					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: PII15					Τίτλος εγγράφου: **Πολιτική διαχείρισης περιστατικών και παραβιάσεων δεδομένων προσωπικού χαρακτήρα**							
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 / Κανονιστική πράξη	Ρήτρα / Έλεγχος / Άρθρο	Εφαρμοσιμότητα	Τύπος κάλυψης	Σχόλιο
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Επικοινωνίες PIMS και τεκμηριωμένα τεκμήρια παραβίασης
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Επιχειρησιακός έλεγχος και σύνδεση με την αξιολόγηση κινδύνου ιδιωτικότητας και την αντιμετώπισή του
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Παρακολούθηση, αξιολόγηση, μη συμμόρφωση, διορθωτικά μέτρα και βελτίωση
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Σχεδιασμός και προετοιμασία διαχείρισης περιστατικών για την επεξεργασία δεδομένων προσωπικού χαρακτήρα
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Απόκριση σε περιστατικά ασφάλειας πληροφοριών που αφορούν δεδομένα προσωπικού χαρακτήρα
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Νομικές, καταστατικές, κανονιστικές και συμβατικές απαιτήσεις και προστασία αρχείων
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Υποστήριξη συμφωνίας πελάτη εκτελούντος την επεξεργασία και υποχρεώσεων πελάτη

GDPR	Article 5(2); Article 24	Controller	Supporting	Λογοδοσία και ευθύνη υπευθύνου επεξεργασίας
GDPR	Article 26	Joint Controller	Supporting	Συντονισμός ευθύνης παραβίασης μεταξύ από κοινού υπευθύνων επεξεργασίας
GDPR	Article 28	Both	Supporting	Συνδρομή εκτελούντος την επεξεργασία και συμβατικές υποχρεώσεις εκτελούντος την επεξεργασία
GDPR	Article 32	Both	Supporting	Ασφάλεια της επεξεργασίας και δυνατότητα ανίχνευσης παραβιάσεων
GDPR	Article 33	Both	Primary	Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα και τεκμηρίωση παραβίασης
GDPR	Article 34	Controller	Primary	Επικοινωνία παραβιάσεων δεδομένων προσωπικού χαρακτήρα προς τα επηρεαζόμενα υποκείμενα των δεδομένων προσωπικού χαρακτήρα
GDPR	Article 39	Conditional	Supporting	Συμβουλές DPO, παρακολούθηση, συνεργασία και υποστήριξη σημείου επαφής
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Αρχές ασφάλειας πληροφοριών και συμμόρφωσης ιδιωτικότητας
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Αρμοδιότητες απόκρισης σε

				περιστατικά δεδομένων προσωπικού χαρακτήρα και αναφορά συμβάντων
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Σχεδιασμός, αξιολόγηση, απόκριση, διδάγματα που αντλήθηκαν και συλλογή τεκμηρίων για περιστατικά
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Κύκλος ζωής της διαδικασίας διαχείρισης περιστατικών
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Πολιτική, σχέδιο, ευαισθητοποίηση, δοκιμές και διδάγματα που αντλήθηκαν για περιστατικά
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Λειτουργίες ανίχνευσης, γνωστοποίησης, αρχικής αξιολόγησης, ανάλυσης, απόκρισης και αναφοράς
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Προσδοκίες για γνωστοποίηση από εκτελούντα την επεξεργασία σε περιβάλλον νέφους και για αρχεία παραβιάσεων
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Αναφορά σημαντικών περιστατικών όπου εφαρμόζεται
DORA Regulation (EU) 2022/2554	Article 17; Article 18; Article 19	Conditional	Supporting	Διαχείριση, ταξινόμηση και αναφορά περιστατικών ICT όπου εφαρμόζεται

1. Πεδίο εφαρμογής

1.1 Η παρούσα πολιτική ορίζει τις απαιτήσεις για την αναγνώριση, αναφορά, αρχική αξιολόγηση, εκτίμηση, περιορισμό, γνωστοποίηση, τεκμηρίωση, κλείσιμο και βελτίωση από περιστατικά που αφορούν δεδομένα προσωπικού χαρακτήρα και παραβιάσεις δεδομένων προσωπικού χαρακτήρα εντός του πεδίου εφαρμογής του PIMS.

