MPP MEDIA PAY PLUS LIMITED

ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ ΚΑΙ ΥΠΗΡΕΣΙΩΝ

Εκδίδεται σε συμμόρφωση με την Απόφαση ΑΔΑΕ αριθ. 304/2025

Εταιρεία	MPP Media Pay Plus Limited
Έδρα	Arch. Makariou III, 161, 5ος όροφος / Γραφείο 5, 3027 Λεμεσός, Κύπρος
Αριθμός μητρώου	HE 392912
Τίτλος εγγράφου	Πολιτική Ασφάλειας Δικτύων και Υπηρεσιών
Έκδοση εγγράφου	1.0
Υπεύθυνος	Υπεύθυνος Ασφάλειας Δικτύων και Υπηρεσιών
Κύκλος αναθεώρησης	Ετήσιος ή σε περίπτωση ουσιώδους μεταβολής

1. Πεδίο Εφαρμογής και Σκοπός

Η παρούσα Πολιτική καθορίζει τα τεχνικά και οργανωτικά μέτρα που λαμβάνει η εταιρεία MPP Media Pay Plus Limited (η «Εταιρεία») για τη διασφάλιση του απορρήτου των ηλεκτρονικών επικοινωνιών και για τη διαχείριση των κινδύνων που αφορούν την ασφάλεια των δημόσιων δικτύων ηλεκτρονικών επικοινωνιών και των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών τις οποίες παρέχει στην Ελλάδα βάσει του καθεστώτος Γενικών Αδειών της ΕΕΤΤ.

Η παρούσα Πολιτική είναι δεσμευτική για όλους τους εργαζομένους, τους εξωτερικούς συνεργάτες, τους προμηθευτές και τα τρίτα μέρη των οποίων οι δραστηριότητες ενδέχεται να επηρεάσουν την ασφάλεια ή το απόρρητο των δικτύων και υπηρεσιών της Εταιρείας.

2. Νομικό και Κανονιστικό Πλαίσιο

- Απόφαση ΑΔΑΕ αριθ. 304/2025 — Κανονισμός για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών (ΦΕΚ Β'/4268/07.08.2025).
- Απόφαση ΑΔΑΕ αριθ. 28/2024 — Κανονισμός για την Ασφάλεια Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών.
- Ν. 3471/2006 για την προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.
- Ν. 5160/2024 για την ενσωμάτωση της Οδηγίας NIS2.
- Υπουργική Απόφαση 1899/2025 σχετικά με τους Υπευθύνους Ασφάλειας.
- Κανονισμός (ΕΕ) 2016/679 (ΓΚΠΔ) και Ν. 4624/2019.
- Κανονισμός Γενικών Αδειών της ΕΕΤΤ.

3. Ρόλοι και Αρμοδιότητες

3.1 Υπεύθυνος Ασφάλειας Δικτύων και Υπηρεσιών

Η Εταιρεία ορίζει Υπεύθυνο Ασφάλειας Δικτύων και Υπηρεσιών, σύμφωνα με την παράγραφο 3.3.2 του Άρθρου 3 της Απόφασης ΑΔΑΕ 304/2025, ο οποίος είναι αρμόδιος για τον σχεδιασμό, την εφαρμογή, τη συντήρηση και την αναθεώρηση της παρούσας Πολιτικής και ενεργεί ως σημείο επαφής με την ΑΔΑΕ. Ο Υπεύθυνος Ασφάλειας πληροί τις απαιτήσεις της Υπουργικής Απόφασης 1899/2025 και αναφέρεται απευθείας στη Διοίκηση. Τρέχων Υπεύθυνος Ασφάλειας: Daniel Dieu – info@mediapayplus.com

3.2 Διοίκηση

Η Διοίκηση της Εταιρείας εγκρίνει την παρούσα Πολιτική, διαθέτει τους αναγκαίους πόρους και αξιολογεί την αποτελεσματικότητά της τουλάχιστον μία φορά ετησίως.

3.3 Προσωπικό

Όλο το προσωπικό υποχρεούται να συμμορφώνεται με την παρούσα Πολιτική, να ολοκληρώνει τη σχετική εκπαίδευση ασφάλειας και να αναφέρει αμελλητί στον Υπεύθυνο Ασφάλειας κάθε περιστατικό ασφάλειας ή υπόνοια αυτού.

3.4 Τρίτα μέρη

Κάθε προμηθευτής ή εξωτερικός συνεργάτης του οποίου οι υπηρεσίες ενδέχεται να επηρεάσουν το απόρρητο ή την ασφάλεια των δικτύων και υπηρεσιών της Εταιρείας δεσμεύεται συμβατικά να συμμορφώνεται με απαιτήσεις ασφάλειας ισοδύναμες με τις οριζόμενες στην παρούσα Πολιτική.

