

				Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: PII19				Τίτλος εγγράφου: Πολιτική ιδιωτικότητας εργαζομένων							
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	Τεκμήρια ιδιωτικότητας εργαζομένων και επιχειρησιακός έλεγχος
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Παρακολούθηση, μη συμμόρφωση και διορθωτική ενέργεια
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9	Controller	Primary	Σκοποί Ανθρώπινου Δυναμικού, σύνδεση με νομική βάση, έναυσμα DPIA, από κοινού ευθύνη και αρχεία
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Both	Supporting	Συμβάσεις εκτελούντων την επεξεργασία δεδομένων Ανθρώπινου Δυναμικού, εντολές, συνδρομή και αρχεία
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11	Controller	Supporting	Υποχρεώσεις εργαζομένων, δικαιώματα και δρομολόγηση αυτοματοποιημένων αποφάσεων
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9	Controller	Primary	Σύνδεση συλλογής, επεξεργασίας, ελαχιστοποίησης και διατήρησης
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Both	Supporting	Αρχεία κοινολόγησης και χειρισμός νομικά δεσμευτικής κοινολόγησης
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Προστασία αρχείων Ανθρώπινου Δυναμικού και τεκμήρια καταγραφής

GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Αρχές ιδιωτικότητας εργαζομένων και λογοδοσία
GDPR	Article 6; Article 9; Article 10	Controller	Supporting	Νομιμότητα, ειδικές κατηγορίες και δεδομένα ελέγχου ιστορικού
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Διαφάνεια και ειδοποιήσεις προς εργαζομένους
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Supporting	Δικαιώματα εργαζομένων και δρομολόγηση αυτοματοποιημένων αποφάσεων
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Διακυβέρνηση, από κοινού υπεύθυνοι επεξεργασίας, εκτελούντες την επεξεργασία, αρχεία, ασφάλεια, DPIA και συμβουλές
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Σκοπός, συλλογή, ελαχιστοποίηση, χρήση, διατήρηση και κοινολόγηση
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Διαφάνεια, συμμετοχή, λογοδοσία, ασφάλεια και συμμόρφωση
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Controller	Supporting	Σκοπός δεδομένων προσωπικού χαρακτήρα, συλλογή, ελαχιστοποίηση, διατήρηση και συμμετοχή υποκειμένου
ISO/IEC 29151:2022	Clause 7.1.2; Clause 7.1.3; Clause 7.2.4; Clause 7.3.2	Controller	Supporting	Έλεγχοι κύκλου ζωής εργατικού δυναμικού για την προστασία δεδομένων προσωπικού χαρακτήρα

ISO/IEC 29151:2022	Clause 15.1.2; Clause 15.2.2; Clause 15.2.3	Both	Supporting	Αξιολόγηση, παρακολούθηση και έλεγχος αλλαγών εκτελούντων την επεξεργασία δεδομένων Ανθρώπινου Δυναμικού
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Κίνδυνος ιδιωτικότητας Ανθρώπινου Δυναμικού και σύνδεση με έναυσμα DPIA
ISO/IEC 27002:2022	Controls 5.34; 6.1; 6.2; 6.5; 6.6	Both	Supporting	Προστασία δεδομένων προσωπικού χαρακτήρα και κύκλος ζωής ασφάλειας πληροφοριών εργατικού δυναμικού
ISO/IEC 27002:2022	Controls 8.15; 8.16	Both	Supporting	Δραστηριότητες καταγραφής και παρακολούθησης

1. Πεδίο εφαρμογής

- 1.1 Η παρούσα πολιτική ορίζει τις απαιτήσεις ιδιωτικότητας εργαζομένων για τη συλλογή, χρήση, κοινολόγηση, σύνδεση διατήρησης, ειδοποίηση, χειρισμό δικαιωμάτων, παρακολούθηση, υποστήριξη από εκτελούντες την επεξεργασία και διαχείριση τεκμηρίων των δεδομένων προσωπικού χαρακτήρα εργαζομένων εντός του Συστήματος Διαχείρισης Πληροφοριών Ιδιωτικότητας.
- 1.2 Για την παρούσα πολιτική, «δεδομένα προσωπικού χαρακτήρα εργαζομένων» περιλαμβάνουν δεδομένα προσωπικού χαρακτήρα που αφορούν εργαζομένους, υποψηφίους για εργασία, πρώην εργαζομένους, αναδόχους, προσωρινό προσωπικό, ασκούμενους, αποσπασμένους εργαζομένους και άλλους συμμετέχοντες στο εργατικό δυναμικό, όταν ο οργανισμός επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα τους για σκοπούς εργατικού δυναμικού, πρόσληψης, απασχόλησης, συνεργασίας, αποδοχών, παροχών, ασφάλειας, συμμόρφωσης, διοίκησης χώρου εργασίας ή συναφείς επιχειρησιακούς σκοπούς.
- 1.3 Η παρούσα πολιτική εφαρμόζεται σε πλαίσια υπευθύνου επεξεργασίας και από κοινού υπευθύνου επεξεργασίας, όπου ο οργανισμός καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα εργαζομένων.
- 1.4 Η παρούσα πολιτική εφαρμόζεται επίσης σε πλαίσια εκτελούντος την επεξεργασία και υπεργολάβου επεξεργασίας, όπου ο οργανισμός επεξεργάζεται δεδομένα προσωπικού χαρακτήρα εργαζομένων για λογαριασμό πελάτη, ανάντη εκτελούντος την επεξεργασία ή άλλου υπευθύνου επεξεργασίας βάσει τεκμηριωμένων εντολών.

