

				Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: PII21				Τίτλος εγγράφου: Πολιτική ιδιωτικότητας για τεχνητή νοημοσύνη και αυτοματοποιημένη λήψη αποφάσεων							
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

<p>Νομική σημείωση (πνευματικά δικαιώματα και περιορισμοί χρήσης) (C) 2025 Clarysec LLC. All rights reserved.</p> <p>Το παρόν έγγραφο αποτελεί πνευματική ιδιοκτησία της Clarysec LLC. Απαγορεύεται η αντιγραφή, επαναχρησιμοποίηση, διανομή ή τροποποίησή του, εν όλω ή εν μέρει, για εμπορικούς ή σκοπούς υλοποίησης χωρίς προηγούμενη ρητή έγγραφη άδεια. Η μη εξουσιοδοτημένη χρήση απαγορεύεται αυστηρά και ενδέχεται να επιφέρει νομικές ενέργειες. Για θέματα αδειοδότησης, επικοινωνήστε με: info@clarysec.com</p>
--

Ευθυγραμμισμένη με πρότυπα και κανονιστικές απαιτήσεις

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Τεκμηριωμένες πληροφορίες και επιχειρησιακός έλεγχος για τεκμήρια επεξεργασίας που αφορούν τεχνητή νοημοσύνη, κατάρτιση προφίλ και αυτοματοποιημένη λήψη αποφάσεων
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Παρακολούθηση, μη συμμόρφωση και διορθωτικά μέτρα για ελέγχους ιδιωτικότητας τεχνητής νοημοσύνης
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9	Controller	Primary	Σκοπός, νομική βάση, εκτίμηση αντικτύπου στην ιδιωτικότητα και αρχεία υπευθύνου επεξεργασίας
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Συμβάσεις εκτελούντων την επεξεργασία και ευθύνες από κοινού υπευθύνων επεξεργασίας για επεξεργασία δεδομένων προσωπικού χαρακτήρα που σχετίζεται με τεχνητή νοημοσύνη
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4	Controller	Primary	Υποχρεώσεις προς υποκείμενα των δεδομένων προσωπικού χαρακτήρα και διαφάνεια για επεξεργασία που σχετίζεται με τεχνητή νοημοσύνη

ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11	Controller	Primary	Εναντίωση, πρόσβαση, διόρθωση, διαγραφή, χειρισμός αιτημάτων και υποχρεώσεις αυτοματοποιημένης λήψης αποφάσεων
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	Όρια συλλογής, επεξεργασίας και ελαχιστοποίησης για εισόδους, εξόδους και παράγωγα δεδομένα τεχνητής νοημοσύνης
ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5	Conditional	Supporting	Διεθνής διαβίβαση, κοινολόγηση και δρομολόγηση αιτημάτων κοινολόγησης για δεδομένα προσωπικού χαρακτήρα που σχετίζονται με τεχνητή νοημοσύνη
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Primary	Συμφωνία εκτελούντος την επεξεργασία, τεκμηριωμένες εντολές, υποστήριξη υποχρεώσεων πελάτη και αρχεία
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Υποστήριξη από εκτελούντα την επεξεργασία για υποχρεώσεις έναντι υποκειμένων, δρομολόγηση διαβιβάσεων και χειρισμός κοινολογήσεων
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Προστασία αρχείων και καταγραφή σχετικά με επεξεργασία δεδομένων

				προσωπικού χαρακτήρα που σχετίζεται με τεχνητή νοημοσύνη
GDPR	Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2)	Controller	Primary	Κατάρτιση προφίλ, θεμιτότητα, διαφάνεια, περιορισμός σκοπού, ελαχιστοποίηση, ακρίβεια και λογοδοσία
GDPR	Article 6; Article 9; Article 10	Controller	Primary	Νομιμότητα, δεδομένα ειδικών κατηγοριών και δικλίδες για δεδομένα ποινικών καταδικών ή αδικημάτων
GDPR	Article 12; Article 13; Article 14; Article 15	Controller	Primary	Διαφανής πληροφόρηση, πρόσβαση και ουσιαστικές πληροφορίες σχετικά με αυτοματοποιημένη λήψη αποφάσεων
GDPR	Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Primary	Διόρθωση, διαγραφή, περιορισμός, εναντίωση και δικαιώματα σχετικά με αυτοματοποιημένη λήψη αποφάσεων
GDPR	Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Ευθύνη υπευθύνου επεξεργασίας, σχεδιασμός/εξορισμού, από κοινού υπεύθυνοι επεξεργασίας, εκτελούντες την επεξεργασία, αρχεία, ασφάλεια, DPIA και καθήκοντα DPO
GDPR	Article 44	Conditional	Referenced	Δρομολόγηση διεθνών διαβιβάσεων για επεξεργασία

