					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: PII07					Τίτλος εγγράφου: **Πολιτική Αξιολόγησης Κινδύνου Ιδιωτικότητας και DPIA**							
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 / Έλεγχος / Άρθρο	Εφαρμοσιμότητα	Τύπος κάλυψης	Σχόλιο
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	Κίνδυνοι και ευκαιρίες PIMS
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Αξιολόγηση κινδύνου ιδιωτικότητας
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Αντιμετώπιση κινδύνου ιδιωτικότητας και σύνδεση με τη SoA
ISO/IEC 27701:2025	Clause 6.3	Both	Supporting	Προγραμματισμένες αλλαγές PIMS και επαναξιολόγηση κινδύνου
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Τεκμηριωμένες πληροφορίες για κίνδυνο ιδιωτικότητας και DPIA
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Επιχειρησιακός σχεδιασμός και έλεγχος
ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Επιχειρησιακή αξιολόγηση κινδύνου ιδιωτικότητας
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Επιχειρησιακή αντιμετώπιση κινδύνου ιδιωτικότητας
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Παρακολούθηση και μέτρηση κινδύνου ιδιωτικότητας
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Ανασκόπηση κινδύνου ιδιωτικότητας από τη διοίκηση
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Μη συμμόρφωση και διορθωτικά μέτρα σχετικά με κίνδυνο

ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Primary	Εκτίμηση αντικτύπου στην ιδιωτικότητα
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Αρχεία επεξεργασίας που υποστηρίζουν την αξιολόγηση κινδύνου
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Συμφωνία πελάτη εκτελούντος την επεξεργασία και υποστήριξη DPIA
ISO/IEC 27701:2025	Annex A.2.2.6	Processor	Supporting	Πληροφορίες εκτελούντος την επεξεργασία που υποστηρίζουν τη συμμόρφωση του πελάτη
GDPR	Article 5(2)	Controller	Supporting	Τεκμήρια λογοδοσίας
GDPR	Article 24	Controller	Supporting	Ευθύνη και μέτρα του υπευθύνου επεξεργασίας
GDPR	Article 25	Controller	Supporting	Προστασία δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού
GDPR	Article 28	Both	Supporting	Υποστήριξη και εντολές εκτελούντος την επεξεργασία
GDPR	Article 30	Both	Supporting	Αρχεία επεξεργασίας που υποστηρίζουν τη DPIA
GDPR	Article 32	Both	Supporting	Κίνδυνος ασφάλειας και δικλίδες ασφαλείας
GDPR	Article 35	Controller	Primary	Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων
GDPR	Article 36	Controller	Primary	Προηγούμενη διαβούλευση
GDPR	Article 39	Conditional	Supporting	Συμβουλές DPO και παρακολούθηση όπου εφαρμόζεται

ISO/IEC 29100:2020	Clause 4.7; Clause 5.11; Clause 5.12	Both	Supporting	Έλεγχοι ιδιωτικότητας, ασφάλεια πληροφοριών και συμμόρφωση ιδιωτικότητας
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Primary	Πεδίο εφαρμογής, οφέλη, εναύσματα και προετοιμασία PIA
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2	Both	Supporting	Πρόγραμμα προστασίας PII και αναγνώριση απαιτήσεων
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7	Both	Supporting	Ενσωμάτωση της οργανωτικής διαχείρισης κινδύνων ιδιωτικότητας

1. Πεδίο εφαρμογής

1.1 Η παρούσα πολιτική καθορίζει τις απαιτήσεις για την αξιολόγηση κινδύνου ιδιωτικότητας, τον έλεγχο αναγκαιότητας DPIA, την εκτέλεση πλήρους DPIA, την αντιμετώπιση κινδύνου, την αποδοχή υπολειπόμενου κινδύνου, τη διαβούλευση, την ανασκόπηση και τη διαχείριση τεκμηρίων για την επεξεργασία PII εντός του πεδίου εφαρμογής του PIMS.

1.2 Η παρούσα πολιτική εφαρμόζεται σε:

1.2.1 νέες και ουσιωδώς τροποποιημένες δραστηριότητες επεξεργασίας PII·

1.2.2 πλαίσια επεξεργασίας υπευθύνου επεξεργασίας, από κοινού υπευθύνου επεξεργασίας, εκτελούντος την επεξεργασία και υπεργολάβου επεξεργασίας·

1.2.3 συστήματα, εφαρμογές, υπηρεσίες, επιχειρησιακές διαδικασίες, προμηθευτές, εκτελούντες την επεξεργασία, υπεργολάβους επεξεργασίας, διεθνείς διαβιβάσεις και ρυθμίσεις κοινοποίησης δεδομένων που επηρεάζουν την επεξεργασία PII·

1.2.4 τεκμήρια κινδύνου ιδιωτικότητας και DPIA που τηρούνται στο REG04 και υποστηρικτικά τεκμήρια που τηρούνται στα REG02, REG03, REG08, REG09, REG10, REG11 και REG12.