1.5 Η παρούσα πολιτική καλύπτει:

- 1.5.1 τη συλλογή δεδομένων εργαζομένων·
 - 1.5.2 τους σκοπούς επεξεργασίας Ανθρώπινου Δυναμικού·
 - 1.5.3 τις ειδοποιήσεις ιδιωτικότητας εργαζομένων·
 - 1.5.4 τον χειρισμό δικαιωμάτων εργαζομένων·
 - 1.5.5 τη σύνδεση διατήρησης·
 - 1.5.6 την παρακολούθηση εργαζομένων·
 - 1.5.7 την εσωτερική κοινολόγηση·
 - 1.5.8 τους ελέγχους εκτελούντων την επεξεργασία δεδομένων Ανθρώπινου Δυναμικού, μισθοδοσίας, HRIS, παροχών, ελέγχου ιστορικού και εξωτερικά ανατιθέμενων υπηρεσιών Ανθρώπινου Δυναμικού, όπου εφαρμόζεται·
 - 1.5.9 τα περιστατικά, τις μη συμμορφώσεις, τις διορθωτικές ενέργειες και τα τεκμήρια βελτίωσης που αφορούν δεδομένα προσωπικού χαρακτήρα εργαζομένων.
- 1.6 Η παρούσα πολιτική δεν δημιουργεί ξεχωριστό μητρώο ιδιωτικότητας Ανθρώπινου Δυναμικού, μητρώο ιδιωτικότητας εργαζομένων, μητρώο επεξεργασίας Ανθρώπινου Δυναμικού, μητρώο παρακολούθησης εργαζομένων, μητρώο ελέγχου ιστορικού, μητρώο προμηθευτών Ανθρώπινου Δυναμικού, μητρώο δικαιωμάτων εργαζομένων ή μητρώο περιστατικών εργαζομένων. Τα τεκμήρια επεξεργασίας εργαζομένων καταγράφονται στα REG02, REG04, REG06, REG07, REG08, REG10 και REG12.
- 1.7 Η παρούσα πολιτική δεν παρέχει συμβουλές εργατικού δικαίου, συμβουλές εργασιακών σχέσεων, νομικό σχολιασμό για συμβούλια εργαζομένων, περιεχόμενο πειθαρχικής διαδικασίας, περιεχόμενο λειτουργικής διαδικασίας μισθοδοσίας ή υποδείγματα εγγράφων απασχόλησης ειδικά για συγκεκριμένη δικαιοδοσία.

1.8 Η παρούσα πολιτική δεν επαναλαμβάνει:

- 1.8.1 τη διακυβέρνηση PIMS στο P1101·
- 1.8.2 τη λογοδοσία ρόλων στο P1102·

- 1.8.3 την απογραφή επεξεργασίας και την ιδιοκτησία νομικής βάσης στο PII03·
- 1.8.4 τη διακυβέρνηση περιεχομένου ειδοποιήσεων ιδιωτικότητας στο PII04·
- 1.8.5 τη λειτουργία συγκατάθεσης και προτιμήσεων στο PII05·
- 1.8.6 τη ροή εργασίας δικαιωμάτων υποκειμένου των δεδομένων προσωπικού χαρακτήρα στο PII06·
- 1.8.7 τη μεθοδολογία κινδύνου ιδιωτικότητας και DPIA στο PII07·
- 1.8.8 τις πύλες προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό στο PII08·
- 1.8.9 τους βασικούς κανόνες συλλογής, χρήσης, κοινολόγησης και κοινοχρησίας στο PII09·
- 1.8.10 την εκτέλεση διατήρησης, διαγραφής και διάθεσης στο PII10·
- 1.8.11 τη διακυβέρνηση ακρίβειας και ποιότητας στο PII11·
- 1.8.12 τη διακυβέρνηση κύκλου ζωής εκτελούντων την επεξεργασία, υπερβολάβων επεξεργασίας και τρίτων στο PII12·
- 1.8.13 τους ελέγχους μηχανισμών διεθνούς διαβίβασης στο PII13·
- 1.8.14 την υλοποίηση ασφάλειας και ελέγχου πρόσβασης στο PII14·
- 1.8.15 τον χειρισμό περιστατικών και παραβιάσεων στο PII15·
- 1.8.16 τη διαχείριση εκπαίδευσης και ευαισθητοποίησης στο PII16·
- 1.8.17 τον έλεγχο τεκμηριωμένων πληροφοριών στο PII17·
- 1.8.18 τη διακυβέρνηση παρακολούθησης, ελέγχου και βελτίωσης PIMS στο PII18·
- 1.8.19 τους ελέγχους AI και αυτοματοποιημένης λήψης αποφάσεων στο PII21, όπου η προαιρετική αυτή πολιτική περιλαμβάνεται.

