					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P17S					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	
ISO/IEC 27002:2022	Έλεγχοι 5.34, 8.10–8	
NIST SP 800-53 Rev. 5	AR-2, PL-5, AC-6, IR-4	
ΓΚΠΔ της ΕΕ	Άρθρα 5, 6, 12-23, 30, 32-34	
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(e), 21(2)(f)	
Κανονισμός DORA της ΕΕ	Άρθρα 6, 15, 17	
COBIT 2019	APO12, DSS05, MEA	

1. Σκοπός

1.1. Η παρούσα πολιτική καθορίζει τον τρόπο με τον οποίο ο οργανισμός προστατεύει τα προσωπικά δεδομένα σύμφωνα με τις νομικές υποχρεώσεις, τα κανονιστικά πλαίσια και τα διεθνή πρότυπα ασφάλειας.

1.2. Διασφαλίζει ότι τα προσωπικά δεδομένα — είτε αφορούν πελάτες, προσωπικό ή συνεργάτες — συλλέγονται, χρησιμοποιούνται, αποθηκεύονται και διαγράφονται με νόμιμο, θεμιτό και ασφαλή τρόπο.

1.3. Η παρούσα πολιτική διασφαλίζει επίσης τη συμμόρφωση με το ISO/IEC 27001:2022 και υποστηρίζει την ετοιμότητα για έλεγχο, εφαρμόζοντας συνεπή προσέγγιση προστασίας της ιδιωτικότητας βάσει κινδύνου.

1.4. Μέσω της παρούσας πολιτικής, ο οργανισμός αποδεικνύει λογοδοσία και ενισχύει την εμπιστοσύνη των πελατών, δίνοντας προτεραιότητα στη διαφάνεια, την ελαχιστοποίηση δεδομένων και την ισχυρή διακυβέρνηση της ιδιωτικότητας.

2. Πεδίο εφαρμογής

2.1. Η παρούσα πολιτική εφαρμόζεται σε:

2.1.1. Όλους τους εργαζομένους, αναδόχους ή παρόχους υπηρεσιών που αποκτούν πρόσβαση, επεξεργάζονται ή διαχειρίζονται προσωπικά δεδομένα

2.1.2. Κάθε σύστημα, εφαρμογή ή τοποθεσία όπου αποθηκεύονται ή διαβιβάζονται προσωπικά δεδομένα

2.1.3. Όλα τα προσωπικά δεδομένα, είτε αποθηκεύονται ηλεκτρονικά, σε έντυπη μορφή, σε υποδομές νέφους ή σε φορητές συσκευές

2.2. Η παρούσα πολιτική εφαρμόζεται σε δεδομένα που σχετίζονται με πελάτες, προσωπικό, προμηθευτές και κάθε άλλο ταυτοποιήσιμο φυσικό πρόσωπο.

2.3. Η πολιτική παραμένει σε ισχύ ανεξαρτήτως του εάν η επεξεργασία των δεδομένων πραγματοποιείται εσωτερικά ή από τρίτους παρόχους υπηρεσιών.

3. Στόχοι

3.1. Να διασφαλίζεται ότι τα προσωπικά δεδομένα τυγχάνουν διαχείρισης σύμφωνα με τη νομοθεσία περί ιδιωτικότητας και τα πρότυπα ασφάλειας, συμπεριλαμβανομένων του ΓΚΠΔ της ΕΕ, της Οδηγίας NIS2 της ΕΕ και του ISO/IEC 27001.

3.2. Να προστατεύονται τα προσωπικά δεδομένα από μη εξουσιοδοτημένη πρόσβαση, κακή χρήση, αλλοίωση ή απώλεια μέσω σαφών τεχνικών και οργανωτικών μέτρων.

3.3. Να διασφαλίζονται τα δικαιώματα ιδιωτικότητας των φυσικών προσώπων, συμπεριλαμβανομένου του δικαιώματος πρόσβασης, διόρθωσης και διαγραφής των δεδομένων τους.