1.2 Η παρούσα πολιτική εφαρμόζεται σε:

1.2.1 τον οργανισμό όταν ενεργεί ως υπεύθυνος επεξεργασίας δεδομένων προσωπικού χαρακτήρα·

1.2.2 τον οργανισμό όταν ενεργεί ως από κοινού υπεύθυνος επεξεργασίας όπου απαιτείται συντονισμός της ευθύνης για παραβίαση·

1.2.3 τον οργανισμό όταν ενεργεί ως εκτελών την επεξεργασία δεδομένων προσωπικού χαρακτήρα·

1.2.4 τον οργανισμό όταν ενεργεί ως υπεργολάβος επεξεργασίας·

1.2.5 συστήματα, εφαρμογές, υπηρεσίες, διεργασίες, προμηθευτές, εκτελούντες την επεξεργασία, υπεργολάβους επεξεργασίας και τρίτα μέρη που επεξεργάζονται, αποθηκεύουν, μεταδίδουν, υποστηρίζουν, προσπελαύνουν ή επηρεάζουν με οποιονδήποτε άλλο τρόπο δεδομένα προσωπικού χαρακτήρα εντός του πεδίου εφαρμογής του PIMS.

1.3 Η παρούσα πολιτική χρησιμοποιεί το REG10 - Μητρώο περιστατικών και παραβιάσεων δεδομένων προσωπικού χαρακτήρα ως το κύριο αντικείμενο τεκμηρίων για τη διαχείριση περιστατικών και παραβιάσεων δεδομένων προσωπικού χαρακτήρα.

1.4 Η παρούσα πολιτική χρησιμοποιεί υποστηρικτικά αντικείμενα τεκμηρίων ως εξής:

1.4.1 REG01 για το πεδίο εφαρμογής του PIMS και το πλαίσιο εφαρμοστέων ενδιαφερόμενων μερών, νομικών, συμβατικών, κλαδικών και πελατειακών απαιτήσεων αναφοράς.

1.4.2 REG02 για επηρεαζόμενες δραστηριότητες επεξεργασίας, κατηγορίες δεδομένων προσωπικού χαρακτήρα, κατηγορίες υποκειμένων των δεδομένων προσωπικού χαρακτήρα, σκοπούς και συστήματα.

1.4.3 REG03 για τη Δήλωση Εφαρμοσιμότητας και τις επικαιροποιήσεις εφαρμοσιμότητας ελέγχων.

1.4.4 REG04 για τη σύνδεση με τον κίνδυνο ιδιωτικότητας, την DPIA και τον υπολειπόμενο κίνδυνο.

1.4.5 REG08 για τεκμήρια διεπαφής περιστατικών με εκτελούντες την επεξεργασία, υπεργολάβους επεξεργασίας, πελάτες, προμηθευτές και τρίτα μέρη.

1.4.6 REG09 για σύνδεση με διεθνείς διαβιβάσεις όταν ένα περιστατικό επηρεάζει διασυνοριακή επεξεργασία.

1.4.7 REG11 για τεκμήρια εκπαίδευσης, ευαισθητοποίησης και επάρκειας απόκρισης σε περιστατικά.

1.4.8 REG12 για τεκμήρια ελέγχου, μη συμμόρφωσης, διορθωτικών μέτρων και βελτίωσης.

1.5 Η παρούσα πολιτική βασίζεται σε συναφείς πολιτικές PIMS για εξειδικευμένους ελέγχους:

1.5.1 Η PII03 διέπει το αποθετήριο επεξεργασίας και τα αρχεία νομικής βάσης.

1.5.2 Η PII04 διέπει τους ελέγχους ειδοποίησης ιδιωτικότητας και διαφάνειας εκτός των επικοινωνιών που αφορούν ειδικά παραβίαση.

1.5.3 Η PII06 διέπει αιτήματα άσκησης δικαιωμάτων υποκειμένων των δεδομένων προσωπικού χαρακτήρα που προκύπτουν πριν, κατά τη διάρκεια ή μετά από περιστατικό.

1.5.4 Η PII07 διέπει τη μεθοδολογία αξιολόγησης κινδύνου ιδιωτικότητας και DPIA.

1.5.5 Η PII08 διέπει τους ελέγχους ιδιωτικότητας ήδη από τον σχεδιασμό και εξ ορισμού.

1.5.6 Η PII10 διέπει τους ελέγχους διατήρησης, διαγραφής και διάθεσης.