2. Σκοπός

- 2.1 Σκοπός της παρούσας πολιτικής είναι να διασφαλίζει ότι τα δεδομένα προσωπικού χαρακτήρα εργαζομένων υποβάλλονται σε επεξεργασία μόνο για τεκμηριωμένους, εγκεκριμένους, διαφανείς, αναλογικούς και λογοδοτούμενους σκοπούς εργατικού δυναμικού, και ότι τα τεκμήρια ιδιωτικότητας εργαζομένων τηρούνται στα κανονικά μητρώα PIMS χωρίς να δημιουργείται ξεχωριστό επίπεδο τεκμηρίων ιδιωτικότητας Ανθρώπινου Δυναμικού.
- 2.2 Η παρούσα πολιτική υποστηρίζει συνεπή χειρισμό της επεξεργασίας εργαζομένων συνδέοντας τις δραστηριότητες επεξεργασίας εργαζομένων με το REG02, τις ειδοποιήσεις ιδιωτικότητας εργαζομένων με το REG07, τα αιτήματα άσκησης δικαιωμάτων εργαζομένων με το REG06, τον κίνδυνο ιδιωτικότητας Ανθρώπινου Δυναμικού και τα εναύσματα DPIA με το REG04, τους εκτελούντες την επεξεργασία δεδομένων Ανθρώπινου Δυναμικού και τους προμηθευτές μισθοδοσίας ή HRIS με το REG08, τα περιστατικά που αφορούν δεδομένα προσωπικού χαρακτήρα εργαζομένων με το REG10, και τις εξαιρέσεις, μη συμμορφώσεις, διορθωτικές ενέργειες και τεκμήρια παρακολούθησης με το REG12.

3. Στόχοι

3.1 Οι στόχοι της παρούσας πολιτικής είναι:

- 3.1.1 να τηρούνται τεκμήρια απογραφής επεξεργασίας εργαζομένων στο REG02·
- 3.1.2 να τεκμηριώνονται οι πηγές συλλογής εργαζομένων, οι κατηγορίες δεδομένων προσωπικού χαρακτήρα, οι σκοποί, τα συστήματα, οι αποδέκτες και η σύνδεση διατήρησης·
- 3.1.3 να τηρούνται τεκμήρια ειδοποιήσεων ιδιωτικότητας εργαζομένων στο REG07·
- 3.1.4 να δρομολογούνται ο κίνδυνος ιδιωτικότητας εργαζομένων και τα εναύσματα DPIA μέσω του REG04·
- 3.1.5 να δρομολογούνται τα αιτήματα άσκησης δικαιωμάτων εργαζομένων μέσω του REG06·

- 3.1.6 να τηρούνται τεκμήρια εκτελούντων την επεξεργασία δεδομένων Ανθρώπινου Δυναμικού, μισθοδοσίας, HRIS, παροχών, ελέγχου ιστορικού και εξωτερικά ανατιθέμενων υπηρεσιών Ανθρώπινου Δυναμικού στο REG08·
- 3.1.7 να διασφαλίζεται ότι η παρακολούθηση εργαζομένων τεκμηριώνεται, είναι αναλογική, ανασκοπείται και κλιμακώνεται μέσω των REG04 και REG12, όπου εφαρμόζεται·
- 3.1.8 να δρομολογούνται τα ύποπτα περιστατικά που αφορούν δεδομένα προσωπικού χαρακτήρα εργαζομένων μέσω του REG10·
- 3.1.9 να καταγράφονται εξαιρέσεις ιδιωτικότητας εργαζομένων, μη συμμορφώσεις, διορθωτικές ενέργειες και ενέργειες βελτίωσης στο REG12·
- 3.1.10 να αποφεύγονται συμβουλές εργατικού δικαίου και νομικός σχολιασμός για συμβούλια εργαζομένων εντός των επιχειρησιακών ρητρών·
- 3.1.11 να αποφεύγονται διπλά μητρώα, ρόλοι, έντυπα, πίνακες ελέγχου ή αντικείμενα τεκμηρίων ειδικά για Ανθρώπινο Δυναμικό.

