					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: PII15-FS					Τίτλος εγγράφου: **Πολιτική διαχείρισης περιστατικών και παραβιάσεων PII στον χρηματοοικονομικό τομέα**							
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

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Επικοινωνίες PIMS και τεκμηριωμένα τεκμήρια περιστατικών
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Σύνδεση επιχειρησιακού ελέγχου, αξιολόγησης κινδύνου ιδιωτικότητας και αντιμετώπισης κινδύνου
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Παρακολούθηση, αξιολόγηση, μη συμμόρφωση, διορθωτική ενέργεια και βελτίωση
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Σχεδιασμός και προετοιμασία διαχείρισης περιστατικών για επεξεργασία PII
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Απόκριση σε περιστατικά ασφάλειας πληροφοριών που αφορούν PII
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	Συμφωνία πελάτη εκτελούντος την επεξεργασία και υποστήριξη υποχρεώσεων πελάτη
GDPR	Article 5(2); Article 24	Controller	Supporting	Λογοδοσία και ευθύνη υπευθύνου επεξεργασίας
GDPR	Article 26	Joint Controller	Supporting	Συντονισμός ευθυνών

				περιστατικών 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 ικανότητα 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 επηρεαζόμενα υποκείμενα των δεδομένων προσωπικού χαρακτήρα
GDPR	Article 39	Conditional	Supporting	Συμβουλές DPO, παρακολούθηση, συνεργασία και υποστήριξη σημείου επαφής
DORA Regulation (EU) 2022/2554	Article 17	Conditional	Primary	Διαδικασία διαχείρισης περιστατικών σχετικών με ICT για χρηματοοικονομικές οντότητες εντός πεδίου εφαρμογής
DORA Regulation (EU) 2022/2554	Article 18	Conditional	Primary	Κριτήρια ταξινόμησης περιστατικών σχετικών με ICT και

				σημαντικών κυβερνοαπειλών
DORA Regulation (EU) 2022/2554	Article 19	Conditional	Primary	Αναφορά μειζόνων περιστατικών σχετικών με ICT και γνωστοποίηση σημαντικών κυβερνοαπειλών
DORA Regulation (EU) 2022/2554	Article 20	Conditional	Supporting	Περιεχόμενο αναφοράς, χρονικά όρια, υποδείγματα και διαδικασίες
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Αναφορά σημαντικών περιστατικών όπου εφαρμόζεται
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 PII 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 περιστατικών, αξιολόγηση, απόκριση, διδάγματα που αντλήθηκαν και συλλογή τεκμηρίων
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Κύκλος ζωής 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, διαλογής, ανάλυσης,

				απόκρισης και αναφοράς
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Προσδοκίες γνωστοποίησης εκτελούντος την επεξεργασία σε δημόσιο περιβάλλον νέφους και αρχείων παραβιάσεων

1. Πεδίο εφαρμογής

1.1 Η παρούσα πολιτική καθορίζει τις απαιτήσεις για την αναγνώριση, αναφορά, διαλογή, ταξινόμηση, αξιολόγηση, περιορισμό, γνωστοποίηση, τεκμηρίωση, κλείσιμο και βελτίωση από περιστατικά PII και παραβιάσεις PII σε πεδία εφαρμογής PIMS του χρηματοοικονομικού τομέα.

1.2 **Σημείωση εφαρμογής:** Η παρούσα πολιτική αποτελεί παραλλαγή αντικατάστασης για τον χρηματοοικονομικό τομέα για το PII15. Δεν πρέπει να εφαρμόζεται ταυτόχρονα με το PII15 για το ίδιο πεδίο εφαρμογής PIMS, επιχειρησιακή μονάδα, προϊόν, περιβάλλον πελάτη, ρυθμιζόμενη υπηρεσία ή όριο τεκμηρίων. Οι οργανισμοί πρέπει να επιλέγουν είτε το PII15 είτε το PII15-FS για το ίδιο πεδίο εφαρμογής, ώστε να αποφεύγονται διπλές υποχρεώσεις διαχείρισης περιστατικών, διπλά μητρώα και διπλή εργασία τεκμηρίων ελέγχου.