				δεδομένων προσωπικού χαρακτήρα που σχετίζεται με τεχνητή νοημοσύνη
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7	Both	Primary	Αρχές σκοπού, συλλογής, ελαχιστοποίησης, χρήσης, διατήρησης, κοινολόγησης, ακρίβειας και ποιότητας
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Διαφάνεια, συμμετοχή του ατόμου, λογοδοσία, ασφάλεια πληροφοριών και συμμόρφωση ιδιωτικότητας
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	Όφελος ΠΙΑ, καθορισμός κατωφλίου και προετοιμασία για αξιολόγηση κινδύνου ιδιωτικότητας σχετική με τεχνητή νοημοσύνη
ISO/IEC 29151:2022	Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10	Both	Supporting	Έλεγχοι σκοπού, συλλογής, ελαχιστοποίησης, χρήσης, διατήρησης, κοινολόγησης, ακρίβειας και συμμετοχής υποκειμένου

1. Πεδίο εφαρμογής

1.1 Η παρούσα πολιτική καθορίζει υποχρεωτικές απαιτήσεις ιδιωτικότητας για δραστηριότητες επεξεργασίας τεχνητής νοημοσύνης, κατάρτισης προφίλ, βαθμολόγησης, σύστασης, υποστήριξης αποφάσεων και αυτοματοποιημένης λήψης αποφάσεων, οι οποίες χρησιμοποιούν, συνάγουν, δημιουργούν, κοινολογούν ή με άλλο τρόπο επεξεργάζονται δεδομένα προσωπικού χαρακτήρα εντός του πεδίου εφαρμογής του PIMS.

1.2 Η παρούσα πολιτική εφαρμόζεται σε:

1.2.1 συστήματα, εφαρμογές, μοντέλα, υπηρεσίες, ροές εργασίας, μηχανές αποφάσεων, εργαλεία βαθμολόγησης, συστήματα συστάσεων, μοντέλα ανάλυσης και διαδικασίες αυτοματοποιημένης λήψης αποφάσεων με δυνατότητες τεχνητής νοημοσύνης που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα·

1.2.2 κατάρτιση προφίλ, τμηματοποίηση, ταξινόμηση, πρόβλεψη, συναγωγή συμπερασμάτων, εξατομίκευση, κατάταξη, επιλεξιμότητα, ανίχνευση απάτης, βαθμολόγηση κινδύνου, αποφάσεις πρόσβασης, αξιολόγηση σχετική με την απασχόληση, κατάρτιση προφίλ σχετική με παιδιά, εξατομίκευση μάρκετινγκ και παρόμοια επεξεργασία στην οποία εμπλέκονται δεδομένα προσωπικού χαρακτήρα·

1.2.3 δεδομένα προσωπικού χαρακτήρα που σχετίζονται με τεχνητή νοημοσύνη και χρησιμοποιούνται για εκπαίδευση, δοκιμές, επικύρωση, ρύθμιση, παρακολούθηση, παραγωγική συναγωγή, ανασκόπηση εξόδων, μέτρηση επιδόσεων, διερεύνηση περιστατικών ή απόσυρση μοντέλου·

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

1.2.5 προμηθευτές, εκτελούντες την επεξεργασία, υπεργολάβους επεξεργασίας, αποδέκτες κοινοχρησίας δεδομένων και διαδρομές διεθνών διαβιβάσεων που σχετίζονται με τεχνητή νοημοσύνη και επεξεργάζονται δεδομένα προσωπικού χαρακτήρα.

