

				Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: PII03				Τίτλος εγγράφου: Πολιτική αποθετηρίου επεξεργασίας PII και νομικής βάσης							
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

Πρότυπο / Κανονισμός	Ρήτρα / Έλεγχος / Άρθρο	Εφαρμοσιμότητα	Τύπος κάλυψης	Σχόλιο
ISO/IEC 27701:2025	Clause 4.1	Both	Supporting	Προσδιορισμός ρόλου PIMS για δραστηριότητες επεξεργασίας
ISO/IEC 27701:2025	Clause 6.1.2	Both	Supporting	Διασύνδεση εναύσματος αξιολόγησης κινδύνου ιδιωτικότητας
ISO/IEC 27701:2025	Clause 6.1.3	Both	Supporting	Διασύνδεση εφαρμοσιμότητας ελέγχων και SoA
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Τεκμηριωμένες πληροφορίες αποθετηρίου επεξεργασίας
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Επιχειρησιακός σχεδιασμός και έλεγχος για αρχεία επεξεργασίας
ISO/IEC 27701:2025	Clause 8.2	Both	Supporting	Διασύνδεση επιχειρησιακής αξιολόγησης κινδύνου ιδιωτικότητας
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Παρακολούθηση και μέτρηση αποθετηρίου
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Μη συμμόρφωση αποθετηρίου και διορθωτικά μέτρα
ISO/IEC 27701:2025	Annex A.1.2.2	Controller	Primary	Προσδιορισμός σκοπού από τον υπεύθυνο επεξεργασίας
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Primary	Προσδιορισμός νομικής βάσης από τον υπεύθυνο επεξεργασίας
ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Supporting	Διασύνδεση ελέγχου αναγκαιότητας DPIA

ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Supporting	Αρχεία ευθυνών επεξεργασίας από κοινού υπευθύνων επεξεργασίας
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Αρχεία υπευθύνου επεξεργασίας σχετικά με την επεξεργασία PII
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Primary	Αρχεία συμφωνίας πελάτη και εντολών για τον εκτελούντα την επεξεργασία
ISO/IEC 27701:2025	Annex A.2.2.3	Processor	Primary	Ευθυγράμμιση σκοπού του εκτελούντος την επεξεργασία με τις εντολές πελάτη
ISO/IEC 27701:2025	Annex A.2.2.7	Processor	Supporting	Αρχεία εκτελούντος την επεξεργασία σχετικά με την επεξεργασία PII
GDPR	Article 5(1)(a)	Controller	Supporting	Διασύνδεση νομιμότητας, δικαιοσύνης και διαφάνειας
GDPR	Article 5(1)(b)	Controller	Supporting	Περιορισμός σκοπού
GDPR	Article 5(1)(c)	Controller	Supporting	Ελαχιστοποίηση δεδομένων
GDPR	Article 5(1)(e)	Controller	Supporting	Διασύνδεση περιορισμού αποθήκευσης
GDPR	Article 5(2)	Controller	Supporting	Τεκμήρια λογοδοσίας
GDPR	Article 6	Controller	Primary	Νομιμότητα της επεξεργασίας
GDPR	Article 9	Conditional	Supporting	Προϋπόθεση επεξεργασίας ειδικών κατηγοριών
GDPR	Article 10	Conditional	Supporting	Προϋπόθεση για δεδομένα ποινικών καταδικών και αδικημάτων
GDPR	Article 24	Controller	Supporting	Ευθύνη και μέτρα υπευθύνου επεξεργασίας