3.4. Να καθορίζονται σαφείς ρόλοι και αρμοδιότητες για την προστασία δεδομένων εντός του οργανισμού.

3.5. Να εφαρμόζονται η ελαχιστοποίηση δεδομένων, η ασφαλής διατήρηση και η έγκαιρη διαγραφή σε όλα τα συστήματα και τις διαδικασίες.

3.6. Να μειώνεται ο κίνδυνος μη συμμόρφωσης, νομικών κυρώσεων, βλάβης της φήμης ή απώλειας εμπιστοσύνης των πελατών.

4. Ρόλοι και αρμοδιότητες

4.1. Γενικός Διευθυντής

4.1.1. Εγκρίνει την παρούσα πολιτική και διασφαλίζει την εφαρμογή της

4.1.2. Παρέχει τους αναγκαίους πόρους για τη διαχείριση των κινδύνων ιδιωτικότητας και την απόκριση σε περιστατικά

4.1.3. Έχει τη συνολική λογοδοσία για τη συμμόρφωση με τη νομοθεσία και τα πρότυπα ιδιωτικότητας

4.2. Υπεύθυνος Προστασίας Δεδομένων ή Συντονιστής Ιδιωτικότητας (εσωτερικός ή εξωτερικός)

4.2.1. Τηρεί αρχεία δραστηριοτήτων επεξεργασίας δεδομένων

4.2.2. Ανταποκρίνεται σε αιτήματα άσκησης δικαιωμάτων των υποκειμένων των δεδομένων και σε ερωτήματα των αρμόδιων αρχών

4.2.3. Υποστηρίζει την αξιολόγηση κινδύνων, την εκπαίδευση και την εφαρμογή της πολιτικής

4.2.4. Τεκμηριώνει περιστατικά παραβίασης και προβαίνει σε γνωστοποίηση στις αρμόδιες αρχές όταν απαιτείται

[... 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. Προγραμματισμένες ανασκοπήσεις

9.1.1. Η παρούσα πολιτική πρέπει να ανασκοπείται τουλάχιστον μία φορά κάθε 12 μήνες από τον Υπεύθυνο Προστασίας Δεδομένων ή τον Συντονιστή Ιδιωτικότητας και να εγκρίνεται από τον Γενικό Διευθυντή

9.1.2. Η ανασκόπηση πρέπει να αξιολογεί τη συνάφεια της πολιτικής, την κανονιστική ευθυγράμμιση και τη λειτουργική αποτελεσματικότητα

9.2. Εναύσματα για ενδιάμεση ανασκόπηση

9.2.1. Η επικαιροποίηση της πολιτικής πρέπει επίσης να δρομολογείται σε απόκριση σε:

9.2.1.1. Νέα ή αναθεωρημένη νομοθεσία προστασίας δεδομένων (π.χ. ΓΚΠΔ της ΕΕ, Κανονισμός DORA της ΕΕ)

9.2.1.2. Περιστατικά ασφάλειας ή παραβιάσεις ιδιωτικότητας που αφορούν προσωπικά δεδομένα

9.2.1.3. Θέση σε λειτουργία νέων συστημάτων, εργαλείων ή υπηρεσιών που επεξεργάζονται προσωπικά δεδομένα

9.2.1.4. Ουσιώδη ευρήματα ελέγχου ή συστάσεις αρμόδιων αρχών

9.3. Έλεγχος αλλαγών και επικοινωνία

9.3.1. Όλες οι αλλαγές στην πολιτική πρέπει να τεκμηριώνονται επίσημα σε αρχείο μεταβολών

9.3.2. Οι αναθεωρημένες εκδόσεις πρέπει να διανέμονται σε όλο το προσωπικό και στους σχετικούς αναδόχους

9.3.3. Οι αρχειοθετημένες εκδόσεις πρέπει να διατηρούνται για σκοπούς διαδρομής ελέγχου συμμόρφωσης