4. Δηλώσεις πολιτικής

4.1 Απογραφή επεξεργασίας εργαζομένων και σκοποί επεξεργασίας Ανθρώπινου Δυναμικού

- 4.1.1 [Controller] The Process Owner / Business Owner MUST καταγράφει κάθε δραστηριότητα επεξεργασίας εργαζομένων στο REG02 πριν από τη συλλογή, δημιουργία, εισαγωγή, χρήση ή κοινόχρηστη χρήση δεδομένων προσωπικού χαρακτήρα εργαζομένων.
- 4.1.2 [Controller] The Process Owner / Business Owner MUST τεκμηριώνει στο REG02 τις κατηγορίες δεδομένων προσωπικού χαρακτήρα εργαζομένων, τον πληθυσμό εργαζομένων, την πηγή συλλογής, τον σκοπό επεξεργασίας, το σύστημα, την κατηγορία εσωτερικών αποδεκτών, την κατηγορία εξωτερικών αποδεκτών και τη σύνδεση διατήρησης πριν εγκριθεί η δραστηριότητα επεξεργασίας.
- 4.1.3 [Controller] The Privacy Lead / PIMS Manager MUST ανασκοπεί κάθε νέα ή ουσιωδώς τροποποιημένη δραστηριότητα επεξεργασίας εργαζομένων στο REG02 πριν εγκριθεί η δραστηριότητα επεξεργασίας για λειτουργία.
- 4.1.4 [Conditional] The Data Protection Officer / Privacy Advisor MUST καταγράφει συμβουλές ιδιωτικότητας στο REG04 πριν από την έγκριση επεξεργασίας εργαζομένων που περιλαμβάνει δεδομένα προσωπικού χαρακτήρα ειδικών κατηγοριών, δεδομένα ποινικών αδικημάτων, έλεγχο ιστορικού, δεδομένα επαγγελματικής υγείας, βιομετρικά δεδομένα, δεδομένα τοποθεσίας, παρακολούθηση εργαζομένων ή επεξεργασία που μπορεί να επηρεάσει ουσιωδώς εργαζόμενο.
- 4.1.5 [Processor] The Privacy Lead / PIMS Manager MUST καταγράφει στο REG08 την εντολή πελάτη, τον σκοπό υπηρεσίας, τις κατηγορίες δεδομένων προσωπικού χαρακτήρα εργαζομένων του πελάτη και τη σύνδεση ρόλου εκτελούντος την επεξεργασία πριν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα εργαζομένων πελάτη ως εξωτερικά ανατιθέμενη υπηρεσία Ανθρώπινου Δυναμικού, μισθοδοσίας, παροχών, HRIS, ελέγχου ή υποστήριξης εργατικού δυναμικού.
- 4.1.6 [Joint Controller] The Privacy Lead / PIMS Manager MUST καταγράφει στο REG08 την κατανομή ευθυνών από κοινού υπευθύνων επεξεργασίας για την επεξεργασία δεδομένων προσωπικού χαρακτήρα εργαζομένων πριν αρχίσει η κοινή δραστηριότητα επεξεργασίας εργαζομένων.

4.2 Συλλογή δεδομένων εργαζομένων και ειδοποιήσεις ιδιωτικότητας εργαζομένων

- 4.2.1 [Controller] The Process Owner / Business Owner MUST περιορίζει τη συλλογή δεδομένων προσωπικού χαρακτήρα εργαζομένων στις κατηγορίες που τεκμηριώνονται στο REG02 πριν

αρχίσει η συλλογή για πρόσληψη, ένταξη, διοίκηση απασχόλησης, διαχείριση παροχών, λειτουργία μισθοδοσίας, έλεγχο, παρακολούθηση ή αποχώρηση.

- 4.2.2 [Controller] The Process Owner / Business Owner MUST καταγράφει στο REG02 την πηγή δεδομένων προσωπικού χαρακτήρα εργαζομένων που συλλέγονται από τρίτους πριν χρησιμοποιηθεί η πηγή συλλογής τρίτου μέρους.
- 4.2.3 [Controller] The Privacy Lead / PIMS Manager MUST τηρεί αρχείο ειδοποίησης ιδιωτικότητας εργαζομένων στο REG07 πριν από την άμεση ή έμμεση συλλογή δεδομένων προσωπικού χαρακτήρα εργαζομένων για νέο ή ουσιωδώς τροποποιημένο σκοπό.
- 4.2.4 [Controller] The Process Owner / Business Owner MUST επιβεβαιώνει ότι η τρέχουσα ειδοποίηση ιδιωτικότητας εργαζομένων που έχει καταγραφεί στο REG07 είναι διαθέσιμη πριν από τη συλλογή για πρόσληψη, τη συλλογή κατά την ένταξη, την ενεργοποίηση παρακολούθησης, την εγγραφή σε παροχές, τον έλεγχο ιστορικού ή ουσιώδη αλλαγή επεξεργασίας εργαζομένων.
- 4.2.5 [Conditional] The Data Protection Officer / Privacy Advisor MUST ανασκοπεί το αρχείο ειδοποίησης ιδιωτικότητας εργαζομένων στο REG07 πριν από τη δημοσίευση, όταν η ειδοποίηση καλύπτει παρακολούθηση εργαζομένων, έλεγχο ιστορικού, δεδομένα προσωπικού χαρακτήρα ειδικών κατηγοριών, δεδομένα ποινικών αδικημάτων, αυτοματοποιημένη λήψη αποφάσεων ή ουσιωδώς τροποποιημένο σκοπό επεξεργασίας εργαζομένων.
- 4.2.6 [Processor] The Vendor / Procurement Owner MUST καταγράφει στο REG08 τις ευθύνες διαύλου συλλογής που απευθύνεται σε εργαζομένους πριν από τη συλλογή δεδομένων προσωπικού χαρακτήρα εργαζομένων για λογαριασμό πελάτη από υπηρεσία Ανθρώπινου Δυναμικού, μισθοδοσίας, HRIS, παροχών, ελέγχου ή εξωτερικά ανατιθέμενη υπηρεσία Ανθρώπινου Δυναμικού που λειτουργεί ως εκτελών την επεξεργασία.