1.3 Η παρούσα πολιτική δεν αντικαθιστά τους ελέγχους απογραφής επεξεργασίας, τους ελέγχους ειδοποιήσεων ιδιωτικότητας, τους ελέγχους συγκατάθεσης, τους ελέγχους δικαιωμάτων υποκειμένων των δεδομένων προσωπικού χαρακτήρα, τους ελέγχους προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό, τους ελέγχους προμηθευτών, τους ελέγχους διεθνών διαβιβάσεων, τους ελέγχους ασφάλειας PII, τους ελέγχους περιστατικών, τους ελέγχους τεκμηριωμένων πληροφοριών ή τους ελέγχους παρακολούθησης/ελέγχου/βελτίωσης. Οι απαιτήσεις αυτές καθορίζονται στις συναφείς πολιτικές που αναφέρονται στην Ενότητα 12.

1.4 Για τους σκοπούς της παρούσας πολιτικής, αξιολόγηση κινδύνου ιδιωτικότητας σημαίνει την τεκμηριωμένη αναγνώριση, ανάλυση, αξιολόγηση, αντιμετώπιση, ανασκόπηση και παρακολούθηση πιθανών δυσμενών επιπτώσεων στην ιδιωτικότητα που απορρέουν από την επεξεργασία PII.

1.5 Για τους σκοπούς της παρούσας πολιτικής, DPIA σημαίνει τεκμηριωμένη εκτίμηση που χρησιμοποιείται για επεξεργασία από υπεύθυνο επεξεργασίας η οποία είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο για τα υποκείμενα των δεδομένων προσωπικού χαρακτήρα και η οποία αξιολογεί την αναγκαιότητα της επεξεργασίας, την αναλογικότητα, τους κινδύνους, τις δικλίδες ασφαλείας, τον υπολειπόμενο κίνδυνο, τις ανάγκες διαβούλευσης και τους όρους έγκρισης.

1.6 Για τους σκοπούς της παρούσας πολιτικής, υψηλός υπολειπόμενος κίνδυνος ιδιωτικότητας σημαίνει κίνδυνο ιδιωτικότητας που παραμένει πάνω από το εγκεκριμένο όριο αποδοχής μετά την προτεινόμενη ή υλοποιημένη αντιμετώπιση κινδύνου.

1.7 Για τους σκοπούς της παρούσας πολιτικής, ουσιώδης αλλαγή σημαίνει κάθε αλλαγή που επηρεάζει το πεδίο εφαρμογής του PIMS, τον σκοπό επεξεργασίας, τη νομική βάση, τις κατηγορίες PII, τις κατηγορίες υποκειμένων των δεδομένων προσωπικού χαρακτήρα, την κλίμακα επεξεργασίας, την τεχνολογία επεξεργασίας, την παρακολούθηση ή την κατάρτιση προφίλ, την αυτοματοποιημένη λήψη αποφάσεων, ευάλωτα υποκείμενα των δεδομένων προσωπικού χαρακτήρα, αποδέκτες, εκτελούντες την επεξεργασία, υπεργολάβους επεξεργασίας, διεθνείς διαβιβάσεις, τη διατήρηση, τους ελέγχους ασφάλειας, το προφίλ κινδύνου, εντολές πελάτη ή το πεδίο πιστοποίησης.

2. Σκοπός

2.1 Σκοπός της παρούσας πολιτικής είναι να διασφαλίσει ότι οι κίνδυνοι ιδιωτικότητας και οι υποχρεώσεις DPIA αναγνωρίζονται, αξιολογούνται, αντιμετωπίζονται, εγκρίνονται, ανασκοπούνται και τεκμηριώνονται πριν η επεξεργασία PII δημιουργήσει μη αποδεκτό κίνδυνο για τα υποκείμενα των δεδομένων προσωπικού χαρακτήρα ή για το PIMS.

2.2 Η παρούσα πολιτική επιτρέπει στον οργανισμό να αποδεικνύει διακυβέρνηση ιδιωτικότητας βάσει κινδύνου, λογοδοσία του υπευθύνου επεξεργασίας για τη DPIA, υποστήριξη DPIA από τον

εκτελούντα την επεξεργασία, τεκμηριωμένη αντιμετώπιση κινδύνου, έγκριση υπολειπόμενου κινδύνου, λήψη αποφάσεων για προηγούμενη διαβούλευση και συνεχή βελτίωση των ελέγχων ιδιωτικότητας.

