμόρφωση με τις οικονομικές και ελεγκτικές πολιτικές της Cisco, καθώς και με τις φορολογικές απαιτήσεις.
TAC Υποστήριξη πληροφοριών	Μέχρι ο Πελάτης α) να ζητήσει τη διαγραφή μέσω ηλεκτρονικού μηνύματος στην privacy@cisco.com ή β) μέσω ανοίγματος αιτήματος στις υπηρεσίες TAC	Η TAC Υποστήριξη πληροφοριών διατηρείται για να εξασφαλίσει αποτελεσματική υποστήριξη σε περίπτωση επαναλαμβανόμενων ζητημάτων και να συμμορφωθεί με τις πολιτικές ελέγχου της Cisco που σχετίζονται με τα επιχειρηματικά αρχεία των υπηρεσιών που παρέχονται στον Πελάτη.
Πληροφορίες που έχουν δημιουργηθεί από τον χρήστη	Ενεργές συνδρομές: • Κατά την κρίση του Πελάτη ή του χρήστη	Οι πληροφορίες που δημιουργούνται από το χρήστη δεν διατηρούνται

	Υπηρεσία που τερματίστηκε: • Διαγράφεται εντός 60 ημερών	στην Πλατφόρμα συσκέψεων της Cisco Webex όταν ο Πελάτης ή ο χρήστης διαγράφει αυτά τα δεδομένα.
Πληροφορίες υποδοχής και χρήσης	7 χρόνια από τότε που η Υπηρεσία τερματίστηκε	Πληροφορίες που παράγονται από συστήματα οργάνων και καταγραφής μέσω της χρήσης και λειτουργίας της Υπηρεσίας διατηρούνται ως μέρος του αρχείου της Cisco για την παροχή υπηρεσιών. Πληροφορίες χρήσης χρησιμοποιούνται για τη διεξαγωγή αναλυτικών στοιχείων και τη μέτρηση της στατιστικής εκτέλεσης διατηρούνται αλλά με ψευδώνυμο.

Τα στοιχεία επεξεργασίας που περιλαμβάνονται στο παρόν προσάρτημα 1 ενδέχεται να τροποποιηθούν, υπό την προϋπόθεση ότι η αλλαγή αυτή δεν μειώνει ουσιωδώς την προστασία των δεδομένων προσωπικού χαρακτήρα της Cisco κάτω από τις αιτήσεις των εφαρμοστέων υποχρεωτικών νόμων. Για μια ενημερωμένη περιγραφή των δραστηριοτήτων επεξεργασίας, ανατρέξτε στο σχετικό Φύλλο Δεδομένων Απορρήτου στο Cisco's Trust Center στη σελίδα https://www.cisco.com/c/en/us/about/trust-center/solutions-privacy-data-sheets.html

ΕΞΑΓΩΓΕΑΣ ΔΕΔΟΜΕΝΩΝ ΕΙΣΑΓΩΓΕΑΣ ΔΕΔΟΜΕΝΩΝ

Όνομα Όνομα

Εξουσιοδοτημένη Υπογραφή Εξουσιοδοτημένη Υπογραφή

ΕΡΜΗΣ
ΔΙΚΗΓΟ
ΠΕΝΤΕΛ
ΤΗΛ: 210
e-mail:
ΑΦΜ:

ΠΑΡΑΡΤΗΜΑ 2 ΣΕ ΣΥΝΗΜΜΕΝΟ Δ

ΟΙ ΠΡΟΚΑΘΟΡΙΣΜΕΝΟΙ ΣΥΜΒΑΤΙΚΟΙ ΟΡΟΙ

Το Παράρτημα 2 του συνημμένου Δ, οι Προκαθορισμένοι Συμβατικοί Όροι, είναι το Παράρτημα Ασφάλειας Πληροφοριών («ΠΑΠ») που βρίσκεται στο συνημμένο. Α

ΣΥΝΗΜΜΕΝΟ Ε

ΓΛΩΣΣΑΡΙΟ ΟΡΩΝ

Όλοι οι όροι με κεφαλαία που δεν ορίζονται στο παρόν Γλωσσάριο έχουν τις έννοιες που ορίζονται αλλού στη ΣΠΠΔ.

Α." **Δεδομένα Διαχείρισης**" σημαίνει δεδομένα που σχετίζονται με υπαλλήλους ή εκπροσώπους του Πελάτη, τα οποία συλλέγονται και χρησιμοποιούνται από την Cisco για τη διαχείριση ή τη διαχείριση της Εκτέλεσης της Cisco, ή του λογαριασμού του Πελάτη, για τους επιχειρηματικούς σκοπούς της Cisco. Τα Διοικητικά Δεδομένα μπορεί να περιλαμβάνουν Προσωπικά Δεδομένα και πληροφορίες σχετικά με τις συμβατικές δεσμεύσεις μεταξύ του Πελάτη και της Cisco, είτε συλλέγονται κατά τη στιγμή της αρχικής καταχώρισης είτε στη συνέχεια σε σχέση με την παράδοση, τη διαχείριση ή την Εκτέλεση. Τα Διοικητικά Δεδομένα είναι Προστατευμένα Δεδομένα.

Β. "**Συνδεδεμένα Μέρη**" σημαίνει κάθε οντότητα που ελέγχει άμεσα ή έμμεσα, ελέγχεται από άλλη οντότητα ή βρίσκεται υπό κοινό έλεγχο με αυτήν, για όσο χρονικό διάστημα υπάρχει τέτοιος έλεγχος. Στην περίπτωση εταιρειών και επιχειρήσεων, ως "έλεγχος" και "ελεγχόμενος" νοείται ο πραγματικός δικαιούχος άνω του πενήντα τοις εκατό (50%) των μετοχών με δικαίωμα ψήφου, των μετοχών, των συμμετοχών ή των ιδίων κεφαλαίων σε μια οικονομική οντότητα. Στην περίπτωση οποιασδήποτε άλλης νομικής οντότητας, ως "έλεγχος" και "ελεγχόμενος" νοείται η ικανότητα άμεσου ή έμμεσου ελέγχου της διαχείρισης ή/και των δραστηριοτήτων της νομικής οντότητας.

Γ. Δεν εφαρμόζεται

Δ. Δεν εφαρμόζεται

Ε. Ως "**εγκεκριμένη δικαιοδοσία**" νοείται ένα κράτος μέλος του Ευρωπαϊκού Οικονομικού Χώρου, ή άλλη δικαιοδοσία που μπορεί να εγκριθεί ως έχει επαρκή νομική προστασία για τα δεδομένα από την Ευρωπαϊκή Επιτροπή που βρίσκεται επί του παρόντος εδώ: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index/en.htm

ΣΤ. Ως "**Σύμβαση Επιχειρηματικής Συνεργασίας**" νοούνται οι ειδικοί όροι και προϋποθέσεις που έχουν προστεθεί ως Συνημμένο Γ και θα εφαρμοστούν όταν η Cisco Επεξεργάζεται Προστατευμένες Πληροφορίες Υγείας.

Ζ. Δεν εφαρμόζεται

Η. Ως «**εμπιστευτικές πληροφορίες**» νοούνται οι εμπιστευτικές πληροφορίες ή υλικά που σχετίζονται με την επιχείρηση, τα προϊόντα, τους πελάτες ή τους υπαλλήλους του Πελάτη και περιλαμβάνουν, χωρίς περιορισμό, εμπορικά μυστικά, τεχνογνωσία, εφευρέσεις, τεχνικές, διαδικασίες, προγράμματα, σχηματικά, έγγραφα πηγής λογισμικού, δεδομένα, λίστες

πελατών, οικονομικές πληροφορίες, τιμολόγηση, ανάπτυξη προϊόντων, σχέδια πωλήσεων και μάρκετινγκ ή πληροφορίες που η Cisco γνωρίζει ή έχει λόγους να γνωρίζει ότι είναι εμπιστευτικές, ιδιόκτητες ή εμπορικές μυστικές πληροφορίες που αποκτά η Cisco από τον Πελάτη ή κατόπιν αιτήματος ή κατεύθυνσης του Πελάτη κατά τη διάρκεια της Εκτέλεσης: i) που έχουν επισημανθεί ως εμπιστευτικές· ii) των οποίων ο εμπιστευτικός χαρακτήρας είναι γνωστός από τον Πελάτη στη Cisco · ή iii) ότι λόγω του χαρακτήρα και της φύσης τους, ένα λογικό πρόσωπο υπό ομοειδείς συνθήκες θα τις αντιμετώπιζε ως εμπιστευτικές.

Θ. Ως" **Δεδομένα Πελάτη**" νοούνται όλα τα δεδομένα (συμπεριλαμβανομένων των αρχείων κειμένου, ήχου, βίντεο ή εικόνας) που παρέχονται είτε από έναν πελάτη σε σχέση με τη χρήση προϊόντων ή υπηρεσιών από τον πελάτη, είτε δεδομένα που αναπτύσσονται κατόπιν συγκεκριμένου αιτήματος ενός πελάτη σύμφωνα με δήλωση εργασίας ή σύμβασης. Τα Δεδομένα Πελάτη δεν περιλαμβάνουν Δεδομένα Διαχείρισης, Δεδομένα Χρηματοδότησης, Δεδομένα Υποστήριξης ή Δεδομένα Τηλεμετρίας.

Ι. " **Υποκείμενο των δεδομένων**" σημαίνει το άτομο στο οποίο αναφέρονται τα Προσωπικά Δεδομένα.

Κ. "**Πελάτης**" σημαίνει το μέρος που διαθέτει προστατευμένα δεδομένα (εμπιστευτικά ή όχι) στο άλλο Μέρος.

Λ. Ως "**ΕΟΧ**" ή "**Ευρωπαϊκός Οικονομικός Χώρος**" νοούνται οι χώρες που είναι μέλη της Ευρωπαϊκής Ζώνης Ελεύθερων Συναλλαγών ("ΕΖΕΣ") και τα τότε σημερινά, και τα κράτη μέλη της Ευρωπαϊκής Ένωσης που θα ενταχθούν μεταγενέστερα

Μ. Δεν εφαρμόζεται

Ν. Δεν εφαρμόζεται

Ξ. Οι "**γενικά αποδεκτές πρακτικές**" αναφέρονται στα επίπεδα ακρίβειας, ποιότητας, φροντίδας, σύνεσης, πληρότητας, επικαιρότητας, ανταπόκρισης, αποδοτικότητας των πόρων, παραγωγικότητας και προληπτικής παρακολούθησης της εκτέλεσης των υπηρεσιών που είναι τουλάχιστον ίσα με τα τότε αποδεκτά πρότυπα του κλάδου των παρόχων πρώτης βαθμίδας των καθηκόντων που προβλέπονται στην εκτέλεση της Συμφωνίας.

Ο. Ως " **Περιστατικό ασφάλειας πληροφοριών**" νοείται η επιτυχής ή επικείμενη απειλή μη εξουσιοδοτημένης πρόσβασης, χρήσης, αποκάλυψης, παραβίασης, τροποποίησης, κλοπής, απώλειας, διαφθοράς ή καταστροφής πληροφοριών· παρεμβολές στις λειτουργίες της τεχνολογίας των πληροφοριών· ή παρεμβολές στις λειτουργίες του συστήματος.

Π. Ως "**Εκτέλεση**" νοούνται οποιεσδήποτε πράξεις από οποιοδήποτε από τα μέρη κατά τη διάρκεια της ολοκλήρωσης των υποχρεώσεων που προβλέπονται βάσει της Συμφωνίας, συμπεριλαμβανομένης της παροχής υπηρεσιών, της παροχής παραδοτέων και του προϊόντος εργασίας, της πρόσβασης σε Προσωπικά Δεδομένα ή της παροχής Λογισμικού ως Υπηρεσίας ("SaaS"), της πλατφόρμας cloud ή των φιλοξενούμενων υπηρεσιών. Οι "**Εκτελέσεις**", η "**Εκτέλεση**" και " **Εκτελώντας**" θα ερμηνεύονται αναλόγως.

Ρ. Ως "**Προσωπικά Δεδομένα**" νοείται κάθε πληροφορία όπως παρατίθεται στο άρθρο 4 παρ. 1 του Γενικού Κανονισμού Προστασίας των Δεδομένων (GDPR). Τα Προσωπικά Δεδομένα θεωρούνται εμπιστευτικές πληροφορίες ασχέτως της πηγής. Τα Προσωπικά Δεδομένα είναι Προστατευμένα Δεδομένα.

Σ. "**Επεξεργασία**" όπως στο άρθρο 4 παρ. 2 του Γενικού Κανονισμού Προστασίας των Δεδομένων (GDPR).

Τ. Ως "**Προστατευμένα Δεδομένα**" νοούνται τα Δεδομένα Διαχείρισης, οι Εμπιστευτικές πληροφορίες, τα Δεδομένα Πελατών, Δεδομένα Χρηματοδότησης, Δεδομένα του Κατόχου Κάρτας, Δεδομένα Υποστήριξης , Δεδομένα Τηλεμετρίας και όλα τα Προσωπικά Δεδομένα.

Υ. Δεν εφαρμόζεται

Φ. " **Cisco** " σημαίνει το Μέρος που λαμβάνει τα Προστατευμένα Δεδομένα.

Χ. Ως " **Αντιπρόσωποι** " νοούνται τα στελέχη, οι Διευθυντές, οι Υπάλληλοι, οι Υπεύθυνοι, οι Υπεύθυνοι Επεξεργασίας, το προσωρινό προσωπικό, οι Εκτελούντες την επεξεργασία και οι Σύμβουλοι του Μέρους και των Συνδεδεμένων Μερών του.

Ψ. Ως " **ευαίσθητα προσωπικά δεδομένα**" ή " **Ειδικές Κατηγορίες Δεδομένων**" νοούνται οι προσωπικές πληροφορίες που απαιτούν ένα επιπλέον επίπεδο προστασίας και ένα υψηλότερο καθήκον φροντίδας. Αυτές οι κατηγορίες ορίζονται από υποχρεωτικούς κανόνες δικαίου και περιλαμβάνουν: πληροφορίες σχετικά με φυλετική ή εθνοτική καταγωγή, πολιτικές απόψεις, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, συμμετοχή σε συνδικαλιστικές οργανώσεις, πληροφορίες που σχετίζονται με την επεξεργασία γενετικού υλικού, βιομετρικού υλικού με σκοπό την μοναδική ταυτοποίηση ενός φυσικού προσώπου, δεδομένα σχετικά με υγειονομικές συνθήκες ή δεδομένα σχετικά με την σεξουαλική ζωή ενός ατόμου ή τις σεξουαλικές προτιμήσεις του, ή οικονομικές πληροφορίες ή πληροφορίες που σχετίζονται με ποινικές καταδίκες. Τα ευαίσθητα προσωπικά δεδομένα και οι ειδικές κατηγορίες δεδομένων αποτελούν μια κατηγορία προσωπικών δεδομένων που είναι ιδιαίτερα ευαίσθητα και ενέχουν μεγαλύτερο κίνδυνο. Ο Πελάτης μπορεί να απαιτήσει πρόσθετες ευθύνες απορρήτου κατά την αντιμετώπιση αυτών των Προσωπικών Δεδομένων, τα οποία θα προσαρτηθούν στη Συμφωνία ή σε δήλωση εργασίας, ανάλογα με την περίπτωση.

Ω. Ως "**Υπηρεσία**" νοείται μια προσφορά υπηρεσιών από την Cisco που περιγράφεται σε μια εφαρμογή υπηρεσίας ή περιγραφή προσφοράς, δήλωση εργασίας, ή παραγγελία αγοράς που απαριθμούνται ως επιλεγμένα από τον Πελάτη.

Αα. Ως "**Δεδομένα υποστήριξης**" νοούνται οι πληροφορίες που η Cisco πραγματοποιεί όταν ο Πελάτης υποβάλλει αίτημα για υπηρεσίες υποστήριξης ή άλλη αντιμετώπιση προβλημάτων, συμπεριλαμβανομένων πληροφοριών σχετικά με το υλικό, το λογισμικό και άλλες λεπτομέρειες που σχετίζονται με το περιστατικό υποστήριξης, όπως πληροφορίες ελέγχου ταυτότητας, πληροφορίες σχετικά με την κατάσταση του προϊόντος, δεδομένα συστήματος και μητρώου σχετικά με εγκαταστάσεις λογισμικού και ρυθμίσεις διάρθρωσης υλικού, καθώς και αρχεία παρακολούθησης σφαλμάτων. Τα δεδομένα υποστήριξης είναι Προστατευμένα Δεδομένα.

Ββ." **Δεδομένα τηλεμετρίας**" σημαίνει πληροφορίες που παράγονται από συστήματα οργάνων και καταγραφής που δημιουργούνται μέσω της χρήσης και της λειτουργίας των προϊόντων ή/και των υπηρεσιών. Τα δεδομένα τηλεμετρίας είναι Προστατευμένα Δεδομένα.