4. Απόρρητο Ηλεκτρονικών Επικοινωνιών

Η Εταιρεία αναγνωρίζει το απόρρητο των ηλεκτρονικών επικοινωνιών ως θεμελιώδη υποχρέωση βάσει του Άρθρου 19 του Συντάγματος, του Ν. 3471/2006 και της Απόφασης ΑΔΑΕ 304/2025.

Το περιεχόμενο των επικοινωνιών που διεκπεραιώνονται μέσω των δικτύων ή υπηρεσιών της Εταιρείας δεν προσπελάζεται, δεν καταγράφεται, δεν κοινοποιείται και δεν διατηρείται, παρά μόνον επί τη βάσει συγκεκριμένης νομικής βάσης — ιδίως για την παροχή της υπηρεσίας που ζητείται από τον συνδρομητή, για την προστασία της ασφάλειας και ακεραιότητας των δικτύων και υπηρεσιών, ή κατόπιν νόμιμης διάταξης εκδοθείσας σύμφωνα με τον Ν. 2225/1994 και υπό την εποπτεία της ΑΔΑΕ.

Τα δεδομένα κίνησης και θέσης υφίστανται επεξεργασία μόνον στον βαθμό που είναι αναγκαίο και για τους σκοπούς που επιτρέπονται από τον Ν. 3471/2006, και διαγράφονται ή ανωνυμοποιούνται όταν παύουν να είναι αναγκαία για τους σκοπούς αυτούς.

5. Διαχείριση Κινδύνων

Η Εταιρεία εφαρμόζει τεκμηριωμένη διαδικασία διαχείρισης κινδύνων, η οποία:

- αναγνωρίζει τα αγαθά που υποστηρίζουν την παροχή των δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών·
- εντοπίζει απειλές και ευπάθειες που θα μπορούσαν να θέσουν σε κίνδυνο το απόρρητο, την ακεραιότητα ή τη διαθεσιμότητα των αγαθών αυτών·
- αξιολογεί την πιθανότητα και τον αντίκτυπο κάθε κινδύνου·
- καθορίζει και εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για την αντιμετώπιση μη αποδεκτών κινδύνων·
- αναθεωρείται τουλάχιστον μία φορά ετησίως και κατόπιν κάθε ουσιώδους μεταβολής στα δίκτυα, τις υπηρεσίες ή το τοπίο απειλών.

Τα αποτελέσματα της αξιολόγησης κινδύνων τεκμηριώνονται και διατηρούνται για έλεγχο από την ΑΔΑΕ.

6. Τεχνικά Μέτρα

6.1 Έλεγχος πρόσβασης

Η πρόσβαση σε συστήματα που επεξεργάζονται δεδομένα ηλεκτρονικών επικοινωνιών παρέχεται με βάση τις αρχές της ελάχιστης προνομίας και της ανάγκης γνώσης, πιστοποιείται με ισχυρά διαπιστευτήρια και επανεξετάζεται περιοδικά.

6.2 Ασφάλεια δικτύου

Τα δίκτυα είναι τμηματοποιημένα· η κίνηση στην περίμετρο και εσωτερικά φιλτράρεται· η διαχειριστική πρόσβαση περιορίζεται σε έμπιστα δίκτυα και προστατεύεται με πολυπαραγοντική ταυτοποίηση.

6.3 Κρυπτογραφία

Το περιεχόμενο των ηλεκτρονικών επικοινωνιών, τα δεδομένα σηματοδοσίας και τα διαπιστευτήρια ταυτοποίησης προστατεύονται κατά τη μετάδοση με σύγχρονα κρυπτογραφικά πρωτόκολλα. Τα κρυπτογραφικά κλειδιά διαχειρίζονται βάσει τεκμηριωμένης διαδικασίας διαχείρισης κλειδιών.

6.4 Καταγραφή και παρακολούθηση

Τα συμβάντα ασφάλειας σε συστήματα και δίκτυα καταγράφονται, προστατεύονται από αλλοίωση, διατηρούνται για ελάχιστη περίοδο δύο (2) ετών και επανεξετάζονται για τον εντοπισμό ανωμαλιών.

6.5 Διαχείριση ευπαθειών και ενημερώσεων

Τα συστήματα διατηρούνται ενημερωμένα· οι ευπάθειες εντοπίζονται μέσω τακτικών σαρώσεων και αποκαθίστανται ανάλογα με τη σοβαρότητά τους.

6.6 Αντίγραφα ασφαλείας και ανθεκτικότητα

Τα αντίγραφα ασφαλείας των δεδομένων παραμετροποίησης και των δεδομένων που αφορούν την ασφάλεια συντηρούνται, προστατεύονται και δοκιμάζονται περιοδικά. Οι υπηρεσίες σχεδιάζονται ώστε να παρουσιάζουν ανθεκτικότητα σε προβλέψιμες αστοχίες.