3. Στόχοι

3.1 Οι στόχοι της παρούσας πολιτικής είναι να:

3.1.1 καθορίσει υποχρεωτικά εναύσματα ελέγχου κινδύνου ιδιωτικότητας·

3.1.2 καθορίσει πότε απαιτείται πλήρης DPIA·

3.1.3 διασφαλίσει ότι οι αποφάσεις DPIA του υπευθύνου επεξεργασίας τεκμηριώνονται και μπορούν να ανασκοπηθούν·

3.1.4 διασφαλίσει ότι η υποστήριξη DPIA από εκτελούντα την επεξεργασία και υπεργολάβο επεξεργασίας τεκμηριώνεται όπου απαιτείται από εντολή πελάτη ή συμφωνία·

3.1.5 διασφαλίσει ότι οι κίνδυνοι ιδιωτικότητας αξιολογούνται πριν προχωρήσει νέα ή ουσιωδώς τροποποιημένη επεξεργασία PII·

3.1.6 διασφαλίσει ότι οι αντιμετωπίσεις κινδύνων ιδιωτικότητας ανατίθενται, υλοποιούνται και επαληθεύονται·

3.1.7 διασφαλίσει ότι οι υψηλοί υπολειπόμενοι κίνδυνοι ιδιωτικότητας κλιμακώνονται και εγκρίνονται πριν αρχίσει ή συνεχιστεί η επεξεργασία·

3.1.8 διασφαλίσει ότι οι αποφάσεις προηγούμενης διαβούλευσης τεκμηριώνονται όπου παραμένει υψηλός υπολειπόμενος κίνδυνος·

3.1.9 διασφαλίσει ότι τα τεκμήρια κινδύνου ιδιωτικότητας και DPIA τηρούνται στο REG04 και συνδέονται με συναφή αντικείμενα τεκμηρίων·

3.1.10 αποφεύγει τη δημιουργία χωριστών μητρώων DPIA, κινδύνου ή διαβούλευσης εκτός του REG04.

4. Δηλώσεις πολιτικής

4.1 Έλεγχος κινδύνου ιδιωτικότητας

4.1.1 [Both] Το Process Owner / Business Owner ΠΡΕΠΕΙ να εκκινεί έλεγχο κινδύνου ιδιωτικότητας στο REG04 πριν αρχίσει νέα ή ουσιωδώς τροποποιημένη επεξεργασία PII που έχει καταχωριστεί στο REG02.

4.1.2 [Both] Το Privacy Lead / PIMS Manager ΠΡΕΠΕΙ να τηρεί κριτήρια ελέγχου κινδύνου ιδιωτικότητας στο REG04 πριν από την αρχική λειτουργία του PIMS και στη συνέχεια ετησίως.

4.1.3 [Controller] Το Process Owner / Business Owner ΠΡΕΠΕΙ να ολοκληρώνει τον έλεγχο αναγκαιότητας DPIA στο REG04 πριν αρχίσει επεξεργασία από υπεύθυνο επεξεργασίας που πληροί τα κριτήρια ελέγχου κινδύνου ιδιωτικότητας.

4.1.4 [Processor] Το Vendor / Procurement Owner ΠΡΕΠΕΙ να καταχωρίζει τις απαιτήσεις υποστήριξης DPIA του πελάτη στο REG08 πριν αρχίσει επεξεργασία από εκτελούντα την επεξεργασία, όταν η συμφωνία πελάτη ή η τεκμηριωμένη εντολή απαιτεί υποστήριξη DPIA.

4.1.5 [Both] Το System Owner / Application Owner ΠΡΕΠΕΙ να παρέχει τεκμήρια σχεδιασμού συστήματος, πρόσβασης, ασφάλειας, καταγραφής και ροής δεδομένων στο REG04 πριν από την έγκριση αξιολόγησης κινδύνου ιδιωτικότητας για νέα ή ουσιωδώς τροποποιημένα συστήματα που επεξεργάζονται PII.

4.1.6 [Both] Το Privacy Lead / PIMS Manager ΠΡΕΠΕΙ να καταχωρίζει το αποτέλεσμα του ελέγχου και την αιτιολόγηση της απόφασης για πλήρη DPIA στο REG04 πριν προχωρήσει η δραστηριότητα επεξεργασίας.

4.2 Εναύσματα DPIA και προσδιορισμός απαίτησης

4.2.1 [Controller] Το Privacy Lead / PIMS Manager ΠΡΕΠΕΙ να απαιτεί πλήρη DPIA στο REG04 πριν αρχίσει επεξεργασία από υπεύθυνο επεξεργασίας που είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο.

4.2.2 [Controller] Το Process Owner / Business Owner ΠΡΕΠΕΙ να παραπέμπει επεξεργασία που περιλαμβάνει μεγάλη κλίμακα, συστηματική παρακολούθηση, κατάρτιση προφίλ, αυτοματοποιημένες αποφάσεις, ειδικές κατηγορίες PII, δεδομένα ποινικών καταδικών ή αδικημάτων, ευάλωτα υποκείμενα των δεδομένων προσωπικού χαρακτήρα, καινοτόμο τεχνολογία ή ουσιωδώς τροποποιημένη επεξεργασία στο Privacy Lead / PIMS Manager στο REG04 πριν αρχίσει η επεξεργασία.