Φύλλο προστασίας προσωπικών δεδομένων

Συσκέψεις της Cisco Webex

Το παρόν Φύλλο Δεδομένων Απορρήτου περιγράφει την επεξεργασία προσωπικών δεδομένων (ή προσωπικών πληροφοριών ταυτοποίησης) από τη Cisco Webex Meetings.

1. Επισκόπηση των δυνατοτήτων συσκέψεων της Cisco Webex

Οι συσκέψεις Cisco Webex (η "Υπηρεσία" ή οι "Συσκέψεις Webex") είναι μια λύση web και τηλεδιάσκεψης που βασίζεται στο cloud διαθέσιμα από τη Cisco σε εταιρείες ή πρόσωπα ("Πελάτες", "εσείς" ή "σας") που το αποκτούν για χρήση από τους εξουσιοδοτημένους χρήστες τους (ο καθένας, ένας «χρήστης»). Η Υπηρεσία δίνει τη δυνατότητα σε υπαλλήλους ανά τον κόσμο και εικονικές ομάδες να συνεργάζονται σε πραγματικό χρόνο από οπουδήποτε, οποτεδήποτε, σε κινητές συσκευές ή συστήματα βίντεο σαν να εργάζονταν στο ίδιο δωμάτιο. Οι λύσεις περιλαμβάνουν συσκέψεις, εκδηλώσεις, υπηρεσιών κατάρτισης και υποστήριξης. Για περισσότερες πληροφορίες σχετικά με τη δυνατότητα πληροφοριών ατόμων για τις συσκέψεις Webex της Cisco, ανατρέξτε στην προσθήκη που ακολουθεί. Για μια λεπτομερή επισκόπηση της Υπηρεσίας, επισκεφθείτε την αρχική σελίδα διάσκεψης της Cisco Web Conferencing.

Επειδή η Υπηρεσία επιτρέπει τη συνεργασία μεταξύ των χρηστών της, και μπορεί αν σας ζητηθεί να παρέχετε τα προσωπικά σας δεδομένα προκειμένου να χρησιμοποιήσετε την Υπηρεσία. Οι ακόλουθες παράγραφοι περιγράφουν την επεξεργασία προσωπικών δεδομένων από τη Cisco σε σχέση με την παράδοση της Υπηρεσίας, την τοποθεσία και τη διαβίβαση των δεδομένων αυτών, καθώς και τον τρόπο με τον οποίο εξασφαλίζεται σύμφωνα με τις αρχές της ιδιωτικότητας, τους νόμους και τους Κανονισμούς. Εάν επιλέξετε να αγοράσετε την Υπηρεσία, θα χρειαστεί να αποκαλύψετε προσωπικά δεδομένα στην Cisco, για να την χρησιμοποιήσετε. Η Cisco θα χρησιμοποιήσει τα προσωπικά σας δεδομένα σύμφωνα με το παρόν Φύλλο Δεδομένων Απορρήτου. Σημειώστε ότι αυτό το Φύλλο Δεδομένων Απορρήτου αποτελεί συμπλήρωμα της Υπηρεσίας Απορρήτου της Cisco Privacy Statement.

2. Επεξεργασία δεδομένων προσωπικού χαρακτήρα

Η Υπηρεσία επιτρέπει στους χρήστες να συνδέονται άμεσα με τρόπο που είναι σχεδόν τόσο προσωπικός όσο μια συνάντηση πρόσωπο με πρόσωπο. Ο οικοδεσπότης της σύσκεψης έχει την επιλογή να καταγράψει την συνάντηση και όλοι οι χρήστες έχουν την επιλογή να το μεταφορτώσουν και να διατηρήσουν τα αρχεία κοινής χρήσης κατά τη διάρκεια και μετά τη λήξη της σύσκεψης, τα οποία μπορεί να είναι ανιχνεύσιμα σε νομικό ζήτημα. Ο οικοδεσπότης της σύσκεψης ενημερώνει όλους τους παρευρισκόμενους πριν από την καταγραφή, εάν ο οικοδεσπότης της σύσκεψης προτίθεται να καταγράψει τη σύσκεψη. Εάν ο οικοδεσπότης της σύσκεψης δεν επιθυμεί να διατηρήσει το περιεχόμενο της σύσκεψης, αυτό εξαφανίζεται από την πλατφόρμα της Webex Meetings αμέσως μετά τη λήξη της σύσκεψης. Εάν είστε χρήστης και εργοδότης σας είναι ο Πελάτης που απέκτησε την Υπηρεσία, όλες οι πληροφορίες που περιγράφονται σε αυτό το Φύλλο Δεδομένων Απορρήτου είναι προσβάσιμες στον εργοδότη σας και υπόκεινται στις πολιτικές του εργοδότη σας σχετικά με την πρόσβαση, τη χρήση, την παρακολούθηση, τη διαγραφή, τη διατήρηση και την εξαγωγή πληροφοριών που σχετίζονται με την Υπηρεσία.

Ομοίως, εάν οι χρήστες συμμετέχουν σε συσκέψεις που φιλοξενούνται από χρήστες σε άλλες εταιρείες, ο οικοδεσπότης της σύσκεψης θα ελέγχει οποιαδήποτε εγγραφή συσκέψεως ή αρχεία που έχουν κοινοποιηθεί κατά τη διάρκεια της σύσκεψης, τα οποία θα υπόκεινται στις εταιρικές πολιτικές του οικοδεσπότη όσον αφορά την πρόσβαση, τη χρήση, παρακολούθηση, διαγραφή, διατήρηση και εξαγωγή πληροφοριών. Σημειώστε, η Cisco δεν έχει κανέναν έλεγχο και δεν είναι υπεύθυνη ή υπόλογη για το απόρρητο των πληροφοριών που έχετε μοιραστεί με άλλους. Ακόμα και μετά την κατάργηση των πληροφοριών από την πλατφόρμα συσκέψεων Webex, αντίγραφα αυτών των πληροφοριών ενδέχεται να παραμείνουν διαθέσιμα αλλού στο βαθμό που έχουν μοιραστεί με άλλους.

Αυτό το φύλλο δεδομένων απορρήτου καλύπτει τη σουίτα συσκέψεων της Cisco Webex, τις εκδηλώσεις της Cisco Webex και την εκπαίδευση της Cisco Webex. Εάν χρησιμοποιείτε την Υπηρεσία μαζί με τις ομάδες της Cisco Webex, ανατρέξτε στο φύλλο δεδομένων απορρήτου της Cisco Webex Teams (διαθέσιμο στο Cisco Trust Center) για περιγραφές των δεδομένων που μπορούν να συλλεχθούν και να υποβληθούν σε επεξεργασία σε σχέση με τις εν λόγω υπηρεσίες. Ο παρακάτω πίνακας απαριθμεί τις κατηγορίες προσωπικών δεδομένων που χρησιμοποιούνται από την Υπηρεσία και περιγράφουν τους λόγους για τους οποίους επεξεργαζόμαστε αυτά τα δεδομένα.

Πίνακας 1 Webex Συναντήσεις, Webex Εκδηλώσεις και Webex Εκπαίδευση

Κατηγορία Προσωπικών Δεδομένων	Τύποι Προσωπικών Δεδομένων	Σκοπός της Επεξεργασίας
Πληροφορίες Καταχώρισης	• Όνομα • Διεύθυνση ηλεκτρονικού ταχυδρομείου • Κωδικός πρόσβασης • Δημόσια Διεύθυνση IP • Πρόγραμμα περιήγησης • Αριθμός τηλεφώνου (προαιρετικά) • Ταχυδρομική Διεύθυνση (προαιρετικά) • Εικονίδιο (προαιρετικά) • Πληροφορίες Τιμολόγησης • Οι πληροφορίες χρήστη που περιλαμβάνονται στον κατάλογο Active Directory του πελάτη (εάν είναι συγχρονισμένος)	Χρησιμοποιούμε τις πληροφορίες καταχώρισης για : • Να εγγραφείτε στην Υπηρεσία • Να εμφανίσουμε την ταυτότητα του εικονιδίου χρήστη σας σε άλλους χρήστες • Να κάνουμε βελτιώσεις στην Υπηρεσία και σε άλλες προϊόντα και υπηρεσίες της Cisco • Να σας Παρέχουμε υποστήριξη • Να σας ειδοποιούμε για δυνατότητες και ενημερώσεις • Να σας αποστείλουμε τις διαφημιστικές ανακοινώσεις της Cisco

		• Να γίνει έλεγχος ταυτότητας και εξουσιοδότησης στην πρόσβαση στο λογαριασμό σας • Να σας χρεώσουμε για την Υπηρεσία • Να εμφανιστούν πληροφορίες καταλόγου σε άλλους χρήστες του Webex

Πληροφορίες υποδοχής της σύσκεψης και χρήσης	• Διεύθυνση IP
	• Αναγνωριστικός παράγοντας χρήστη
	• Τύπος υλικού
	• Τύπος και έκδοση λειτουργικού συστήματος
	• Έκδοση προγράμματος πελάτη
	• Διευθύνσεις IP κατά μήκος της διαδρομής δικτύου
	• Διεύθυνση mac του τελικού σημείου (ανάλογα με την περίπτωση)
	• Έκδοση υπηρεσίας
	• Δράσεις που έχουν αναληφθεί
	• Πληροφορίες περιόδου λειτουργίας σύσκεψης (τίτλος, ημερομηνία και ώρα, συχνότητα, μέση και πραγματική διάρκεια, ποσότητα, ποιότητα, δραστηριότητα δικτύου και συνδεσιμότητα δικτύου)
	• Αριθμός συσκέψεων
	• Αριθμός περιόδων λειτουργίας κοινής χρήσης οθόνης και κοινής χρήσης εκτός οθόνης
	• Αριθμός συμμετεχόντων
	• Πληροφορίες υποδοχής*
	  • Όνομα οικοδεσπότη της σύσκεψης
	  • Διεύθυνση URL τοποθεσίας σύσκεψης
		Χρησιμοποιούμε πληροφορίες κεντρικού υπολογιστή και χρήσης για:
		• Να κατανοήσετε τον τρόπο με τον οποίο χρησιμοποιείται η Υπηρεσία
		• Να διαγνώσουμε τεχνικά ζητήματα
		• Να διεξάγουμε ανάλυση στοιχείων και στατιστική ανάλυση σε συγκεντρωτική μορφή για την βελτίωση των τεχνικών εκτελέσεων της Υπηρεσίας
		• Να απαντήσουμε σε αιτήματα υποστήριξης πελατών
		• Να σας χρεώσουμε για την Υπηρεσία

	• Χρόνος έναρξης/λήξης της Σύσκεψης • Τύπος Εγγραφής • Πληροφορίες παρευρισκόμενων στη σύσκεψη* ▪ Όνομα χρήστη των παρευρισκόμενων ▪ Χρόνος έναρξης / λήξης της σύσκεψης ▪ Πληροφορίες εγγραφής • Ανάλυση οθόνης • Μέθοδος συνδέσμου • Πληροφορίες εκτέλεσης, αντιμετώπισης προβλημάτων και διαγνωστικών πληροφοριών • Πληροφορίες κλήσης των συμμετεχόντων, συμπεριλαμβανομένης της διεύθυνσης ηλεκτρονικού ταχυδρομείου, της διεύθυνσης IP, το όνομα χρήστη, τους αριθμούς τηλεφώνων, πληροφορίες της συσκευής δωματίου *χρησιμοποιούνται για σκοπούς τιμολόγησης	
Πληροφορίες που δημιουργούνται από το χρήστη	• Εγγραφές συσκέψεων και κλήσεων • Μεταγραφή εγγραφής κλήσεων • Μεταφορτωμένα αρχεία (μόνο για την Webex Εκδηλώσεις και Εκπαίδευση)	Χρησιμοποιούμε πληροφορίες που δημιουργούνται από τον χρήστη: • Για να παρέχουμε στην Υπηρεσία προαιρετικά εξαρτήματα που περιλαμβάνουν εγγραφές συσκέψεων

Βοήθεια τεχνικής υποστήριξης

Εάν ένας Πελάτης επικοινωνήσει με το Κέντρο Τεχνικής Βοήθειας (TAC) της Cisco για διάγνωση και επίλυση προβλημάτων, η Cisco TAC μπορεί να λάβει και να επεξεργαστεί προσωπικά δεδομένα από την Υπηρεσία. Το Φύλλο Δεδομένων Απορρήτου παροχής υπηρεσιών της Cisco TAC περιγράφει την επεξεργασία των δεδομένων αυτών.

Πλατφόρμα ανάλυσης Webex

Η Cisco Webex Control Hub Analytics παρέχει τάσεις χρήσης και πολύτιμες πληροφορίες που μπορούν να χρησιμοποιηθούν για να σας βοηθήσουν με στρατηγικές για να προωθήσουμε και να βελτιστοποιήσουμε την υιοθέτηση σε όλες τις ομάδες. Η πλατφόρμα Webex Analytics χρησιμοποιεί πληροφορίες εγγραφής, κεντρικού υπολογιστή και χρήση για την παροχή προηγμένων δυνατοτήτων και αναφορών ανάλυσης.

3. Διασυνοριακές μεταφορές

Η Υπηρεσία αξιοποιεί τα δικά της κέντρα δεδομένων για την παροχή της Υπηρεσίας σε παγκόσμιο επίπεδο. Εάν συμμετάσχετε σε μια σύσκεψη χρησιμοποιώντας το Cisco Webex Teams, παρακαλώ ανατρέξτε στο Φύλλο δεδομένων απορρήτου της Cisco Webex Teams για τις ισχύουσες πληροφορίες απορρήτου, συμπεριλαμβανομένων των τοποθεσιών του κέντρου δεδομένων. Τα κέντρα δεδομένων συσκέψεων της Webex βρίσκονται αυτήν τη στιγμή στις ακόλουθες χώρες (οι θέσεις των κέντρων δεδομένων ενδέχεται να αλλάζουν από καιρό σε καιρό και το παρόν Φύλλο Δεδομένων Απορρήτου θα ενημερωθεί ώστε να αντικατοπτρίζει αυτές τις αλλαγές):

[ΕΙΚΟΝΑ]

Θέσεις κέντρου δεδομένων της Cisco:	Θέσεις σημείου παρουσίας Internet (iPOP):
Άμστερνταμ, Ολλανδία	Άμστερνταμ, Ολλανδία
Μπανγκαλόρ, Ινδία	Καλιφόρνια, ΗΠΑ
Καλιφόρνια, ΗΠΑ	Χονγκ Κονγκ, Κίνα
Λονδίνο, Ηνωμένο Βασίλειο	Ιλλινόις, ΗΠΑ
Νέα Υόρκη, ΗΠΑ	Νιου Τζέρσεϋ, ΗΠΑ
Βόρεια Καρολίνα, ΗΠΑ*	Σίδνεϊ, Αυστραλία
Σιγκαπούρη, Σιγκαπούρη	Τέξας, ΗΠΑ
Σίδνεϊ, Αυστραλία	
Τέξας, ΗΠΑ*	
Τόκιο, Ιαπωνία	
Τορόντο, Καναδάς	
Βιρτζίνια, ΗΠΑ	

Οι πληροφορίες που δημιουργούνται από το χρήστη αποθηκεύονται στο κέντρο δεδομένων στην τοποθεσία του Πελάτη, όπως παρέχεται κατά τη διαδικασία παραγγελίας. Ωστόσο, τα δεδομένα χρέωσης αποθηκεύονται στο Τέξας, ΗΠΑ και Βόρεια Καρολίνα, ΗΠΑ. Τα δεδομένα του Webex Analytics αποθηκεύονται στην Καλιφόρνια, τις ΗΠΑ και το Τέξας, ΗΠΑ.

Ένα σημείο παρουσίας Internet (iPOP) χρησιμοποιείται για τη γεωγραφική δρομολόγηση της κυκλοφορίας από κοντινές περιοχές σε θέσεις κέντρου δεδομένων της Cisco. Προορίζεται για τη δρομολόγηση της κυκλοφορίας Webex Meeting μέσω της υποδομής της Cisco και τη βελτίωση της εκτέλεσης. Τα δεδομένα που δρομολογούνται μέσω αυτών των σημείων παρουσίας στο διαδίκτυο παραμένουν κρυπτογραφημένα και δεν αποθηκεύονται.

Η Cisco έχει επενδύσει σε διάφορους μηχανισμούς μεταφοράς για να επιτρέψει τη νόμιμη χρήση δεδομένων σε όλες τις δικαιοδοσίες. Ειδικότερα:

- .....
- .....
- .....
- .....
- .....

4. Έλεγχος πρόσβασης

Οι πελάτες και η Cisco μπορούν να έχουν πρόσβαση σε προσωπικά δεδομένα της Υπηρεσίας, όπως περιγράφεται στον παρακάτω πίνακα.