10. Συναφείς πολιτικές και διασυνδέσεις

10.1. Η παρούσα πολιτική λειτουργεί σε συνδυασμό με άλλες πολιτικές SME για τη δημιουργία ενός πλήρους και εφαρμόσιμου πλαισίου ιδιωτικότητας:

10.1.1. P13S – Πολιτική Ταξινόμησης και Επισήμανσης Δεδομένων: Διασφαλίζει ότι τα προσωπικά δεδομένα ταξινομούνται κατάλληλα, ώστε να μπορούν να εφαρμόζονται μέτρα προστασίας της ιδιωτικότητας βάσει κινδύνου.

10.1.2. P14S – Πολιτική Διατήρησης και Διάθεσης Δεδομένων: Παρέχει σαφείς κανόνες για το χρονικό διάστημα διατήρησης των προσωπικών δεδομένων και τις ασφαλείς μεθόδους διάθεσής τους μετά τη λήξη της περιόδου διατήρησης.

10.1.3. P16S – Πολιτική Απόκρυψης Δεδομένων και Ψευδωνυμοποίησης: Καθορίζει πώς πρέπει να μετασχηματίζονται τα προσωπικά αναγνωριστικά πριν από τη χρήση δεδομένων σε περιβάλλον μη παραγωγικής λειτουργίας ή πριν από την εξωτερική κοινοποίησή τους.

10.1.4. P30S – Πολιτική Αντιμετώπισης Περιστατικών: Καλύπτει τα βήματα που απαιτούνται για την απόκριση σε παραβιάσεις δεδομένων, συμπεριλαμβανομένης της γνωστοποίησης σε αρμόδιες αρχές και επηρεαζόμενα φυσικά πρόσωπα εντός των απαιτούμενων προθεσμιών.

10.1.5. P2S – Πολιτική Ρόλων και Αρμοδιοτήτων Διακυβέρνησης: Αποσαφηνίζει τη δομή λογοδοσίας και τους ρόλους λήψης αποφάσεων που εφαρμόζονται στην εφαρμογή και την εποπτεία της ιδιωτικότητας.

10.2. Οι συναφείς αυτές πολιτικές πρέπει να ανασκοπούνται και να εφαρμόζονται από κοινού, ώστε να διασφαλίζεται ολοκληρωμένη κάλυψη της ιδιωτικότητας σε συστήματα, προσωπικό και προμηθευτές.

11. Πρότυπα και πλαίσια αναφοράς

11.1. ISO/IEC 27001

11.1.1. Ρήτρα 5.1 – Απαιτεί από την ανώτατη διοίκηση να επιδεικνύει ηγεσία και δέσμευση για την προστασία των προσωπικών δεδομένων.

11.1.2. Ρήτρα 6.1.3 – Επιβάλλει την αντιμετώπιση των κινδύνων που σχετίζονται με την επεξεργασία προσωπικών πληροφοριών.

11.1.3. Ρήτρα 8.1 – Απαιτεί την εφαρμογή λειτουργικών ελέγχων για την προστασία των δεδομένων καθ' όλη τη διάρκεια του κύκλου ζωής τους.

11.2. ISO/IEC 27002

11.2.1. Έλεγχος 5.34 – Παρέχει οδηγίες εφαρμογής για την προστασία της ιδιωτικότητας και τον ασφαλή χειρισμό προσωπικά ταυτοποιήσιμων πληροφοριών (PII).

11.2.2. Έλεγχος 8.10 – Αντιμετωπίζει την ασφαλή διάθεση προσωπικών δεδομένων ώστε να αποτρέπεται η υπολειμματική γνωστοποίηση.

11.2.3. Έλεγχος 8.11 – Υποστηρίζει τη χρήση απόκρυψης και ψευδωνυμοποίησης για την ελαχιστοποίηση δεδομένων.