1.3 Η παρούσα πολιτική δεν δημιουργεί πλήρες πλαίσιο διακυβέρνησης τεχνητής νοημοσύνης, σύστημα διαχείρισης τεχνητής νοημοσύνης, απογραφή τεχνητής νοημοσύνης, απογραφή μοντέλων, μητρώο κινδύνων μοντέλων, μητρώο δίκαιης μεταχείρισης, μητρώο αλγορίθμων, μητρώο περιστατικών τεχνητής νοημοσύνης, επιτροπή τεχνητής νοημοσύνης, ρόλο ιδιοκτήτη μοντέλου, ρόλο ιδιοκτήτη συστήματος τεχνητής νοημοσύνης, ροή εργασίας νομικής συμβουλής ή χωριστό έντυπο έγκρισης τεχνητής νοημοσύνης.

1.4 Η παρούσα πολιτική δεν αντικαθιστά:

1.4.1 την PII03 για την απογραφή επεξεργασίας, τη νομική βάση και την ιδιοκτησία ROPA·

1.4.2 την PII04 για τη διακυβέρνηση ειδοποιήσεων ιδιωτικότητας·

1.4.3 την PII05 για τη διαχείριση συγκατάθεσης και προτιμήσεων·

1.4.4 την PII06 για τη ροή εργασίας δικαιωμάτων υποκειμένων των δεδομένων προσωπικού χαρακτήρα·

1.4.5 την PII07 για την αξιολόγηση κινδύνου ιδιωτικότητας και τη μεθοδολογία DPIA·

1.4.6 την PII08 για πύλες προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό και εξ ορισμού·

1.4.7 την PII09 για ελέγχους συλλογής, χρήσης, κοινολόγησης και κοινοχρησίας·

1.4.8 την PII10 για την εκτέλεση διατήρησης, διαγραφής και διάθεσης·

1.4.9 την PII11 για ελέγχους ακρίβειας και ποιότητας·

1.4.10 την PII12 για τη διακυβέρνηση κύκλου ζωής εκτελούντων την επεξεργασία, υπεργολάβων επεξεργασίας και τρίτων μερών·

1.4.11 την PII13 για ελέγχους διεθνών διαβιβάσεων·

- 1.4.12 την PII14 για ασφάλεια και έλεγχο πρόσβασης·
- 1.4.13 την PII15 για χειρισμό περιστατικών και παραβιάσεων·
- 1.4.14 την PII18 για παρακολούθηση, έλεγχο και βελτίωση·
- 1.4.15 την PII19 για την ιδιωτικότητα εργαζομένων·
- 1.4.16 την PII20 για την ιδιωτικότητα των παιδιών·
- 1.4.17 την PII22 για την ιδιωτικότητα μάρκετινγκ και τα cookies.

2. Σκοπός

- 2.1 Σκοπός της παρούσας πολιτικής είναι να διασφαλίζει ότι οι δραστηριότητες τεχνητής νοημοσύνης, κατάρτισης προφίλ και αυτοματοποιημένης λήψης αποφάσεων που αφορούν δεδομένα προσωπικού χαρακτήρα αναγνωρίζονται, τεκμηριώνονται, αξιολογούνται ως προς τον κίνδυνο, είναι διαφανείς, επιδεκτικές αμφισβήτησης, παρακολουθούνται και ελέγχονται μέσω του PIMS, χωρίς να δημιουργούνται διπλά τεχνουργήματα διακυβέρνησης ειδικά για την τεχνητή νοημοσύνη.
- 2.2 Η παρούσα πολιτική διασφαλίζει ότι οι υποχρεώσεις ιδιωτικότητας για επεξεργασία δεδομένων προσωπικού χαρακτήρα που σχετίζεται με τεχνητή νοημοσύνη τεκμηριώνονται μέσω των REG02, REG04, REG06, REG07, REG08, REG09, REG10 και REG12.