Κατηγορία Προσωπικών Δεδομένων	Ποιος έχει πρόσβαση	Σκοπός της επεξεργασίας

Πληροφορίες Καταχώρισης	Χρήστης μέσω της σελίδας My Webex Πελάτης μέσω της σελίδας διαχείρισης ιστοτόπου ή το Κέντρο ελέγχου Webex Cisco	Τροποποίηση, έλεγχος και διαγραφή πληροφοριών Τροποποίηση, έλεγχος και διαγραφή σύμφωνα με την πολιτική προσωπικών δεδομένων του Πελάτη Υποστήριξη της Υπηρεσίας σύμφωνα με την πρόσβαση στα δεδομένα της Cisco και της διαδικασίας ελέγχων ασφαλείας
Πληροφορίες υποδοχής και χρήσης	Ο οικοδεσπότης μέσω της σελίδας My Webex Ο Πελάτης μπορεί να δει αυτές τις πληροφορίες μέσω της σελίδα διαχείρισης ιστοτόπου, το κέντρο ελέγχου Webex ή μπορεί να παρέχεται διαφορετικά από τη Cisco Cisco	Προβολή πληροφοριών περιόδου λειτουργίας της σύσκεψης Προβολή πληροφοριών χρήσης, περιόδου λειτουργίας σύσκεψης και ρύθμισης παραμέτρων Υποστήριξη της Cisco και βελτίωση της Υπηρεσίας από την Cisco Webex Ομάδα υποστήριξης και ανάπτυξης συναντήσεων
Πληροφορίες που δημιουργούνται από το χρήστη	Χρήστης μέσω της σελίδας My Webex Πελάτης που χρησιμοποιεί APIs που παρέχονται με την Υπηρεσία ή μέσω της σελίδας διαχείρισης ιστοτόπου ή του Webex Κέντρο ελέγχου Cisco	Τροποποίηση, έλεγχος και διαγραφή με βάση τις προτιμήσεις του χρήστη Τροποποίηση, έλεγχος και διαγραφή σύμφωνα με την πολιτική προσωπικών δεδομένων του Πελάτη Ενώ η Cisco διαχειρίζεται την Υπηρεσία, η Cisco δεν θα έχει πρόσβαση σε αυτά τα δεδομένα εκτός αν είναι κοινόχρηστα με τη Cisco από τον Πελάτη, και θα έχει πρόσβαση μόνο σύμφωνα με τους ελέγχους πρόσβασης και ασφάλειας δεδομένων της Cisco.

	Άλλοι πελάτες και χρήστες (όταν γίνεται κοινοποίηση κατά τη διάρκεια μιας σύσκεψης)	Μπορεί να γίνει πρόσβαση στο περιεχόμενο που επιλέγετε να μοιραστείτε κατά τη διάρκεια μιας σύσκεψης από τους χρήστες στη σύσκεψη, όπου και αν βρίσκονται. Ακόμη και μετά την αφαίρεση πληροφορίων από την Υπηρεσία, αντίγραφα μπορεί να παραμείνουν προσβάσιμα αλλού στο βαθμό που έχουν μοιραστεί με άλλους.

5. Φορητότητα δεδομένων

Η Υπηρεσία επιτρέπει στους Πελάτες και τους χρήστες να εξάγουν όλες τις πληροφορίες που δημιουργούνται από το χρήστη. Ο διαχειριστής ενός Πελάτη μπορεί να το πράξει χρησιμοποιώντας APIs που παρέχεται με την Υπηρεσία (μόνο εγγραφές) ή μέσω της Σελίδας διαχείρισης ιστοτόπου, ενώ οι μεμονωμένοι χρήστες μπορούν να το πράξουν μέσω της ιστοσελίδας My Webex. Οι καταγραφές των συσκέψεων είναι διαθέσιμες σε ιδιόκτητες μορφές ARF και τυπικές μορφές mp4 ανάλογα με τον τύπο του λογαριασμού. Η Cisco προσφέρει ένα δωρεάν πρόγραμμα αναπαραγωγής ARF για να μετατρέψετε αρχεία ARF σε μορφή mp4.

Οι πελάτες επιτρέπεται να εξάγουν προσωπικά δεδομένα που συλλέγονται σχετικά με τους χρήστες τους στην πλατφόρμα συναντήσεων Webex χρησιμοποιώντας APIs ή μέσω της ιστοσελίδας Admin Configuration. Δεν υπάρχει χρονικός περιορισμό στην εξαγωγή αυτών των δεδομένων.

6. Διαγραφή και διατήρηση δεδομένων

Με την επιφύλαξη των πολιτικών εταιρικής διατήρησης του εργοδότη τους, οι χρήστες με ενεργή συνδρομή έχουν πλήρη έλεγχο στην έκταση των Πληροφοριών που δημιουργούνται από το χρήστη (π.χ. καταγραφές και αρχεία που ξεκινούν ή μεταφορτώνουν) αποθηκεύονται στην πλατφόρμα συσκέψεων της Webex και μπορούν να διαγράψουν τέτοιες Πληροφορίες που δημιουργούνται από το χρήστη από το λογαριασμό τους μέσω της σελίδας My Webex ανά πάσα στιγμή κατά τη διάρκεια της συνδρομής τους. Οι επαγγελματικοί πελάτες έχουν τη δυνατότητα να ορίσουν περιόδους διατήρησης σε ολόκληρο τον οργανισμό για καταγραφές με χρήση APIs. Μετά τον τερματισμό ή τη λήξη της Υπηρεσίας, οι Πληροφορίες που δημιουργούνται από το χρήστη διαγράφονται από την πλατφόρμα της συσκέψεων της Webex εντός 60 ημερών.

Οι πελάτες μπορούν να ζητήσουν τη διαγραφή άλλων προσωπικών δεδομένων που διατηρούνται στην πλατφόρμα συσκέψεων της Webex στέλνοντας ένα αίτημα στη Cisco (βλ. επιλογές επικοινωνίας στην ενότητα 11 παρακάτω) ή το άνοιγμα αιτήματος υπηρεσίας TAC, και εκτός εάν τα δεδομένα προσωπικού χαρακτήρα απαιτείται να διατηρηθούν για νόμιμους επιχειρηματικούς σκοπούς της Cisco, η Cisco προσπαθεί να διαγράψει τα δεδομένα που ζητήθηκαν από τα συστήματά της εντός 30 ημερών. Ο παρακάτω πίνακας περιγράφει την περίοδο διατήρησης και τους επιχειρηματικούς λόγους που η Cisco διατηρεί τα δεδομένα προσωπικού χαρακτήρα. Οι χρήστες που ζητούν διαγραφή άλλων προσωπικών δεδομένων που διατηρούνται στην πλατφόρμα συσκέψεων Webex πρέπει να ζητήσουν διαγραφή από το διαχειριστή της ιστοσελίδας του εργοδότη τους.

Κατηγορία Προσωπικών Δεδομένων	Περίοδος Διατήρησης	Λόγος και Κριτήρια Διατήρησης
Πληροφορίες Καταχώρισης	7 χρόνια από τότε που η Υπηρεσία τερματίστηκε	Τα δεδομένα που συλλέγονται ως μέρος της εγγραφής, συμπεριλαμβανομένων των πληροφοριών που παρέχονται από τους Πελάτες, ως μέρος της οικονομικής δέουσας επιμέλειας της Cisco, αποτελούν επιχειρηματικά αρχεία της Cisco και τηρούνται για τη συμμόρφωση με τις οικονομικές και ελεγκτικές πολιτικές της Cisco, καθώς και φορολογικές απαιτήσεις.
Πληροφορίες που δημιουργούνται από το χρήστη	Ενεργές συνδρομές: • Κατά την κρίση του Πελάτη ή του χρήστη Υπηρεσία που τερματίστηκε: • Διαγράφεται εντός 60 ημερών	Οι πληροφορίες που δημιουργούνται από το χρήστη δεν διατηρούνται στην Πλατφόρμα συσκέψεων της Webex όταν ο Πελάτης ή ο χρήστης διαγράφει αυτά τα δεδομένα.
Πληροφορίες υποδοχής και χρήσης	7 χρόνια από τότε που η Υπηρεσία τερματίστηκε	Πληροφορίες που παράγονται από συστήματα οργάνων και καταγραφής μέσω της χρήσης και λειτουργίας της Υπηρεσίας διατηρούνται ως μέρος του αρχείου της Cisco για την παροχή υπηρεσιών. Πληροφορίες χρήσης χρησιμοποιούνται για τη διεξαγωγή αναλυτικών στοιχείων και τη μέτρηση της στατιστικής εκτέλεσης διατηρούνται αλλά με ψευδώνυμο.

7. Ασφάλεια Προσωπικών Δεδομένων

Η Υπηρεσία θεσπίζει τεχνικά και οργανωτικά μέτρα ασφαλείας που αποσκοπούν στην προστασία των προσωπικών σας δεδομένων από μη εξουσιοδοτημένη χρήση πρόσβασης ή αποκάλυψης όπως απαιτεί ο νόμος. Πρόσθετες πληροφορίες σχετικά με την τεχνική κρυπτογράφησης συνοψίζονται στον πίνακα και τις παραγράφους παρακάτω.

Κατηγορία Προσωπικών Δεδομένων	Τύπος Κρυπτογράφησης
Πληροφορίες Καταχώρισης (εξαιρουμένων των κωδικών πρόσβασης, συζητείται κατωτέρω)	Κρυπτογραφημένο κατά τη μεταφορά, αλλά όχι σε ηρεμία
Κωδικοί Πρόσβασης	Κρυπτογραφημένοι και κατακερματισμένοι κατά τη μεταφορά και σε ηρεμία
Πληροφορίες υποδοχής και χρήσης	Κρυπτογραφημένο κατά τη μεταφορά, αλλά όχι σε ηρεμία
Πληροφορίες που δημιουργούνται από το χρήστη	Ξεκινώντας τον Μάιο του 2018, η Cisco παρουσίασε την κρυπτογράφηση των καταχωρίσεων σε ηρεμία. Οποιαδήποτε νέα καταχώριση δημιουργήθηκε στη σελίδα σας μετά την ενεργοποίηση αυτού του χαρακτηριστικού θα κρυπτογραφείται αυτόματα κατά τη μεταφορά και σε ηρεμία. Εγγραφές που δημιουργήθηκαν στην Webex Meetings FedRAMP-εξουσιοδοτημένη υπηρεσία κρυπτογραφούνται κατά τη μεταφορά και σε ηρεμία.

Προστασία δεδομένων σε ηρεμία

Η υπηρεσία κρυπτογραφεί ευαίσθητα δεδομένα σε ηρεμία. Τα δεδομένα που δεν κρυπτογραφούνται σε ηρεμία προστατεύονται από υψηλής ασφάλειας μηχανισμούς και επιχειρησιακές διαδικασίες προστασίας κέντρου δεδομένων.

Τα κέντρα δεδομένων webex meetings διαθέτουν υποδομή επικοινωνίας με που οδηγεί στην εκτέλεση, ενσωμάτωση, ευελιξία, δυνατότητα κλιμάκωσης και διαθεσιμότητα.

Κρυπτογράφηση κατά το χρόνο εκτέλεσης

Όλες οι επικοινωνίες στην πλατφόρμα συσκέψεων της Webex πραγματοποιούνται μέσω κρυπτογραφημένων καναλιών. Μετά τη δημιουργία μιας περιόδου λειτουργίας, όλα τα μέσα αναπαραγωγής (ήχος, VOIP, βίντεο, κοινή χρήση οθόνης και κοινή χρήση εγγράφων) κρυπτογραφούνται. Στη συνέχεια, η υπηρεσία κρυπτογραφεί εκ νέου τη ροή πολυμέσων πριν από την αποστολή του σε άλλους χρήστες. Σημειώστε ότι εάν ένας πελάτης επιτρέπει στους παρευρισκόμενους να συμμετέχουν στις συσκέψεις του χρησιμοποιώντας τα σημεία λήξης βίντεο τρίτων μερών, ενδέχεται αυτοί οι συμμετέχοντες να στέλνουν τα δεδομένα της σύσκεψης σας χωρίς κρυπτογράφηση στο Διαδίκτυο. Οι Ροές πολυμέσων που ρέουν από ένα χρήστη στους διακομιστές της Cisco Webex Meeting αποκρυπτογραφούνται αφού διασχίσουν τα τείχη προστασίας της Cisco. Αυτό επιτρέπει στη Cisco να παρέχει εγγραφή με βάση το διαδίκτυο και βάση SIP υποστήριξη κλήσεων για σημεία τερματισμού βίντεο.

Κρυπτογράφηση από άκρο σε άκρο (Προαιρετικό)

Για επιχειρήσεις που απαιτούν υψηλότερο επίπεδο ασφάλειας, η Υπηρεσία παρέχει επίσης κρυπτογράφηση από άκρο σε άκρο. Με αυτήν την επιλογή, η Υπηρεσία δεν αποκρυπτογραφεί τις ροές πολυμέσων. Σε αυτό το μοντέλο, η κυκλοφορία δεν μπορεί να αποκρυπτογραφηθεί από το διακομιστή συσκέψεων της Cisco Webex. Η επιλογή

κρυπτογράφησης από άκρο σε άκρο είναι διαθέσιμη για συσκέψεις Webex και υποστήριξη Webex. Σημειώστε ότι όταν είναι ενεργοποιημένη η κρυπτογράφηση από άκρο σε άκρο δεν υποστηρίζονται οι ακόλουθες δυνατότητες:

- Εγγραφές που βασίζονται σε δίκτυο
- Συμμετοχή πριν τον οικοδεσπότη
- Η πλατφόρμα αναπαραγωγής βίντεο της Cisco Webex (παλαιότερα γνωστή ως συνεργασία στο σύννεφο Meeting Rooms)

8. Τρίτοι πάροχοι υπηρεσιών (εκτελούντες την επεξεργασία)

Μοιραζόμαστε πληροφορίες εγγραφής, πληροφορίες οικοδεσπότη ή/και πληροφορίες χρήσης με παρόχους υπηρεσιών, υπεύθυνους επεξεργασίας ή τρίτα μέρη για να βοηθήσουν στην παροχή και τη βελτίωση της Υπηρεσίας. Τα δεδομένα που μοιράζονται μπορεί να περιλαμβάνουν συγκεντρωτικά στατιστικά στοιχεία ή δεδομένα με ψευδώνυμο. Όλη η ανταλλαγή πληροφοριών πραγματοποιείται σύμφωνα με τη Δήλωση Προστασίας Προσωπικών Δεδομένων της Cisco και συνάπτουμε συμβάσεις με τρίτους παρόχους υπηρεσιών που μπορούν να παρέχουν το ίδιο επίπεδο της προστασίας των δεδομένων και της ασφάλειας των πληροφοριών που μπορείτε να περιμένετε από τη Cisco. Δεν νοικιάζουμε ή πωλούμε τις πληροφορίες σας.

Εάν ένας Πελάτης αποκτήσει την Υπηρεσία μέσω ενός συνεργάτη της Cisco, ενδέχεται να κοινοποιήσουμε οποιαδήποτε ή όλες τις πληροφορίες που περιγράφονται στα παρόν Φύλλο Δεδομένων στον συνεργάτη. Οι πελάτες έχουν τη δυνατότητα να απενεργοποιήσουν αυτήν την κοινή χρήση πληροφοριών με συνεργάτες της Cisco.

9. Διαχείριση περιστατικών ασφάλειας πληροφοριών

Διαδικασίες παραβίασης και ειδοποίησης συμβάντων

Η ομάδα Προστασίας & Ιδιωτικότητας μαζί με τον Οργανισμό Προστασίας & Εμπιστοσύνης της Cisco συντονίζει τη Διαδικασία Απόκρισης Περιστατικών Δεδομένων και διαχειρίζεται την επιχείρηση σε όλη την αντιμετώπιση συμβάντων με επίκεντρο τα δεδομένα. Ο Διοικητής Περιστατικών κατευθύνει και συντονίζει την αντιμετώπιση της Cisco, αξιοποιώντας διάφορες ομάδες συμπεριλαμβανομένης της Ομάδας Αντιμετώπισης Περιστατικών Ασφάλειας Προϊόντων της Cisco (PSIRT), της Ομάδας Αντιμετώπισης Συμβάντων Ασφαλείας της Cisco (CSIRT) καιτης Ομάδας Προηγμένων Πρωτοβουλιών Ασφάλειας (ASIG).

Η PSIRT διαχειρίζεται την παραλαβή, τη διερεύνηση και τη δημόσια αναφορά τρωτών σημείων ασφαλείας που σχετίζονται με τα προϊόντα της Cisco και τα Δίκτυα. Η ομάδα συνεργάζεται με Πελάτες, ανεξάρτητους ερευνητές ασφαλείας, συμβούλους, βιομηχανικούς οργανισμούς και άλλους προμηθευτές για τον εντοπισμό πιθανών ζητημάτων ασφαλείας με τα προϊόντα και τα δίκτυα της Cisco. Το Κέντρο Ασφαλείας της Cisco περιγράφει λεπτομερώς τη διαδικασία αναφοράς των συμβάντων ασφαλείας.