[... 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] The Process Owner / Business Owner MUST καταγράφει αίτημα εξαίρεσης στο REG12 πριν από απόκλιση από οποιαδήποτε απαίτηση της παρούσας πολιτικής.
- 9.1.2 [Conditional] The Data Protection Officer / Privacy Advisor MUST καταγράφει συμβουλές στο REG12 πριν από την έγκριση εξαίρεσης που επηρεάζει παρακολούθηση εργαζομένων, χειρισμό δικαιωμάτων εργαζομένων, έλεγχο ιστορικού, δεδομένα προσωπικού χαρακτήρα ειδικών κατηγοριών, δεδομένα ποινικών αδικημάτων ή επεξεργασία εργαζομένων υψηλού αντικτύπου.
- 9.1.3 [Conditional] Top Management MUST εγκρίνει εξαιρέσεις ιδιωτικότητας εργαζομένων στο REG12 πριν από την ενεργοποίηση, όταν η εξαίρεση επηρεάζει επεξεργασία εργαζομένων υψηλού κινδύνου, παρακολούθηση εργαζομένων, εξωτερική κοινολόγηση, εξάρτηση από εκτελούντα την επεξεργασία ή ανεπίλυτη διορθωτική ενέργεια.
- 9.1.4 [All] The Privacy Lead / PIMS Manager MUST αποδίδει ημερομηνία λήξης που δεν υπερβαίνει τις 90 ημέρες σε κάθε εξαίρεση ιδιωτικότητας εργαζομένων στο REG12 πριν ενεργοποιηθεί η εξαίρεση.
- 9.1.5 [All] The Privacy Lead / PIMS Manager MUST ανασκοπεί κάθε εξαίρεση ιδιωτικότητας εργαζομένων στο REG12 εντός πέντε εργάσιμων ημερών πριν από τη λήξη.
- 9.1.6 [All] The Privacy Lead / PIMS Manager MUST κλείνει ή κλιμακώνει κάθε ληγμένη εξαίρεση ιδιωτικότητας εργαζομένων στο REG12 εντός πέντε εργάσιμων ημερών μετά τη λήξη.

10. Εφαρμογή και τήρηση

- 10.1.1 [All] The Privacy Lead / PIMS Manager MUST καταγράφει μη συμμόρφωση στο REG12 εντός πέντε εργάσιμων ημερών όταν η επεξεργασία δεδομένων προσωπικού χαρακτήρα εργαζομένων δεν διαθέτει τα απαιτούμενα τεκμήρια σε REG02, REG07, REG08, REG04 ή REG06.
- 10.1.2 [Conditional] The Incident Response Coordinator MUST καταγράφει στο REG10 ύποπτη μη εξουσιοδοτημένη πρόσβαση, κοινολόγηση, απώλεια ή διακύβευση δεδομένων προσωπικού χαρακτήρα εργαζομένων εντός μίας εργάσιμης ημέρας από τον εντοπισμό.
- 10.1.3 [Controller] The Privacy Lead / PIMS Manager MUST αποτρέπει την έγκριση νέας παρακολούθησης εργαζομένων στο REG12 όταν λείπουν τα απαιτούμενα τεκμήρια σε REG02, REG04 ή REG07.
- 10.1.4 [Both] The Vendor / Procurement Owner MUST αναστέλλει στο REG08 νέα κοινολόγηση δεδομένων προσωπικού χαρακτήρα εργαζομένων σε προμηθευτή Ανθρώπινου Δυναμικού όταν λείπουν τα απαιτούμενα τεκμήρια εκτελούντος την επεξεργασία, υπεργολάβου επεξεργασίας, εντολής ή συνδρομής.
- 10.1.5 [All] Top Management MUST ανασκοπεί επαναλαμβανόμενες μη συμμορφώσεις ιδιωτικότητας εργαζομένων στο REG12 όταν η ίδια κατηγορία εμφανίζεται δύο ή περισσότερες φορές εντός κυλιόμενης περιόδου 12 μηνών.
- 10.1.6 [All] The Internal Audit / Compliance Reviewer MUST επαληθεύει τα τεκμήρια κλεισίματος στο REG12 πριν κλείσει ευρήματα ελέγχου που αφορούν επεξεργασία ιδιωτικότητας εργαζομένων, ειδοποιήσεις εργαζομένων, παρακολούθηση εργαζομένων, δικαιώματα εργαζομένων ή προμηθευτές Ανθρώπινου Δυναμικού.