GDPR	Article 26	Joint Controller	Supporting	Αρχεία ρύθμισης από κοινού υπευθύνων επεξεργασίας
GDPR	Article 28	Both	Supporting	Αρχεία εντολών και συμφωνιών εκτελούντος την επεξεργασία
GDPR	Article 30	Both	Primary	Αρχεία δραστηριοτήτων επεξεργασίας
GDPR	Article 35	Controller	Supporting	Διασύνδεση ελέγχου αναγκαιότητας DPIA
ISO/IEC 29100:2020	Clause 5.3	Both	Supporting	Νομιμότητα και εξειδίκευση σκοπού
ISO/IEC 29100:2020	Clause 5.4	Both	Supporting	Περιορισμός συλλογής
ISO/IEC 29100:2020	Clause 5.5	Both	Supporting	Ελαχιστοποίηση δεδομένων
ISO/IEC 29100:2020	Clause 5.6	Both	Supporting	Περιορισμός χρήσης, διατήρησης και γνωστοποίησης
ISO/IEC 29100:2020	Clause 5.10	Both	Supporting	Λογοδοσία
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7	Controller	Supporting	Έλεγχοι σκοπού προστασίας PII, συλλογής, ελαχιστοποίησης, χρήσης, διατήρησης και γνωστοποίησης
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Both	Supporting	Διασύνδεση οφέλους και εναύσματος PIA

1. Πεδίο εφαρμογής

1.1 Η παρούσα πολιτική ορίζει τις απαιτήσεις για τη διατήρηση του αποθετηρίου επεξεργασίας PII / ROPA και την τεκμηρίωση της νομικής βάσης, των σκοπών επεξεργασίας, των ρόλων επεξεργασίας, των κατηγοριών PII, των κατηγοριών υποκειμένων των δεδομένων προσωπικού χαρακτήρα, των αποδεκτών, των αναφορών διατήρησης, των αναφορών μεταφοράς, των εντολών προς εκτελούντες την επεξεργασία, των αρχείων από κοινού υπευθύνων επεξεργασίας και της διασύνδεσης με τον έλεγχο αναγκαιότητας κινδύνου ιδιωτικότητας.

1.2 Η παρούσα πολιτική εφαρμόζεται στα ακόλουθα:

1.2.1 όλες τις δραστηριότητες επεξεργασίας PII εντός του πεδίου εφαρμογής του PIMS·

1.2.2 επεξεργασία που εκτελείται ως υπεύθυνος επεξεργασίας, από κοινού υπεύθυνος επεξεργασίας, εκτελών την επεξεργασία ή υπεργολάβος επεξεργασίας·

1.2.3 επεξεργασία που εκτελείται από επιχειρησιακές διαδικασίες, συστήματα, εφαρμογές, προμηθευτές, εκτελούντες την επεξεργασία, υπεργολάβους επεξεργασίας και αποδέκτες κοινοποίησης δεδομένων·

1.2.4 νέα επεξεργασία, επεξεργασία με ουσιώδεις αλλαγές και αποσυρθείσα επεξεργασία·

1.2.5 τεκμήρια που τηρούνται στο REG02 και υποστηρικτικά τεκμήρια στα REG01, REG03, REG04, REG05, REG07, REG08, REG09 και REG12.

1.3 Η παρούσα πολιτική δεν αντικαθιστά τους αναλυτικούς ελέγχους ειδοποιήσεων ιδιωτικότητας, τους ελέγχους συγκατάθεσης, τη μεθοδολογία DPIA, την εκτέλεση διατήρησης, την επιλογή μηχανισμού διεθνούς μεταφοράς, τους ελέγχους συμβάσεων εκτελούντων την επεξεργασία, τους ελέγχους ασφάλειας PII ή τους ελέγχους τεκμηριωμένων πληροφοριών. Οι απαιτήσεις αυτές ορίζονται στις συναφείς πολιτικές που παρατίθενται στην Ενότητα 12.

1.4 Για την παρούσα πολιτική, καταχώριση αποθετηρίου επεξεργασίας σημαίνει καταχώριση REG02 που περιγράφει διακριτή δραστηριότητα επεξεργασίας PII, συμπεριλαμβανομένων του σκοπού, του ρόλου, του ιδιοκτήτη, των κατηγοριών PII, των κατηγοριών υποκειμένων των δεδομένων προσωπικού χαρακτήρα, της νομικής βάσης ή της αναφοράς εντολής πελάτη, των συστημάτων, των αποδεκτών, της αναφοράς διατήρησης, της αναφοράς μεταφοράς, της κατάστασης κινδύνου ιδιωτικότητας και της κατάστασης ανασκόπησης.