Η Υπηρεσία Ειδοποιήσεων της Cisco επιτρέπει στους Πελάτες να εγγραφούν και να λάβουν σημαντικές πληροφορίες προϊόντων και τεχνολογίας της Cisco, συμπεριλαμβανομένων των συμβουλών ασφαλείας της Cisco για κρίσιμα και υψηλής σοβαρότητας θέματα ευαλωτότητας της ασφαλείας. Αυτή η υπηρεσία επιτρέπει στους Πελάτες να επιλέγουν το χρονοδιάγραμμα των ειδοποιήσεων και τη μέθοδο παράδοσης ειδοποιήσεων (μήνυμα

ηλεκτρονικού ταχυδρομείου ή τροφοδοσία RSS). Το επίπεδο πρόσβασης καθορίζεται από τη σχέση του συνδρομητή με τη Cisco. Εάν έχετε απορίες ή ανησυχίες σχετικά με οποιοδήποτε προϊόν ή ειδοποιήσεις ασφαλείας, επικοινωνήστε με τον αντιπρόσωπο πωλήσεων της Cisco.

10. **Πιστοποιήσεις και συμμόρφωση με τους νόμους περί απορρήτου**

Ο Οργανισμός Προστασίας & Εμπιστοσύνης και η νομική υπηρεσία της Cisco παρέχουν υπηρεσίες διαχείρισης κινδύνων και συμμόρφωσης και διαβούλευσης για να βοηθήσουν στην προώθηση της ασφάλειας και της κανονιστικής συμμόρφωσης στο σχεδιασμό των προϊόντων και των υπηρεσιών της Cisco. Η Υπηρεσία και οι υποκείμενες διαδικασίες της έχουν σχεδιαστεί για να ανταποκρίνονται στις υποχρεώσεις της Cisco βάσει του Γενικού Κανονισμού της ΕΕ για την προστασία των δεδομένων και άλλων νόμων περί προστασίας της ιδιωτικής ζωής σε όλο τον κόσμο.

Η Cisco αξιοποιεί τους ακόλουθους μηχανισμούς μεταφοράς της ιδιωτικότητας που σχετίζονται με τη νόμιμη χρήση δεδομένων σε όλες τις δικαιοδοσίες.

- .....
- .....
- .....
- .....
- .....

Εκτός από τη συμμόρφωση με τα αυστηρά εσωτερικά πρότυπά μας, η Cisco διατηρεί επίσης συνεχώς επικυρώσεις τρίτων για να αποδείξει τη δέσμευσή μας για την ασφάλεια των πληροφοριών. Η Υπηρεσία έχει λάβει τις ακόλουθες πιστοποιήσεις:

• ISO 27001 + 27017

• Βεβαίωση SOC 2 Τύπου II + C5

• FedRAMP

11. Γενικές πληροφορίες και Συνήθεις ερωτήσεις για τον GDPR

Για περισσότερες πληροφορίες σχετικά με τις τεχνικές και λειτουργικές δυνατότητες ασφαλείας της Υπηρεσίας, παρακαλώ ανατρέξτε στη Σελίδα Security White Paper

Για πιο γενικές πληροφορίες και συχνές ερωτήσεις σχετικά με το Πρόγραμμα Συμμόρφωσης ασφαλείας της Cisco και την ετοιμότητα της Cisco για τον GDPR, επισκεφθείτε την σελίδα [...]

1η Τροποποίηση: Πληροφορίες ατόμων για την Cisco Webex (Προαιρετικό)

Το παρόν Φύλλο Δεδομένων Απορρήτου περιγράφει την επεξεργασία προσωπικών δεδομένων (ή προσωπικών πληροφοριών ταυτοποίησης) από τις Πληροφορίες ατόμων της Cisco Webex Meetings και τις ομάδες Webex της Cisco.

1. Επισκόπηση των δυνατοτήτων πληροφοριών ατόμων

Η λειτουργία "Πληροφορίες ατόμων" ("Πληροφορίες ατόμων" ή "Δυνατότητα") παρέχει στους χρήστες της Cisco Webex ολοκληρωμένες, δημόσιες, διαθέσιμες επιχειρηματικές και επαγγελματικές πληροφορίες για τους συμμετέχοντες στη συνάντηση, παρέχοντας στους χρήστες το πλαίσιο και την αυξημένη διορατικότητα για τα άτομα με τα οποία συνεργάζονται.

Μόνο ο διαχειριστής τοποθεσίας του Πελάτη έχει τη δυνατότητα να ενεργοποιήσει τη δυνατότητα για τον οργανισμό και τους χρήστες του. Οι μεμονωμένοι χρήστες δεν μπορούν να επιλέξουν να χρησιμοποιήσουν τις Πληροφορίες ατόμων ανεξάρτητα από το διαχειριστή της τοποθεσίας τους. Οι χρήστες σε έναν ενεργοποιημένο οργανισμό μπορούν να εξαιρεθούν από τα Στατιστικά ατόμων, αποκρύπτοντας το προφίλ τους από την προβολή άλλων συμμετεχόντων στη σύσκεψη. Αυτό επιτυγχάνεται με δύο τρόπους:

1. Είσοδος σε σύσκεψη και επιλογή του συνδέσμου "Απόκρυψη προφίλ",

2. Είσοδος σε people.webex.com και κάνοντας κλικ στο "Απόκρυψη προφίλ"

2. Επεξεργασία δεδομένων προσωπικού χαρακτήρα

Οι Πληροφορίες Ατόμων συγκεντρώνουν επιχειρηματικά και επαγγελματικά προφίλ για συμμετέχοντες στη σύσκεψη χρησιμοποιώντας δημόσια διαθέσιμες και νόμιμες πηγές πληροφοριών, δημοσιευμένα συγγραφικά έργα, άρθρα ειδήσεων, αποτελέσματα μηχανών αναζήτησης, μέσω APIs και μέσω περιεχομένου που παρέχεται από τον κάτοχο του προφίλ.

Οι παρακάτω πίνακες παραθέτουν τα προσωπικά δεδομένα που χρησιμοποιούνται από τις Πληροφορίες Ατόμων και περιγράφουν τους λόγους για τους οποίους επεξεργαζόμαστε αυτά τα δεδομένα.

Κατηγορία Προσωπικών Δεδομένων	Τύποι Προσωπικών Δεδομένων	Σκοπός της Επεξεργασίας
Δημόσια διαθέσιμα επιχειρηματικά, επαγγελματικά και βιογραφικά δεδομένα	• Φωτογραφίες προφίλ • Ειδήσεις • Tweets • Συγγραφή Έργων • Βασικό σύστημα Εισόδου/Εξόδου • Ιστορικό Απασχόλησης • Ιστορία της Εκπαίδευσης	Για να προμηθευτούμε το προφίλ "Πληροφορίες ατόμων" και να ενεργοποιήσουμε την αναζήτηση εντός της δυνατότητας

	• Σύνδεσμοι Ιστού για ένα συγκεκριμένο άτομο .	
Πληροφορίες Λογαριασμού και Χρήσης	• Στοιχεία λογαριασμού σε επίπεδο χρήστη (συμπεριλαμβανομένου του ηλεκτρονικού ταχυδρομείου, του ονόματος και της αλληλεπίδρασης του ιστότοπου και χρήση πλατφόρμας)	• Για την παροχή υποστήριξης και βελτίωσης της δυνατότητας • Για την Ανάλυση προϊόντων (π.χ. συχνότητα επεξεργασιών προφίλ, επιτυχή φόρτωση προφίλ σε μια σύσκεψη κ.λπ.)
Δεδομένα Καταλόγου	• Εάν η επιλογή της υπηρεσίας καταλόγου Active Directory είναι ενεργοποιημένη από το διαχειριστή της τοποθεσίας, επαγγελματικές πληροφορίες, συμπεριλαμβανομένων των ακόλουθων μπορούν να συλλεχθούν από τον Κατάλογο της την εσωτερικής εταιρείας (όπως έχει επιλεγεί από το διαχειριστή της τοποθεσίας: • Τίτλος • Αριθμός τηλεφώνου • Τοποθεσία • Οργάνωση • Τμήμα • Φωτογραφία • Ρόλος • Δομή υποβολής εκθέσεων	• Για την αύξηση του προφίλ του χρήστη για τις Πληροφορίες ατόμων, παρέχοντας ειδικό πλαίσιο της εταιρείας σε συμμετέχοντες στη συνάντηση που ανήκουν στον ίδιο οργανισμό. Αυτά τα δεδομένα θα είναι ορατά μόνο σε συμμετέχοντες εντός του οργανισμού του χρήστη.
Πληροφορίες που δημιουργούνται από το χρήστη	• πληροφορίες που προσθέτει ο χρήστης στο προφίλ του στις Πληροφορίες Ατόμων	• Για την αύξηση του προφίλ του χρήστη για τις Πληροφορίες Ατόμων (ορατό σε χρήστες)

3. Διασυνοριακές μεταφορές

Τα δεδομένα από τις Πληροφορίες Ατόμων αποθηκεύονται σε τρίτους διακομιστές που παρέχονται από τις Υπηρεσίες Web της Amazon ("AWS") και την Algolia. Οι διακομιστές AWS βρίσκονται στο Όρεγκον, το Οχάιο και τη Βιρτζίνια. Οι διακομιστές της Algolia βρίσκονται στην Καλιφόρνια.

Η Cisco έχει επενδύσει σε διάφορους μηχανισμούς μεταφοράς για να καταστεί δυνατή η νόμιμη χρήση δεδομένων σε όλες τις δικαιοδοσίες, όπως αναλυτικά περιγράφεται στη Cisco Webex Meetings ή στα Δελτία Δεδομένων Απορρήτου των Ομάδων.

4.Έλεγχος πρόσβασης

Κατηγορία Προσωπικών Δεδομένων	**Ποιος έχει πρόσβαση**	**Σκοπός της πρόσβασης**
Δημόσια διαθέσιμα επιχειρηματικά, επαγγελματικά και βιογραφικά δεδομένα	Πελάτης Cisco Χρήστες Πληροφοριών Ατόμων εντός του οργανισμού του Πελάτη	Για την παροχή της Δυνατότητας
Πληροφορίες Λογαριασμού	Cisco	Για την Υποστήριξη της Εγγραφής Για την συσχέτιση των χρηστών με τα σωστά προφίλ Για την Ανάλυση προκειμένου να βελτιωθεί η Υπηρεσία
Δεδομένα Καταλόγου Πελάτη	Πελάτης Πελάτης (Προσωπικό και Διοίκηση) Χρήστες Πληροφοριών Ατόμων εντός του οργανισμού του Πελάτη Cisco	Για την ενεργοποίηση / απενεργοποίηση της Δυνατότητας Τα δεδομένα του Καταλόγου παρέχονται και διατηρούνται από τον διαχειριστή του πελάτη για να επιτρέπει την ένταξη στο προφίλ των Πληροφοριών Ατόμων Τα δεδομένα του καταλόγου εξάγονται και ολοκληρώνονται με τα δεδομένα του προφίλ του πελάτη για την υποστήριξη της ανάπτυξης του προφίλ
Πληροφορίες που δημιουργούνται από το χρήστη	Χρήστης	Οι χρήστες μπορεί να έχουν πρόσβαση στις δικές τους πληροφορίες που έχουν δημιουργήσει οι ίδιοι (για την επεξεργασία ή διαγραφή του περιεχομένου)

5.Φορητότητα δεδομένων

Οι μεμονωμένοι χρήστες μπορούν να λάβουν αντίγραφο των δικών τους προφίλ με Πληροφορίες Ατόμων, συμπεριλαμβανομένων των δεδομένων που έχουν οι ίδιοι δημιουργήσει, με επικοινωνία στο privacy@cisco.com .

6.Διαγραφή και διατήρηση δεδομένων

Τύπος Προσωπικών Δεδομένων	**Περίοδος Διατήρησης**	**Κριτήρια για την διατήρηση**
Δημόσια διαθέσιμα επιχειρηματικά και επαγγελματικά δεδομένα	Αποκτήθηκαν από δημόσιες ιστοσελίδες : Αόριστο Αποκτήθηκαν μέσω της χρήσης APIs από τρίτα μέρη, σύμφωνα με τις συμβατικές υποχρεώσεις	Επιχειρηματικά και επαγγελματικά δεδομένα διαθέσιμα δημοσίως προέρχονται από δημόσιες πηγές. Διατηρούνται επ' αόριστον με προεπιλογή. Κατόπιν αιτήματος, η δημοσιότητα και οι σύνδεσμοι στην πηγή των δεδομένων μπορεί να μειωθεί και να περιοριστεί από την παρακολούθηση και τη δημοσιότητα. Καθώς τα διαθέσιμα δημοσίως δεδομένα προέρχονται εκτός της Cisco Webex, κάθε μόνιμη αλλαγή ή αποκάλυψη πρέπει να απευθύνεται και να απαιτείται από την αρχική πηγή. Κατόπιν αιτήματος των χρηστών, τα δεδομένα μπορούν να αρχειοθετούνται προκειμένου να μην εμφανίζονται. Αυτό επιτρέπει στα δεδομένα να παραμένουν μόνιμα κρυμμένα αντί να επανεμφανίζονται με μια νέα αναζήτηση ενώ προηγουμένως έχουν απομακρυνθεί.
Πληροφορίες Λογαριασμού	Ενεργοί Συνδρομητές: Στην ευχέρεια του Πελάτη ή του χρήστη	Οι χρήστες μπορούν να ζητήσουν την απομάκρυνση των Πληροφοριών

	Απενεργοποιημένοι Λογαριασμοί: Διαγράφονται εντός τριάντα (30) ημερών	Λογαριασμού τους αποστέλλοντας αίτημα στην Υπηρεσία TACservice.H Cisco θα ανταποκριθεί σε ανάλογα αιτήματα εντός 30 ημερών.
Δεδομένα Καταλόγου	Ενεργοί Συνδρομητές: Στην ευχέρεια του Πελάτη ή του χρήστη Απενεργοποιημένοι Λογαριασμοί: Διαγράφονται εντός τριάντα (30) ημερών	Οι Διαχειριστές μπορούν να απενεργοποιήσουν την δυνατότητα Active Directory ενώ ακόμη ενεργοποιούν τις Πληροφορίες Ατόμων. Τα Δεδομένα Καταλόγου δύσκολα θα διαγραφούν στην προκείμενη περίπτωση της απενεργοποίησης. Τα δεδομένα που δεν είναι καταλόγου θα παραμείνουν,, με εξαίρεση το όνομα και το ηλεκτρονικό ταχυδρομείο για τους χρήστες που είχαν μόνο δεδομένα καταλόγου στο προφίλ τους πριν από την απενεργοποίηση.
Πληροφορίες που δημιουργούνται από το χρήστη	Ενεργοί Συνδρομητές: Στην ευχέρεια του Πελάτη ή του χρήστη Απενεργοποιημένοι Λογαριασμοί: Διαγράφονται εντός τριάντα (30) ημερών	Οι χρήστες μπορούν να διαγράψουν τις πληροφορίες που έχουν δημιουργηθεί από τον χρήστη οποτεδήποτε.

7. Προστασία προσωπικών δεδομένων

Κατηγορία προσωπικών δεδομένων	**Τύπος Κρυπτογράφησης**
Δημόσια διαθέσιμα επιχειρηματικά και επαγγελματικά δεδομένα	Κρυπτογραφημένα κατά τη μεταφορά, AES 256 για αποθήκευση, διαχείριση πλήκτρων μέσω AWS KMS
Πληροφορίες υποδοχής και χρήσης	Κρυπτογραφημένα κατά τη μεταφορά, AES 256 για αποθήκευση, διαχείριση πλήκτρων μέσω AWS KMS
Δεδομένα Καταλόγου	Κρυπτογραφημένα κατά τη μεταφορά, AES 256 για αποθήκευση, διαχείριση πλήκτρων μέσω AWS KMS
Πληροφορίες που δημιουργούνται από το χρήστη	Κρυπτογραφημένα κατά τη μεταφορά, AES 256 για αποθήκευση, διαχείριση πλήκτρων μέσω AWS KMS

8.Τρίτοι πάροχοι υπηρεσιών (εκτελούντες την επεξεργασία)

Οι συνεργάτες της Cisco με τους παρόχους υπηρεσιών με τους συνάπτουν συμβάσεις για την παροχή του ίδιου επιπέδου προστασίας δεδομένων και ασφάλειας πληροφοριών που μπορείτε να περιμένετε από τη Cisco. Μια τρέχουσα λίστα εκτελούντων την επεξεργασία για τις πληροφορίες ατόμων είναι παρακάτω:

Εκτελών την επεξεργασία	Προσωπικά Δεδομένα	Τύπος Υπηρεσίας	Τοποθεσία του κέντρου δεδομένων
Υπηρεσίες ιστότοπου Amazon Algolia Εύρος	• Δημοσίως διαθέσιμα επιχειρηματικά και επαγγελματικά δεδομένα • Πληροφορίες υποδοχής και χρήσης • Δεδομένα καταλόγου • Πληροφορίες που δημιουργούνται από τον χρήστη • Δημοσίως διαθέσιμα επιχειρηματικά και επαγγελματικά βιογραφικά δεδομένα • Πληροφορίες υποδοχής και χρήσης	Αποθήκευση στο Cloud Πλήρης αναζήτηση κειμένου Ανάλυση χρήστη	Όρεγκον Οχάιο Βιρτζίνια Καλιφόρνια Καλιφόρνια

2η Τροποποίηση: Δυνατότητα αναγνώρισης προσώπου

για την Cisco Webex Meetings (προαιρετικό)

Αυτή η προσθήκη στο Φύλλο Δεδομένων Απορρήτου της Webex Meetings περιγράφει την επεξεργασία των προσωπικών δεδομένων (ή προσωπικές πληροφορίες ταυτοποίησης) από τη λειτουργία αναγνώρισης προσώπου για την Cisco Webex Meetings.