1.5.7 Η PII12 διέπει τους ελέγχους σχέσεων ιδιωτικότητας με εκτελούντες την επεξεργασία, υπεργολάβους επεξεργασίας, προμηθευτές και τρίτα μέρη.

1.5.8 Η PII13 διέπει τους μηχανισμούς διεθνούς διαβίβασης δεδομένων προσωπικού χαρακτήρα και τα αρχεία κινδύνου διαβίβασης.

1.5.9 Η PII14 διέπει τους προληπτικούς και ανιχνευτικούς ελέγχους ασφάλειας και πρόσβασης δεδομένων προσωπικού χαρακτήρα.

1.5.10 Η PII16 διέπει την εκπαίδευση, την ευαισθητοποίηση και την επάρκεια σε θέματα ιδιωτικότητας.

1.5.11 Η PII17 διέπει τις τεκμηριωμένες πληροφορίες και τη διαχείριση τεκμηρίων.

1.5.12 Η PII18 διέπει την παρακολούθηση, τον εσωτερικό έλεγχο, την ανασκόπηση της διοίκησης, τη μη συμμόρφωση, τα διορθωτικά μέτρα και τη συνεχή βελτίωση.

1.6 Για την παρούσα πολιτική:

1.6.1 «Περιστατικό που αφορά δεδομένα προσωπικού χαρακτήρα» σημαίνει ύποπτο ή επιβεβαιωμένο συμβάν που έχει επηρεάσει, ενδέχεται να έχει επηρεάσει ή θα μπορούσε ευλόγως να επηρεάσει την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα, τη νόμιμη επεξεργασία ή τον εξουσιοδοτημένο χειρισμό δεδομένων προσωπικού χαρακτήρα.

1.6.2 «Παραβίαση δεδομένων προσωπικού χαρακτήρα» σημαίνει επιβεβαιωμένο περιστατικό που αφορά δεδομένα προσωπικού χαρακτήρα και περιλαμβάνει μη εξουσιοδοτημένη, παράνομη, τυχαία ή ακούσια καταστροφή, απώλεια, αλλοίωση, κοινολόγηση, πρόσβαση, μη διαθεσιμότητα ή συμβιβασμό δεδομένων προσωπικού χαρακτήρα.

1.6.3 «Αξιολόγηση παραβίασης» σημαίνει την τεκμηριωμένη αξιολόγηση του κατά πόσον ένα περιστατικό που αφορά δεδομένα προσωπικού χαρακτήρα συνιστά παραβίαση δεδομένων προσωπικού χαρακτήρα, ποια δεδομένα προσωπικού χαρακτήρα και ποια υποκείμενα των δεδομένων προσωπικού χαρακτήρα επηρεάζονται, ποιοι κίνδυνοι ενδέχεται να προκύψουν, ποιες γνωστοποιήσεις ή επικοινωνίες απαιτούνται και ποια διορθωτική ενέργεια χρειάζεται.

1.6.4 «Επίγνωση» σημαίνει το σημείο κατά το οποίο ο οργανισμός έχει εύλογο βαθμό βεβαιότητας ότι έχει συμβεί περιστατικό ασφάλειας ή ιδιωτικότητας και ότι δεδομένα προσωπικού χαρακτήρα έχουν συμβιβαστεί ή ενδέχεται να έχουν συμβιβαστεί.

1.6.5 «Περιστατικό που αφορά δεδομένα προσωπικού χαρακτήρα υψηλού αντικτύπου» σημαίνει περιστατικό που αφορά δεδομένα προσωπικού χαρακτήρα και το οποίο σχετίζεται με επεξεργασία υψηλού κινδύνου, ειδικές κατηγορίες ή εξαιρετικά ευαίσθητα δεδομένα προσωπικού χαρακτήρα, μεγάλης κλίμακας δεδομένα προσωπικού χαρακτήρα, ευάλωτα φυσικά πρόσωπα, ρυθμιζόμενους πελάτες, αντίκτυπο σε πολλές δικαιοδοσίες, ουσιώδη αντίκτυπο σε πελάτες, συμβιβασμό προνομιούχας πρόσβασης, δημόσια έκθεση, ransomware, μη διαθεσιμότητα υπηρεσίας ή σημαντικό επιχειρησιακό αντίκτυπο ή αντίκτυπο στη φήμη.