4.2.3 [Controller] Το Data Protection Officer / Privacy Advisor ΠΡΕΠΕΙ να καταχωρίζει συμβουλές στο REG04 πριν από την έγκριση απόφασης απαίτησης πλήρους DPIA για επεξεργασία υψηλού κινδύνου από υπεύθυνο επεξεργασίας.

4.2.4 [Both] Το Process Owner / Business Owner ΠΡΕΠΕΙ να επαναλαμβάνει τον έλεγχο κινδύνου ιδιωτικότητας στο REG04 πριν χρησιμοποιήσει PII για νέο σκοπό, προσθέσει νέο αποδέκτη, εισαγάγει νέο εκτελούντα την επεξεργασία ή υπεργολάβο επεξεργασίας, αλλάξει αρχιτεκτονική συστήματος ή ξεκινήσει νέα διεθνή διαβίβαση.

4.2.5 [Processor] Το Privacy Lead / PIMS Manager ΠΡΕΠΕΙ να τεκμηριώνει αν απαιτείται υποστήριξη DPIA από εκτελούντα την επεξεργασία στο REG08 εντός 10 εργάσιμων ημερών από τη λήψη αιτήματος υποστήριξης DPIA πελάτη.

4.2.6 [Subprocessor] Το Vendor / Procurement Owner ΠΡΕΠΕΙ να τεκμηριώνει ανάντη απαιτήσεις υποστήριξης DPIA στο REG08 πριν αρχίσει υπεργολαβική επεξεργασία, όταν ο ανάντη πελάτης ή η συμφωνία εκτελούντος την επεξεργασία απαιτεί τέτοια υποστήριξη.

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

9. Εξαιρέσεις

9.1 Εξαιρέσεις κινδύνου ιδιωτικότητας και DPIA

9.1.1 [All] Το Process Owner / Business Owner ΠΡΕΠΕΙ να ζητά κάθε εξαίρεση από την παρούσα πολιτική στο REG12 πριν προκύψει η απόκλιση.

9.1.2 [All] Το Privacy Lead / PIMS Manager ΠΡΕΠΕΙ να αξιολογεί τον αντίκτυπο κάθε ζητούμενης εξαίρεσης στην ιδιωτικότητα, στη νομοθεσία, στην πιστοποίηση, στις λειτουργίες και στα υποκείμενα των δεδομένων προσωπικού χαρακτήρα στο REG04 ή στο REG12 εντός 10 εργάσιμων ημερών από το αίτημα.

9.1.3 [All] Το Data Protection Officer / Privacy Advisor ΠΡΕΠΕΙ να καταχωρίζει συμβουλές στο REG12 πριν από την έγκριση κάθε εξαίρεσης που επηρεάζει επεξεργασία υψηλού κινδύνου, ολοκλήρωση πλήρους DPIA, προηγούμενη διαβούλευση, υψηλό υπολειπόμενο κίνδυνο ιδιωτικότητας ή υποστήριξη DPIA πελάτη.

9.1.4 [All] Το Top Management ΠΡΕΠΕΙ να εγκρίνει εξαιρέσεις κινδύνου ιδιωτικότητας ή DPIA που επηρεάζουν επεξεργασία υψηλού κινδύνου, πεδίο πιστοποίησης, προηγούμενη διαβούλευση ή ανεπίλυτο υψηλό υπολειπόμενο κίνδυνο ιδιωτικότητας στο REG12 πριν τεθεί σε ισχύ η εξαίρεση.

9.1.5 [All] Το Privacy Lead / PIMS Manager ΠΡΕΠΕΙ να ορίζει ημερομηνία λήξης που δεν υπερβαίνει τις 90 ημέρες στο REG12 για κάθε εγκεκριμένη εξαίρεση κινδύνου ιδιωτικότητας ή DPIA πριν από την έγκριση.

9.1.6 [All] Το Process Owner / Business Owner ΠΡΕΠΕΙ να κλείνει ή να επαναξιολογεί κάθε εξαίρεση κινδύνου ιδιωτικότητας ή DPIA στο REG12 εντός πέντε εργάσιμων ημερών από τη λήξη.

10. Εφαρμογή

10.1 Εφαρμογή απαιτήσεων κινδύνου ιδιωτικότητας και DPIA

10.1.1 [All] Το Privacy Lead / PIMS Manager ΠΡΕΠΕΙ να καταχωρίζει ελλιπή, ανακριβή, μη ολοκληρωμένα, εκπρόθεσμα ή μη εγκεκριμένα τεκμήρια κινδύνου ιδιωτικότητας ή DPIA του REG04 ως μη συμμόρφωση στο REG12 εντός πέντε εργάσιμων ημερών από την αναγνώριση.