1. Επισκόπηση των δυνατοτήτων αναγνώρισης προσώπου

Η Cisco παρουσίασε τη λειτουργία αναγνώρισης προσώπου ("Αναγνώριση προσώπου" ή "Δυνατότητα") για να παρέχει στους χρήστες του Webex Meetings τη δυνατότητα ταυτοποίησης και αναγνώρισης των εγγεγραμμένων συμμετεχόντων στη συνάντηση Webex (π.χ. συσχετισμός των ονομάτων των συμμετεχόντων με τις θέσεις τους σε ένα βίντεο σύσκεψης Webex), δίνοντας στους χρήστες αυξημένη σύνδεση με τους συμμετέχοντες στη σύσκεψη. Η δυνατότητα αναγνωρίζει ένα πρόσωπο μετατρέποντάς το σε αφηρημένο φορέα του προσώπου. Ένας φορέας προσώπου είναι ένας κατάλογος αριθμών που χαρακτηρίζουν τα προεξέχοντα χαρακτηριστικά του προσώπου ενός χρήστη που χρησιμοποιείται στη συνέχεια για τον προσδιορισμό του οριζόμενου στη σύσκεψη. Αυτό το επίπεδο άντλησης επιτρέπει στο σύστημα να αναγνωρίσει το ίδιο πρόσωπο ακόμα και όταν αλλάζουν πράγματα όπως ο φωτισμός και η θέση.

Η αναγνώριση προσώπου είναι απενεργοποιημένη από προεπιλογή και απαιτεί θετική ενέργεια τόσο από τον πελάτη όσο και από το χρήστη για να ενεργοποιηθεί. Πρώτον, ο διαχειριστής του πελάτη μπορεί να ενεργοποιήσει την Αναγνώριση προσώπου χρησιμοποιώντας το Κέντρο ελέγχου Webex. Ωστόσο, η δυνατότητα δεν θα είναι διαθέσιμη στο λογαριασμό του χρήστη μέχρι να την επιλέξει ο χρήστης στο https://settings.webex.com. Επειδή η λειτουργία βασίζεται στον φορέα προσώπου που προέρχεται από εικόνες προφίλ, ο χρήστης πρέπει να έχει μια εικόνα που λαμβάνεται κατά τη στιγμή της ενεργοποίησης.

2. **Επεξεργασία δεδομένων προσωπικού χαρακτήρα**

Εάν ο χρήστης επιλέξει τη δυνατότητα αναγνώρισης προσώπου, η ιστοσελίδα χρησιμοποιεί την κάμερα της συσκευής του χρήστη για να τραβήξει μια φωτογραφία προφίλ. Αυτή η εικόνα αποστέλλεται στο cloud Webex όπου ο αλγόριθμος της δυνατότητας δημιουργεί ένα φορέα προσώπου από την εικόνα, ώστε να μπορεί να χρησιμοποιηθεί για την αντιστοίχιση, όπως περιγράφεται περαιτέρω παρακάτω. Τόσο η εικόνα όσο και ο φορέας του προσώπου κρυπτογραφούνται και αποθηκεύονται με ασφάλεια. Η εικόνα μπορεί να χρησιμοποιηθεί για τη δημιουργία ενός νέου φορέα προσώπου σε περίπτωση που η Cisco ενημερώσει ή τροποποιήσει τον αλγόριθμο με τον οποίο δημιουργούνται οι φορείς προσώπου. Σε περίπτωση που ένας πελάτης ή χρήστης επικοινωνήσει με τη Cisco για υποστήριξη με τη Δυνατότητα, η Cisco μπορεί επίσης να χρησιμοποιήσει την εικόνα κατά τη διαδικασία αντιμετώπισης προβλημάτων. Κατά τη διάρκεια κάθε συνεδρίασης, δημιουργείται ένας δεύτερος φορέας προσώπου και στη συνέχεια αντιστοιχείται στο Webew cloud κατά το αποθηκευμένο φορέα του προσώπου. Αυτός ο δεύτερος φορέας προσώπου δεν διατηρείται.

Οι παρακάτω πίνακες παραθέτουν κατάλογο προσωπικών δεδομένων που χρησιμοποιούνται από τη Δυνατότητα και περιγράφουν τους λόγους για τους οποίους επεξεργαζόμαστε αυτά τα Δεδομένα.

Κατηγορία Προσωπικών Δεδομένων	Τύποι Προσωπικών Δεδομένων	Σκοπός της Επεξεργασίας
Εγγραφή	• Όνομα (Ονοματεπώνυμο) • Διεύθυνση ηλεκτρονικού ταχυδρομείου • Όνομα χρήστη	• Να παρουσιάσει το όνομα του αναγνωρισμένου χρήστη. • Να σας εγγράψει στη Δυνατότητα

		και στην ενεργοποίηση της.
Βιομετρικά Στοιχεία	• Εικόνα προσώπου του χρήστη • Επαλήθευση φορέα προσώπου	• Να δημιουργήσει επαλήθευση φορέα προσώπου και να παρέχει τη δυνατότητα αναγνώρισης προσώπου. • Να παράγει έναν νέο φορέα προσώπου στην περίπτωση της αλλαγής ή ενημέρωσης του αλγορίθμου της Δυνατότητας. • Να παρέχει τη Δυνατότητα αναγνώρισης προσώπου.
Πληροφορίες υποδοχής και χρήσης	• Πληροφορίες σχετικά με την ακρίβεια του προϊόντος, συμπεριλαμβανομένων: ▪ Της επιτυχίας / αποτυχίας της επαλήθευσης του φορέα προσώπου ▪ Της ανταπόκρισης του χρήστη	• Να παρέχει υποστήριξη και ανάλυση προϊόντος
Τοποθεσία	• Δεδομένα εγγύτητας του δωματίου συνάντησης	• Τα Δεδομένα εγγύτητας χρησιμοποιούνται για την βελτίωση της Αναγνώρισης Προσώπου για να εξασφαλιστεί ότι ο φορέας προσώπου επαληθεύτηκε με τους σωστούς χρήστες στις σωστές τοποθεσίες.
Ημερολόγιο	• Πληροφορίες του Ημερολογίου του δωματίου συνάντησης	• Οι Πληροφορίες Ημερολογίου χρησιμοποιούνται για την βελτίωση της Αναγνώρισης

		Προσώπου για να εξασφαλιστεί ότι ο φορέας προσώπου επαληθεύτηκε με τους σωστούς χρήστες στις σωστές τοποθεσίες .

3. Έλεγχος Πρόσβασης

Κατηγορία Προσωπικών Δεδομένων	**Ποιος έχει πρόσβαση**	**Σκοπός της πρόσβασης**
Εγγραφή	Cisco Πελάτης Χρήστες μέσω της σελίδας https://settings.webex.com/Cisco	• Να παρουσιάσει το όνομα του αναγνωρισμένου χρήστη. • Να σας εγγράψει στη Δυνατότητα και στην ενεργοποίηση της. • Για την παρακολούθηση της κατάστασης εγγραφής της αναγνώρισης προσώπου. • Για την παρακολούθηση και τροποποίηση των λεπτομερειών εγγραφής της αναγνώρισης προσώπου.
Βιομετρικά Στοιχεία	Cisco	• Για την παροχή της Δυνατότητας αναγνώρισης προσώπου. • Για την βελτίωση του αλγορίθμου • Για την αποκατάσταση των ζητημάτων ενός πελάτη ή χρήστη κατόπιν αιτήματος υποστήριξης.

		• Για την παροχή της Δυνατότητας αναγνώρισης προσώπου.
Πληροφορίες υποδοχής και χρήσης	Cisco	• Για την παροχή υποστήριξης και ανάλυσης προϊόντος.
Τοποθεσία	Cisco	• Τα Δεδομένα εγγύτητας χρησιμοποιούνται για την βελτίωση της Αναγνώρισης Προσώπου για να εξασφαλιστεί ότι ο φορέας προσώπου επαληθεύτηκε με τους σωστούς χρήστες στις σωστές τοποθεσίες.
Ημερολόγιο	Cisco	• Οι Πληροφορίες Ημερολογίου χρησιμοποιούνται για την βελτίωση της Αναγνώρισης Προσώπου για να εξασφαλιστεί ότι ο φορέας προσώπου επαληθεύτηκε με τους σωστούς χρήστες στις σωστές τοποθεσίες.

5.Φορητότητα Δεδομένων

Ενώ η Webex Meetings επιτρέπει στους Πελάτες και τους χρήστες να εξάγουν δεδομένα όπως περιγράφονται στο Τμήμα 5 του φύλλου Δεδομένων Απορρήτου της Webex Meetings, δεν υποστηρίζει την αυτόματη εξαγωγή Δεδομένων Αναγνώρισης Προσώπου :

6.Διαγραφή και διατήρηση δεδομένων

Τύπος Προσωπικών Δεδομένων	Περίοδος Διατήρησης	Λόγος και Κριτήρια Διατήρησης
Εγγραφή	Το όνομα χρήστη διατηρείται για όλους τους ενεργούς χρήστες	Το όνομα χρήστη χρησιμοποιείται για την παρακολούθηση της

	συσκέψεων της Webex. Μόλις ένας χρήστης διαγράφεται από το λογαριασμό ενός Πελάτη, το όνομα χρήστη διαγράφεται επίσης από την Υπηρεσία αναγνώρισης προσώπου. Όλες οι άλλες πληροφορίες εγγραφής δεν αποθηκεύονται ή διατηρούνται από την Υπηρεσία αναγνώρισης προσώπου καθώς αυτές οι πληροφορίες είναι ήδη αποθηκευμένες από τις συσκέψεις της Webex.	εγγραφής σας στη Δυνατότητα. Τα ονόματα εμφανίζονται σε μια αντιστοιχία στη δυνατότητα αναγνώρισης προσώπου.
Βιομετρικά Στοιχεία	Εικόνες: Οι χρήστες ελέγχουν την διατήρηση της εικόνα τους. Η εικόνα διατηρείται για όσο διάστημα η δυνατότητα είναι ενεργοποιημένη και ο χρήστης αφήνει την εικόνα συσχετιστεί με το προφίλ. Η εικόνα μπορεί να διαγραφεί οποιαδήποτε στιγμή από το χρήστη. Οι εικόνες για όλους τους χρήστες διαγράφονται κατά τη διακοπή λειτουργίας της Υπηρεσίας από τον Πελάτη. Οι φορείς του προσώπου διατηρούνται για όσο διάστημα διατηρούνται και οι εικόνες του προσώπου, αλλά αποθηκεύονται ξεχωριστά. Οι φορείς προσώπου διαγράφονται κατά την διακοπή λειτουργίας της Υπηρεσίας.	Η εικόνα χρησιμοποιείται για την παροχή της δυνατότητας αναγνώρισης προσώπου, του προσώπου φορέα σε περίπτωση επικαιροποίησης του αλγορίθμου και στην αποκατάσταση των προβλημάτων όταν ζητείται από έναν πελάτη ή χρήστη. Οι φορείς προσώπου χρησιμοποιούνται για την παροχή της Δυνατότητας αναγνώρισης προσώπου.

Πληροφορίες υποδοχής και χρήσης	2 εβδομάδες	Για την παροχή υποστήριξης και ανάλυσης προϊόντος.
Τοποθεσία	2 μέρες	Τα Δεδομένα εγγύτητας χρησιμοποιούνται για την βελτίωση της Αναγνώρισης Προσώπου για να εξασφαλιστεί ότι ο φορέας προσώπου επαληθεύτηκε με τους σωστούς χρήστες στις σωστές τοποθεσίες.
Ημερολόγιο	Η αναγνώριση προσώπου δεν αποθηκεύει ή διατηρεί τις πληροφορίες αυτές ξεχωριστά από ότι έχουν ήδη διατηρηθεί από την Webex Meetings.	Οι Πληροφορίες Ημερολογίου χρησιμοποιούνται για την βελτίωση της Αναγνώρισης Προσώπου για να εξασφαλιστεί ότι ο φορέας προσώπου επαληθεύτηκε με τους σωστούς χρήστες στις σωστές τοποθεσίες.

7.**Προστασία Προσωπικών Δεδομένων**

Ο παρακάτω πίνακας συνοψίζει τις τεχνικές κρυπτογράφησης των δεδομένων ειδικά για τη Δυνατότητα Αναγνώρισης Προσώπου.

Κατηγορία Προσωπικών Δεδομένων	**Τύπος Κρυπτογράφησης**
Εγγραφή	Κρυπτογραφημένο κατά τη μεταφορά, AES 256 για αποθήκευση
Εικόνες	Κρυπτογραφημένο κατά τη μεταφορά, AES 256 για αποθήκευση
Βιομετρικά στοιχεία	Κρυπτογραφημένο κατά τη μεταφορά, AES 256 για αποθήκευση
Πληροφορίες υποδοχής και χρήσης	Κρυπτογραφημένο κατά τη μεταφορά, AES 256 για αποθήκευση
Τοποθεσία	Κρυπτογραφημένο κατά τη μεταφορά, AES 256 για αποθήκευση

ΔΙΕΥΚΡΙΝΙΣΤΙΚΟ ΠΑΡΑΡΤΗΜΑ στο Συνημμένο Γ

Φύλλο Προστασίας Απορρήτου της Cisco Webex Meetings v. 4.1

Αυτό το διευκρινιστικό Παράρτημα έχει ημερομηνία έναρξης ισχύος την 13η.3.2020

Σε συνέχεια της ΣΥΜΒΑΣΗΣ ΠΛΑΙΣΙΟ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ("ΣΠΠΔ") που συνάφθηκε μεταξύ της **Cisco International Limited** με κύρια έδρα στο Ηνωμένο Βασίλειο, Αγγλία, 9-11 New Square Park, Bedfont Lakes, Feltham, TW14 8HA και των Συνδεδεμένων Μερών της ("**Cisco**") και του **Υπουργείου Παιδείας και Θρησκευμάτων της Ελλάδος** με έδρα στην οδό Ανδρέα Παπανδρέου αρ. 37, 15180 Μαρούσι, Αθήνα ("**Πελάτης**"), (από κοινού **"Μέρη"**) και αναφορικά με το Φύλλο Προστασίας Απορρήτου της Cisco Webex Meetings v. 4.1 ("ΦΠΑ") που επισυνάπτεται σε αυτή, τα έρη συμφωνούν ότι οι ακόλουθες επιμέρους ρυθμίσεις θα υπερισχύουν σε σχέση με το εν λόγω Φύλλο Δεδομένων Απορρήτου:

1. [PDS αρ. 2 – Πίνακας] **Διεύθυνση ηλεκτρονικού ταχυδρομείου**. Είναι αναγκαίο να ενεργοποιήσετε την υπηρεσία, αλλά οι χρήστες μπορούν να εισάγουν μια "ψεύτικη" διεύθυνση ηλεκτρονικού ταχυδρομείου.
2. [PDS αρ. 2] **Ανάλυση της πλατφόρμας Webex**. Αυτό αναφέρεται μόνο στα ανώνυμα δεδομένα επικοινωνίας.
3. [PDS αρ. 3] **Αντιστοίχιση Δεδομένων.** Είναι κατανοητό μεταξύ των Μερών ότι αυτή η δοκιμή των συνεδριάσεων Webex και τυχόν στοιχεία είναι μόνο για σκοπούς επίδειξης και, σε κάθε περίπτωση, η διασυνοριακή μεταφορά δεδομένων θα γίνεται σύμφωνα με τους όρους και τις προϋποθέσεις της MDPA.
4. [PDS αρ. 3] **Διασυνοριακή Μεταφορά Δεδομένων.** Η Cisco δια του παρόντος διευκρινίζει ότι το πλησιέστερο κέντρο δεδομένων βρίσκεται στο Άμστερνταμ. Συνεπώς, οι πληροφορίες που δημιουργούνται από τον χρήστη (μεταδεδομένα διάσκεψης) θα παραμείνουν εντός της ΕΕ. Σε περίπτωση μείζονος συμβάντος δυσλειτουργίας δικτύου στο κέντρο δεδομένων, οι πληροφορίες που δημιούργησε ο Χρήστης μπορεί, ωστόσο, να δρομολογηθούν σε άλλο κέντρο δεδομένων που καθορίζεται στο φύλλο δεδομένων ή στην αντιστοίχιση δεδομένων.
5. [PDS αρ. 3] **Μηχανισμός Μεταφοράς.** Η ΣΠΠΔ και αυτό το Διευκρινιστικό Παράρτημα θα υπερισχύουν.
6. [PDS αρ. 4] **Έλεγχος Πρόσβασης.** Όπως παρατίθενται στο Συνημμένο Α " ΕΚΘΕΜΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ" στο MDPA.
7. [PDS αρ. 5] **Φορητότητα Δεδομένων.** Δεδομένου ότι κατά τη διάρκεια της δοκιμής, η λειτουργία των εγγραφών είναι απενεργοποιημένη, το δικαίωμα αυτό δεν ισχύει. Οι πελάτες ή οι Χρήστες μπορούν, ωστόσο, να υποβάλουν αίτηση φορητότητας δεδομένων μόνο για πληροφορίες που δημιουργούνται από το Χρήστη. Σε αυτή την περίπτωση, η Cisco θα καταστήσει τις πληροφορίες που δημιουργούνται από το χρήστη διαθέσιμες στον Πελάτη σε μορφή που θα είναι κατάλληλη για τον Πελάτη και τους Χρήστες και θα επιτρέπει την εξαγωγή του αντίστοιχου API.
8. [PDS αρ. 6] **Η διαγραφή των 60 ημερών.** Όταν η Υπηρεσία τερματιστεί, ο Πελάτης, ωστόσο, έχει την επιλογή να διαγράψει τις πληροφορίες που δημιουργούνται από τον Χρήστη, εάν έχουν εφαρμοστεί νωρίτερα.
9. [PDS αρ. 8] **Τρίτα Μέρη.** Αυτό περιορίζεται μόνο σε "Περιορισμένες Πληροφορίες Υποδοχής και Χρήσης, κυκλοφορία μέσων συνάντησης", δηλαδή πληροφορίες επικοινωνίας και δεδομένα κίνησης μέσων, όχι προσωπικά δεδομένα που πρέπει να παρέχονται κατόπιν αιτήματος.