7. Οργανωτικά Μέτρα

7.1 Ενημέρωση και εκπαίδευση σε θέματα ασφάλειας

Όλο το προσωπικό λαμβάνει εκπαίδευση ευαισθητοποίησης σε θέματα ασφάλειας κατά την πρόσληψη και τουλάχιστον μία φορά ετησίως μετέπειτα, με πρόσθετη εκπαίδευση ανά ρόλο για το προσωπικό που χειρίζεται δεδομένα ηλεκτρονικών επικοινωνιών.

7.2 Υποχρεώσεις εμπιστευτικότητας

Όλο το προσωπικό και τα τρίτα μέρη δεσμεύονται με έγγραφες υποχρεώσεις εμπιστευτικότητας που καλύπτουν τα δεδομένα ηλεκτρονικών επικοινωνιών.

7.3 Διαχείριση προμηθευτών

Οι απαιτήσεις ασφάλειας ενσωματώνονται στις συμβάσεις με τους προμηθευτές. Οι προμηθευτές που έχουν πρόσβαση σε δεδομένα ηλεκτρονικών επικοινωνιών αξιολογούνται πριν από τη σύναψη της συνεργασίας και περιοδικά έκτοτε.

7.4 Φυσική ασφάλεια

Οι εγκαταστάσεις που φιλοξενούν υποδομή δικτύων και υπηρεσιών προστατεύονται έναντι μη εξουσιοδοτημένης φυσικής πρόσβασης, περιβαλλοντικών απειλών και διακοπών τροφοδοσίας.

7.5 Διαχείριση αλλαγών

Οι αλλαγές που επηρεάζουν την ασφάλεια των δικτύων ή των υπηρεσιών αξιολογούνται, δοκιμάζονται και εγκρίνονται πριν τεθούν σε παραγωγή.

8. Διαχείριση Περιστατικών

Η Εταιρεία τηρεί τεκμηριωμένη διαδικασία διαχείρισης περιστατικών, η οποία καλύπτει τον εντοπισμό, την ταξινόμηση, την ανάσχεση, την εξάλειψη, την αποκατάσταση και την αξιολόγηση μετά το περιστατικό.

Τα περιστατικά ασφάλειας που παραβιάζουν ή ενδέχεται να παραβιάσουν το απόρρητο των ηλεκτρονικών επικοινωνιών, ή που έχουν σημαντικό αντίκτυπο στην ασφάλεια των δικτύων ή των υπηρεσιών, γνωστοποιούνται στην ΑΔΑΕ αμελλητί και εν πάση περιπτώσει εντός των προθεσμιών που ορίζει η ΑΔΑΕ στους εφαρμοστέους Κανονισμούς της και, όπου απαιτείται, στην Εθνική Αρχή Κυβερνοασφάλειας κατ' Άρθρο 29 του Ν. 5160/2024. Οι παραβιάσεις δεδομένων προσωπικού χαρακτήρα γνωστοποιούνται στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα σύμφωνα με το Άρθρο 12 του Ν. 3471/2006 και τον ΓΚΠΔ, καθώς και στα θιγόμενα φυσικά πρόσωπα όπου απαιτείται από τον νόμο.

Τα σημαντικά περιστατικά γνωστοποιούνται στην ΑΔΑΕ με αρχική προειδοποίηση εντός 24 ωρών, με αναφορά περιστατικού εντός 72 ωρών και με τελική αναφορά εντός ενός μηνός, σύμφωνα με τον Ν. 5160/2024.

Τα αρχεία περιστατικών διατηρούνται για έλεγχο από την ΑΔΑΕ για ελάχιστη περίοδο δύο (2) ετών.

9. Έλεγχος και Αναθεώρηση

Η παρούσα Πολιτική και τα μέτρα εφαρμογής της επανεξετάζονται από τον Υπεύθυνο Ασφάλειας τουλάχιστον μία φορά ετησίως, καθώς και μετά από κάθε σημαντικό περιστατικό, κανονιστική μεταβολή ή ουσιώδη αλλαγή στα δίκτυα ή τις υπηρεσίες της Εταιρείας. Τα αποτελέσματα της επανεξέτασης υποβάλλονται προς έγκριση στη Διοίκηση.

Η Εταιρεία συνεργάζεται πλήρως με τους ελέγχους και τις επιθεωρήσεις της ΑΔΑΕ.

10. Εφαρμογή και Κυρώσεις

Οι παραβιάσεις της παρούσας Πολιτικής μπορούν να επισύρουν πειθαρχικά μέτρα, έως και την καταγγελία της σύμβασης εργασίας ή συνεργασίας, και δύνανται να αναφερθούν στις αρμόδιες αρχές όπου απαιτείται από τον νόμο.

Εγκρίθηκε από: Eliza McDaniel

Υπογραφή / Ημερομηνία: 11/0/2026