1.3 Η παρούσα πολιτική εφαρμόζεται σε:

1.3.1 τον οργανισμό όταν ενεργεί ως υπεύθυνος επεξεργασίας PII σε πλαίσιο χρηματοοικονομικού τομέα·

1.3.2 τον οργανισμό όταν ενεργεί ως από κοινού υπεύθυνος επεξεργασίας όπου απαιτείται συντονισμός ευθυνών για περιστατικό ή παραβίαση·

1.3.3 τον οργανισμό όταν ενεργεί ως εκτελών την επεξεργασία PII για πελάτες του χρηματοοικονομικού τομέα·

1.3.4 τον οργανισμό όταν ενεργεί ως υπεργολάβος επεξεργασίας για πελάτες του χρηματοοικονομικού τομέα ή ανάντη εκτελούντες την επεξεργασία·

1.3.5 συστήματα, εφαρμογές, υπηρεσίες, διεργασίες, προμηθευτές, εκτελούντες την επεξεργασία, υπεργολάβους επεξεργασίας και τρίτα μέρη που επεξεργάζονται, αποθηκεύουν, μεταδίδουν, υποστηρίζουν, προσπελάζουν ή άλλως επηρεάζουν PII εντός του πεδίου εφαρμογής PIMS του χρηματοοικονομικού τομέα.

1.4 Η παρούσα πολιτική χρησιμοποιεί το REG10 - Μητρώο περιστατικών και παραβιάσεων PII ως το κύριο αντικείμενο τεκμηρίων για τη διαχείριση περιστατικών και παραβιάσεων PII στον χρηματοοικονομικό τομέα.

1.5 Η παρούσα πολιτική χρησιμοποιεί υποστηρικτικά αντικείμενα τεκμηρίων ως εξής:

1.5.1 Το REG01 για το πεδίο εφαρμογής PIMS και το πλαίσιο εφαρμοστέων ενδιαφερόμενων μερών, τομεακών, πελατειακών, συμβατικών και αναφορικών απαιτήσεων.

1.5.2 Το REG02 για επηρεαζόμενες δραστηριότητες επεξεργασίας, κατηγορίες PII, κατηγορίες υποκειμένων των δεδομένων προσωπικού χαρακτήρα, σκοπούς, συστήματα και υπηρεσίες.

1.5.3 Το REG03 για τη Δήλωση Εφαρμοσιμότητας και επικαιροποιήσεις εφαρμοσιμότητας ελέγχων, συμπεριλαμβανομένης της αντικατάστασης του PII15 από το PII15-FS για το ίδιο πεδίο εφαρμογής.

1.5.4 Το REG04 για τη σύνδεση κινδύνου ιδιωτικότητας, DPIA, υπολειπόμενου κινδύνου και αντιμετώπισης κινδύνου.

1.5.5 Το REG08 για τεκμήρια διεπαφής περιστατικών εκτελούντων την επεξεργασία, υπεργολάβων επεξεργασίας, πελατών, προμηθευτών και τρίτων μερών.

1.5.6 Το REG09 για σύνδεση διεθνών διαβιβάσεων όταν ένα περιστατικό επηρεάζει διασυνοριακή επεξεργασία.

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

1.5.8 Το REG12 για τεκμήρια ελέγχου, μη συμμόρφωσης, διορθωτικής ενέργειας, ανασκόπησης της διοίκησης και βελτίωσης.

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

1.6.1 Το PII03 διέπει την απογραφή επεξεργασίας και τα αρχεία νομικής βάσης.

1.6.2 Το PII04 διέπει τους ελέγχους ειδοποιήσεων ιδιωτικότητας και διαφάνειας εκτός των ειδικών επικοινωνιών παραβίασης.

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

1.6.4 Το PII07 διέπει τη μεθοδολογία αξιολόγησης κινδύνου ιδιωτικότητας και DPIA.

1.6.5 Το PII08 διέπει τους ελέγχους προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό και εξ ορισμού.

1.6.6 Το PII10 διέπει τους ελέγχους διατήρησης, διαγραφής και διάθεσης.

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

1.6.8 Το PII13 διέπει τους μηχανισμούς διεθνών διαβιβάσεων PII και τα αρχεία κινδύνου διαβίβασης.

1.6.9 Το PII14 διέπει προληπτικούς και ανιχνευτικούς ελέγχους ασφάλειας και πρόσβασης για PII.

1.6.10 Το PII16 διέπει την εκπαίδευση, ευαισθητοποίηση και επάρκεια σε θέματα ιδιωτικότητας.

1.6.11 Το PII17 διέπει την τεκμηριωμένη πληροφορία και τη διαχείριση τεκμηρίων.