11.2.4. Έλεγχος 8.12 – Αποτρέπει τη μη εξουσιοδοτημένη διαρροή δεδομένων μέσω ελέγχων στην πρόσβαση και τη χρήση των δεδομένων.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AR-2 – Αναθέτει ρόλους και αρμοδιότητες για τη διαχείριση του κινδύνου ιδιωτικότητας.

11.3.2. PL-5 – Απαιτεί την τεκμηρίωση σχεδίου ιδιωτικότητας που καλύπτει τη χρήση και την προστασία δεδομένων.

11.3.3. AC-6 – Επιβάλλει την αρχή του ελάχιστου προνομίου και τον έλεγχο πρόσβασης για προσωπικά δεδομένα.

11.3.4. IR-4 – Απαιτεί διαδικασίες χειρισμού περιστατικών για παραβιάσεις που αφορούν προσωπικά δεδομένα.

11.4. ΓΚΠΔ της ΕΕ

11.4.1. Άρθρο 5 – Ορίζει τις βασικές αρχές της νόμιμης, θεμιτής και διαφανούς επεξεργασίας δεδομένων.

11.4.2. Άρθρο 6 – Απαιτεί έγκυρη νομική βάση για κάθε δραστηριότητα επεξεργασίας προσωπικών δεδομένων.

11.4.3. Άρθρα 12–23 – Περιγράφουν τα δικαιώματα των υποκειμένων των δεδομένων, συμπεριλαμβανομένων της πρόσβασης, της διόρθωσης, της διαγραφής και της εναντίωσης.

11.4.4. Άρθρο 30 – Επιβάλλει την τήρηση αρχείων δραστηριοτήτων επεξεργασίας.

11.4.5. Άρθρο 32 – Απαιτεί κατάλληλα τεχνικά και οργανωτικά μέτρα ασφάλειας.

11.4.6. Άρθρα 33–34 – Καθορίζουν τις υποχρεώσεις γνωστοποίησης παραβίασης προς τις αρχές και τα υποκείμενα των δεδομένων.

11.5. Οδηγία NIS2 της ΕΕ

11.5.1. Άρθρο 21(2)(e) – Απαιτεί μέτρα για τη διασφάλιση της προστασίας δεδομένων σε ευθυγράμμιση με τις πολιτικές κυβερνοασφάλειας.

11.5.2. Άρθρο 21(2)(f) – Επιβάλλει μηχανισμούς για τη διαχείριση της ασφάλειας προσωπικών και εμπιστευτικών δεδομένων σε συστήματα ΤΠΕ.

11.6. Κανονισμός DORA της ΕΕ

11.6.1. Άρθρο 6 – Απαιτεί εσωτερικά πλαίσια διακυβέρνησης που διαχειρίζονται τον κίνδυνο και την προστασία δεδομένων.

11.6.2. Άρθρο 15 – Υποχρεώνει τις χρηματοοικονομικές οντότητες να διασφαλίζουν ότι οι τρίτοι πάροχοι προστατεύουν τα προσωπικά δεδομένα και υποστηρίζουν τη συμμόρφωση με τις κανονιστικές απαιτήσεις.

11.6.3. Άρθρο 17 – Απαιτεί από τους οργανισμούς να διασφαλίζουν ότι τα συστήματα ΤΠΕ που επεξεργάζονται προσωπικά δεδομένα είναι ασφαλή, ανθεκτικά και τελούν υπό παρακολούθηση.

11.7. COBIT 2019

11.7.1. APO12 – Διαχείριση Κινδύνων: Απαιτεί αναγνώριση και αντιμετώπιση κινδύνων ιδιωτικότητας και προστασίας δεδομένων.

11.7.2. DSS05 – Διαχείριση Υπηρεσιών Ασφάλειας: Επιβάλλει δικλίδες ασφαλείας για την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε προσωπικά δεδομένα.

11.7.3. MEA03 – Παρακολούθηση συμμόρφωσης: Απαιτεί από τους οργανισμούς να διασφαλίζουν συνεχή συμμόρφωση με τη νομοθεσία περί ιδιωτικότητας και προστασίας δεδομένων.