3. Στόχοι

3.1 Οι στόχοι της παρούσας πολιτικής είναι να:

- 3.1.1 αναγνωρίζει στην REG02 την επεξεργασία τεχνητής νοημοσύνης, κατάρτισης προφίλ και αυτοματοποιημένης λήψης αποφάσεων που αφορά δεδομένα προσωπικού χαρακτήρα·
- 3.1.2 τεκμηριώνει στην REG02 σκοπούς, νομική βάση, κατηγορίες δεδομένων προσωπικού χαρακτήρα, πηγές δεδομένων, συναγόμενα δεδομένα, εξόδους, αποδέκτες και αποτελέσματα αποφάσεων που σχετίζονται με τεχνητή νοημοσύνη·
- 3.1.3 ενεργοποιεί τον έλεγχο κινδύνου ιδιωτικότητας και τη δρομολόγηση DPIA μέσω της REG04·
- 3.1.4 διασφαλίζει ότι οι ειδοποιήσεις ιδιωτικότητας και οι ουσιαστικές πληροφορίες που σχετίζονται με τεχνητή νοημοσύνη καταγράφονται στην REG07·
- 3.1.5 δρομολογεί αιτήματα δικαιωμάτων, εναντίωσης, ανθρωπίνης ανασκόπησης και δυνατότητας αμφισβήτησης μέσω της REG06·
- 3.1.6 ελέγχει εκτελούντες την επεξεργασία, υπεργολάβους επεξεργασίας, προμηθευτές και ρυθμίσεις κοινοχρησίας δεδομένων που σχετίζονται με τεχνητή νοημοσύνη μέσω της REG08·
- 3.1.7 δρομολογεί διεθνείς διαβιβάσεις που σχετίζονται με τεχνητή νοημοσύνη μέσω της REG09·
- 3.1.8 κλιμακώνει ύποπτα περιστατικά δεδομένων προσωπικού χαρακτήρα, κακή χρήση, μη εξουσιοδοτημένη κοινολόγηση και δυσμενή αποτελέσματα ιδιωτικότητας που σχετίζονται με τεχνητή νοημοσύνη μέσω των REG10 και REG12·
- 3.1.9 καταγράφει στην REG12 παρακολούθηση, εξαιρέσεις, μη συμμορφώσεις, διορθωτικά μέτρα και βελτιώσεις.

4. Δηλώσεις πολιτικής

4.1 Αναγνώριση τεχνητής νοημοσύνης, κατάρτισης προφίλ και αυτοματοποιημένης λήψης αποφάσεων

- 4.1.1 [Controller] Όταν προτείνεται νέο ή ουσιωδώς τροποποιημένο σύστημα, εφαρμογή, μοντέλο, ροή εργασίας, υπηρεσία ή επιχειρησιακή διαδικασία, ο Process Owner / Business Owner πρέπει να προσδιορίζει αν χρησιμοποιεί τεχνητή νοημοσύνη, κατάρτιση προφίλ, βαθμολόγηση, σύσταση, υποστήριξη αποφάσεων ή αυτοματοποιημένη λήψη αποφάσεων που αφορά δεδομένα προσωπικού χαρακτήρα και να καταγράφει τον προσδιορισμό στην REG02.
- 4.1.2 [Controller] Πριν αρχίσει η επεξεργασία δεδομένων προσωπικού χαρακτήρα που σχετίζεται με τεχνητή νοημοσύνη, ο Process Owner / Business Owner πρέπει να τεκμηριώνει στην

REG02 τον σκοπό επεξεργασίας, τις κατηγορίες δεδομένων προσωπικού χαρακτήρα, τις κατηγορίες υποκειμένων των δεδομένων προσωπικού χαρακτήρα, τις πηγές δεδομένων, τις κατηγορίες συναγόμενων ή παράγωγων δεδομένων, τις κατηγορίες εξόδων, τις κατηγορίες αποδεκτών, τη νομική βάση και τη σύνδεση με τη διατήρηση.