1.6.6 «Ουσιώδης αλλαγή περιστατικού» σημαίνει νέα ή μεταβληθείσα πληροφορία που επηρεάζει το πεδίο, τη σοβαρότητα, τις κατηγορίες δεδομένων προσωπικού χαρακτήρα, τον αντίκτυπο στα υποκείμενα των δεδομένων προσωπικού χαρακτήρα, την απόφαση γνωστοποίησης, τον αντίκτυπο σε πελάτες, τη βασική αιτία, τον περιορισμό, την ανάκαμψη, τα διορθωτικά μέτρα ή τις υποχρεώσεις εξωτερικής αναφοράς του περιστατικού.

2. Σκοπός

2.1 Σκοπός της παρούσας πολιτικής είναι να διασφαλίζει ότι τα περιστατικά που αφορούν δεδομένα προσωπικού χαρακτήρα και οι παραβιάσεις δεδομένων προσωπικού χαρακτήρα αντιμετωπίζονται με συνέπεια, έγκαιρα, νόμιμα, με ασφάλεια και με τεκμήρια έτοιμα για έλεγχο.

2.2 Η παρούσα πολιτική υποστηρίζει τη λογοδοσία απαιτώντας τα περιστατικά που αφορούν δεδομένα προσωπικού χαρακτήρα και οι παραβιάσεις δεδομένων προσωπικού χαρακτήρα να καταγράφονται στο REG10 και να συνδέονται με επηρεαζόμενα αρχεία επεξεργασίας, κινδύνους ιδιωτικότητας, σχέσεις με εκτελούντες την επεξεργασία και υπεργολάβους επεξεργασίας, αρχεία διαβιβάσεων, διορθωτικά μέτρα και αρχεία εκπαίδευσης, όταν ενεργοποιούνται.

2.3 Η παρούσα πολιτική διασφαλίζει ότι οι υποχρεώσεις υπευθύνου επεξεργασίας, από κοινού υπευθύνου επεξεργασίας, εκτελούντος την επεξεργασία και υπεργολάβου επεξεργασίας αντιμετωπίζονται μέσω διακριτών κανόνων εφαρμοσιμότητας, διατηρώντας παράλληλα ένα ενιαίο μοντέλο τεκμηρίων περιστατικών και παραβιάσεων.

3. Στόχοι

3.1 Οι στόχοι της παρούσας πολιτικής είναι να:

3.1.1 διασφαλίζει ότι τα ύποπτα περιστατικά που αφορούν δεδομένα προσωπικού χαρακτήρα αναφέρονται και καταγράφονται έγκαιρα·

3.1.2 διασφαλίζει ότι τα περιστατικά που αφορούν δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε αρχική αξιολόγηση και ταξινομούνται με συνεπή κριτήρια·

3.1.3 διασφαλίζει ότι οι αξιολογήσεις παραβίασης εξετάζουν τα επηρεαζόμενα δεδομένα προσωπικού χαρακτήρα, τα υποκείμενα των δεδομένων προσωπικού χαρακτήρα, τα συστήματα, τις δραστηριότητες επεξεργασίας, τους εκτελούντες την επεξεργασία, τους υπεργολάβους επεξεργασίας, τις διαβιβάσεις, τους κινδύνους και τις διορθωτικές ενέργειες·

3.1.4 διασφαλίζει ότι οι αποφάσεις γνωστοποίησης από υπεύθυνο επεξεργασίας και επικοινωνίας με υποκείμενα των δεδομένων προσωπικού χαρακτήρα τεκμηριώνονται·

3.1.5 διασφαλίζει ότι οι γνωστοποιήσεις παραβίασης από εκτελούντες την επεξεργασία και υπεργολάβους επεξεργασίας προς πελάτες ή ανάντη μέρη πραγματοποιούνται χωρίς αδικαιολόγητη καθυστέρηση και σύμφωνα με τις εφαρμοστέες συμφωνίες·

3.1.6 διασφαλίζει ότι τα τεκμήρια διατηρούνται και προστατεύονται κατά τον χειρισμό περιστατικών·

3.1.7 διασφαλίζει ότι ο περιορισμός, η εξάλειψη, η ανάκαμψη και η επικύρωση παρακολουθούνται μέσω του REG10·