1.6.12 Το PII18 διέπει την παρακολούθηση, τον εσωτερικό έλεγχο, την ανασκόπηση της διοίκησης, τη μη συμμόρφωση, τη διορθωτική ενέργεια και τη συνεχή βελτίωση.

1.6.13 Το PII23 διέπει ελέγχους εκτελούντος την επεξεργασία PII σε περιβάλλον νέφους, όπου οι υποχρεώσεις εκτελούντος την επεξεργασία σε περιβάλλον νέφους εμπίπτουν στο πεδίο εφαρμογής.

1.7 Για την παρούσα πολιτική:

1.7.1 «Περιστατικό PII» σημαίνει ύποπτο ή επιβεβαιωμένο συμβάν που έχει επηρεάσει, μπορεί να έχει επηρεάσει ή θα μπορούσε ευλόγως να επηρεάσει την εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα, νόμιμη επεξεργασία ή εξουσιοδοτημένο χειρισμό PII.

1.7.2 «Παραβίαση PII» σημαίνει επιβεβαιωμένο περιστατικό PII που περιλαμβάνει μη εξουσιοδοτημένη, παράνομη, τυχαία ή ακούσια καταστροφή, απώλεια, αλλοίωση, κοινολόγηση, πρόσβαση, μη διαθεσιμότητα ή διακύβευση PII.

1.7.3 «Περιστατικό PII του χρηματοοικονομικού τομέα» σημαίνει περιστατικό PII που επηρεάζει, μπορεί να επηρεάσει ή συνδέεται ευλόγως με ρυθμιζόμενες χρηματοοικονομικές υπηρεσίες, πελάτες του χρηματοοικονομικού τομέα, χρηματοοικονομικούς αντισυμβαλλόμενους, χρηματοοικονομικές συναλλαγές, χρηματοοικονομικές λειτουργίες ή επεξεργασία PII στον χρηματοοικονομικό τομέα.

1.7.4 «Μείζον περιστατικό του χρηματοοικονομικού τομέα» σημαίνει περιστατικό PII του χρηματοοικονομικού τομέα ή συναφές περιστατικό ICT που πληροί τεκμηριωμένα κριτήρια ουσιώδους σημασίας ή αναφοράς στο REG10.

1.7.5 «Σημαντική κυβερνοαπειλή» σημαίνει κυβερνοαπειλή που καταγράφεται στο REG10 και θα μπορούσε να επηρεάσει ουσιωδώς υπηρεσίες, επεξεργασία PII, πελάτες, αντισυμβαλλόμενους ή λειτουργίες του χρηματοοικονομικού τομέα εντός πεδίου εφαρμογής.

1.7.6 «Αξιολόγηση παραβίασης» σημαίνει την τεκμηριωμένη αξιολόγηση του αν ένα περιστατικό PII αποτελεί παραβίαση PII, ποια PII και ποια υποκείμενα των δεδομένων προσωπικού χαρακτήρα επηρεάζονται, ποιοι κίνδυνοι μπορεί να προκύψουν, ποιες γνωστοποιήσεις ή επικοινωνίες απαιτούνται και ποια διορθωτική ενέργεια χρειάζεται.

1.7.7 «Επίγνωση» σημαίνει το χρονικό σημείο κατά το οποίο ο οργανισμός έχει εύλογο βαθμό βεβαιότητας ότι έχει συμβεί περιστατικό ασφάλειας ή ιδιωτικότητας και ότι PII έχουν παραβιαστεί ή μπορεί να έχουν παραβιαστεί.

1.7.8 «Περιστατικό PII υψηλού αντικτύπου στον χρηματοοικονομικό τομέα» σημαίνει περιστατικό PII που περιλαμβάνει επεξεργασία υψηλού κινδύνου, ειδικές κατηγορίες ή άκρως ευαίσθητα PII, μεγάλης κλίμακας PII, ευάλωτα άτομα, ρυθμιζόμενους πελάτες, ουσιώδη διακοπή υπηρεσιών, χρηματοοικονομικούς αντισυμβαλλόμενους, χρηματοοικονομικές συναλλαγές, αντίκτυπο σε πολλές δικαιοδοσίες, διακύβευση προνομιούχας πρόσβασης, δημόσια έκθεση, ransomware, μη διαθεσιμότητα υπηρεσίας ή σημαντικό επιχειρησιακό, πελατειακό, χρηματοοικονομικό ή φήμης αντίκτυπο.