10.1.2 [Controller] Το Process Owner / Business Owner ΠΡΕΠΕΙ να αναστέλλει νέα επεξεργασία υψηλού κινδύνου από υπεύθυνο επεξεργασίας όταν λείπουν απαιτούμενα τεκμήρια έγκρισης DPIA του REG04 πριν από την έναρξη.

10.1.3 [Both] Το System Owner / Application Owner ΠΡΕΠΕΙ να αποκλείει τη θέση σε λειτουργία συστημάτων που επεξεργάζονται PII όταν λείπουν απαιτούμενα τεκμήρια αντιμετώπισης κινδύνου του REG04 πριν από την έγκριση θέσης σε λειτουργία.

10.1.4 [Both] Το Vendor / Procurement Owner ΠΡΕΠΕΙ να αποκλείει την ένταξη προμηθευτή, εκτελούντος την επεξεργασία, υπεργολάβου επεξεργασίας ή ρύθμισης κοινοποίησης δεδομένων όταν λείπουν απαιτούμενα τεκμήρια κινδύνου ιδιωτικότητας ή υποστήριξης DPIA του REG04 πριν από την έγκριση της συμφωνίας.

10.1.5 [All] Το Top Management ΠΡΕΠΕΙ να ανασκοπεί ανεπίλυτες σημαντικές μη συμμορφώσεις κινδύνου ιδιωτικότητας ή DPIA στο REG12 κατά την ανασκόπηση από τη διοίκηση.

10.1.6 [All] Το Privacy Lead / PIMS Manager ΠΡΕΠΕΙ να κλιμακώνει επαναλαμβανόμενες μη τηρηθείσες προθεσμίες ελέγχου REG04, ανασκόπησης DPIA ή αντιμετώπισης κινδύνου στο Top Management στο REG12 εντός πέντε εργάσιμων ημερών μετά τη δεύτερη εμφάνιση σε περίοδο 12 μηνών.

10.1.7 [All] Το Internal Audit / Compliance Reviewer ΠΡΕΠΕΙ να επαληθεύει την αποτελεσματικότητα διορθωτικών ενεργειών για μη συμμορφώσεις κινδύνου ιδιωτικότητας και DPIA στο REG12 στον επόμενο προγραμματισμένο έλεγχο ή εντός 60 ημερών από το κλείσιμο, όποιο συμβεί πρώτο.

11. Ανασκόπηση και συντήρηση

11.1 Ανασκόπηση και συντήρηση πολιτικής

11.1.1 [All] Το Privacy Lead / PIMS Manager ΠΡΕΠΕΙ να ανασκοπεί την παρούσα πολιτική στο REG12 ετησίως και εντός 30 ημερών από ουσιώδη αλλαγή σε απαιτήσεις κινδύνου ιδιωτικότητας, DPIA, προηγούμενης διαβούλευσης, υποστήριξης εκτελούντος την επεξεργασία ή πιστοποίησης.

11.1.2 [All] Το Privacy Lead / PIMS Manager ΠΡΕΠΕΙ να ανασκοπεί τα κριτήρια ελέγχου REG04, τα κριτήρια εναυσμάτων DPIA, τα κριτήρια διαβάθμισης κινδύνου και τα κριτήρια αποδοχής υπολειπόμενου κινδύνου στο REG12 ετησίως.

11.1.3 [All] Το Data Protection Officer / Privacy Advisor ΠΡΕΠΕΙ να ανασκοπεί αλλαγές της παρούσας πολιτικής που είναι σημαντικές για την ιδιωτικότητα στο REG12 πριν από την έγκριση.

11.1.4 [All] Το Top Management ΠΡΕΠΕΙ να εγκρίνει ουσιώδεις αλλαγές στην παρούσα πολιτική στο REG12 πριν από τη δημοσίευση.

11.1.5 [All] Το Privacy Lead / PIMS Manager ΠΡΕΠΕΙ να επικαιροποιεί τα REG03 και REG04 εντός 15 εργάσιμων ημερών μετά από εγκεκριμένες αλλαγές πολιτικής που τροποποιούν την εφαρμοσιμότητα ελέγχων, τα κριτήρια κινδύνου ή τις απαιτήσεις ελέγχου αναγκαιότητας DPIA.

11.1.6 [All] Το Privacy Lead / PIMS Manager ΠΡΕΠΕΙ να καταχωρίζει την επικοινωνία εγκεκριμένων αλλαγών της παρούσας πολιτικής στο REG11 εντός 30 ημερών από τη δημοσίευση.

