					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P17					Τίτλος εγγράφου: **Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας**							
Έκδοση: 1.0		Ημερομηνία έναρξης ισχύος: 01.01.2025			Ιδιοκτήτης εγγράφου:							
X	Πολιτική		Πρότυπο		Διαδικασία		Έντυπο		Μητρώο		Άλλο	

Ιστορικό αναθεωρήσεων				
Αριθμός αναθεώρησης	**Ημερομηνία αναθεώρησης**	**Αλλαγές**	**Ελέγχθηκε από**	**Ιδιοκτήτης διεργασίας**

Εγκρίσεις			
Όνομα	**Θέση**	**Ημερομηνία**	**Υπογραφή**

Ευθυγραμμισμένη με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο/Κανονισμός	Ρήτρα/Άρθρο	Σχόλιο
ISO/IEC 27001:2022	Ρήτρες 5.1, 6.1.3, 8.1, 10	Σχετικοί γενικοί και τεχνικοί έλεγχοι, καθώς και έλεγχοι συνεχούς βελτίωσης για την προστασία δεδομένων
ISO/IEC 27002:2022	Έλεγχοι 5.34, 8.10, 8.11, 8.12	Έλεγχοι για τον χειρισμό PII, τη διατήρηση, τη διαγραφή, την ανωνυμοποίηση και τα δικαιώματα των υποκειμένων των δεδομένων
NIST SP 800-53 Rev.5	AR-1, AR-2, AR-4, AR-5; PL-2, PL-8; AC-2, AC-6; AU-2, AU-6, AU-9; IR-4, IR-5, IR-6; PM-1, PM-21, PM-23	Απαιτήσεις διακυβέρνησης, κινδύνου, διαχείρισης πρόσβασης, καταγραφής, απόκρισης σε παραβιάσεις και προγράμματος ιδιωτικότητας
ΓΚΠΔ της ΕΕ	Άρθρα 5, 6, 12–23, 25, 28, 30, 32–34; Αιτιολογική σκέψη 78	Βασικές απαιτήσεις ιδιωτικότητας, λογοδοσίας, δικαιωμάτων υποκειμένων, DSRs, παραβιάσεων και αρχών προστασίας ήδη από τον σχεδιασμό και εξ ορισμού
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(e), (f)	Έλεγχοι ασφάλειας βάσει κινδύνου για ουσιώδεις και σημαντικές οντότητες
Κανονισμός DORA της ΕΕ	Άρθρα 6(2)(d), 11(1)(c), 15(1), 17	Διακυβέρνηση, κίνδυνος τρίτων μερών και απαιτήσεις ασφαλούς επεξεργασίας
COBIT 2019	APO12, DSS01, DSS05, MEA	Διαχείριση κινδύνων, ασφαλείς λειτουργίες, εποπτεία συμμόρφωσης

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει υποχρεωτικές οργανωτικές αρχές και τεχνικές απαιτήσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα και την εφαρμογή της προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό σε όλα τα περιβάλλοντα.

1.2 Τυποποιεί τις ευθύνες του οργανισμού βάσει διεθνών προτύπων και κανονιστικών πλαισίων, διασφαλίζοντας ότι τα δεδομένα προσωπικού χαρακτήρα συλλέγονται, υποβάλλονται σε επεξεργασία, διατηρούνται, κοινοποιούνται και διατίθενται νόμιμα, με ασφάλεια και με διαφάνεια.

1.3 Η παρούσα πολιτική ενισχύει επίσης τη συμμόρφωση με τους εφαρμοστέους νόμους και τα πλαίσια ιδιωτικότητας, συμπεριλαμβανομένων του ΓΚΠΔ της ΕΕ, της Οδηγίας NIS2 της ΕΕ, του Κανονισμού DORA της ΕΕ, του ISO/IEC 27001:2022 και του COBIT 2019.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλες τις οργανωτικές μονάδες, το προσωπικό και τα συστήματα που εμπλέκονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων των εξής:

2.1.1 Εργαζόμενοι, ανάδοχοι και πάροχοι υπηρεσιών τρίτων.