1.7.9 «Ουσιώδης αλλαγή περιστατικού» σημαίνει νέα ή μεταβληθείσα πληροφορία που επηρεάζει το πεδίο, τη σοβαρότητα, τις κατηγορίες PII, τον αντίκτυπο στα υποκείμενα των δεδομένων προσωπικού χαρακτήρα, τον αντίκτυπο στις υπηρεσίες, την ταξινόμηση για τον χρηματοοικονομικό τομέα, την απόφαση γνωστοποίησης, τον αντίκτυπο στον πελάτη, τη βασική αιτία, τον περιορισμό, την ανάκαμψη, τη διορθωτική ενέργεια ή τις υποχρεώσεις εξωτερικής αναφοράς.

2. Σκοπός

2.1 Σκοπός της παρούσας πολιτικής είναι να διασφαλίσει ότι τα περιστατικά και οι παραβιάσεις PII σε πλαίσια χρηματοοικονομικού τομέα αντιμετωπίζονται με συνέπεια, ταχύτητα, νομιμότητα, ασφάλεια και με τεκμήρια έτοιμα για έλεγχο.

2.2 Η παρούσα πολιτική υποστηρίζει τη λογοδοσία απαιτώντας την καταγραφή των περιστατικών και παραβιάσεων PII του χρηματοοικονομικού τομέα στο REG10 και τη σύνδεσή τους με επηρεαζόμενα αρχεία επεξεργασίας, κινδύνους ιδιωτικότητας, σχέσεις με εκτελούντες την επεξεργασία και υπεργολάβους επεξεργασίας, αρχεία διαβίβασης, διορθωτικές ενέργειες, αρχεία εκπαίδευσης, αποφάσεις αναφοράς χρηματοοικονομικού τομέα και τεκμήρια ανασκόπησης της διοίκησης όπου 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 για τον χρηματοοικονομικό τομέα.

3. Στόχοι

3.1 Οι στόχοι της παρούσας πολιτικής είναι να:

3.1.1 διασφαλίζει ότι ύποπτα περιστατικά PII του χρηματοοικονομικού τομέα αναφέρονται και καταγράφονται άμεσα·

3.1.2 διασφαλίζει ότι τα περιστατικά PII του χρηματοοικονομικού τομέα υποβάλλονται σε διαλογή και ταξινομούνται με συνεπή κριτήρια ιδιωτικότητας, ασφάλειας, λειτουργίας και τομέα·

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

3.1.4 διασφαλίζει ότι οι αποφάσεις γνωστοποίησης από τον υπεύθυνο επεξεργασίας και επικοινωνίας προς τα 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 εναύσματα αναφοράς του χρηματοοικονομικού τομέα αξιολογούνται, τεκμηριώνονται και παρακολουθούνται όπου εφαρμόζονται·

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

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

3.1.9 διασφαλίζει ότι σημαντικές κυβερνοαπειλές και μείζονα περιστατικά του χρηματοοικονομικού τομέα δρομολογούνται στις κατάλληλες ροές λήψης αποφάσεων και αναφοράς·

3.1.10 διασφαλίζει ότι τα διδάγματα από περιστατικά οδηγούν σε διορθωτική ενέργεια, εκπαίδευση, βελτίωση ελέγχων και ανασκόπηση της διοίκησης·

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

3.1.12 διασφαλίζει ότι το PII15-FS αντικαθιστά το PII15 για το ίδιο πεδίο εφαρμογής του χρηματοοικονομικού τομέα και δεν δημιουργεί διπλή εργασία τεκμηρίων PII15.

4. Δηλώσεις πολιτικής

4.1 Ενεργοποίηση παραλλαγής, ετοιμότητα και παραλαβή αναφορών

4.1.1 [Conditional] To Privacy Lead / PIMS Manager πρέπει να τεκμηριώνει την ενεργοποίηση του PII15-FS στο REG01 και στο REG03 πριν η παρούσα πολιτική χρησιμοποιηθεί για πεδίο εφαρμογής PIMS του χρηματοοικονομικού τομέα.

4.1.2 [Conditional] To Privacy Lead / PIMS Manager πρέπει να τεκμηριώνει στο REG03 και στο REG12 ότι το PII15 δεν εφαρμόζεται ταυτόχρονα για το ίδιο πεδίο εφαρμογής PIMS του χρηματοοικονομικού τομέα πριν εγκριθεί το PII15-FS.