12. Συναφείς πολιτικές

12.1 Η παρούσα πολιτική υποστηρίζεται από τις ακόλουθες συναφείς πολιτικές:

12.2 PII01 - Πολιτική Συστήματος Διαχείρισης Πληροφοριών Ιδιωτικότητας

12.3 PII02 - Πολιτική ρόλων, αρμοδιοτήτων και λογοδοσίας ιδιωτικότητας

12.4 PII03 - Πολιτική απογραφής επεξεργασίας PII και νομικής βάσης

12.5 PII04 - Πολιτική ειδοποιήσεων ιδιωτικότητας και διαφάνειας

12.6 PII05 - Πολιτική διαχείρισης συγκατάθεσης και προτιμήσεων

12.7 PII06 - Πολιτική διαχείρισης δικαιωμάτων υποκειμένων των δεδομένων προσωπικού χαρακτήρα

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

12.9 PII09 - Πολιτική συλλογής, χρήσης, γνωστοποίησης και κοινοποίησης PII

12.10 PII10 - Πολιτική διατήρησης, διαγραφής και διάθεσης PII

12.11 PII11 - Πολιτική ακρίβειας και ποιότητας PII

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

12.13 PII13 - Πολιτική διεθνών διαβιβάσεων PII

12.14 PII14 - Πολιτική ασφάλειας και ελέγχου πρόσβασης PII

12.15 PII15 - Πολιτική διαχείρισης περιστατικών και παραβιάσεων PII

12.16 PII17 - Πολιτική τεκμηριωμένων πληροφοριών και διαχείρισης τεκμηρίων PIMS

12.17 PII18 - Πολιτική παρακολούθησης, ελέγχου και βελτίωσης PIMS

13. Πρότυπα και πλαίσια αναφοράς

13.1 Η παρούσα πολιτική αντιστοιχίζεται στα ακόλουθα πρότυπα και κανονισμούς. Η αντιστοίχιση εξηγεί πώς η πολιτική υποστηρίζει τις παρατιθέμενες απαιτήσεις και προσδιορίζει τις εσωτερικές ρήτρες που τις υλοποιούν ή τις υποστηρίζουν.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.1** - Αντιστοιχίζεται στην αναγνώριση και τον σχεδιασμό ενεργειών για κινδύνους και ευκαιρίες ιδιωτικότητας, με χρήση κριτηρίων ελέγχου, ορίων κινδύνου, κλιμάκωσης και εισροών ανασκόπησης από τη διοίκηση. Addressed by clauses [4.1.2; 4.4.5; 4.5.6; 6.1.1; 6.1.2; 8.1.2].

13.2.2 **Clause 6.1.2** - Αντιστοιχίζεται στη διεξαγωγή ελέγχου κινδύνου ιδιωτικότητας, αξιολόγησης κινδύνου ιδιωτικότητας, διαβάθμισης κινδύνου, επαναξιολόγησης και αξιολόγησης εναυσμάτων DPIA πριν προχωρήσει νέα ή ουσιωδώς τροποποιημένη επεξεργασία. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.6; 4.2.1; 4.2.4; 4.3.1; 4.3.7; 4.6.1].

13.2.3 **Clause 6.1.3** - Αντιστοιχίζεται στον σχεδιασμό αντιμετώπισης κινδύνου ιδιωτικότητας, τις επικαιροποιήσεις εφαρμοσιμότητας ελέγχων, την υλοποίηση αντιμετώπισης, την αποδοχή υπολειπόμενου κινδύνου και τη σύνδεση με τη SoA. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 6.1.5; 7.1.7; 11.1.5].

13.2.4 **Clause 6.3** - Αντιστοιχίζεται σε προγραμματισμένες αλλαγές PIMS και επεξεργασίας που ενεργοποιούν επαναξιολόγηση κινδύνου ιδιωτικότητας και ανασκόπηση DPIA. Addressed by clauses [4.2.4; 4.6.1; 11.1.1].

13.2.5 **Clause 7.5** - Αντιστοιχίζεται σε ελεγχόμενες τεκμηριωμένες πληροφορίες για έλεγχο κινδύνου ιδιωτικότητας, τεκμήρια DPIA, αντιμετώπιση κινδύνου, αποδοχή υπολειπόμενου κινδύνου, αποφάσεις προηγούμενης διαβούλευσης, εξαιρέσεις, μη συμμορφώσεις και τεκμήρια ανασκόπησης πολιτικής. Addressed by clauses [4.1.6; 4.3.7; 4.4.1; 4.5.1; 5.1.2; 7.1.1; 9.1.1; 10.1.1; 11.1.1].

13.2.6 **Clause 8.1** - Αντιστοιχίζεται στη λειτουργία ελέγχων κινδύνου ιδιωτικότητας και DPIA πριν από τη θέση σε λειτουργία, την ένταξη, την έγκριση επεξεργασίας, το κλείσιμο αντιμετώπισης και τη σύνδεση με διορθωτικές ενέργειες. Addressed by clauses [4.1.1; 4.1.5; 7.1.2; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 7.1.7; 7.1.8].