3.1.8 διασφαλίζει ότι αξιολογούνται, όπου εφαρμόζεται, τα εναύσματα ρυθμιζόμενης, συμβατικής, πελατειακής και κλαδικής αναφοράς·

3.1.9 διασφαλίζει ότι τα διδάγματα που αντλήθηκαν από περιστατικά οδηγούν σε διορθωτικά μέτρα και συνεχή βελτίωση·

3.1.10 διασφαλίζει ότι τα αρχεία περιστατικών και παραβιάσεων είναι διαθέσιμα για έλεγχο, ανασκόπηση της διοίκησης, διασφάλιση πελατών και κανονιστική ανασκόπηση, όπου εφαρμόζεται.

4. Δηλώσεις πολιτικής

4.1 Ετοιμότητα και υποδοχή περιστατικών

4.1.1 [Both] The Privacy Lead / PIMS Manager MUST τηρεί κριτήρια χειρισμού περιστατικών και παραβιάσεων δεδομένων προσωπικού χαρακτήρα στο REG10 τουλάχιστον ετησίως και μετά από κάθε ουσιώδη αλλαγή στο πεδίο εφαρμογής του PIMS, στο νομικό πλαίσιο, στις συμβατικές υποχρεώσεις ή στην επεξεργασία υψηλού κινδύνου.

4.1.2 [All] The Incident Response Coordinator MUST καταγράφει κάθε αναφερθέν ή ανιχνευθέν ύποπτο περιστατικό που αφορά δεδομένα προσωπικού χαρακτήρα στο REG10 εντός μίας εργάσιμης ημέρας από την παραλαβή του ή νωρίτερα όταν μπορεί να ενεργοποιηθεί εφαρμοστέο χρονοδιάγραμμα γνωστοποίησης ή αναφοράς προς πελάτη.

4.1.3 [Both] The System Owner / Application Owner MUST διατηρεί συναφή αρχεία καταγραφής συστήματος, ειδοποιήσεις, αρχεία πρόσβασης, τεκμήρια ρύθμισης παραμέτρων και τεκμήρια ανάκαμψης που συνδέονται με το REG10, όταν ύποπτο περιστατικό επηρεάζει σύστημα ή εφαρμογή που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα.

4.1.4 [Both] The Information Security Lead MUST ολοκληρώνει την αρχική τεχνική αξιολόγηση κάθε συμβάντος ασφάλειας που αφορά δεδομένα προσωπικού χαρακτήρα εντός 24 ωρών από την ανίχνευση και καταγράφει την αρχική σοβαρότητα, τα επηρεαζόμενα περιουσιακά στοιχεία και την κατάσταση περιορισμού στο REG10.

4.2 Ταξινόμηση και αξιολόγηση παραβίασης

4.2.1 [Both] The Incident Response Coordinator MUST ταξινομεί κάθε καταχώριση REG10 ως συμβάν που δεν αφορά δεδομένα προσωπικού χαρακτήρα, ύποπτο περιστατικό που αφορά δεδομένα προσωπικού χαρακτήρα, επιβεβαιωμένο περιστατικό που αφορά δεδομένα προσωπικού χαρακτήρα ή επιβεβαιωμένη παραβίαση δεδομένων προσωπικού χαρακτήρα εντός 24 ωρών από την υποδοχή ή επικαιροποιεί την καταχώριση REG10 με τον λόγο για τον οποίο η ταξινόμηση παραμένει σε εκκρεμότητα.

4.2.2 [Both] The Privacy Lead / PIMS Manager MUST προσδιορίζει την επηρεαζόμενη δραστηριότητα επεξεργασίας, τις κατηγορίες δεδομένων προσωπικού χαρακτήρα, τις κατηγορίες υποκειμένων των δεδομένων προσωπικού χαρακτήρα, τα συστήματα, τους εκτελούντες την επεξεργασία, τους υπεργολάβους επεξεργασίας, τις τοποθεσίες διαβίβασης και τους κινδύνους ιδιωτικότητας στα REG02, REG04, REG08, REG09 και REG10 πριν οριστικοποιηθεί η απόφαση γνωστοποίησης παραβίασης.