- 4.1.3 [Controller] Πριν χρησιμοποιηθεί σε περιβάλλον παραγωγής η κατάρτιση προφίλ, η βαθμολόγηση, η σύσταση, η υποστήριξη αποφάσεων ή η αυτοματοποιημένη λήψη αποφάσεων, ο Process Owner / Business Owner πρέπει να τεκμηριώνει στην REG02 και στην REG04 το πλαίσιο απόφασης, το αναμενόμενο αποτέλεσμα για τα υποκείμενα των δεδομένων προσωπικού χαρακτήρα, την ανθρώπινη συμμετοχή και τη διαδρομή δικαιωμάτων.
- 4.1.4 [Joint Controller] Πριν εκτελεστεί επεξεργασία δεδομένων προσωπικού χαρακτήρα σχετική με τεχνητή νοημοσύνη με από κοινού υπεύθυνο επεξεργασίας, ο Privacy Lead / PIMS Manager πρέπει να τεκμηριώνει στην REG08 την ευθύνη για τον ορισμό σκοπού, την ειδοποίηση, τον χειρισμό δικαιωμάτων, την υποστήριξη DPIA, τη διακυβέρνηση εκτελούντων την επεξεργασία και την κλιμάκωση περιστατικών.
- 4.1.5 [Processor] Πριν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω υπηρεσίας σχετικής με τεχνητή νοημοσύνη για πελάτη, ο Process Owner / Business Owner πρέπει να επιβεβαιώνει ότι οι εντολές πελάτη, οι επιτρεπόμενοι σκοποί, οι απαγορευμένες χρήσεις, ο χειρισμός εξόδων και οι υποχρεώσεις συνδρομής τεκμηριώνονται στην REG08.
- 4.1.6 [Both] Πριν ενεργοποιηθεί επεξεργασία δεδομένων προσωπικού χαρακτήρα σχετική με τεχνητή νοημοσύνη, ο Privacy Lead / PIMS Manager πρέπει να επιβεβαιώνει ότι η επεξεργασία συνδέεται με τα εφαρμοστέα κανονικά αντικείμενα τεκμηρίων και ότι δεν δημιουργείται χωριστό μητρώο ειδικό για την τεχνητή νοημοσύνη εκτός των REG02, REG04, REG06, REG07, REG08, REG09, REG10 ή REG12.

4.2 Αξιολόγηση κινδύνου ιδιωτικότητας και δρομολόγηση DPIA

- 4.2.1 [Controller] Πριν από την έναρξη ή την ουσιαστική τροποποίηση επεξεργασίας δεδομένων προσωπικού χαρακτήρα σχετικής με τεχνητή νοημοσύνη, ο Privacy Lead / PIMS Manager πρέπει να ολοκληρώνει τον έλεγχο κινδύνου ιδιωτικότητας και να καταγράφει την απόφαση DPIA στην REG04.
- 4.2.2 [Conditional] Όταν η επεξεργασία που σχετίζεται με τεχνητή νοημοσύνη περιλαμβάνει κατάρτιση προφίλ, αυτοματοποιημένες αποφάσεις, αξιολόγηση μεγάλης κλίμακας, δεδομένα ειδικών κατηγοριών, δεδομένα ποινικών αδικημάτων, ευάλωτα υποκείμενα των δεδομένων προσωπικού χαρακτήρα, αξιολόγηση εργαζομένων, παιδιά, παρακολούθηση συμπεριφοράς, δεδομένα τοποθεσίας, βιομετρικά δεδομένα, βαθμολόγηση υψηλού αντικτύπου ή σημαντικά αποτελέσματα, ο Data Protection Officer / Privacy Advisor πρέπει να ανασκοπεί τον κίνδυνο ιδιωτικότητας και να καταγράφει τη συμβουλή στην REG04.
- 4.2.3 [Controller] Πριν από τη θέση σε λειτουργία σε περιβάλλον παραγωγής επεξεργασίας δεδομένων προσωπικού χαρακτήρα σχετικής με τεχνητή νοημοσύνη, ο Process Owner / Business Owner πρέπει να τεκμηριώνει στην REG04 ή στην REG12 τις ενέργειες αντιμετώπισης κινδύνου, την κατάσταση υπολειπόμενου κινδύνου και τεκμήρια ετοιμότητας για θέση σε λειτουργία.
- 4.2.4 [Controller] Πριν τα δεδομένα προσωπικού χαρακτήρα επαναχρησιμοποιηθούν για εκπαίδευση, δοκιμές, επικύρωση, ρύθμιση, παρακολούθηση ή βελτίωση μοντέλου τεχνητής νοημοσύνης για νέο ή ουσιαστικά τροποποιημένο σκοπό, ο Process Owner / Business Owner πρέπει να ολοκληρώνει ανασκόπηση ιδιωτικότητας και να καταγράφει την απόφαση στην REG02 και στην REG04.
- 4.2.5 [Conditional] Όταν ο υπολειπόμενος κίνδυνος ιδιωτικότητας παραμένει υψηλός μετά την προγραμματισμένη αντιμετώπιση, το Top Management πρέπει να εγκρίνει, να απορρίπτει ή να