10. [PDS αρ. 11] **Πώς να ασκήσετε τα δικαιώματα του υποκειμένου των δεδομένων σας.** Τα δικαιώματα αυτά πρέπει να ασκούνται μόνο από ιδιώτες.
11. [PDS Προσθήκη Ένα] **Δυνατότητα πληροφοριών ατόμων.** Δεν εφαρμόζεται
12. [PDS Προσθήκη Δύο] **Αναγνώριση Προσώπου.** Δεν εφαρμόζεται

("Πελάτης)	(" Cisco")
	[ΥΠΟΓΡΑΦΗ]
Εξουσιοδοτημένη Υπογραφή	Εξουσιοδοτημένη Υπογραφή
Όνομα	Όνομα
	Julia O'shea
	ΔΙΕΥΘΥΝΤΡΙΑ ΟΙΚΟΝΟΜΙΚΗΣ ΔΙΑΧΕΙΡΙΣΗΣ
Ημερομηνία	Ημερομηνία
13.3.2020	[ΕΓΚΡΙΘΗΚΕ ΑΠΟ ΝΟΜΙΚΟ ΤΜΗΜΑ]

Η παρούσα στην ελληνική γλώσσα μετάφραση αφορά το συνημμένο στην αγγλική γλώσσα έγγραφο.

Αθήνα, 9/11/2020

Η μεταφράσασα δικηγόρος

ΕΙΡΗΝΗ ΚΑΠΕΛΛΑΚΗ
ΔΙΚΗΓΟΡΟΣ · ΑΜ ΔΣΑ 31124
ΠΕΝΤΕΛΗΣ 58 - ΚΗΦΙΣΙΑ 145 62
ΤΗΛ: 210 8013843 - 6945087480
e-mail: ekapellaki@gmail.com
ΑΦΜ: 103403699 - ΔΟΥ: ΚΗΦΙΣΙΑΣ

End User Information Form

For End Users of the Cisco Flex Plans

To purchase the Cisco Collaboration Flex Plan or Cisco Spark Flex Plan under the Enterprise Agreement ("EA") buying model for you and your Participating Affiliate(s), an authorized representative of the End User must complete this form in its entirety and sign it. This form will be used for provisioning and entitlement under the Flex Plan, as well as to ensure that you understand the terms of use that apply to your Flex Plan. Cisco will provide a quote to your reseller for the selected buying model, based upon the information that you provide in this form. Your reseller will in turn provide a quote to you. Your signature is required on this form prior to receiving access to the program.

End User Overview

Defined Terms Used in This Section

"**Participating Affiliates**" means Your Affiliates whose Meter counts are included on the EUIF.

"**Affiliate**" means, with respect to a party, any entity that directly or indirectly Controls, or is Controlled by, or is under common Control with such party. "**Control**" means to: (a) own more than 50% of the relevant party; or (b) be able to direct the affairs of the relevant party through any lawful means (*e.g.*, a contract that allows control).

"**End User**", "**You**" or "**Your**" mean the final purchasing entity as identified on the EUIF.

End User Information	
End User's full legal name	MINISTRY OF EDUCATION AND RELIGIOUS AFFAIRS
Address of End User's principal place of business	ANDREA PAPANDREOU 37 MAROUSI, ATTIKI, 151 80 GREECE

Participating Affiliates
Cisco requires any Participating Affiliate(s) for which you are purchasing coverage to be included in this End User Information Form. Cisco relies on this list to define the scope of the agreement, ensure accurate pricing, as well as effective provisioning and support.
Participating Affiliate(s)
☐ None ☐ Only listed Participating Affiliates (to be recorded immediately below)
Participating Affiliates

Cisco Collaboration

Additional Defined Terms Used in This Section

"**Employees**" means full or part-time employees of You and Your Participating Affiliates.

"**Contractors**" means non-Employees who (i) work on Your or Your Participating Affiliates' behalf, (ii) whose work is under Your or Your Participating Affiliates' control or supervision pursuant to a consulting, staffing or other similar written contract, and (iii) have access to Your or Your Participating Affiliates' systems or networks in the ordinary course of providing their services to You or Your Participating Affiliates.

"**Knowledge Workers**" means You and Your Participating Affiliates' Employees and Contractors who utilize devices capable of running the Software, Cloud Services, or related browser plug-ins as part of their job duties.

Your Suite(s) purchased under the Flex Plan
Cisco requires customers purchasing Enterprise Agreement to complete and sign this End User Information form. You will have access to the Software and/or Services in the Suite(s) you purchase and which are identified on your EUIF.
☐ Meetings Enterprise Agreement ☐ Calling Enterprise Agreement

Knowledge Worker Count Worksheet

Cisco Flex Plan EA Offers	Value
Total quantity of Employees of the End User and Participating Affiliates	a.
+ Total quantity of Contractors of the End User and Participating Affiliates	b.
= Total Employees and Contractors (add a. and b.)	c.
Knowledge Worker count	d.

Cisco Collaboration Flex Plan Education EA only	Value
Total quantity of faculty/staff (Knowledge Workers) at educational institution	a. 82000
Knowledge Worker faculty/staff count	b.
Total quantity of students at educational institution (expected to have access to Meetings) - These are not part of the Knowledge Worker count.	1

End User Information Form Acceptance

THE UNDERSIGNED REPRESENTS THAT THEY ARE AUTHORIZED TO SIGN THIS FORM ON THE END USER'S BEHALF AND THAT THE INFORMATION PROVIDED, INCLUDING METER COUNTS FOR THE END USER AND ITS PARTICIPATING AFFILIATES, IS ACCURATE AS OF THE DATE OF SIGNATURE. THE UNDERSIGNED UNDERSTANDS THAT THE APPROVED SOURCE RELIES UPON THE INFORMATION PROVIDED IN THIS FORM TO ESTABLISH THE PRICE QUOTE FOR THE END USER'S PURCHASE.

FOR FLEX PLAN EA: I HAVE READ THE ENTERPRISE AGREEMENT PROGRAM TERMS ("PROGRAM TERMS") INCLUDED BELOW, AND UNDERSTAND THAT IN THE EVENT OF AN EA PURCHASE, THESE PROGRAM TERMS APPLY TO THE SOFTWARE AND SERVICES AS DESCRIBED IN THE PROGRAM TERMS.

Full Legal Name of the End User Organization (e.g., company, government entity) You Represent	
Last Name, First Name	Gika Anastasia
Title	Secretary General of Ministry of Education
Date	January 7, 2021 | 9:59:42 PST
End User Authorized Representative Signature	DocuSigned by: 3D040E27E3384AC...

Cisco Enterprise Agreement Program Terms and Conditions for End Users

These terms and conditions together with the applicable Enrollment Descriptions and EUIF (collectively, "**EA Program Terms**") govern any Suites that You order under the Cisco Enterprise Agreement Program ("**Purchased Suites**"). The EA Program Terms do not modify the terms of any Cisco products or services You purchase outside of the Cisco Enterprise Agreement Program.

By signing these terms and conditions You agree to the EA Program Terms and the Licensing Documents. If You do not agree to the EA Program Terms or Licensing Documents, You may not Consume the Software or Cloud Services. Notwithstanding the foregoing, You are not obligated to make a purchase by entering into the EA Program Terms, and neither the EA Program Terms nor the Licensing Documents will apply until You place an order as further described in section 1, below.

1. **Orders.** To purchase Suites under the EA Program Terms, You must first submit the applicable EUIF and Enrollment Description signed by Your authorized representative to the Approved Source. The EUIF must list: (a) Your Participating Affiliates; (b) the Purchased Suites; (c) the Suite Term; and (d) accurate Meter counts for You and all Participating Affiliates. You will then be required to place an order for the Purchased Suites according to the process set forth in Your purchasing agreement with the Approved Source.

2. **Access To Purchased Suites.** Subject to Your payment of the applicable fees to the Approved Source, Cisco will grant You and all Participating Affiliates the right to Consume the Purchased Suites during the Suite Term via the EA Workspace or as otherwise set forth in the applicable Enrollment Description. You must pay for all Software and Cloud Services Consumed. You are responsible for keeping all login credentials to the EA Workspace secure and for the actions of any individual You or a Participating Affiliate authorize to access the EA Workspace, including payment for any Software or Cloud Services Consumed by such individuals.

3. **Enterprise-wide Commitment.** The Approved Source relies on the information You provide in the EUIF to establish the Enterprise-wide Commitment. During the Suite Term, Your payment obligation related to the Enterprise-wide Commitment may increase as a result of any of the following: (a) You exceed the Initial Growth Cap (as described in section 5); (b) You exceed the Initial Entitlement or the previous year's Entitlement subject to a True Forward (as described in section 6); or (c) You purchase an additional Suite (as described in section 9).

4. **Term & Termination.**

   a. **Term.** The Term of the EA Program Terms will commence on the date of signature below and continue so long as there is an active Purchased Suite, unless earlier terminated in accordance with section 4(c)(i), below.

   b. **Suite Term.** The Suite Term for each Purchased Suite will commence on the Suite Start Date and last for the period set forth in the EUIF, unless terminated in accordance with section 4(c)(i), below.

   c. **Termination.**

      i. Either party may terminate the EA Program Terms or a Purchased Suite if the other party materially breaches the EA Program Terms and does not cure the breach within 30 days of written notice of the breach.

ii. In the event of Your uncured material breach of the EA Program Terms for non-payment of fees to the Approved Source, Cisco may, in lieu of termination of the Program Terms pursuant to section 4(c)(i), suspend Your right to Consume the Software and Cloud Services in the Purchased Suite and suspend Your access to the EA Workspace, until Your breach has been cured.

iii. In the event of Your termination for Cisco's uncured material breach of the EA Program Terms, Cisco will refund to the Approved Source (or You, if You purchased directly from Cisco) any fees You paid covering the period after the effective date of termination.

iv. Other than as provided in this section 4 and to the extent permitted by law, the EA Program Terms and any orders placed thereunder are non-cancellable and may not be terminated.

d. **Effect of Termination; End of Suite Term.** Upon termination or at the end of the Suite Term:

i. The following rights will terminate with respect to the Purchased Suites: (1) Your right to Consume Cloud Services and Software; (2) Your right to access the EA Workspace; (3) Your right to receive Support Services; and

ii. You must destroy the product activation keys (PAKs) provided in connection with the Purchased Suites.

5. **Initial Growth Cap.** If You exceed the Initial Growth Cap during the first six months of the Suite Term, the Approved Source may charge You for such Consumption above the Initial Growth Cap. If the Purchased Suite includes a Growth Allowance (described in the applicable Enrollment Description), the Growth Allowance cannot be used to offset fees for exceeding the Initial Growth Cap.

6. **True Forward.**

a. Cisco performs a True Forward for the Purchased Suites on each anniversary of the Suite Start Date. On the first anniversary of the Suite Start Date, if You have exceeded the Initial Entitlement, the Approved Source will charge You for the Consumption above the Initial Entitlement through the remainder of the Suite Term. On each subsequent anniversary of the Suite Start Date, the Approved Source will charge You for any Consumption above the previous year's Entitlement through the remainder of the Suite Term.

b. Your True Forward payment obligation for each Purchased Suite will be calculated by comparing Your Consumption of Software and Cloud Services to Your Entitlement for the previous year. Any payment owed to the Approved Source will be determined as follows and reflected in the price quote from the Approved source: the unit price less any applicable discount or incentive multiplied by the quantity by which You exceeded Your then-current Entitlement. The price used to calculate any True Forward fees will be established when You place the order for each Purchased Suite.

c. For some Suites, a portion of Your True Forward payment obligation may be offset by the residual value remaining in Software or Cloud Services in the same Suite. This process is called value shift, and the applicable Enrollment Description indicates whether and to the extent value shift applies to a given Suite.

d. There is no fee for exceeding the Entitlement in the final year of the Suite Term.

7. **Updates to Purchased Suites.** Cisco may enhance or refine the Purchased Suites at no additional cost to You. Such updates will not materially reduce the core functionality of the Purchased Suites.

8. **End of Life**. Notwithstanding anything in the EA Program Terms to the contrary, Cisco reserves the right to discontinue a Suite with at least three years' prior notice. If a Purchased Suite is discontinued, Cisco will either: (a) provide You a substantially similar replacement Suite for the remainder of the Suite Term; or (b) issue a credit to the Approved Source (or You, if You purchased directly from Cisco) for any fees You paid for the Purchased Suite covering the period after the last date such Purchased Suite is available for You to Consume. Such credit can be applied towards the future purchase of Cisco products and services.

9. **Purchasing Additional Suites**. You may purchase additional Suites by submitting a new EUIF and order to the Approved Source. Additional Suites may co-terminate with a pre-existing Purchased Suite provided there are at least 12 months remaining in the Suite Term of such pre-existing Purchased Suite. Otherwise, additional Purchased Suites will be given a new Suite Term and will be subject to the then-current EA Program Terms in accordance with section 10, below.

10. **Modifications**. As our business evolves, Cisco may modify the EA Program Terms. Updated EA Program Terms do not apply to pre-existing Purchased Suites or to future orders that co-terminate to a pre-existing Purchased Suite, which will be governed by the version of the EA Program Terms already in effect for the pre-existing Purchased Suite.

11. **Participating Affiliates**. You are responsible for Your Participating Affiliates' compliance with the EA Program Terms.

12. **Support Services**. Basic Support Services are included in the price of the Purchased Suite and described in the applicable Enrollment Description and Licensing Documents. Higher levels of Support Services may be available for You to purchase and, if You elect to do so, will be described in documentation provided to You at the time of purchase.

13. **Importation Fee for Embedded Software**. For Purchased Suites that include Embedded Software, the value of Embedded Software will be deducted from the purchase price of the related Cisco hardware. If You are required to pay an Importation Fee, Your jurisdiction may use the value of both the hardware and Embedded Software to calculate the Importation Fee. Accordingly, the Importation Fee on the value of the combined products may be higher than if calculated solely using the price of the hardware.

14. **Delivery of Embedded Software**. Embedded Software is delivered pre-installed on Cisco hardware to the address provided on the purchase order for the Cisco hardware. Your use of the smart licensing account Cisco designates for the Embedded Software will ensure accurate pricing of the Embedded Software.

15. **No Assignment & Transfer**. Neither the EA Program Terms, nor any right or obligation herein may be assigned or transferred by a party (including under Cisco's Software Transfer and Relicensing Policy) without the other party's prior written consent, which may not be unreasonably conditioned, withheld, or delayed. Any attempted assignment without the other party's consent shall be void and of no effect. Notwithstanding the foregoing, Cisco may assign the EA Program Terms and any right or obligation herein to a Cisco Affiliate without Your consent.

16. **Verification**. Upon reasonable request from Cisco, You will assist Cisco in verifying the quantity of Software and Cloud Services that You have Consumed. If the verification discloses Consumption above Your then-current Entitlement, the Approved Source will charge You for the excess Consumption in accordance with the EA Program Terms.

17. **Combined Discounts**. The pricing, discounts, and other incentives offered in connection with a Purchased Suite may not be combined with any other price reductions, discounts, promotional pricing, rebates, credits, trade-in, or other pricing programs or incentives offered by Cisco unless expressly agreed by Cisco in writing.