13.2.7 **Clause 8.2** - Αντιστοιχίζεται στην επιχειρησιακή αξιολόγηση κινδύνου ιδιωτικότητας για αλλαγές επεξεργασίας που είναι νέες, τροποποιημένες, σχετικές με σύστημα, προμηθευτή ή διαβίβαση ή προκύπτουν από περιστατικό. Addressed by clauses [4.1.1; 4.2.4; 4.3.1; 4.3.5; 4.5.5; 4.6.1].

13.2.8 **Clause 8.3** - Αντιστοιχίζεται στην επιχειρησιακή αντιμετώπιση κινδύνου ιδιωτικότητας, την ανάθεση αντιμετώπισης, την υλοποίηση αντιμετώπισης, την κλιμάκωση εκπρόθεσμης αντιμετώπισης και την επαλήθευση αποτελεσματικότητας. Addressed by clauses [4.4.1; 4.4.3; 4.4.4; 4.4.6; 4.4.7; 8.1.3; 10.1.7].

13.2.9 **Clause 9.1** - Αντιστοιχίζεται στην παρακολούθηση και μέτρηση κάλυψης ελέγχου, κατάστασης DPIA, ανοικτών κινδύνων, εκπρόθεσμων ενεργειών αντιμετώπισης, ενεργειών προμηθευτών, ενεργειών αντιμετώπισης ασφάλειας, ενεργειών επαναξιολόγησης περιστατικών και ευρημάτων ελέγχου. Addressed by clauses [4.6.3; 4.6.4; 4.6.5; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 8.1.8].

13.2.10 **Clause 9.3** - Αντιστοιχίζεται στην ανασκόπηση από τη διοίκηση υψηλών υπολειπόμενων κινδύνων ιδιωτικότητας, εκπρόθεσμων ενεργειών αντιμετώπισης, κατάστασης πλήρους DPIA, αποφάσεων προηγούμενης διαβούλευσης και σημαντικών εξαιρέσεων κινδύνου ιδιωτικότητας. Addressed by clauses [4.6.6; 6.1.1; 6.1.2; 6.1.3; 10.1.5].

13.2.11 **Clause 10.2** - Αντιστοιχίζεται σε μη συμμορφώσεις κινδύνου ιδιωτικότητας και DPIA, εξαιρέσεις, άνοιγμα διορθωτικών ενεργειών, κλιμάκωση και επαλήθευση αποτελεσματικότητας. Addressed by clauses [4.4.6; 9.1.1; 9.1.2; 9.1.4; 9.1.6; 10.1.1; 10.1.5; 10.1.6; 10.1.7].

13.2.12 **Annex A.1.2.6** - Αντιστοιχίζεται στην αξιολόγηση της ανάγκης για εκτίμηση αντικτύπου στην ιδιωτικότητα και στην υλοποίησή της όπου ενδείκνυται, για νέα ή τροποποιημένη επεξεργασία από υπεύθυνο επεξεργασίας. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.2.13 **Annex A.1.2.9** - Αντιστοιχίζεται στα αρχεία επεξεργασίας που υποστηρίζουν εισροές αξιολόγησης κινδύνου ιδιωτικότητας και DPIA, συμπεριλαμβανομένων σκοπού, κατηγοριών, συστημάτων, αποδεκτών, διαβιβάσεων και προμηθευτών. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.2.14 **Annex A.2.2.2** - Αντιστοιχίζεται στις συμφωνίες πελατών εκτελούντων την επεξεργασία και στις υποχρεώσεις υποστήριξης DPIA πελάτη. Addressed by clauses [4.1.4; 4.2.5; 4.5.4; 5.1.7; 7.1.6].

13.2.15 **Annex A.2.2.6** - Αντιστοιχίζεται στην παροχή, από τον εκτελούντα την επεξεργασία, πληροφοριών που απαιτούνται για τη συμμόρφωση του πελάτη, συμπεριλαμβανομένων της υποστήριξης DPIA και των τεκμηρίων υποστήριξης πελάτη. Addressed by clauses [4.2.5; 4.2.6; 4.5.4; 8.1.5].

13.3 GDPR

13.3.1 **Article 5(2)** - Αντιστοιχίζεται στα τεκμήρια λογοδοσίας για έλεγχο αναγκαιότητας DPIA, αποφάσεις πλήρους DPIA, αντιμετώπιση κινδύνου, αποδοχή υπολειπόμενου κινδύνου, αποφάσεις προηγούμενης διαβούλευσης, εξαιρέσεις, ευρήματα ελέγχου και διορθωτικές ενέργειες. Addressed by clauses [4.1.6; 4.3.7; 4.4.5; 4.5.1; 4.6.4; 10.1.1; 10.1.7].