απαιτεί περαιτέρω αντιμετώπιση πριν από τη χρήση σε παραγωγή και να καταγράφει την απόφαση στην REG04 και στην REG12.

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

9. Εξαιρέσεις

- 9.1 [All] Πριν από απόκλιση από απαίτηση ιδιωτικότητας σχετική με τεχνητή νοημοσύνη στην παρούσα πολιτική, ο αιτών Process Owner / Business Owner πρέπει να υποβάλλει αιτιολόγηση εξαίρεσης και τεκμήρια αντισταθμιστικού ελέγχου στην REG12.
- 9.2 [Conditional] Όταν εξαίρεση επηρεάζει την κατάρτιση προφίλ, την αυτοματοποιημένη λήψη αποφάσεων, την ανθρώπινη ανασκόπηση, τη δυνατότητα αμφισβήτησης, τη διαφάνεια, το αποτέλεσμα DPIA, τη βαθμολόγηση υψηλού αντικτύπου, την επεξεργασία σχετική με παιδιά, την επεξεργασία σχετική με εργαζομένους, τους περιορισμούς εκτελούντων την επεξεργασία ή τις διεθνείς διαβιβάσεις, ο Data Protection Officer / Privacy Advisor πρέπει να ανασκοπεί την εξαίρεση και να καταγράφει τη συμβουλή στην REG04 ή στην REG12.
- 9.3 [Conditional] Όταν εξαίρεση δημιουργεί ή διατηρεί υψηλό υπολειπόμενο κίνδυνο ιδιωτικότητας, το Top Management πρέπει να εγκρίνει ή να απορρίπτει την εξαίρεση και να καταγράφει την απόφαση στην REG04 και στην REG12.
- 9.4 [All] Πριν λήξει εγκεκριμένη εξαίρεση ιδιωτικότητας σχετική με τεχνητή νοημοσύνη, ο Privacy Lead / PIMS Manager πρέπει να ανασκοπεί την κατάσταση κλεισίματος, ανανέωσης ή διορθωτικού μέτρου και να καταγράφει το αποτέλεσμα στην REG12.

10. Εφαρμογή

- 10.1 [All] Όταν εντοπίζεται μη συμμόρφωση με την παρούσα πολιτική, ο Privacy Lead / PIMS Manager πρέπει να καταγράφει τη μη συμμόρφωση και το διορθωτικό μέτρο στην REG12.
- 10.2 [Both] Όταν υπάρχει υποψία μη εξουσιοδοτημένης επεξεργασίας, κοινολόγησης, πρόσβασης, κακής χρήσης μοντέλου, αστοχίας δικαιωμάτων ή δυσμενούς αποτελέσματος ιδιωτικότητας που σχετίζεται με τεχνητή νοημοσύνη, ο Incident Response Coordinator πρέπει να εκκινεί κλιμάκωση περιστατικού και να καταγράφει τεκμήρια στην REG10 και στην REG12.
- 10.3 [Both] Όταν εκτελών την επεξεργασία, υπεργολάβος επεξεργασίας, προμηθευτής ή αποδέκτης κοινοχρησίας δεδομένων δεν ανταποκρίνεται σε υποχρεώσεις ιδιωτικότητας σχετικές με τεχνητή νοημοσύνη, ο Vendor / Procurement Owner πρέπει να καταγράφει ενέργεια αποκατάστασης, κλιμάκωσης ή τερματισμού στην REG08 και στην REG12.
- 10.4 [All] Όταν προκύπτουν επαναλαμβανόμενες ή συστημικές μη συμμορφώσεις ιδιωτικότητας σχετικές με τεχνητή νοημοσύνη, το Top Management πρέπει να ανασκοπεί το ζήτημα και να καταγράφει τη διοικητική ενέργεια στην REG12.