4.1.3 [All] To Incident Response Coordinator πρέπει να καταγράφει κάθε αναφερθέν ή ανιχνευθέν ύποπτο περιστατικό PII του χρηματοοικονομικού τομέα στο REG10 εντός μίας εργάσιμης ημέρας από την παραλαβή του ή νωρίτερα όταν μπορεί να ενεργοποιηθεί εφαρμοστέο χρονοδιάγραμμα γνωστοποίησης, πελάτη ή αναφοράς.

4.1.4 [Conditional] To Privacy Lead / PIMS Manager πρέπει να τηρεί κριτήρια χειρισμού περιστατικών και παραβιάσεων PII του χρηματοοικονομικού τομέα στο REG10 τουλάχιστον ετησίως και μετά από κάθε ουσιώδη αλλαγή στο πεδίο εφαρμογής PIMS, στο νομικό πλαίσιο, στις υποχρεώσεις πελατών, στις συμβατικές υποχρεώσεις, στο τομεακό πλαίσιο αναφοράς ή στην επεξεργασία υψηλού κινδύνου.

4.1.5 [Both] To Information Security Lead πρέπει να επιβεβαιώνει τις απαιτήσεις διατήρησης τεκμηρίων περιστατικού στο REG10 εντός 24 ωρών αφού ένα ύποπτο περιστατικό επηρεάσει σύστημα, υπηρεσία ή εφαρμογή που επεξεργάζεται PII.

4.1.6 [Conditional] To Vendor / Procurement Owner πρέπει να τηρεί απαιτήσεις επικοινωνίας για περιστατικά και δρομολόγησης τεκμηρίων τρίτων μερών του χρηματοοικονομικού τομέα στο REG08 πριν από την ένταξη και τουλάχιστον ετησίως για εκτελούντες την επεξεργασία, υπεργολάβους επεξεργασίας, προμηθευτές και παρόχους αναφοράς με εξωτερική ανάθεση εντός πεδίου εφαρμογής.

4.2 Ταξινόμηση και αξιολόγηση παραβίασης

4.2.1 [All] To Incident Response Coordinator πρέπει να ταξινομεί κάθε καταχώριση REG10 εντός 24 ωρών από την παραλαβή ως συμβάν μη σχετικό με PII, ύποπτο περιστατικό PII, επιβεβαιωμένο περιστατικό PII, επιβεβαιωμένη παραβίαση PII, περιστατικό PII του χρηματοοικονομικού τομέα, μείζον περιστατικό του χρηματοοικονομικού τομέα, σημαντική κυβερνοαπειλή ή καταχώριση με εκκρεμή ταξινόμηση.

4.2.2 [Conditional] To Information Security Lead πρέπει να αξιολογεί στο REG10 τις επηρεαζόμενες υπηρεσίες, πελάτες, αντισυμβαλλόμενους, συναλλαγές, χρόνο μη διαθεσιμότητας υπηρεσίας, γεωγραφική διασπορά, απώλεια δεδομένων, κρισιμότητα

υπηρεσίας και οικονομικό αντίκτυπο όταν ένα περιστατικό PII μπορεί να επηρεάσει χρηματοοικονομικές υπηρεσίες ή λειτουργίες.

4.2.3 [Both] To Privacy Lead / PIMS Manager πρέπει να προσδιορίζει την επηρεαζόμενη δραστηριότητα επεξεργασίας, τις κατηγορίες PII, 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.

4.2.4 [Controller] To Data Protection Officer / Privacy Advisor πρέπει να αξιολογεί τον κίνδυνο για τα επηρεαζόμενα υποκείμενα των δεδομένων προσωπικού χαρακτήρα για κάθε επιβεβαιωμένη ή ευλόγως ύποπτη παραβίαση PII και να καταγράφει στο REG10 τη σύσταση γνωστοποίησης, την αιτιολόγηση κινδύνου και τη συμβουλή πριν ληφθεί η απόφαση εξωτερικής γνωστοποίησης.

4.2.5 [Joint Controller] To Privacy Lead / PIMS Manager πρέπει να καταγράφει την κατανομή ευθυνών περιστατικού από κοινού υπευθύνων επεξεργασίας στο REG08 και στο REG10 εντός 24 ωρών από τον εντοπισμό κοινής ευθύνης για ύποπτη ή επιβεβαιωμένη παραβίαση PII.