2.1.2 Δεδομένα που συλλέγονται από εσωτερικές και εξωτερικές πηγές σε όλες τις επιχειρησιακές λειτουργίες.

2.1.3 Φυσικά και ψηφιακά μέσα, συμπεριλαμβανομένων υπηρεσιών νέφους, πλατφορμών SaaS, φορητών συσκευών και έντυπων αρχείων.

2.1.4 Όλα τα περιβάλλοντα, συμπεριλαμβανομένων του περιβάλλοντος παραγωγής, της ανάπτυξης, των δοκιμών και των συστημάτων αντιγράφων ασφαλείας, όπου ενδέχεται να υπάρχουν δεδομένα προσωπικού χαρακτήρα.

2.2 Καλύπτει όλες τις δραστηριότητες επεξεργασίας που ρυθμίζονται από τους εφαρμοστέους νόμους και τα πρότυπα ιδιωτικότητας, συμπεριλαμβανομένων ενδεικτικά των εξής:

2.2.1 Συλλογή, αποθήκευση, χρήση, διαβίβαση και διάθεση δεδομένων προσωπικού χαρακτήρα.

2.2.2 Άσκηση δικαιωμάτων υποκειμένων των δεδομένων, τεκμηρίωση της νομικής βάσης και διαχείριση συγκατάθεσης.

2.2.3 Διασυνοριακές διαβιβάσεις, γνωστοποίηση παραβιάσεων και κοινοποίηση δεδομένων σε τρίτα μέρη.

2.2.4 Ασφαλή σχεδιασμό και εφαρμογή της προστασίας της ιδιωτικότητας εξ ορισμού σε συστήματα και διεργασίες.

3. Στόχοι

3.1 Να διασφαλίζεται η νόμιμη, διαφανής και υπόλογη επεξεργασία δεδομένων προσωπικού χαρακτήρα σε ευθυγράμμιση με το ISO/IEC 27001:2022 και τις συναφείς νομικές απαιτήσεις.

3.2 Να ενσωματώνονται οι αρχές προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό και εξ ορισμού σε όλα τα πληροφοριακά συστήματα, τις υπηρεσίες και τις επιχειρησιακές διεργασίες.

3.3 Να εφαρμόζονται τεχνικά και οργανωτικά μέτρα που διασφαλίζουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων προσωπικού χαρακτήρα σε όλο τον κύκλο ζωής της πληροφορίας.

3.4 Να καθορίζονται ρόλοι διακυβέρνησης και δομές λογοδοσίας για την προστασία δεδομένων, συμπεριλαμβανομένων των αρμοδιοτήτων του Υπευθύνου Προστασίας Δεδομένων (DPO), της Ασφάλειας Πληροφοριών, της Νομικής και Κανονιστικής Συμμόρφωσης και των Ιδιοκτητών Πληροφοριών.

3.5 Να διασφαλίζεται πλήρης συμμόρφωση με τα Άρθρα 5, 6, 25, 30 και 32 του ΓΚΠΔ, καθώς και με τις απαιτήσεις μείωσης κινδύνου και ανθεκτικότητας βάσει NIS2 και DORA.

3.6 Να διαφυλάσσονται τα δικαιώματα των υποκειμένων των δεδομένων, συμπεριλαμβανομένων της πρόσβασης, της διόρθωσης, της διαγραφής, του περιορισμού, της φορητότητας, της εναντίωσης και της προστασίας από αυτοματοποιημένη λήψη αποφάσεων.

3.7 Να μετριάζονται οι κανονιστικοί, νομικοί και λειτουργικοί κίνδυνοι, καθώς και η ζημία στη φήμη, που απορρέουν από μη εξουσιοδοτημένη πρόσβαση, κακή χρήση ή απώλεια δεδομένων προσωπικού χαρακτήρα.

4. Ρόλοι και αρμοδιότητες

4.1 Ανώτατη Διοίκηση

4.1.1 Παρέχει στρατηγική εποπτεία και διαθέτει επαρκείς πόρους για την υποστήριξη του προγράμματος ιδιωτικότητας.