11. Ανασκόπηση και συντήρηση

- 11.1.1 [All] The Privacy Lead / PIMS Manager MUST ανασκοπεί την παρούσα πολιτική στο REG12 τουλάχιστον ετησίως.
- 11.1.2 [Conditional] The Privacy Lead / PIMS Manager MUST ανασκοπεί την παρούσα πολιτική στο REG12 εντός 30 ημερών από ουσιώδη αλλαγή σε επεξεργασία εργαζομένων, παρακολούθηση εργαζομένων, συστήματα Ανθρώπινου Δυναμικού, ρυθμίσεις μισθοδοσίας, παρόχους HRIS, παρόχους παροχών, παρόχους ελέγχου ιστορικού ή εξωτερικά ανατιθέμενες υπηρεσίες Ανθρώπινου Δυναμικού.
- 11.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST ανασκοπεί τις προτεινόμενες ουσιώδεις αλλαγές στην παρούσα πολιτική στο REG12 πριν από την έγκριση από Top Management.
- 11.1.4 [All] Top Management MUST εγκρίνει ουσιώδεις αλλαγές στην παρούσα πολιτική στο REG12 πριν από τη δημοσίευση.
- 11.1.5 [All] The Privacy Lead / PIMS Manager MUST επικαιροποιεί τα REG02, REG07 ή REG08 εντός 15 εργάσιμων ημερών αφότου εγκεκριμένη αλλαγή πολιτικής επηρεάσει αρχεία επεξεργασίας εργαζομένων, ειδοποιήσεις ιδιωτικότητας εργαζομένων ή τεκμήρια προμηθευτών Ανθρώπινου Δυναμικού.
- 11.1.6 [All] The Internal Audit / Compliance Reviewer MUST καταγράφει παρατηρήσεις αποτελεσματικότητας ανασκόπησης για την παρούσα πολιτική στο REG12 κατά τον προγραμματισμένο κύκλο εσωτερικού ελέγχου PIMS.

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 ειδοποίησης ιδιωτικότητας και διαφάνειας
- 12.6 PII05 - Πολιτική διαχείρισης συγκατάθεσης και προτιμήσεων
- 12.7 PII06 - Πολιτική διαχείρισης δικαιωμάτων υποκειμένου των δεδομένων προσωπικού χαρακτήρα
- 12.8 PII07 - Πολιτική αξιολόγησης κινδύνου ιδιωτικότητας και DPIA
- 12.9 PII08 - Πολιτική προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό και εξ ορισμού
- 12.10 PII09 - Πολιτική συλλογής, χρήσης, κοινολόγησης και κοινοχρησίας PII
- 12.11 PII10 - Πολιτική διατήρησης, διαγραφής και διάθεσης PII
- 12.12 PII11 - Πολιτική ακρίβειας και ποιότητας PII
- 12.13 PII12 - Πολιτική διαχείρισης ιδιωτικότητας εκτελούντων την επεξεργασία, υπεργολάβων επεξεργασίας και τρίτων μερών
- 12.14 PII13 - Πολιτική διεθνούς διαβίβασης PII
- 12.15 PII14 - Πολιτική ασφάλειας PII και ελέγχου πρόσβασης
- 12.16 PII15 - Πολιτική διαχείρισης περιστατικών και παραβιάσεων PII
- 12.17 PII16 - Πολιτική εκπαίδευσης, ευαισθητοποίησης και επάρκειας σε θέματα ιδιωτικότητας
- 12.18 PII17 - Πολιτική τεκμηριωμένων πληροφοριών και διαχείρισης τεκμηρίων PIMS
- 12.19 PII18 - Πολιτική παρακολούθησης, ελέγχου και βελτίωσης PIMS
- 12.20 PII21 - Πολιτική ιδιωτικότητας για AI και αυτοματοποιημένη λήψη αποφάσεων, όπου περιλαμβάνεται στο πεδίο της προαιρετικής πρόσθετης έκδοσης