1.5 Για την παρούσα πολιτική, ουσιώδης αλλαγή επεξεργασίας σημαίνει κάθε αλλαγή στον σκοπό επεξεργασίας, στη νομική βάση, στον ρόλο PIMS, στην κατηγορία PII, στην κατηγορία υποκειμένων των δεδομένων προσωπικού χαρακτήρα, στον αποδέκτη, στο σύστημα, στον προμηθευτή, στον υπεργολάβο επεξεργασίας, στην τοποθεσία επεξεργασίας, στη μεταφορά, στον κανόνα διατήρησης, στην ταξινόμηση ασφάλειας, στην ειδοποίηση ιδιωτικότητας, στην εξάρτηση από συγκατάθεση, στην κατάσταση DPIA, στην εντολή πελάτη ή στο πεδίο εφαρμογής πιστοποίησης.

2. Σκοπός

2.1 Σκοπός της παρούσας πολιτικής είναι να διασφαλίσει ότι ο οργανισμός μπορεί να αναγνωρίζει, να τεκμηριώνει, να αιτιολογεί, να ανασκοπεί και να αποδεικνύει τις δραστηριότητες επεξεργασίας PII εντός του πεδίου εφαρμογής του PIMS.

2.2 Η παρούσα πολιτική επιτρέπει στον οργανισμό να διατηρεί πλήρες, επικαιροποιημένο και έτοιμο για έλεγχο αποθετήριο επεξεργασίας PII, το οποίο υποστηρίζει τη νόμιμη επεξεργασία, τη λογοδοσία, τις ειδοποιήσεις ιδιωτικότητας, τη διαχείριση συγκατάθεσης, την αξιολόγηση κινδύνου ιδιωτικότητας, τον έλεγχο αναγκαιότητας DPIA, τη διατήρηση, τη διακυβέρνηση μεταφορών, τη διακυβέρνηση εκτελούντων την επεξεργασία και την παρακολούθηση του PIMS.

3. Στόχοι

3.1 Οι στόχοι της παρούσας πολιτικής είναι να:

- 3.1.1 καθιερώνει το REG02 ως το έγκυρο αποθετήριο επεξεργασίας PII και αντικείμενο τεκμηρίων ROPA.
- 3.1.2 διασφαλίζει ότι κάθε δραστηριότητα επεξεργασίας PII έχει υπόλογο ιδιοκτήτη.
- 3.1.3 διακρίνει τις καταχωρίσεις επεξεργασίας υπευθύνου επεξεργασίας, από κοινού υπευθύνου επεξεργασίας, εκτελούντος την επεξεργασία και υπεργολάβου επεξεργασίας.
- 3.1.4 τεκμηριώνει συγκεκριμένους σκοπούς επεξεργασίας πριν από την έναρξη της επεξεργασίας.
- 3.1.5 τεκμηριώνει τη νομική βάση για επεξεργασία από υπεύθυνο επεξεργασίας πριν από την έναρξη της επεξεργασίας.
- 3.1.6 τεκμηριώνει τις εντολές πελάτη για επεξεργασία από εκτελούντα την επεξεργασία και υπεργολάβο επεξεργασίας πριν από την έναρξη της επεξεργασίας.
- 3.1.7 τεκμηριώνει κατηγορίες PII, κατηγορίες υποκειμένων των δεδομένων προσωπικού χαρακτήρα, αποδέκτες, αναφορές διατήρησης, αναφορές μεταφοράς, συστήματα και σχέσεις προμηθευτών.
- 3.1.8 συνδέει τις καταχωρίσεις αποθετηρίου με τεκμήρια ειδοποίησης ιδιωτικότητας, συγκατάθεσης, DPIA, κινδύνου, προμηθευτή, μεταφοράς, ελέγχου και ελέγχου συμμόρφωσης, όπου εφαρμόζεται.
- 3.1.9 διασφαλίζει ότι οι καταχωρίσεις αποθετηρίου επεξεργασίας ανασκοποούνται, επικαιροποιούνται και διορθώνονται όταν αλλάζει η επεξεργασία.
- 3.1.10 αποφεύγει τη δημιουργία χωριστών μητρώων νομικής βάσης ή αποθετηρίων επεξεργασίας εκτός του REG02.