4.1.2 Εγκρίνει την παρούσα πολιτική και διασφαλίζει την εφαρμογή της σε όλο τον οργανισμό.

4.2 Υπεύθυνος Προστασίας Δεδομένων (DPO)

4.2.1 Ενεργεί ανεξάρτητα για την εποπτεία της συμμόρφωσης με τους κανονισμούς προστασίας δεδομένων.

4.2.2 Τηρεί το Αρχείο Δραστηριοτήτων Επεξεργασίας (RoPA) σύμφωνα με το Άρθρο 30 του ΓΚΠΔ.

4.2.3 Ηγείται της επικοινωνίας με τις εποπτικές αρχές, διενεργεί Εκτιμήσεις Αντικτύπου σχετικά με την Προστασία Δεδομένων (DPIAs) και διαχειρίζεται τις διαδικασίες γνωστοποίησης παραβιάσεων.

4.2.4 Ανασκοπεί τις εξαιρέσεις ιδιωτικότητας και τηρεί το Μητρώο Εξαιρέσεων Ιδιωτικότητας.

[... Οι ενότητες 4.3–8 δεν περιλαμβάνονται σε αυτή την προεπισκόπηση. Αγοράστε το πλήρες έγγραφο για πρόσβαση στο πλήρες περιεχόμενο. ...]

9. Απαιτήσεις ανασκόπησης και επικαιροποίησης

9.1 Η παρούσα πολιτική πρέπει να ανασκοπείται τουλάχιστον ετησίως ή νωρίτερα υπό τις ακόλουθες συνθήκες:

9.1.1 σημαντικές νομικές ή κανονιστικές επικαιροποιήσεις (π.χ. τροποποιήσεις του ΓΚΠΔ, προθεσμίες DORA)

9.1.2 νέα συστήματα ή δραστηριότητες επεξεργασίας που αφορούν δεδομένα προσωπικού χαρακτήρα

9.1.3 ευρήματα Εσωτερικού Ελέγχου που υποδεικνύουν κενά πολιτικής

9.1.4 ουσιώδη περιστατικά παραβίασης ή ανατροφοδότηση από εποπτική αρχή

9.2 Αρμοδιότητες ανασκόπησης

9.2.1 Ο DPO οφείλει να εκκινεί την ανασκόπηση της πολιτικής, σε συντονισμό με τη Νομική, τη Διαχείριση Κινδύνων, την Ασφάλεια Πληροφοριών και την Ανώτατη Διοίκηση.

9.2.2 Όλες οι επικαιροποιήσεις πρέπει να καταγράφονται στο Μητρώο Εγγράφων του ΣΔΑΠ και να διανέμονται στα ενδιαφερόμενα μέρη που επηρεάζονται.

9.3 Έλεγχος αλλαγών

9.3.1 Κάθε αναθεώρηση της παρούσας πολιτικής πρέπει να εγκρίνεται επίσημα από την Ανώτατη Διοίκηση.

9.3.2 Οι παρωχημένες εκδόσεις πρέπει να αρχειοθετούνται με ασφάλεια και η επικαιροποιημένη έκδοση πρέπει να περιλαμβάνει τεκμηριωμένο ιστορικό μεταβολών.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 P1 – Πολιτική Ασφάλειας Πληροφοριών. Καθορίζει τις υπερκείμενες αρχές διακυβέρνησης ασφάλειας που στηρίζουν την παρούσα πολιτική ιδιωτικότητας. Η P1 υποστηρίζει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων προσωπικού χαρακτήρα σε όλα τα συστήματα και τις υπηρεσίες.

10.2 P6 – Πολιτική Διαχείρισης Κινδύνων. Καθορίζει τη μεθοδολογία αντιμετώπισης κινδύνων του οργανισμού, η οποία είναι ουσιώδης για την αξιολόγηση κινδύνων ιδιωτικότητας, τις διαδικασίες DPIA και τις αξιολογήσεις υπολειπόμενου κινδύνου που απαιτούνται βάσει του ΓΚΠΔ και της Ρήτρας 6.1.3 του ISO/IEC 27001.