13. Πρότυπα και πλαίσια αναφοράς

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

13.2 ISO/IEC 27701:2025

- 13.2.1 **Clause 7.5; Clause 8.1** - Αντιστοιχίζεται σε τεκμηριωμένα τεκμήρια ιδιωτικότητας εργαζομένων, πύλες επιχειρησιακής έγκρισης, αρχεία εκτελούντων την επεξεργασία δεδομένων Ανθρώπινου Δυναμικού, ειδοποιήσεις εργαζομένων, αρχεία παρακολούθησης, χειρισμό εξαιρέσεων και τεκμήρια υλοποίησης. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.3; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1.1; 7.1.3].
- 13.2.2 **Clause 9.1; Clause 10.2** - Αντιστοιχίζεται σε παρακολούθηση ιδιωτικότητας εργαζομένων, μετρικές, τεκμήρια ελέγχου, δειγματοληψία παρακολούθησης εργαζομένων, χειρισμό μη συμμορφώσεων, διορθωτική ενέργεια και βελτίωση. Addressed by clauses [4.3.6; 4.4.5; 4.5.5; 4.6.7; 8.1.1; 8.1.4; 8.1.7; 10.1.1; 10.1.5].
- 13.2.3 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9** - Αντιστοιχίζεται σε σκοπούς επεξεργασίας εργαζομένων, σύνδεση με νομική βάση, δρομολόγηση κινδύνου ιδιωτικότητας και DPIA, κατανομή από κοινού υπευθύνων επεξεργασίας και αρχεία επεξεργασίας σε REG02 και REG04. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.6; 4.2.2; 4.6.1; 4.6.2].
- 13.2.4 **Annex A.1.2.7; Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7** - Αντιστοιχίζεται σε συμβάσεις εκτελούντων την επεξεργασία δεδομένων Ανθρώπινου Δυναμικού, τεκμηριωμένες εντολές, επεξεργασία δεδομένων προσωπικού χαρακτήρα εργαζομένων πελάτη, συνδρομή εκτελούντων την επεξεργασία και αρχεία εκτελούντων την επεξεργασία στο REG08. Addressed by clauses [4.1.5; 4.2.6; 4.4.4; 4.5.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5].

- 13.2.5 **Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11** - Αντιστοιχίζεται σε χειρισμό δικαιωμάτων εργαζομένων, συμβουλές για σύνθετα δικαιώματα και δρομολόγηση αυτοματοποιημένων αποφάσεων ή επεξεργασίας υψηλού αντικτύπου μέσω REG06 και REG04. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.3].
- 13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9** - Αντιστοιχίζεται σε περιορισμό συλλογής εργαζομένων, εγκεκριμένη εσωτερική χρήση, ελαχιστοποίηση, σύνδεση διατήρησης και δρομολόγηση εξαιρέσεων διατήρησης. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.6.1].
- 13.2.7 **Annex A.1.5.4; Annex A.1.5.5; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Αντιστοιχίζεται σε εξωτερικές κοινολογήσεις δεδομένων προσωπικού χαρακτήρα εργαζομένων, αρχεία κοινοχρησίας δεδομένων, εξουσιοδότηση κοινολόγησης εκτελούντος την επεξεργασία και δρομολόγηση περιστατικών σχετικών με κοινολόγηση. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.7.6].
- 13.2.8 **Annex A.3.14; Annex A.3.25** - Αντιστοιχίζεται στην προστασία αρχείων ιδιωτικότητας εργαζομένων, στα τεκμήρια αρχείων καταγραφής παρακολούθησης εργαζομένων και σε ύποπτη κακή χρήση ή διακύβευση δεδομένων παρακολούθησης εργαζομένων. Addressed by clauses [4.6.4; 4.6.6; 4.6.7; 7.1.2].

13.3 GDPR

- 13.3.1 **Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)** - Αντιστοιχίζεται σε νόμιμη, θεμιτή, διαφανή, περιορισμένη στον σκοπό, ελαχιστοποιημένη, συνδεδεμένη με διατήρηση και λογοδοτούμενη επεξεργασία δεδομένων προσωπικού χαρακτήρα εργαζομένων. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.1; 4.3.3; 4.4.1; 4.4.5].
- 13.3.2 **Article 6; Article 9; Article 10** - Αντιστοιχίζεται σε σύνδεση με νομική βάση, δρομολόγηση δεδομένων προσωπικού χαρακτήρα εργαζομένων ειδικών κατηγοριών, δρομολόγηση ευαίσθητων δεδομένων προσωπικού χαρακτήρα που σχετίζονται με επαγγελματική υγεία και απασχόληση, και δρομολόγηση δεδομένων ποινικών αδικημάτων ή ελέγχου ιστορικού. Addressed by clauses [4.1.2; 4.1.3; 4.1.4; 4.2.2; 4.7.3].
- 13.3.3 **Article 12; Article 13; Article 14** - Αντιστοιχίζεται σε διαφάνεια προς εργαζομένους, αρχεία ειδοποιήσεων ιδιωτικότητας εργαζομένων, εναύσματα ειδοποίησης για άμεση και έμμεση συλλογή, και τεκμήρια ειδοποίησης παρακολούθησης. Addressed by clauses [4.2.3; 4.2.4; 4.2.5; 4.6.5].
- 13.3.4 **Article 15; Article 16; Article 17; Article 18; Article 21; Article 22** - Αντιστοιχίζεται σε δρομολόγηση δικαιωμάτων εργαζομένων, τεκμήρια αιτημάτων, συμβουλές για σύνθετα αιτήματα και δρομολόγηση αυτοματοποιημένων αποφάσεων. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.3].
- 13.3.5 **Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39** - Αντιστοιχίζεται σε διακυβέρνηση υπευθύνου επεξεργασίας, κατανομή από κοινού υπευθύνων επεξεργασίας, διακυβέρνηση εκτελούντων την επεξεργασία δεδομένων Ανθρώπινου Δυναμικού, αρχεία επεξεργασίας, ασφαλή χειρισμό, δρομολόγηση DPIA και συμμετοχή συμβούλου ιδιωτικότητας. Addressed by clauses [4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.3.4; 4.3.5; 4.6.2; 4.6.3; 4.6.6; 4.7.1; 4.7.6].