4. Δηλώσεις πολιτικής

4.1 Βασική γραμμή αποθετηρίου επεξεργασίας

- 4.1.1 [Both] Ο Process Owner / Business Owner MUST δημιουργεί καταχώριση αποθετηρίου επεξεργασίας στο REG02 πριν αρχίσει οποιαδήποτε νέα δραστηριότητα επεξεργασίας PII.
- 4.1.2 [Both] Ο Process Owner / Business Owner MUST καταγράφει τα απαιτούμενα πεδία REG02 για κάθε δραστηριότητα επεξεργασίας πριν αρχίσει η δραστηριότητα.
- 4.1.3 [Both] Ο Privacy Lead / PIMS Manager MUST εγκρίνει το απαιτούμενο σύνολο πεδίων REG02 στο REG12 πριν από την αρχική λειτουργία του PIMS και ετησίως στη συνέχεια.
- 4.1.4 [Both] Ο Process Owner / Business Owner MUST ταξινομεί τον ρόλο PIMS του οργανισμού για κάθε δραστηριότητα επεξεργασίας στο REG02 πριν αρχίσει η δραστηριότητα.
- 4.1.5 [Both] Ο System Owner / Application Owner MUST συνδέει κάθε σύστημα ή εφαρμογή που επεξεργάζεται PII με τη σχετική δραστηριότητα επεξεργασίας REG02 πριν από τη θέση του συστήματος σε λειτουργία.
- 4.1.6 [Both] Ο Vendor / Procurement Owner MUST συνδέει κάθε σχέση με εκτελούντα την επεξεργασία, υπεργολάβο επεξεργασίας, κοινοποίηση σε τρίτο μέρος ή από κοινού υπεύθυνο επεξεργασίας στο REG08 με τη σχετική δραστηριότητα επεξεργασίας REG02 πριν από την έγκριση συμφωνίας ή την ένταξη.

4.2 Αρχεία σκοπού και νομικής βάσης υπευθύνου επεξεργασίας

- 4.2.1 [Controller] Ο Process Owner / Business Owner MUST τεκμηριώνει τον συγκεκριμένο σκοπό επεξεργασίας στο REG02 πριν συλλεχθεί, χρησιμοποιηθεί, γνωστοποιηθεί ή υποβληθεί με άλλον τρόπο σε επεξεργασία το PII.
- 4.2.2 [Controller] Ο Privacy Lead / PIMS Manager MUST επικυρώνει τη νομική βάση που καταγράφεται στο REG02 πριν αρχίσει η επεξεργασία από υπεύθυνο επεξεργασίας και πριν τεθεί σε ισχύ οποιαδήποτε αλλαγή σκοπού.