10.3 P13 – Πολιτική Ταξινόμησης και Επισήμανσης Δεδομένων. Καθοδηγεί την κατηγοριοποίηση προσωπικών και ευαίσθητων δεδομένων, αποτελώντας τη βάση για την εφαρμογή κατάλληλων ελέγχων ιδιωτικότητας, συμπεριλαμβανομένης της εφαρμογής της διατήρησης, του περιορισμού της πρόσβασης και της ασφαλούς διάθεσης.

10.4 P14 – Πολιτική Διατήρησης και Διάθεσης Δεδομένων. Υποστηρίζει άμεσα τις απαιτήσεις ιδιωτικότητας βάσει των Άρθρων 5(1)(e) και 17 του ΓΚΠΔ, διασφαλίζοντας ότι τα δεδομένα προσωπικού χαρακτήρα διατηρούνται μόνο για όσο διάστημα είναι αναγκαίο και διατίθενται με ασφάλεια σύμφωνα με τις νομικές υποχρεώσεις.

10.5 P16 – Πολιτική Απόκρυψης Δεδομένων και Ψευδωνυμοποίησης. Καθορίζει ελέγχους για τη μείωση της δυνατότητας ταυτοποίησης των δεδομένων προσωπικού χαρακτήρα μέσω τεχνικών μέτρων όπως tokenization, δυναμική απόκρυψη και ψευδωνυμοποίηση, εφαρμόζοντας έτσι το Άρθρο 32 του ΓΚΠΔ και τον Έλεγχο 5.34 του ISO/IEC 27002.

10.6 P30 – Πολιτική Αντιμετώπισης Περιστατικών. Περιγράφει τα υποχρεωτικά πρωτόκολλα απόκρισης σε παραβιάσεις που ενσωματώνονται με τον χειρισμό παραβιάσεων ιδιωτικότητας και τα χρονοδιαγράμματα γνωστοποίησης που απαιτούνται βάσει των Άρθρων 33 και 34 του ΓΚΠΔ.

10.7 P33 – Πολιτική Ελέγχου και Παρακολούθησης Συμμόρφωσης. Εφαρμόζει προγραμματισμένες αξιολογήσεις της αποτελεσματικότητας του προγράμματος ιδιωτικότητας, της εφαρμογής της πολιτικής και της παρακολούθησης διορθωτικών ενεργειών σε όλες τις οργανωτικές μονάδες και στους τρίτους εκτελούντες την επεξεργασία.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Ρήτρα 5.1 – Ηγεσία και δέσμευση: Καθορίζει ευθύνη σε επίπεδο διοίκησης για την προστασία των δεδομένων προσωπικού χαρακτήρα και την εφαρμογή των αρχών ιδιωτικότητας.

11.1.2 Ρήτρα 6.1.3 – Αντιμετώπιση κινδύνων ασφάλειας πληροφοριών: Υποστηρίζει την αναγνώριση, αξιολόγηση και αντιμετώπιση κινδύνων ιδιωτικότητας μέσω DPIAs και εξαιρέσεων.

11.1.3 Ρήτρα 8.1 – Επιχειρησιακός σχεδιασμός και έλεγχος: Απαιτεί τεχνικές και διαδικαστικές δικλίδες ασφαλείας ώστε να διασφαλίζεται η ασφαλής επεξεργασία δεδομένων προσωπικού χαρακτήρα.

11.1.4 Ρήτρα 10.1 – Συνεχής βελτίωση: Επιβάλλει την περιοδική αξιολόγηση και προσαρμογή του προγράμματος ιδιωτικότητας.

11.2 ISO/IEC 27002:2022 Έλεγχοι 5.34, 8.10, 8.11, 8.12: Παρέχει καθοδήγηση σχετικά με τον χειρισμό PII, την εφαρμογή της διατήρησης, τη διαγραφή, την ανωνυμοποίηση και τη διαφάνεια ως προς τα δικαιώματα των υποκειμένων.