4.2.6 [Processor] To Privacy Lead / PIMS Manager πρέπει να αξιολογεί τις εντολές πελάτη, τις συμβατικές υποχρεώσεις γνωστοποίησης και τις υποχρεώσεις συνεργασίας στο REG08 και στο REG10 εντός 24 ωρών αφού ύποπτη ή επιβεβαιωμένη παραβίαση PII επηρεάσει επεξεργασία που εκτελείται ως εκτελών την επεξεργασία.

4.2.7 [Subprocessor] To Vendor / Procurement Owner πρέπει να προσδιορίζει την ανάντη αλυσίδα γνωστοποίησης και την απαιτούμενη δρομολόγηση τεκμηρίων στο REG08 και στο REG10 εντός 24 ωρών αφού ύποπτο ή επιβεβαιωμένο περιστατικό PII επηρεάσει επεξεργασία που εκτελείται ως υπεργολάβος επεξεργασίας.

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

9.1.2 [Conditional] To Top Management πρέπει να εγκρίνει κάθε εξαίρεση που επηρεάζει ουσιωδώς τον χρόνο γνωστοποίησης παραβίασης, τον χρόνο αναφοράς χρηματοοικονομικού τομέα, 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 στο REG10 και στο REG12.

9.1.3 [Conditional] To Data Protection Officer / Privacy Advisor πρέπει να τεκμηριώνει συμβουλή για κάθε καθυστερημένη γνωστοποίηση, απόφαση μη γνωστοποίησης, εξαίρεση αναφοράς ή εξαιρετική προσέγγιση επικοινωνίας πριν από το κλείσιμο περιστατικού, με τη συμβουλή να διατηρείται στο REG10.

9.1.4 [Both] To Vendor / Procurement Owner πρέπει να καταγράφει εξαιρέσεις προμηθευτή, εκτελούντος την επεξεργασία, υπεργολάβου επεξεργασίας, πελάτη ή παρόχου εξωτερικής ανάθεσης που επηρεάζουν την απόκριση σε περιστατικά του χρηματοοικονομικού τομέα στο REG08 και στο REG12 εντός πέντε εργάσιμων ημερών μετά τον εντοπισμό της εξαίρεσης.

9.1.5 [All] To Privacy Lead / PIMS Manager πρέπει να ανασκοπεί ανοικτές εξαιρέσεις από την παρούσα πολιτική τουλάχιστον μηνιαίως μέχρι το κλείσιμο, με την κατάσταση ανασκόπησης να διατηρείται στο REG12.

10. Εφαρμογή και τήρηση

10.1.1 [All] Το Process Owner / Business Owner πρέπει να κλιμακώνει την αποτυχία αναφοράς ύποπτου περιστατικού PII του χρηματοοικονομικού τομέα, διατήρησης τεκμηρίων, τήρησης ανατεθειμένων ενεργειών ή συνεργασίας με την αξιολόγηση παραβίασης προς το Privacy Lead / PIMS Manager εντός δύο εργάσιμων ημερών μετά την ανακάλυψη, με τα τεκμήρια να διατηρούνται στο REG12.

10.1.2 [Both] Το Incident Response Coordinator πρέπει να κλιμακώνει καθυστερημένη αναφορά, μη πραγματοποιηθείσα ταξινόμηση, ελλείποντα τεκμήρια, μη πραγματοποιηθείσα κλιμάκωση ή εκπρόθεσμη ενέργεια περιορισμού προς το Privacy Lead / PIMS Manager εντός μίας εργάσιμης ημέρας μετά τον εντοπισμό του ζητήματος, με τα τεκμήρια να διατηρούνται στο REG10 και στο REG12.

10.1.3 [Both] Το Privacy Lead / PIMS Manager πρέπει να καταγράφει μη συμμόρφωση REG12 όταν παραβίαση της παρούσας πολιτικής επηρεάζει την παραλαβή περιστατικού, τη διαλογή, τον περιορισμό, τη γνωστοποίηση, την αναφορά, την ακεραιότητα τεκμηρίων, την επικοινωνία ή τη διορθωτική ενέργεια.

10.1.4 [Both] Το Vendor / Procurement Owner πρέπει να εκκινεί αποκατάσταση προμηθευτή, εκτελούντος την επεξεργασία, υπεργολάβου επεξεργασίας ή παρόχου εξωτερικής ανάθεσης μέσω του REG08 και του REG12 εντός πέντε εργάσιμων ημερών όταν τρίτο μέρος δεν ανταποκρίνεται στις συμφωνημένες υποχρεώσεις περιστατικού, παραβίασης, τεκμηρίων ή αναφοράς.