4.2.3 [Controller] The Data Protection Officer / Privacy Advisor MUST αξιολογεί τον κίνδυνο για τα επηρεαζόμενα υποκείμενα των δεδομένων προσωπικού χαρακτήρα για κάθε επιβεβαιωμένη ή ευλόγως ύποπτη παραβίαση δεδομένων προσωπικού χαρακτήρα και καταγράφει τη σύσταση γνωστοποίησης, την αιτιολόγηση κινδύνου και τις συμβουλές στο REG10 πριν ληφθεί η απόφαση εξωτερικής γνωστοποίησης.

4.2.4 [Processor] The Privacy Lead / PIMS Manager MUST προσδιορίζει τον επηρεαζόμενο υπεύθυνο επεξεργασίας ή πελάτη και τις εφαρμοστέες συμβατικές απαιτήσεις γνωστοποίησης μόλις ο οργανισμός λάβει γνώση παραβίασης δεδομένων προσωπικού χαρακτήρα που επηρεάζει δεδομένα προσωπικού χαρακτήρα πελάτη, και MUST καταγράφει το αποτέλεσμα στα REG08 και REG10.

4.2.5 [Joint Controller] The Privacy Lead / PIMS Manager MUST επαληθεύει τη συμφωνημένη ευθύνη παραβίασης, την κύρια ευθύνη επικοινωνίας και τη ρύθμιση συντονισμού πριν από οποιαδήποτε εξωτερική γνωστοποίηση ή επικοινωνία από από κοινού υπεύθυνο επεξεργασίας, και MUST καταγράφει την απόφαση στα REG08 και REG10.

4.2.6 [Conditional] The Privacy Lead / PIMS Manager MUST αξιολογεί τα εφαρμοστέα εναύσματα αναφοράς που απορρέουν από νομικές, κλαδικές, χρηματοοικονομικού τομέα, κυβερνοασφάλειας, συμβατικές, πελατειακές απαιτήσεις και απαιτήσεις αποδεκτών υπηρεσιών για κάθε περιστατικό που αφορά δεδομένα προσωπικού χαρακτήρα υψηλού αντικτύπου και καταγράφει το αποτέλεσμα εφαρμοσιμότητας στα REG01, REG08 και REG10.

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

9. Εξαιρέσεις

9.1.1 [Both] The Privacy Lead / PIMS Manager MUST καταγράφει κάθε εξαίρεση από την παρούσα πολιτική στο REG12 πριν από την εφαρμογή ή εντός 24 ωρών μετά από επείγουσα ενέργεια όταν δεν ήταν εφικτή η προηγούμενη έγκριση.

9.1.2 [Both] Top Management MUST εγκρίνει κάθε εξαίρεση που επηρεάζει ουσιωδώς τον χρόνο γνωστοποίησης παραβίασης, τη δημόσια επικοινωνία, τη δέσμευση προς πελάτη, τη διατήρηση τεκμηρίων ή τον κίνδυνο για υποκείμενα των δεδομένων προσωπικού χαρακτήρα πριν κλείσει το περιστατικό, με τα τεκμήρια έγκρισης να διατηρούνται στα REG10 και REG12.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST τεκμηριώνει συμβουλές για κάθε καθυστερημένη γνωστοποίηση, απόφαση μη γνωστοποίησης ή εξαιρετική προσέγγιση επικοινωνίας πριν από το κλείσιμο του περιστατικού, με τις συμβουλές να διατηρούνται στο REG10.

9.1.4 [Both] The Vendor / Procurement Owner MUST καταγράφει εξαιρέσεις που επιβάλλονται από προμηθευτή, εκτελούντα την επεξεργασία, υπεργολάβο επεξεργασίας ή πελάτη και επηρεάζουν την απόκριση σε περιστατικό στα REG08 και REG12 εντός πέντε εργάσιμων ημερών από τον εντοπισμό της εξαίρεσης.

10. Εφαρμογή

10.1.1 [All] The Process Owner / Business Owner MUST κλιμακώνει την αποτυχία αναφοράς ύποπτου περιστατικού που αφορά δεδομένα προσωπικού χαρακτήρα, διατήρησης τεκμηρίων, τήρησης ανατεθειμένων ενεργειών ή συνεργασίας με την αξιολόγηση παραβίασης προς το Privacy Lead / PIMS Manager εντός δύο εργάσιμων ημερών από την ανακάλυψη, με τα τεκμήρια να διατηρούνται στο REG12.