18. **Entire Agreement**. The EA Program Terms constitute the entire agreement between the parties concerning the Cisco Enterprise Agreement Program and supersede all prior oral or written communications between the parties concerning the program.

19. **Order of Precedence**. The documents comprising the EA Program Terms are complimentary, and to the extent possible, construed and interpreted consistently. In the event of an inconsistency, conflict, or ambiguity between the EA Program Terms, the order of precedence for any Purchased Suite is first the EUIF, then the Enrollment Description, and then these terms and conditions. The EA Program Terms take precedent over the applicable Licensing Documents.

20. **Definitions**.

    a. "**Affiliate**" means, with respect to a party, any entity that directly or indirectly Controls, or is Controlled by, or is under common Control with such party. "**Control**" means to: (a) own more than 50% of the relevant party; or (b) be able to direct the affairs of the relevant party through any lawful means (*e.g.*, a contract that allows control).

    b. "**Approved Source**" means Cisco or a Cisco authorized reseller, distributor, or systems integrator.

    c. "**Cisco**" means Cisco Systems, Inc. or its applicable Affiliate delivering the EA Program Terms.

    d. "**Cloud Service**" means the Cisco hosted software-as-a-service listed in the applicable Enrollment Description.

    e. "**Consume**" or "**Consumption**" means to download, install, activate, provision, enable, or otherwise access Software or Cloud Services.

    f. "**EA Program**" has the meaning given to it in the introductory paragraph.

    g. "**EA Program Terms**" has the meaning given to it in the introductory paragraph.

    h. "**EA Workspace**" means the portal from where You Consume Software and Cloud Services and view and manage Your Entitlement.

    i. "**Embedded Software**" means Software that is delivered on newly purchased Cisco hardware.

    j. "**End User**," "**You**," or "**Your**" means the final purchasing entity as identified on the EUIF.

    k. "**Enterprise-wide Commitment**" means Your purchase commitment in the Purchased Suite for You and all Participating Affiliates, as reflected on the EUIF.

    l. "**Entitlement**" means, at any point in time during the Suite Term, the type and quantity of Software and Services as determined by the Meter counts for which You have already paid the applicable fees to the Approved Source.

    m. "**Enrollment**" means a combination of Suites belonging to the same Cisco product family. Cisco DNA, Cisco Data Center, Cisco Security Choice, Cisco Meraki, and Cisco Collaboration Flex Plan each represent an Enrollment.

n. "**Enrollment Description**" means the supplemental program terms and description governing an Enrollment.

o. "**EUIF**" means the End User Information Form for the Purchased Suite.

p. "**EULA**" mean's Cisco End User License Agreement, available at cisco.com/go/eula.

q. "**Growth Allowance**" means the right to exceed the Initial Entitlement without incurring additional fees as set forth in the applicable Enrollment Description.

r. "**Importation Fee**" means an import duty or tax on the purchase of Cisco hardware.

s. "**Initial Entitlement**" means Your Entitlement at the start of the Suite Term as determined by the Meter counts for You and all Participating Affiliates provided on the EUIF.

t. "**Initial Growth Cap**" means 105% of the Initial Entitlement.

u. "**Licensing Documents**" means the EULA and SEULAs for the Software and the EULA and ODs for the Cloud Services in the Purchased Suites (or similar terms existing between You and Cisco). The applicable Licensing Documents are listed in the Enrollment Description for each Purchased Suite.

v. "**Meter**" means the unit of measurement for Software or Cloud Services Consumption.

w. "**OD**" means the offer description and supplemental licensing terms governing Cloud Services.

x. "**Participating Affiliates**" means Your Affiliates whose Meter counts are included on the EUIF.

y. "**Purchased Suites**" has the meaning given to it in the introductory paragraph.

z. "**Services**" means both Cloud Services and Support Services.

aa. "**SEULA**" means the supplemental licensing terms governing Software.

bb. "**Software**" means the Cisco software listed in the applicable Enrollment Description.

cc. "**Suite**" means a combination of Software and Services in an Enrollment.

dd. "**Suite Start Date**" means, with respect to each Purchased Suite, the earliest date any Software or Cloud Service in the Purchased Suite is made available for You to Consume.

ee. "**Suite Term**" means, with respect to each Purchased Suite, the duration of the Purchased Suite.

ff. "**Support Services**" means maintenance, technical assistance, or other support provided for the Software and Cloud Services in a Purchased Suite.

gg. "**Term**" means the duration of the EA Program Terms.

hh. "**True Forward**" means an annual adjustment to account for exceeding the previous year's Entitlement.

Cisco Collaboration Flex Plan Enrollment Description & Supplemental EA Program Terms

This Enrollment Description lists the available Suites and additional terms and conditions that apply to the Cisco Collaboration Flex Plan Enrollment. You may purchase any or all of the Suites available under the Cisco Collaboration Flex Plan Enrollment, but the collection of Software and Cloud Services that comprise a Suite may not be modified.

Suite	Included Licenses	License Type	Licensing Documents	Meter
Cisco Collaboration Flex Plan Meetings Enterprise Agreement	Cisco Meeting Server	Software	Cisco Collaboration Flex Plan OD; EULA	Deployed Knowledge Worker
	Cisco Webex Meetings	Cloud Service		
	Cisco Webex Teams	Cloud Service		

Suite	Included Licenses	License Type	Licensing Documents	Meter
Cisco Collaboration Flex Plan Calling Enterprise Agreement	Cisco Webex Teams	Cloud Service	Cisco Collaboration Flex Plan OD; EULA	Deployed Knowledge Worker
	Cisco Webex Calling; or Cisco Webex Calling for SP; or Cisco Webex Calling (formerly Cisco Spark Call)	Cloud Service		
	UCM Cloud Calling	Cloud Service		
	Partner-Hosted Unified Communications Calling	Software		
	On-Premises Unified Communications Manager Calling	Software		

Suite	Included Licenses	License Type	Licensing Documents	Meter
Cisco Collaboration Flex Plan for Education Meetings Enterprise Agreement	Cisco Meeting Server	Software	Cisco Collaboration Flex Plan OD; EULA	Deployed Knowledge Worker; Student
	Cisco Webex Meetings	Cloud Service		
	Cisco Webex Teams	Cloud Service		

Suite	Included Licenses	License Type	Licensing Documents	Meter
Cisco Collaboration Flex Plan for Education Calling Enterprise Agreement	Cisco Webex Calling (formerly Cisco Spark Call)	Cloud Service	Cisco Collaboration Flex Plan OD; EULA	Deployed Knowledge Worker
	On-Premises Unified Communications Manager Calling	Software		

Suite	Included Licenses	License Type	Licensing Documents	Meter
Cisco Collaboration Flex Plan Enterprise Agreement for Public Sector	Cisco FedRAMP Webex Meetings	Cloud Service	Cisco Collaboration Flex Plan OD; EULA	Deployed Knowledge Worker
	Unified Communications Manager Cloud for Government	Cloud Service		

Supplemental Terms and Conditions

Applicable Meters

The Meter for the Cisco Collaboration Flex Plan Enrollment is the number of Deployed Knowledge Workers.

"**Deployed Knowledge Worker**" means a Knowledge Worker who has a profile configured within the Software or Cloud Service provisioning platform and associates that profile with the applicable desk phone, Jabber client, Webex Teams client, mobile phone, video device, or personal computing device. You must assign each Knowledge Worker a cloud, on-premises, or hosted account to be treated as a single Deployed Knowledge Worker. A Knowledge Worker who is assigned more than one configuration (cloud, on-premises, or hosted) will be counted as multiple Deployed Knowledge Workers. If at any time during the Term You change a Deployed Knowledge Worker's deployment type, You may be required to pay additional applicable fees immediately upon such change. "**Knowledge Worker**" means an employee or contractor who utilizes devices capable of running the Software, Cloud Services, or related browser plug-ins as part of their job duties.

If You purchase the Cisco Collaboration Flex Plan for Education Meetings Enterprise Agreement Suite, Your Students may Consume the Purchased Suite free of charge. "**Student**" means an individual who is currently enrolled or registered at Your institution for academic study on a full- or part-time basis. Employees, contractors, alumni, former students, prospective students, and students on an extended leave or indefinite absence are not considered Students. You will be required to provide a Student count on the EUIF. Thirty days prior to the True Forward event, you or your Reseller must update your order to reflect the number of Students provisioned at that time, which will be used to determine if you have exceeded your Growth Allowance. Failure to update your subscription will result in the additional Students being counted as Deployed Knowledge Workers for purposes of the True Forward.

Access to Purchased Suites

The Cisco Collaboration Flex Plan Enrollment does not utilize the EA Workspace. Subject to Your payment of the applicable fees to the Approved Source, Cisco will grant You and all Participating Affiliates access to the Purchased Suites via automated integrated electronic delivery tools and email notification to the point of contact designated in the order.

Purchasing Additional Suites

During the Suite Term, You may add another Cisco Collaboration Flex Plan Suite without submitting a new EUIF.

Common Area Licenses

Common area licenses are calling licenses not associated with Knowledge Workers that are intended to be used in lobbies, conference rooms, and other public spaces. If Your Consumption of common area licenses exceeds 50% of Your then-current Deployed Knowledge Worker count, the Approved Source may charge You for such excess Consumption.

Term and Termination

At the end of the Suite Term, the Purchased Suite will automatically renew for one year (a "**Renewal Suite Term**") unless: (a) You elect on the order not to auto-renew; or (b) at least 30 days before the end of then-current Suite Term, You notify the Approved Source of Your intention not to renew the Purchased Suite. If the Growth Allowance has not been exceeded, the Purchased Suite will renew for the Knowledge Worker count on the EUIF. If the Growth Allowance has been exceeded, the Purchased Suite will renew for the Deployed Knowledge Worker count at the end of the then-current Suite Term.

Notwithstanding the foregoing, the Approved Source will notify You of any fee changes reasonably in advance of the Renewal Term. The new fees will apply for the upcoming Renewal Term unless You notify the Approved Source that You do not accept the fee changes before the next Suite Start Date.

Growth Allowance

The Growth Allowance for the Cisco Collaboration Flex Plan Enrollment is 20%. During the Suite Term, You may Consume up to 120% of the Initial Entitlement without incurring any additional charges. The True Forward is calculated once You exceed the Growth Allowance. For clarity, if You exceed the Initial Entitlement but do not exceed the Growth Allowance, You will not incur any True Forward charges.

Support Services

The basic Support Services are set forth in the Cisco Collaboration Flex Plan OD.

End User Information Form

For End Users of the Cisco Flex Plans

To purchase the Cisco Collaboration Flex Plan or Cisco Spark Flex Plan under the Enterprise Agreement ("EA") buying model for you and your Participating Affiliate(s), an authorized representative of the End User must complete this form in its entirety and sign it. This form will be used for provisioning and entitlement under the Flex Plan, as well as to ensure that you understand the terms of use that apply to your Flex Plan. Cisco will provide a quote to your reseller for the selected buying model, based upon the information that you provide in this form. Your reseller will in turn provide a quote to you. **Your signature is required on this form prior to receiving access to the program.**

End User Overview

Defined Terms Used in This Section

"**Participating Affiliates**" means Your Affiliates whose Meter counts are included on the EUIF.

"**Affiliate**" means, with respect to a party, any entity that directly or indirectly Controls, or is Controlled by, or is under common Control with such party. "**Control**" means to: (a) own more than 50% of the relevant party; or (b) be able to direct the affairs of the relevant party through any lawful means (*e.g.*, a contract that allows control).

"**End User**", "**You**" or "**Your**" mean the final purchasing entity as identified on the EUIF.

End User Information	
End User's full legal name	MINISTRY OF EDUCATION AND RELIGIOUS AFFAIRS
Address of End User's principal place of business	ANDREA PAPANDREOU 37 MAROUSI, ATTIKI, 151 80 GREECE

Participating Affiliates
Cisco requires any Participating Affiliate(s) for which you are purchasing coverage to be included in this End User Information Form. Cisco relies on this list to define the scope of the agreement, ensure accurate pricing, as well as effective provisioning and support.
Participating Affiliate(s)
☐ None ☐ Only listed Participating Affiliates (to be recorded immediately below)
Participating Affiliates

Cisco Collaboration

Additional Defined Terms Used in This Section

"**Employees**" means full or part-time employees of You and Your Participating Affiliates.

"**Contractors**" means non-Employees who (i) work on Your or Your Participating Affiliates' behalf, (ii) whose work is under Your or Your Participating Affiliates' control or supervision pursuant to a consulting, staffing or other similar written contract, and (iii) have access to Your or Your Participating Affiliates' systems or networks in the ordinary course of providing their services to You or Your Participating Affiliates.

"**Knowledge Workers**" means You and Your Participating Affiliates' Employees and Contractors who utilize devices capable of running the Software, Cloud Services, or related browser plug-ins as part of their job duties.

Your Suite(s) purchased under the Flex Plan
Cisco requires customers purchasing Enterprise Agreement to complete and sign this End User Information form. You will have access to the Software and/or Services in the Suite(s) you purchase and which are identified on your EUIF.
☐ Meetings Enterprise Agreement ☐ Calling Enterprise Agreement

Knowledge Worker Count Worksheet

Cisco Flex Plan EA Offers	**Value**
Total quantity of Employees of the End User and Participating Affiliates	a.
+ Total quantity of Contractors of the End User and Participating Affiliates	b.
= Total Employees and Contractors (add a. and b.)	c.
Knowledge Worker count	d.

Cisco Collaboration Flex Plan Education EA only	**Value**
Total quantity of faculty/staff (Knowledge Workers) at educational institution	a. 72000
Knowledge Worker faculty/staff count	b.
Total quantity of students at educational institution (expected to have access to Meetings) - These are not part of the Knowledge Worker count.	1

End User Information Form Acceptance

THE UNDERSIGNED REPRESENTS THAT THEY ARE AUTHORIZED TO SIGN THIS FORM ON THE END USER'S BEHALF AND THAT THE INFORMATION PROVIDED, INCLUDING METER COUNTS FOR THE END USER AND ITS PARTICIPATING AFFILIATES, IS ACCURATE AS OF THE DATE OF SIGNATURE. THE UNDERSIGNED UNDERSTANDS THAT THE APPROVED SOURCE RELIES UPON THE INFORMATION PROVIDED IN THIS FORM TO ESTABLISH THE PRICE QUOTE FOR THE END USER'S PURCHASE.

FOR FLEX PLAN EA: I HAVE READ THE ENTERPRISE AGREEMENT PROGRAM TERMS ("PROGRAM TERMS") INCLUDED BELOW, AND UNDERSTAND THAT IN THE EVENT OF AN EA PURCHASE, THESE PROGRAM TERMS APPLY TO THE SOFTWARE AND SERVICES AS DESCRIBED IN THE PROGRAM TERMS.

Full Legal Name of the End User Organization (e.g., company, government entity) You Represent	
Last Name, First Name	Gika Anastasia
Title	Secretary General of Ministry of Education
Date	January 7, 2021 | 10:30:22 PST
End User Authorized Representative Signature	DocuSigned by: 3D040E27E3384AC...

Cisco Enterprise Agreement Program Terms and Conditions for End Users

These terms and conditions together with the applicable Enrollment Descriptions and EUIF (collectively, "**EA Program Terms**") govern any Suites that You order under the Cisco Enterprise Agreement Program ("**Purchased Suites**"). The EA Program Terms do not modify the terms of any Cisco products or services You purchase outside of the Cisco Enterprise Agreement Program.

By signing these terms and conditions You agree to the EA Program Terms and the Licensing Documents. If You do not agree to the EA Program Terms or Licensing Documents, You may not Consume the Software or Cloud Services. Notwithstanding the foregoing, You are not obligated to make a purchase by entering into the EA Program Terms, and neither the EA Program Terms nor the Licensing Documents will apply until You place an order as further described in section 1, below.

1. **Orders.** To purchase Suites under the EA Program Terms, You must first submit the applicable EUIF and Enrollment Description signed by Your authorized representative to the Approved Source. The EUIF must list: (a) Your Participating Affiliates; (b) the Purchased Suites; (c) the Suite Term; and (d) accurate Meter counts for You and all Participating Affiliates. You will then be required to place an order for the Purchased Suites according to the process set forth in Your purchasing agreement with the Approved Source.

2. **Access To Purchased Suites.** Subject to Your payment of the applicable fees to the Approved Source, Cisco will grant You and all Participating Affiliates the right to Consume the Purchased Suites during the Suite Term via the EA Workspace or as otherwise set forth in the applicable Enrollment Description. You must pay for all Software and Cloud Services Consumed. You are responsible for keeping all login credentials to the EA Workspace secure and for the actions of any individual You or a Participating Affiliate authorize to access the EA Workspace, including payment for any Software or Cloud Services Consumed by such individuals.

3. **Enterprise-wide Commitment.** The Approved Source relies on the information You provide in the EUIF to establish the Enterprise-wide Commitment. During the Suite Term, Your payment obligation related to the Enterprise-wide Commitment may increase as a result of any of the following: (a) You exceed the Initial Growth Cap (as described in section 5); (b) You exceed the Initial Entitlement or the previous year's Entitlement subject to a True Forward (as described in section 6); or (c) You purchase an additional Suite (as described in section 9).