- 4.2.3 [Controller] Ο Data Protection Officer / Privacy Advisor MUST καταγράφει συμβουλή στο REG12 πριν από την έγκριση νέας νομικής βάσης για επεξεργασία υψηλού κινδύνου, ειδικές κατηγορίες PII, δεδομένα ποινικών καταδικών ή αδικημάτων ή ουσιωδώς αλλαγμένη επεξεργασία υπευθύνου επεξεργασίας.
- 4.2.4 [Controller] Ο Process Owner / Business Owner MUST συνδέει το REG02 με το REG05 πριν η επεξεργασία υπευθύνου επεξεργασίας βασιστεί στη συγκατάθεση ως νομική βάση.
- 4.2.5 [Controller] Ο Process Owner / Business Owner MUST καταγράφει την αναφορά αξιολόγησης έννομου συμφέροντος στο REG04 πριν η επεξεργασία υπευθύνου επεξεργασίας βασιστεί σε έννομα συμφέροντα.
- 4.2.6 [Conditional] Ο Process Owner / Business Owner MUST καταγράφει την προϋπόθεση επεξεργασίας ειδικών κατηγοριών στο REG02 πριν από την επεξεργασία ειδικών κατηγοριών PII.
- 4.2.7 [Conditional] Ο Privacy Lead / PIMS Manager MUST καταγράφει τη βάση εξουσιοδότησης για δεδομένα ποινικών καταδικών ή αδικημάτων στο REG02 πριν από την επεξεργασία δεδομένων ποινικών καταδικών ή αδικημάτων.
- 4.2.8 [Controller] Ο Process Owner / Business Owner MUST τεκμηριώνει τη συμβατότητα σκοπών επεξεργασίας και τον έλεγχο αναγκαιότητας κινδύνου ιδιωτικότητας στο REG02 και στο REG04 πριν χρησιμοποιήσει PII για νέο σκοπό που δεν έχει καταγραφεί προηγουμένως.

[... 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 αποθετηρίου επεξεργασίας και νομικής βάσης

- 9.1.1 [All] Ο Process Owner / Business Owner MUST ζητά εξαιρέση στο REG12 πριν λειτουργήσει δραστηριότητα επεξεργασίας PII χωρίς απαιτούμενο πεδίο REG02, καταχώριση νομικής βάσης, αναφορά εντολής πελάτη ή κατάσταση ανασκόπησης.
- 9.1.2 [All] Ο Privacy Lead / PIMS Manager MUST αξιολογεί τον αντίκτυπο κάθε εξαίρεσης αποθετηρίου επεξεργασίας στην ιδιωτικότητα, στην πιστοποίηση και στη λειτουργία στο REG12 εντός 10 εργάσιμων ημερών από το αίτημα.
- 9.1.3 [All] Ο Data Protection Officer / Privacy Advisor MUST καταγράφει συμβουλή στο REG12 πριν από την έγκριση οποιασδήποτε εξαίρεσης που αφορά νομική βάση, ειδική κατηγορία PII, δεδομένα ποινικών καταδικών ή αδικημάτων, επεξεργασία υψηλού κινδύνου, διασύνδεση διεθνούς μεταφοράς ή περιορισμό εντολής πελάτη.
- 9.1.4 [All] Το Top Management MUST εγκρίνει εξαιρέσεις αποθετηρίου επεξεργασίας που υπερβαίνουν τις 30 ημέρες, επηρεάζουν επεξεργασία υψηλού κινδύνου ή επηρεάζουν το πεδίο εφαρμογής πιστοποίησης στο REG12 πριν τεθεί σε ισχύ η εξαίρεση.
- 9.1.5 [All] Ο Privacy Lead / PIMS Manager MUST ορίζει ημερομηνία λήξης που δεν υπερβαίνει τις 90 ημέρες στο REG12 για κάθε εγκεκριμένη εξαίρεση αποθετηρίου επεξεργασίας πριν από την έγκριση.
- 9.1.6 [All] Ο Process Owner / Business Owner MUST κλείνει ή επαναξιολογεί κάθε εξαίρεση αποθετηρίου επεξεργασίας στο REG12 εντός πέντε εργάσιμων ημερών από τη λήξη.

10. Εφαρμογή και τήρηση

10.1 Εφαρμογή απαιτήσεων αποθετηρίου επεξεργασίας και νομικής βάσης

- 10.1.1 [All] Ο Privacy Lead / PIMS Manager MUST καταγράφει ελλιπή, ανακριβή, παρωχημένα ή μη εγκεκριμένα τεκμήρια αποθετηρίου επεξεργασίας REG02 ως μη συμμόρφωση στο REG12 εντός πέντε εργάσιμων ημερών από τον εντοπισμό.