11. Ανασκόπηση και συντήρηση

- 11.1 [All] Τουλάχιστον ετησίως, ο Privacy Lead / PIMS Manager πρέπει να ανασκοπεί την παρούσα πολιτική ως προς τη συνεχιζόμενη καταλληλότητά της και να καταγράφει το αποτέλεσμα της ανασκόπησης στην REG12.
- 11.2 [Conditional] Όταν νόμοι, υπηρεσίες, μοντέλα, πηγές δεδομένων, πρακτικές κατάρτισης προφίλ, λογική αυτοματοποιημένης λήψης αποφάσεων, ρυθμίσεις προμηθευτών, διαδρομές διαβίβασης ή κίνδυνοι ιδιωτικότητας μεταβάλλονται ουσιαστικά, ο Privacy Lead / PIMS Manager πρέπει να ανασκοπεί τους επηρεαζόμενους ελέγχους ιδιωτικότητας που σχετίζονται με τεχνητή νοημοσύνη και να καταγράφει το αποτέλεσμα στην REG02, στην REG04 ή στην REG12.
- 11.3 [Controller] Τουλάχιστον ετησίως και μετά από ουσιαστικές αλλαγές διαδρομής χρήση σχετικές με τεχνητή νοημοσύνη, ο Process Owner / Business Owner πρέπει να ανασκοπεί τεκμήρια

διαφάνειας, ουσιαστικών πληροφοριών, ανθρώπινης ανασκόπησης και διαδρομής δικαιωμάτων και να καταγράφει την ανασκόπηση στην REG06 και στην REG07.

- 11.4 [All] Αφού κλείσουν διορθωτικά μέτρα ιδιωτικότητας σχετικά με τεχνητή νοημοσύνη, ο Internal Audit / Compliance Reviewer πρέπει να επαληθεύει την αποτελεσματικότητα και να καταγράφει τεκμήρια επαλήθευσης στην REG12.

12. Συναφείς πολιτικές

- 12.1 PII01 - Πολιτική Συστήματος Διαχείρισης Πληροφοριών Ιδιωτικότητας
- 12.2 PII02 - Πολιτική ρόλων, αρμοδιοτήτων και λογοδοσίας ιδιωτικότητας
- 12.3 PII03 - Πολιτική απογραφής επεξεργασίας δεδομένων προσωπικού χαρακτήρα και νομικής βάσης
- 12.4 PII04 - Πολιτική ειδοποιήσεων ιδιωτικότητας και διαφάνειας
- 12.5 PII05 - Πολιτική διαχείρισης συγκατάθεσης και προτιμήσεων
- 12.6 PII06 - Πολιτική διαχείρισης δικαιωμάτων υποκειμένων των δεδομένων προσωπικού χαρακτήρα
- 12.7 PII07 - Πολιτική αξιολόγησης κινδύνου ιδιωτικότητας και DPIA
- 12.8 PII08 - Πολιτική προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό και εξ ορισμού
- 12.9 PII09 - Πολιτική συλλογής, χρήσης, κοινολόγησης και κοινοχρησίας δεδομένων προσωπικού χαρακτήρα
- 12.10 PII10 - Πολιτική διατήρησης, διαγραφής και διάθεσης δεδομένων προσωπικού χαρακτήρα
- 12.11 PII11 - Πολιτική ακρίβειας και ποιότητας δεδομένων προσωπικού χαρακτήρα
- 12.12 PII12 - Πολιτική διαχείρισης ιδιωτικότητας εκτελούντων την επεξεργασία, υπεργολάβων επεξεργασίας και τρίτων μερών
- 12.13 PII13 - Πολιτική διεθνών διαβιβάσεων δεδομένων προσωπικού χαρακτήρα
- 12.14 PII14 - Πολιτική ασφάλειας και ελέγχου πρόσβασης δεδομένων προσωπικού χαρακτήρα
- 12.15 PII15 - Πολιτική διαχείρισης περιστατικών και παραβιάσεων δεδομένων προσωπικού χαρακτήρα
- 12.16 PII17 - Πολιτική τεκμηριωμένων πληροφοριών και διαχείρισης τεκμηρίων PIMS
- 12.17 PII18 - Πολιτική παρακολούθησης, ελέγχου και βελτίωσης PIMS
- 12.18 PII19 - Πολιτική ιδιωτικότητας εργαζομένων
- 12.19 PII20 - Πολιτική ιδιωτικότητας παιδιών
- 12.20 PII22 - Πολιτική ιδιωτικότητας μάρκετινγκ και cookies