10.1.2 [Both] The Privacy Lead / PIMS Manager MUST καταγράφει μη συμμόρφωση REG12 όταν παραβίαση της παρούσας πολιτικής επηρεάζει την υποδοχή περιστατικού, την αρχική αξιολόγηση, τον περιορισμό, τη γνωστοποίηση, την ακεραιότητα τεκμηρίων, την επικοινωνία ή τη διορθωτική ενέργεια.

10.1.3 [Both] The Vendor / Procurement Owner MUST εκκινεί αποκατάσταση προμηθευτή ή εκτελούντος την επεξεργασία μέσω των REG08 και REG12 εντός πέντε εργάσιμων ημερών όταν εκτελών την επεξεργασία, υπεργολάβος επεξεργασίας, προμηθευτής ή άλλο τρίτο μέρος δεν εκπληρώνει συμφωνημένες υποχρεώσεις περιστατικού ή παραβίασης.

10.1.4 [Both] Top Management MUST ανασκοπεί ουσιώδεις ή επαναλαμβανόμενες μη συμμορφώσεις διαχείρισης περιστατικών στην επόμενη προγραμματισμένη ανασκόπηση της διοίκησης, με τις αποφάσεις και τις απαιτούμενες ενέργειες να διατηρούνται στο REG12.

11. Ανασκόπηση και συντήρηση

11.1.1 [Both] The Privacy Lead / PIMS Manager MUST ανασκοπεί την παρούσα πολιτική τουλάχιστον ετησίως και καταγράφει το αποτέλεσμα της ανασκόπησης, τις απαιτούμενες αλλαγές και την κατάσταση έγκρισης στο REG12.

11.1.2 [Both] The Incident Response Coordinator MUST ενεργοποιεί ανασκόπηση της παρούσας πολιτικής μετά από περιστατικό εντός 30 ημερολογιακών ημερών μετά το κλείσιμο κάθε περιστατικού που αφορά δεδομένα προσωπικού χαρακτήρα υψηλού αντικτύπου ή επιβεβαιωμένης παραβίασης δεδομένων προσωπικού χαρακτήρα, με τα τεκμήρια ανασκόπησης να διατηρούνται στα REG10 και REG12.

11.1.3 [Conditional] The Privacy Lead / PIMS Manager MUST ανασκοπεί την παρούσα πολιτική εντός 30 ημερολογιακών ημερών αφότου λάβει γνώση ουσιώδους αλλαγής σε εφαρμοστέες νομικές, κλαδικές, πελατειακές, συμβατικές, σχετικές με εκτελούντα την επεξεργασία ή υπεργολάβο επεξεργασίας ή σχετικές με διαβίβαση απαιτήσεις αναφοράς περιστατικών, με τα τεκμήρια ανασκόπησης να διατηρούνται στα REG01, REG08, REG09 και REG12.

11.1.4 [Both] The Internal Audit / Compliance Reviewer MUST ανασκοπεί την εφαρμογή της παρούσας πολιτικής τουλάχιστον ετησίως μέσω του προγράμματος εσωτερικού ελέγχου PIMS, με τα ευρήματα ελέγχου και τις διορθωτικές ενέργειες να διατηρούνται στο REG12.

11.1.5 [Both] Top Management MUST ανασκοπεί τάσεις περιστατικών, σημαντικές παραβιάσεις, απόδοση γνωστοποιήσεων, εκπρόθεσμες διορθωτικές ενέργειες και αποτελεσματικότητα πολιτικής κατά την προγραμματισμένη ανασκόπηση της διοίκησης, με τα αποτελέσματα να διατηρούνται στο REG12.

12. Συναφείς πολιτικές

12.1 Η παρούσα πολιτική πρέπει να διαβάζεται σε συνδυασμό με:

12.2 PII01 - Πολιτική Συστήματος Διαχείρισης Πληροφοριών Ιδιωτικότητας

12.3 PII02 - Πολιτική ρόλων, αρμοδιοτήτων και λογοδοσίας ιδιωτικότητας

12.4 PII03 - Πολιτική αποθετηρίου επεξεργασίας δεδομένων προσωπικού χαρακτήρα και νομικής βάσης

12.5 PII04 - Πολιτική ειδοποίησης ιδιωτικότητας και διαφάνειας

12.6 PII06 - Πολιτική διαχείρισης δικαιωμάτων υποκειμένων των δεδομένων προσωπικού χαρακτήρα

12.7 PII07 - Πολιτική αξιολόγησης κινδύνου ιδιωτικότητας και DPIA

12.8 PII08 - Πολιτική ιδιωτικότητας ήδη από τον σχεδιασμό και εξ ορισμού

12.9 PII10 - Πολιτική διατήρησης, διαγραφής και διάθεσης δεδομένων προσωπικού χαρακτήρα

12.10 PII12 - Πολιτική διαχείρισης ιδιωτικότητας εκτελούντων την επεξεργασία, υπεργολάβων επεξεργασίας και τρίτων μερών

12.11 PII13 - Πολιτική διεθνών διαβιβάσεων δεδομένων προσωπικού χαρακτήρα

12.12 PII14 - Πολιτική ασφάλειας και ελέγχου πρόσβασης δεδομένων προσωπικού χαρακτήρα

12.13 PII16 - Πολιτική εκπαίδευσης, ευαισθητοποίησης και επάρκειας ιδιωτικότητας

12.14 PII17 - Πολιτική τεκμηριωμένων πληροφοριών και διαχείρισης τεκμηρίων PIMS

12.15 PII18 - Πολιτική παρακολούθησης, ελέγχου και βελτίωσης PIMS

13. Πρότυπα και πλαίσια αναφοράς

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.7; 4.5.1; 4.5.3; 4.5.4; 5.2.2; 6.2.2; 7.1.1; 7.1.7; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.2.2; 4.3.4; 4.6.3; 6.3.1; 7.1.4; 11.1.2].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 6.4.1; 6.5.1; 8.1.1; 8.1.4; 10.1.2; 11.1.4; 11.1.5].

13.4 ISO/IEC 27701:2025 - Annex A.3.11. Addressed by clauses [4.1.1; 4.1.2; 4.2.6; 4.4.1; 5.1.1; 5.4.1; 7.1.1; 7.1.2; 7.1.6].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.4; 4.2.1; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.3; 4.4.4; 4.5.1; 4.5.4; 6.3.1].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.2.6; 4.4.6; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.4; 6.2.2; 9.1.2; 11.1.3].

13.7 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.6. Addressed by clauses [4.2.4; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.2; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 4.6.2; 5.2.1; 6.3.1; 8.1.3; 11.1.5].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.1; 4.4.3; 5.3.1; 6.2.2; 11.1.3].

13.10 GDPR - Article 28. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.11 GDPR - Article 32. Addressed by clauses [4.1.3; 4.1.4; 4.3.2; 4.3.3; 4.5.2; 4.6.3; 5.5.1; 7.1.4; 8.1.2; 11.1.2].

13.12 GDPR - Article 33. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.1; 4.5.4; 8.1.3; 9.1.3].

13.13 GDPR - Article 34. Addressed by clauses [4.2.3; 4.2.5; 4.4.2; 4.4.3; 4.4.7; 4.5.4; 8.1.3; 9.1.3].

13.14 GDPR - Article 39. Addressed by clauses [4.2.3; 4.4.2; 5.3.1; 6.2.2; 9.1.3; 11.1.3].

13.15 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.2.2; 4.3.2; 4.3.3; 4.5.3; 4.6.2; 4.6.3; 5.2.2; 6.4.1; 8.1.4; 11.1.4].

13.16 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.3; 4.6.5; 7.1.3; 7.1.6].

13.17 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.5.1; 4.5.2; 4.6.1; 4.6.2; 7.1.2; 7.1.6].

13.18 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.2; 4.6.1; 5.4.1; 7.1.6; 11.1.2].

13.19 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.1; 4.6.1; 4.6.5; 5.1.1; 7.1.1; 7.1.3; 7.1.6; 8.1.6; 11.1.1; 11.1.2].

13.20 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.1; 4.4.4; 4.5.1; 5.4.2; 6.1.2; 8.1.2].

13.21 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5].

13.22 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.2.6; 4.4.6; 4.4.7; 5.3.1; 6.2.2; 8.1.3; 11.1.3].

13.23 DORA Regulation (EU) 2022/2554 - Article 17; Article 18; Article 19. Addressed by clauses [4.2.1; 4.2.6; 4.4.6; 4.4.7; 5.1.2; 6.2.1; 8.1.3; 11.1.3; 11.1.5].