13.4 ISO/IEC 29100:2020

- 13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Αντιστοιχίζεται σε προσδιορισμό σκοπού εργαζομένων, περιορισμό συλλογής, ελαχιστοποίηση, περιορισμό χρήσης, περιορισμό διατήρησης και περιορισμό κοινολόγησης. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.1; 4.4.2; 4.6.1].

13.4.2 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12** - Αντιστοιχίζεται σε διαφάνεια, συμμετοχή εργαζομένων, υποστήριξη δικαιωμάτων εργαζομένων, λογοδοσία, ασφάλεια πληροφοριών και τεκμήρια συμμόρφωσης ιδιωτικότητας. Addressed by clauses [4.2.3; 4.2.4; 4.5.1; 4.5.2; 4.5.5; 4.6.4; 4.6.6; 4.6.7; 4.7.6].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10** - Αντιστοιχίζεται σε αρχεία σκοπών δεδομένων προσωπικού χαρακτήρα, ελέγχους συλλογής, ελαχιστοποίηση, σύνδεση διατήρησης, περιορισμό κοινολόγησης και συμμετοχή εργαζομένων ή υποστήριξη πρόσβασης. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.3.1; 4.3.4; 4.4.1; 4.4.2; 4.5.1; 4.5.4].

13.5.2 **Clause 7.1.2; Clause 7.1.3; Clause 7.2.4; Clause 7.3.2** - Αντιστοιχίζεται σε ελέγχους κύκλου ζωής εργατικού δυναμικού για την προστασία δεδομένων προσωπικού χαρακτήρα που σχετίζονται με ελέγχους, όρους, σύνδεση εφαρμογής σε παραβίαση ιδιωτικότητας και ανασκόπηση διατήρησης κατά τη λήξη ή αλλαγή απασχόλησης. Addressed by clauses [4.1.4; 4.2.2; 4.4.2; 4.4.5; 10.1.1; 10.1.5].

13.5.3 **Clause 15.1.2; Clause 15.2.2; Clause 15.2.3** - Αντιστοιχίζεται σε αξιολόγηση εκτελούντων την επεξεργασία δεδομένων Ανθρώπινου Δυναμικού, παρακολούθηση εκτελούντων την επεξεργασία δεδομένων Ανθρώπινου Δυναμικού, ανασκόπηση προμηθευτών Ανθρώπινου Δυναμικού και τεκμήρια αλλαγής υπηρεσίας στο REG08. Addressed by clauses [4.4.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6].

13.6 ISO/IEC 29134:2020

13.6.1 **Clause 5.1; Clause 6.2** - Αντιστοιχίζεται στα οφέλη της εκτίμησης αντικτύπου ιδιωτικότητας και στον προσδιορισμό κινδύνου ιδιωτικότητας Ανθρώπινου Δυναμικού ή εναύσματος DPIA για παρακολούθηση εργαζομένων και επεξεργασία υψηλού αντικτύπου δεδομένων προσωπικού χαρακτήρα εργαζομένων, χωρίς να επαναλαμβάνει τη μέθοδο DPIA. Addressed by clauses [4.1.4; 4.3.3; 4.6.2; 4.6.3].

13.7 ISO/IEC 27002:2022

13.7.1 Controls 5.34; 6.1; 6.2; 6.5; 6.6 - Αντιστοιχίζεται σε προστασία δεδομένων προσωπικού χαρακτήρα, έλεγχο, όρους εργατικού δυναμικού, αρμοδιότητες μετά από αλλαγή απασχόλησης και προσδοκίες εμπιστευτικότητας ως ελέγχους κύκλου ζωής εργατικού δυναμικού που υποστηρίζουν δεδομένα προσωπικού χαρακτήρα. Addressed by clauses [4.1.4; 4.2.2; 4.4.2; 4.4.4; 4.7.2; 4.7.3].

13.7.2 Controls 8.15; 8.16 - Αντιστοιχίζεται σε αρχεία καταγραφής παρακολούθησης εργαζομένων, δραστηριότητες παρακολούθησης, περιορισμό σκοπού αρχείων καταγραφής και ανασκόπηση τεκμηρίων παρακολούθησης. Addressed by clauses [4.6.1; 4.6.2; 4.6.4; 4.6.6; 4.6.7].