13. Πρότυπα και πλαίσια αναφοράς

- 13.1 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.6; 4.8.1; 6.1; 7.1; 7.5; 11.1].
- 13.2 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.2; 4.6.5; 4.8.2; 6.5; 8.1; 8.2; 8.3; 8.4; 8.5; 10.1; 11.4].
- 13.3 ISO/IEC 27701:2025 - Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.3; 4.2.4; 4.8.1; 7.1; 7.2].
- 13.4 ISO/IEC 27701:2025 - Annex A.1.2.7; Annex A.1.2.8. Addressed by clauses [4.1.4; 4.7.1; 4.7.2; 4.7.3; 5.7; 6.3; 7.6].
- 13.5 ISO/IEC 27701:2025 - Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 7.3; 11.3].
- 13.6 ISO/IEC 27701:2025 - Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11. Addressed by clauses [4.1.3; 4.3.2; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4; 11.3].

- 13.7 ISO/IEC 27701:2025 - Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5. Addressed by clauses [4.2.4; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 7.1; 7.5].
- 13.8 ISO/IEC 27701:2025 - Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5. Addressed by clauses [4.7.3; 4.7.4; 4.7.5; 7.7].
- 13.9 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.5; 4.3.5; 4.5.5; 4.7.1; 4.7.2; 5.7; 6.3; 7.6].
- 13.10 ISO/IEC 27701:2025 - Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.3.5; 4.5.5; 4.7.1; 4.7.2; 4.7.4; 4.7.5; 7.6; 7.7].
- 13.11 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.25. Addressed by clauses [4.4.4; 4.6.1; 4.6.3; 4.8.1; 5.4; 7.5; 7.8; 10.2].
- 13.12 GDPR - Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2). Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.5; 4.8.1; 8.1].
- 13.13 GDPR - Article 6; Article 9; Article 10. Addressed by clauses [4.1.2; 4.2.4; 4.4.3; 4.7.3; 7.1].
- 13.14 GDPR - Article 12; Article 13; Article 14; Article 15. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.5.2; 4.5.3; 7.3; 11.3].
- 13.15 GDPR - Article 16; Article 17; Article 18; Article 21; Article 22. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4].
- 13.16 GDPR - Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.2; 4.2.5; 4.4.4; 4.7.1; 4.8.2; 5.3; 6.2; 6.4; 7.2].
- 13.17 GDPR - Article 44. Addressed by clauses [4.7.4; 7.7; 8.4].
- 13.18 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7. Addressed by clauses [4.1.2; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.7.5].
- 13.19 ISO/IEC 29100:2020 - Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.3.1; 4.3.2; 4.5.1; 4.5.2; 4.6.3; 4.8.1; 4.8.2; 8.5; 10.1].
- 13.20 ISO/IEC 29134:2020 - Clause 5.1; Clause 6.2; Clause 6.3. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.6.4; 6.4; 7.2; 9.2].
- 13.21 ISO/IEC 29151:2022 - Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10. Addressed by clauses [4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.2; 4.5.4; 4.7.5].