13.3.2 **Article 24** - Αντιστοιχίζεται στην ευθύνη του υπευθύνου επεξεργασίας για κατάλληλα μέτρα κινδύνου ιδιωτικότητας, ανασκόπηση υψηλού υπολειπόμενου κινδύνου, έγκριση από τη διοίκηση και συντήρηση πολιτικής. Addressed by clauses [4.4.5; 4.5.3; 6.1.2; 10.1.5; 11.1.4].

13.3.3 **Article 25** - Αντιστοιχίζεται σε τεκμήρια προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό και προστασίας της ιδιωτικότητας εξ ορισμού που χρησιμοποιούνται στην αξιολόγηση κινδύνου και πριν από την έγκριση θέσης σε λειτουργία. Addressed by clauses [4.1.5; 4.3.4; 7.1.5].

13.3.4 **Article 28** - Αντιστοιχίζεται στην υποστήριξη DPIA από εκτελούντα την επεξεργασία και υπεργολάβο επεξεργασίας, τον χειρισμό εντολών πελάτη και τα τεκμήρια αντιμετώπισης κινδύνου προμηθευτών. Addressed by clauses [4.1.4; 4.2.5; 4.2.6; 4.4.4; 4.5.4; 7.1.6; 8.1.5].

13.3.5 **Article 30** - Αντιστοιχίζεται στα αρχεία επεξεργασίας που υποστηρίζουν τις εισροές αξιολόγησης κινδύνου ιδιωτικότητας και DPIA. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.3.6 **Article 32** - Αντιστοιχίζεται στις εισροές κινδύνου ασφάλειας PII, την επιλογή δικλίδων ασφαλείας, την αντιμετώπιση κινδύνου ασφάλειας και τις επικαιροποιήσεις κατάστασης ελέγχων ασφάλειας. Addressed by clauses [4.1.5; 4.3.3; 4.4.2; 8.1.6].

13.3.7 **Article 35** - Αντιστοιχίζεται στον έλεγχο αναγκαιότητας DPIA, τον προσδιορισμό απαίτησης πλήρους DPIA, το περιεχόμενο DPIA, τις συμβουλές DPO, την ανασκόπηση και τον αποκλεισμό επεξεργασίας υψηλού κινδύνου χωρίς την απαιτούμενη έγκριση DPIA. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.3.6; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.3.8 **Article 36** - Αντιστοιχίζεται στη λήψη αποφάσεων προηγούμενης διαβούλευσης, τις συμβουλές DPO, την έγκριση από το Top Management και ενέργειες συνέχισης, αναστολής, ανασχεδιασμού ή διαβούλευσης όπου παραμένει υψηλός υπολειπόμενος κίνδυνος. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 6.1.2].

13.3.9 **Article 39** - Αντιστοιχίζεται στις συμβουλές και την παρακολούθηση από το Data Protection Officer / Privacy Advisor, όπου εφαρμόζεται, για αποφάσεις DPIA, επεξεργασία υψηλού κινδύνου, προηγούμενη διαβούλευση και αλλαγές πολιτικής. Addressed by clauses [4.2.3; 4.3.6; 4.5.2; 5.1.3; 6.1.3; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.11; Clause 5.12** - Αντιστοιχίζεται στην αναγνώριση ελέγχων ιδιωτικότητας, στις δικλίδες ασφάλειας, στη συμμόρφωση ιδιωτικότητας, στα τεκμήρια κινδύνου ιδιωτικότητας, στην παρακολούθηση και στην ανασκόπηση. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.7; 4.6.3; 4.6.5; 8.1.6; 10.1.7].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Αντιστοιχίζεται στο πεδίο εφαρμογής, τα οφέλη, τον προσδιορισμό εναυσμάτων, την προετοιμασία, τις εισροές αξιολόγησης, τα τεκμήρια ενδιαφερόμενων μερών και τη δομή αναφοράς DPIA της διαδικασίας PIA που τηρούνται στο REG04. Addressed by clauses [4.1.1; 4.1.3; 4.1.6; 4.2.1; 4.3.1; 4.3.2; 4.3.7; 7.1.1].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2** - Αντιστοιχίζεται στις απαιτήσεις προγράμματος προστασίας PII, στην αναγνώριση απαιτήσεων προστασίας PII, στην επιλογή μέτρων ελέγχου βάσει κινδύνου και στη σύνδεση με την αντιμετώπιση κινδύνου ιδιωτικότητας. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 6.1.5].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7** - Αντιστοιχίζεται στις αρχές οργανωτικού κινδύνου ιδιωτικότητας, στην ηγεσία, στην ενσωμάτωση, στην αξιολόγηση κινδύνου, στην αντιμετώπιση κινδύνου, στην παρακολούθηση και ανασκόπηση, καθώς και στην καταγραφή και αναφορά. Addressed by clauses [4.1.2; 4.3.1; 4.3.7; 4.4.1; 4.4.5; 4.6.3; 4.6.4; 5.1.1; 6.1.1; 6.1.2; 8.1.1; 8.1.3].