- 10.1.2 [Controller] Ο Process Owner / Business Owner MUST αναστέλλει νέα επεξεργασία υπευθύνου επεξεργασίας όταν τα απαιτούμενα τεκμήρια σκοπού ή νομικής βάσης λείπουν από το REG02 πριν από την έναρξη λειτουργίας.
- 10.1.3 [Processor] Ο Process Owner / Business Owner MUST αναστέλλει νέα επεξεργασία εκτελούντος την επεξεργασία όταν τα απαιτούμενα τεκμήρια εντολών πελάτη λείπουν από το REG02 ή το REG08 πριν από την έναρξη υπηρεσίας.
- 10.1.4 [Both] Ο System Owner / Application Owner MUST αποκλείει τη θέση συστήματος σε λειτουργία για επεξεργασία PII όταν λείπει η απαιτούμενη διασύνδεση αποθετηρίου REG02 πριν από την έγκριση θέσης σε λειτουργία.
- 10.1.5 [Both] Ο Vendor / Procurement Owner MUST αποκλείει την έναρξη προμηθευτή, εκτελούντος την επεξεργασία, υπεργολάβου επεξεργασίας, τρίτου αποδέκτη ή από κοινού υπευθύνου επεξεργασίας όταν λείπουν τα απαιτούμενα τεκμήρια διασύνδεσης REG02 και REG08 πριν από την έγκριση συμφωνίας.
- 10.1.6 [All] Το Top Management MUST ανασκοπεί ανεπίλυτες μείζονες μη συμμορφώσεις αποθετηρίου επεξεργασίας ή νομικής βάσης στο REG12 κατά την ανασκόπηση της διοίκησης.
- 10.1.7 [All] Ο Internal Audit / Compliance Reviewer MUST επαληθεύει την αποτελεσματικότητα διορθωτικών ενεργειών για μη συμμορφώσεις αποθετηρίου επεξεργασίας στο REG12 κατά τον 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] Ο Privacy Lead / PIMS Manager MUST ανασκοπεί την παρούσα πολιτική στο REG12 ετησίως και εντός 30 ημερών από ουσιώδη αλλαγή σε αποθετήριο επεξεργασίας, νομική βάση, εντολή εκτελούντος την επεξεργασία, ROPA ή απαιτήσεις πιστοποίησης.
- 11.1.2 [All] Ο Privacy Lead / PIMS Manager MUST ανασκοπεί τις ελάχιστες απαιτήσεις πεδίων REG02 στο REG12 ετησίως και εντός 30 ημερών από ουσιώδη νομική, κανονιστική, συμβατική ή επεξεργαστική αλλαγή.
- 11.1.3 [All] Ο Data Protection Officer / Privacy Advisor MUST ανασκοπεί αλλαγές σημαντικές για την ιδιωτικότητα στην παρούσα πολιτική στο REG12 πριν από την έγκριση.
- 11.1.4 [All] Το Top Management MUST εγκρίνει ουσιώδεις αλλαγές στην παρούσα πολιτική στο REG12 πριν από τη δημοσίευση.
- 11.1.5 [All] Ο Privacy Lead / PIMS Manager MUST επικαιροποιεί τα REG03 και REG04 εντός 15 εργάσιμων ημερών μετά από εγκεκριμένες αλλαγές πολιτικής που μεταβάλλουν την εφαρμοσιμότητα ελέγχων ή τις απαιτήσεις ελέγχου αναγκαιότητας κινδύνου ιδιωτικότητας.
- 11.1.6 [All] Ο Privacy Lead / PIMS Manager MUST καταγράφει την επικοινωνία εγκεκριμένων αλλαγών στην παρούσα πολιτική 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 PII04 - Πολιτική ειδοποίησης ιδιωτικότητας και διαφάνειας
- 12.5 PII05 - Πολιτική διαχείρισης συγκατάθεσης και προτιμήσεων
- 12.6 PII07 - Πολιτική αξιολόγησης κινδύνου ιδιωτικότητας και DPIA
- 12.7 PII08 - Πολιτική ιδιωτικότητας ήδη από τον σχεδιασμό και εξ ορισμού
- 12.8 PII09 - Πολιτική συλλογής, χρήσης, γνωστοποίησης και κοινοποίησης PII
- 12.9 PII10 - Πολιτική διατήρησης, διαγραφής και διάθεσης PII