10.1.5 [Conditional] Το Top Management πρέπει να ανασκοπεί ουσιώδεις ή επαναλαμβανόμενες μη συμμορφώσεις PII15-FS στην επόμενη προγραμματισμένη ανασκόπηση της διοίκησης, με τις αποφάσεις και τις απαιτούμενες ενέργειες να διατηρούνται στο REG12.

10.1.6 [All] Το Privacy Lead / PIMS Manager πρέπει να ενεργοποιεί επανορθωτική εκπαίδευση στο REG11 εντός 30 ημερολογιακών ημερών όταν μη συμμόρφωση προς την πολιτική περιλαμβάνει ευαισθητοποίηση ρόλου, καθυστερημένη αναφορά, αποτυχία κλιμάκωσης, αποτυχία χειρισμού τεκμηρίων ή αποτυχία επικοινωνίας.

11. Ανασκόπηση και συντήρηση

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

11.1.2 [Conditional] Το Incident Response Coordinator πρέπει να ενεργοποιεί ανασκόπηση της παρούσας πολιτικής μετά το περιστατικό εντός 30 ημερολογιακών ημερών μετά το κλείσιμο κάθε περιστατικού PII υψηλού αντικτύπου στον χρηματοοικονομικό τομέα, επιβεβαιωμένης παραβίασης PII, μείζονος περιστατικού του χρηματοοικονομικού τομέα ή σημαντικής κυβερνοαπειλής, με τα τεκμήρια ανασκόπησης να διατηρούνται στο REG10 και στο REG12.

11.1.3 [Conditional] Το Privacy Lead / PIMS Manager πρέπει να ανασκοπεί την παρούσα πολιτική εντός 30 ημερολογιακών ημερών αφού λάβει γνώση ουσιώδους αλλαγής σε νομικές, τομεακές, πελατειακές, συμβατικές, σχετικές με εκτελούντες την επεξεργασία, υπεργολάβους επεξεργασίας, υποδείγματα αναφοράς, χρονοδιαγράμματα αναφοράς ή σχετικές με διαβιβάσεις απαιτήσεις αναφοράς περιστατικών, με τα τεκμήρια ανασκόπησης να διατηρούνται στα REG01, REG08, REG09 και REG12.

11.1.4 [Both] Το Internal Audit / Compliance Reviewer πρέπει να 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 [Conditional] Το Top Management πρέπει να ανασκοπεί τάσεις περιστατικών, σημαντικές παραβιάσεις, απόδοση αναφοράς, εκπρόθεσμες διορθωτικές ενέργειες και

αποτελεσματικότητα πολιτικής κατά την προγραμματισμένη ανασκόπηση της διοίκησης, με τα αποτελέσματα να διατηρούνται στο REG12.

11.1.6 [Conditional] Το Privacy Lead / PIMS Manager πρέπει να ανασκοπεί τη σχέση αντικατάστασης μεταξύ του PII15-FS και του PII15 τουλάχιστον ετησίως και μετά από κάθε αλλαγή οριοθέτησης PIMS, ώστε να επαληθεύει ότι και οι δύο πολιτικές δεν εφαρμόζονται για το ίδιο πεδίο εφαρμογής του χρηματοοικονομικού τομέα, με τα τεκμήρια ανασκόπησης να διατηρούνται στο REG03 και στο REG12.

12. Συναφείς πολιτικές

12.1 Η παρούσα πολιτική πρέπει να διαβάζεται σε συνδυασμό με:

12.1.1 PII01 - Πολιτική Συστήματος Διαχείρισης Πληροφοριών Ιδιωτικότητας

12.1.2 PII02 - Πολιτική ρόλων, αρμοδιοτήτων και λογοδοσίας ιδιωτικότητας

12.1.3 PII03 - Πολιτική απογραφής επεξεργασίας PII και νομικής βάσης

12.1.4 PII04 - Πολιτική ειδοποιήσεων ιδιωτικότητας και διαφάνειας

12.1.5 PII06 - Πολιτική διαχείρισης δικαιωμάτων υποκειμένων των δεδομένων προσωπικού χαρακτήρα

12.1.6 PII07 - Πολιτική αξιολόγησης κινδύνου ιδιωτικότητας και DPIA

12.1.7 PII08 - Πολιτική προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό και εξ ορισμού

12.1.8 PII10 - Πολιτική διατήρησης, διαγραφής και διάθεσης PII

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

12.1.10 PII13 - Πολιτική διεθνών διαβιβάσεων PII

12.1.11 PII14 - Πολιτική ασφάλειας και ελέγχου πρόσβασης PII

12.1.12 PII16 - Πολιτική εκπαίδευσης, ευαισθητοποίησης και επάρκειας σε θέματα ιδιωτικότητας

12.1.13 PII17 - Πολιτική τεκμηριωμένης πληροφορίας και διαχείρισης τεκμηρίων PIMS

12.1.14 PII18 - Πολιτική παρακολούθησης, ελέγχου και βελτίωσης PIMS

12.1.15 PII23 - Πολιτική εκτελούντος την επεξεργασία PII σε περιβάλλον νέφους, όπου οι υποχρεώσεις εκτελούντος την επεξεργασία σε περιβάλλον νέφους του χρηματοοικονομικού τομέα εμπίπτουν στο πεδίο εφαρμογής

12.2 Το PII15 - Πολιτική διαχείρισης περιστατικών και παραβιάσεων PII είναι η βασική πολιτική περιστατικών και παραβιάσεων. Το PII15-FS είναι παραλλαγή αντικατάστασης για τον χρηματοοικονομικό τομέα για το PII15. Το PII15 και το PII15-FS δεν πρέπει να εφαρμόζονται ταυτόχρονα για το ίδιο πεδίο εφαρμογής PIMS, επιχειρησιακή μονάδα, προϊόν, περιβάλλον πελάτη, ρυθμιζόμενη υπηρεσία ή όριο τεκμηρίων.

13. Πρότυπα και πλαίσια αναφοράς

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.8; 4.5.1; 4.5.4; 4.5.5; 5.2.2; 7.1.1; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.1.3; 4.2.3; 4.3.1; 4.3.4; 4.3.5; 4.7.3; 6.1.4; 7.1.4].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.7.1; 4.7.2; 4.7.6; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 9.1.1; 10.1.1; 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; 4.1.4; 4.1.6; 5.1.1; 6.1.1; 7.1.2; 7.1.6; 7.1.7].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.6.1; 4.6.2].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 4.5.7; 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 [4.2.6; 4.2.7; 4.3.6; 4.4.4; 4.4.5; 4.4.10; 4.5.6; 5.7.1; 7.1.3; 8.1.5; 10.1.4].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.5.1; 4.7.2; 5.2.1; 6.1.1; 8.1.2; 11.1.6].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.6; 4.5.1].

13.10 GDPR - Article 28. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3; 10.1.4].

13.11 GDPR - Article 32. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.2; 4.7.3; 7.1.4].

13.12 GDPR - Article 33. Addressed by clauses [4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.5.4; 8.1.2].

13.13 GDPR - Article 34. Addressed by clauses [4.4.3; 4.5.4].

13.14 GDPR - Article 39. Addressed by clauses [4.2.4; 4.4.3; 5.3.1; 6.1.4; 9.1.3].

13.15 DORA Regulation (EU) 2022/2554 - Article 17. Addressed by clauses [4.1.3; 4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.3; 4.3.4; 4.3.6; 4.4.7; 4.5.1; 4.7.1; 5.4.1; 6.1.2; 7.1.7].

13.16 DORA Regulation (EU) 2022/2554 - Article 18. Addressed by clauses [4.2.1; 4.2.2; 4.6.1; 4.6.2; 4.6.3; 8.1.3].

13.17 DORA Regulation (EU) 2022/2554 - Article 19. Addressed by clauses [4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.5; 8.1.3].

13.18 DORA Regulation (EU) 2022/2554 - Article 20. Addressed by clauses [4.4.8; 4.5.5; 6.1.4; 7.1.2; 8.1.3; 11.1.3].

13.19 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.4.7; 4.4.8; 4.5.5; 6.1.4; 8.1.3; 11.1.3].

13.20 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.4.3; 4.5.1; 4.5.3; 4.7.2; 5.2.1; 8.1.2].

13.21 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.7.1].

13.22 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.4; 4.3.6; 4.5.2; 4.7.1; 4.7.2; 7.1.7; 10.1.2].

13.23 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.4; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1.7].

13.24 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.4; 4.1.6; 4.7.1; 4.7.5; 7.1.6; 7.1.7; 10.1.6].

13.25 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.1; 4.7.1].

13.26 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3].