4. **Term & Termination.**

   a. **Term.** The Term of the EA Program Terms will commence on the date of signature below and continue so long as there is an active Purchased Suite, unless earlier terminated in accordance with section 4(c)(i), below.

   b. **Suite Term.** The Suite Term for each Purchased Suite will commence on the Suite Start Date and last for the period set forth in the EUIF, unless terminated in accordance with section 4(c)(i), below.

   c. **Termination.**

      i. Either party may terminate the EA Program Terms or a Purchased Suite if the other party materially breaches the EA Program Terms and does not cure the breach within 30 days of written notice of the breach.

ii. In the event of Your uncured material breach of the EA Program Terms for non-payment of fees to the Approved Source, Cisco may, in lieu of termination of the Program Terms pursuant to section 4(c)(i), suspend Your right to Consume the Software and Cloud Services in the Purchased Suite and suspend Your access to the EA Workspace, until Your breach has been cured.

iii. In the event of Your termination for Cisco's uncured material breach of the EA Program Terms, Cisco will refund to the Approved Source (or You, if You purchased directly from Cisco) any fees You paid covering the period after the effective date of termination.

iv. Other than as provided in this section 4 and to the extent permitted by law, the EA Program Terms and any orders placed thereunder are non-cancellable and may not be terminated.

d. **Effect of Termination; End of Suite Term**. Upon termination or at the end of the Suite Term:

i. The following rights will terminate with respect to the Purchased Suites: (1) Your right to Consume Cloud Services and Software; (2) Your right to access the EA Workspace; (3) Your right to receive Support Services; and

ii. You must destroy the product activation keys (PAKs) provided in connection with the Purchased Suites.

5. **Initial Growth Cap**. If You exceed the Initial Growth Cap during the first six months of the Suite Term, the Approved Source may charge You for such Consumption above the Initial Growth Cap. If the Purchased Suite includes a Growth Allowance (described in the applicable Enrollment Description), the Growth Allowance cannot be used to offset fees for exceeding the Initial Growth Cap.

6. **True Forward**.

a. Cisco performs a True Forward for the Purchased Suites on each anniversary of the Suite Start Date. On the first anniversary of the Suite Start Date, if You have exceeded the Initial Entitlement, the Approved Source will charge You for the Consumption above the Initial Entitlement through the remainder of the Suite Term. On each subsequent anniversary of the Suite Start Date, the Approved Source will charge You for any Consumption above the previous year's Entitlement through the remainder of the Suite Term.

b. Your True Forward payment obligation for each Purchased Suite will be calculated by comparing Your Consumption of Software and Cloud Services to Your Entitlement for the previous year. Any payment owed to the Approved Source will be determined as follows and reflected in the price quote from the Approved source: the unit price less any applicable discount or incentive multiplied by the quantity by which You exceeded Your then-current Entitlement. The price used to calculate any True Forward fees will be established when You place the order for each Purchased Suite.

c. For some Suites, a portion of Your True Forward payment obligation may be offset by the residual value remaining in Software or Cloud Services in the same Suite. This process is called value shift, and the applicable Enrollment Description indicates whether and to the extent value shift applies to a given Suite.

d. There is no fee for exceeding the Entitlement in the final year of the Suite Term.

7. **Updates to Purchased Suites**. Cisco may enhance or refine the Purchased Suites at no additional cost to You. Such updates will not materially reduce the core functionality of the Purchased Suites.

8. **End of Life**. Notwithstanding anything in the EA Program Terms to the contrary, Cisco reserves the right to discontinue a Suite with at least three years' prior notice. If a Purchased Suite is discontinued, Cisco will either: (a) provide You a substantially similar replacement Suite for the remainder of the Suite Term; or (b) issue a credit to the Approved Source (or You, if You purchased directly from Cisco) for any fees You paid for the Purchased Suite covering the period after the last date such Purchased Suite is available for You to Consume. Such credit can be applied towards the future purchase of Cisco products and services.

9. **Purchasing Additional Suites**. You may purchase additional Suites by submitting a new EUIF and order to the Approved Source. Additional Suites may co-terminate with a pre-existing Purchased Suite provided there are at least 12 months remaining in the Suite Term of such pre-existing Purchased Suite. Otherwise, additional Purchased Suites will be given a new Suite Term and will be subject to the then-current EA Program Terms in accordance with section 10, below.

10. **Modifications**. As our business evolves, Cisco may modify the EA Program Terms. Updated EA Program Terms do not apply to pre-existing Purchased Suites or to future orders that co-terminate to a pre-existing Purchased Suite, which will be governed by the version of the EA Program Terms already in effect for the pre-existing Purchased Suite.

11. **Participating Affiliates**. You are responsible for Your Participating Affiliates' compliance with the EA Program Terms.

12. **Support Services**. Basic Support Services are included in the price of the Purchased Suite and described in the applicable Enrollment Description and Licensing Documents. Higher levels of Support Services may be available for You to purchase and, if You elect to do so, will be described in documentation provided to You at the time of purchase.

13. **Importation Fee for Embedded Software**. For Purchased Suites that include Embedded Software, the value of Embedded Software will be deducted from the purchase price of the related Cisco hardware. If You are required to pay an Importation Fee, Your jurisdiction may use the value of both the hardware and Embedded Software to calculate the Importation Fee. Accordingly, the Importation Fee on the value of the combined products may be higher than if calculated solely using the price of the hardware.

14. **Delivery of Embedded Software**. Embedded Software is delivered pre-installed on Cisco hardware to the address provided on the purchase order for the Cisco hardware. Your use of the smart licensing account Cisco designates for the Embedded Software will ensure accurate pricing of the Embedded Software.

15. **No Assignment & Transfer**. Neither the EA Program Terms, nor any right or obligation herein may be assigned or transferred by a party (including under Cisco's Software Transfer and Relicensing Policy) without the other party's prior written consent, which may not be unreasonably conditioned, withheld, or delayed. Any attempted assignment without the other party's consent shall be void and of no effect. Notwithstanding the foregoing, Cisco may assign the EA Program Terms and any right or obligation herein to a Cisco Affiliate without Your consent.

16. **Verification**. Upon reasonable request from Cisco, You will assist Cisco in verifying the quantity of Software and Cloud Services that You have Consumed. If the verification discloses Consumption above Your then-current Entitlement, the Approved Source will charge You for the excess Consumption in accordance with the EA Program Terms.

17. **Combined Discounts**. The pricing, discounts, and other incentives offered in connection with a Purchased Suite may not be combined with any other price reductions, discounts, promotional pricing, rebates, credits, trade-in, or other pricing programs or incentives offered by Cisco unless expressly agreed by Cisco in writing.

18. **Entire Agreement**. The EA Program Terms constitute the entire agreement between the parties concerning the Cisco Enterprise Agreement Program and supersede all prior oral or written communications between the parties concerning the program.

19. **Order of Precedence**. The documents comprising the EA Program Terms are complimentary, and to the extent possible, construed and interpreted consistently. In the event of an inconsistency, conflict, or ambiguity between the EA Program Terms, the order of precedence for any Purchased Suite is first the EUIF, then the Enrollment Description, and then these terms and conditions. The EA Program Terms take precedent over the applicable Licensing Documents.

20. **Definitions**.

    a. "**Affiliate**" means, with respect to a party, any entity that directly or indirectly Controls, or is Controlled by, or is under common Control with such party. "**Control**" means to: (a) own more than 50% of the relevant party; or (b) be able to direct the affairs of the relevant party through any lawful means (*e.g.*, a contract that allows control).

    b. "**Approved Source**" means Cisco or a Cisco authorized reseller, distributor, or systems integrator.

    c. "**Cisco**" means Cisco Systems, Inc. or its applicable Affiliate delivering the EA Program Terms.

    d. "**Cloud Service**" means the Cisco hosted software-as-a-service listed in the applicable Enrollment Description.

    e. "**Consume**" or "**Consumption**" means to download, install, activate, provision, enable, or otherwise access Software or Cloud Services.

    f. "**EA Program**" has the meaning given to it in the introductory paragraph.

    g. "**EA Program Terms**" has the meaning given to it in the introductory paragraph.

    h. "**EA Workspace**" means the portal from where You Consume Software and Cloud Services and view and manage Your Entitlement.

    i. "**Embedded Software**" means Software that is delivered on newly purchased Cisco hardware.

    j. "**End User**," "**You**," or "**Your**" means the final purchasing entity as identified on the EUIF.

    k. "**Enterprise-wide Commitment**" means Your purchase commitment in the Purchased Suite for You and all Participating Affiliates, as reflected on the EUIF.

    l. "**Entitlement**" means, at any point in time during the Suite Term, the type and quantity of Software and Services as determined by the Meter counts for which You have already paid the applicable fees to the Approved Source.

    m. "**Enrollment**" means a combination of Suites belonging to the same Cisco product family. Cisco DNA, Cisco Data Center, Cisco Security Choice, Cisco Meraki, and Cisco Collaboration Flex Plan each represent an Enrollment.

n. "**Enrollment Description**" means the supplemental program terms and description governing an Enrollment.

o. "**EUIF**" means the End User Information Form for the Purchased Suite.

p. "**EULA**" mean's Cisco End User License Agreement, available at cisco.com/go/eula.

q. "**Growth Allowance**" means the right to exceed the Initial Entitlement without incurring additional fees as set forth in the applicable Enrollment Description.

r. "**Importation Fee**" means an import duty or tax on the purchase of Cisco hardware.

s. "**Initial Entitlement**" means Your Entitlement at the start of the Suite Term as determined by the Meter counts for You and all Participating Affiliates provided on the EUIF.

t. "**Initial Growth Cap**" means 105% of the Initial Entitlement.

u. "**Licensing Documents**" means the EULA and SEULAs for the Software and the EULA and ODs for the Cloud Services in the Purchased Suites (or similar terms existing between You and Cisco). The applicable Licensing Documents are listed in the Enrollment Description for each Purchased Suite.

v. "**Meter**" means the unit of measurement for Software or Cloud Services Consumption.

w. "**OD**" means the offer description and supplemental licensing terms governing Cloud Services.

x. "**Participating Affiliates**" means Your Affiliates whose Meter counts are included on the EUIF.

y. "**Purchased Suites**" has the meaning given to it in the introductory paragraph.

z. "**Services**" means both Cloud Services and Support Services.

aa. "**SEULA**" means the supplemental licensing terms governing Software.

bb. "**Software**" means the Cisco software listed in the applicable Enrollment Description.

cc. "**Suite**" means a combination of Software and Services in an Enrollment.

dd. "**Suite Start Date**" means, with respect to each Purchased Suite, the earliest date any Software or Cloud Service in the Purchased Suite is made available for You to Consume.

ee. "**Suite Term**" means, with respect to each Purchased Suite, the duration of the Purchased Suite.

ff. "**Support Services**" means maintenance, technical assistance, or other support provided for the Software and Cloud Services in a Purchased Suite.

gg. "**Term**" means the duration of the EA Program Terms.

hh. "**True Forward**" means an annual adjustment to account for exceeding the previous year's Entitlement.

Cisco Collaboration Flex Plan Enrollment Description & Supplemental EA Program Terms

This Enrollment Description lists the available Suites and additional terms and conditions that apply to the Cisco Collaboration Flex Plan Enrollment. You may purchase any or all of the Suites available under the Cisco Collaboration Flex Plan Enrollment, but the collection of Software and Cloud Services that comprise a Suite may not be modified.

Suite	Included Licenses	License Type	Licensing Documents	Meter
Cisco Collaboration Flex Plan Meetings Enterprise Agreement	Cisco Meeting Server	Software	Cisco Collaboration Flex Plan OD; EULA	Deployed Knowledge Worker
	Cisco Webex Meetings	Cloud Service		
	Cisco Webex Teams	Cloud Service		

Suite	Included Licenses	License Type	Licensing Documents	Meter
Cisco Collaboration Flex Plan Calling Enterprise Agreement	Cisco Webex Teams	Cloud Service	Cisco Collaboration Flex Plan OD; EULA	Deployed Knowledge Worker
	Cisco Webex Calling; or Cisco Webex Calling for SP; or Cisco Webex Calling (formerly Cisco Spark Call)	Cloud Service		
	UCM Cloud Calling	Cloud Service		
	Partner-Hosted Unified Communications Calling	Software		
	On-Premises Unified Communications Manager Calling	Software		

Suite	Included Licenses	License Type	Licensing Documents	Meter
Cisco Collaboration Flex Plan for Education Meetings Enterprise Agreement	Cisco Meeting Server	Software	Cisco Collaboration Flex Plan OD; EULA	Deployed Knowledge Worker; Student
	Cisco Webex Meetings	Cloud Service		
	Cisco Webex Teams	Cloud Service		

Suite	Included Licenses	License Type	Licensing Documents	Meter
Cisco Collaboration Flex Plan for Education Calling Enterprise Agreement	Cisco Webex Calling (formerly Cisco Spark Call)	Cloud Service	Cisco Collaboration Flex Plan OD; EULA	Deployed Knowledge Worker
	On-Premises Unified Communications Manager Calling	Software		

Suite	Included Licenses	License Type	Licensing Documents	Meter
Cisco Collaboration Flex Plan Enterprise Agreement for Public Sector	Cisco FedRAMP Webex Meetings	Cloud Service	Cisco Collaboration Flex Plan OD; EULA	Deployed Knowledge Worker
	Unified Communications Manager Cloud for Government	Cloud Service		

Supplemental Terms and Conditions

Applicable Meters

The Meter for the Cisco Collaboration Flex Plan Enrollment is the number of Deployed Knowledge Workers.

"**Deployed Knowledge Worker**" means a Knowledge Worker who has a profile configured within the Software or Cloud Service provisioning platform and associates that profile with the applicable desk phone, Jabber client, Webex Teams client, mobile phone, video device, or personal computing device. You must assign each Knowledge Worker a cloud, on-premises, or hosted account to be treated as a single Deployed Knowledge Worker. A Knowledge Worker who is assigned more than one configuration (cloud, on-premises, or hosted) will be counted as multiple Deployed Knowledge Workers. If at any time during the Term You change a Deployed Knowledge Worker's deployment type, You may be required to pay additional applicable fees immediately upon such change. "**Knowledge Worker**" means an employee or contractor who utilizes devices capable of running the Software, Cloud Services, or related browser plug-ins as part of their job duties.

If You purchase the Cisco Collaboration Flex Plan for Education Meetings Enterprise Agreement Suite, Your Students may Consume the Purchased Suite free of charge. "**Student**" means an individual who is currently enrolled or registered at Your institution for academic study on a full- or part-time basis. Employees, contractors, alumni, former students, prospective students, and students on an extended leave or indefinite absence are not considered Students. You will be required to provide a Student count on the EUIF. Thirty days prior to the True Forward event, you or your Reseller must update your order to reflect the number of Students provisioned at that time, which will be used to determine if you have exceeded your Growth Allowance. Failure to update your subscription will result in the additional Students being counted as Deployed Knowledge Workers for purposes of the True Forward.

Access to Purchased Suites

The Cisco Collaboration Flex Plan Enrollment does not utilize the EA Workspace. Subject to Your payment of the applicable fees to the Approved Source, Cisco will grant You and all Participating Affiliates access to the Purchased Suites via automated integrated electronic delivery tools and email notification to the point of contact designated in the order.

Purchasing Additional Suites

During the Suite Term, You may add another Cisco Collaboration Flex Plan Suite without submitting a new EUIF.

Common Area Licenses

Common area licenses are calling licenses not associated with Knowledge Workers that are intended to be used in lobbies, conference rooms, and other public spaces. If Your Consumption of common area licenses exceeds 50% of Your then-current Deployed Knowledge Worker count, the Approved Source may charge You for such excess Consumption.

Term and Termination

At the end of the Suite Term, the Purchased Suite will automatically renew for one year (a "**Renewal Suite Term**") unless: (a) You elect on the order not to auto-renew; or (b) at least 30 days before the end of then-current Suite Term, You notify the Approved Source of Your intention not to renew the Purchased Suite. If the Growth Allowance has not been exceeded, the Purchased Suite will renew for the Knowledge Worker count on the EUIF. If the Growth Allowance has been exceeded, the Purchased Suite will renew for the Deployed Knowledge Worker count at the end of the then-current Suite Term.

Notwithstanding the foregoing, the Approved Source will notify You of any fee changes reasonably in advance of the Renewal Term. The new fees will apply for the upcoming Renewal Term unless You notify the Approved Source that You do not accept the fee changes before the next Suite Start Date.

Growth Allowance

The Growth Allowance for the Cisco Collaboration Flex Plan Enrollment is 20%. During the Suite Term, You may Consume up to 120% of the Initial Entitlement without incurring any additional charges. The True Forward is calculated once You exceed the Growth Allowance. For clarity, if You exceed the Initial Entitlement but do not exceed the Growth Allowance, You will not incur any True Forward charges.

Support Services

The basic Support Services are set forth in the Cisco Collaboration Flex Plan OD.