11.3 NIST SP 800-53 Rev.5

11.3.1 AR-1, AR-2, AR-4, AR-5: Καθορίζουν αρμοδιότητες διακυβέρνησης, ρόλων, λογοδοσίας και εκπαίδευσης ιδιωτικότητας.

11.3.2 PL-2, PL-8: Απαιτούν την ενσωμάτωση ελέγχων ιδιωτικότητας στον κύκλο ζωής συστημάτων και στην επιχειρησιακή αρχιτεκτονική.

11.3.3 AC-2, AC-6: Εφαρμόζουν ελάχιστο προνόμιο και διαχείριση λογαριασμών για την προστασία δεδομένων προσωπικού χαρακτήρα.

11.3.4 AU-2, AU-6, AU-9: Επιβάλλουν καταγραφή, ιχνηλασιμότητα και ακεραιότητα ελέγχου για την πρόσβαση σε δεδομένα προσωπικού χαρακτήρα.

11.3.5 IR-4, IR-5, IR-6: Καθορίζουν δομημένες διαδικασίες ανίχνευσης, ανάλυσης και αναφοράς για παραβιάσεις ιδιωτικότητας.

11.3.6 PM-1, PM-21, PM-23: Θεσπίζουν ένα ολοκληρωμένο πρόγραμμα ιδιωτικότητας, ευθυγραμμισμένο με στρατηγικούς στόχους κινδύνου και διακυβέρνησης δεδομένων.

11.4 ΓΚΠΔ της ΕΕ (2016/679)

11.4.1 Άρθρα 5, 6, 12–23, 25, 28, 30, 32–34: Ρυθμίζουν τη νόμιμη επεξεργασία, τον περιορισμό του σκοπού, τα δικαιώματα των υποκειμένων των δεδομένων, τη λογοδοσία, την προστασία δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού, τις υποχρεώσεις τρίτων μερών και τη διαχείριση παραβιάσεων.

11.4.2 Αιτιολογική σκέψη 78: Ενισχύει τις αρχές προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό.

11.5 Οδηγία NIS2 της ΕΕ (2022/2555)

11.5.1 Άρθρο 21(2)(e) και (f): Απαιτεί την εφαρμογή ελέγχων ασφάλειας βάσει κινδύνου και την προστασία των δεδομένων προσωπικού χαρακτήρα για τις οντότητες που εμπίπτουν στο πεδίο εφαρμογής ως ουσιώδεις και σημαντικές.

11.6 Κανονισμός DORA της ΕΕ (2022/2554)

11.6.1 Άρθρο 6(2)(d): Εφαρμόζει εσωτερική διακυβέρνηση για τον κίνδυνο ΤΠΕ που σχετίζεται με πρακτικές διαχείρισης δεδομένων.

11.6.2 Άρθρο 11(1)(c): Επιβάλλει εποπτεία κινδύνου τρίτων μερών για υπηρεσίες που σχετίζονται με δεδομένα.

11.6.3 Άρθρα 15(1) και 17: Απαιτούν ασφαλή επεξεργασία δεδομένων από παρόχους υπηρεσιών και έγκαιρες γνωστοποιήσεις προς τις εποπτικές αρχές μετά από περιστατικά που σχετίζονται με ΤΠΕ.

11.7 COBIT 2019

11.7.1 APO12 – Διαχείριση Κινδύνων: Ενσωματώνει τον κίνδυνο ιδιωτικότητας στην ευρύτερη εποπτεία επιχειρησιακού κινδύνου.

11.7.2 DSS01 – Διαχειριζόμενες Λειτουργίες και DSS05 – Υπηρεσίες Ασφάλειας: Διασφαλίζουν ασφαλείς λειτουργίες, συμπεριλαμβανομένων του ελέγχου πρόσβασης, της διατήρησης και της ακεραιότητας συστημάτων.

11.7.3 MEA03 – Παρακολούθηση συμμόρφωσης: Απαιτεί συνεχή ανασκόπηση της κατάστασης συμμόρφωσης έναντι κανονιστικών και απορρεουσών από τις πολιτικές υποχρεώσεων ιδιωτικότητας.