- 12.10 PII11 - Πολιτική ακρίβειας και ποιότητας PII
- 12.11 PII12 - Πολιτική διαχείρισης ιδιωτικότητας εκτελούντων την επεξεργασία, υπεργολάβων επεξεργασίας και τρίτων μερών
- 12.12 PII13 - Πολιτική διεθνών μεταφορών PII
- 12.13 PII14 - Πολιτική ασφάλειας PII και ελέγχου πρόσβασης
- 12.14 PII17 - Πολιτική τεκμηριωμένων πληροφοριών και διαχείρισης τεκμηρίων PIMS
- 12.15 PII18 - Πολιτική παρακολούθησης, ελέγχου και βελτίωσης PIMS

13. Πρότυπα και πλαίσια αναφοράς

- 13.1 Η παρούσα πολιτική αντιστοιχίζεται στα ακόλουθα πρότυπα και κανονισμούς. 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 4.1** - Αντιστοιχίζεται στον προσδιορισμό του ρόλου PIMS του οργανισμού για κάθε δραστηριότητα επεξεργασίας και στη διάκριση πλαισίων υπευθύνου επεξεργασίας, από κοινού υπευθύνου επεξεργασίας, εκτελούντος την επεξεργασία και υπεργολάβου επεξεργασίας. Addressed by clauses [4.1.4; 4.3.1; 4.3.4; 4.3.5].
- 13.2.2 **Clause 6.1.2** - Αντιστοιχίζεται στη διασύνδεση εναύσματος αξιολόγησης κινδύνου ιδιωτικότητας για νέες και ουσιαστές αλλαγμένες δραστηριότητες επεξεργασίας PII. Addressed by clauses [4.2.8; 4.5.2; 4.5.3].
- 13.2.3 **Clause 6.1.3** - Αντιστοιχίζεται στη σύνδεση δραστηριοτήτων επεξεργασίας με την εφαρμοσιμότητα ελέγχων και τα τεκμήρια Δήλωσης Εφαρμοσιμότητας PIMS. Addressed by clauses [4.5.4; 7.1.5; 11.1.5].
- 13.2.4 **Clause 7.5** - Αντιστοιχίζεται στη διατήρηση αρχείων αποθετηρίου επεξεργασίας, νομικής βάσης, εντολών εκτελούντος την επεξεργασία, ανασκόπησης, εξαιρέσεων και διορθωτικών ενεργειών ως ελεγχόμενων τεκμηριωμένων πληροφοριών. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.2; 4.3.1; 4.4.1; 4.5.1; 7.1.1; 7.1.3; 9.1.1; 10.1.1].
- 13.2.5 **Clause 8.1** - Αντιστοιχίζεται στον επιχειρησιακό σχεδιασμό και έλεγχο για τη δημιουργία, επικύρωση, επικαιροποίηση, ανασκόπηση και απόσυρση καταχωρίσεων αποθετηρίου επεξεργασίας πριν αρχίσει ή αλλάξει η επεξεργασία. Addressed by clauses [4.1.1; 4.1.5; 4.1.6; 4.5.1; 4.5.6; 7.1.2; 7.1.6; 7.1.7; 7.1.8].
- 13.2.6 **Clause 8.2** - Αντιστοιχίζεται στη διασύνδεση επιχειρησιακής αξιολόγησης κινδύνου ιδιωτικότητας από καταχωρίσεις αποθετηρίου επεξεργασίας και εναύσματα ουσιαστικής αλλαγής επεξεργασίας. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].
- 13.2.7 **Clause 9.1** - Αντιστοιχίζεται στην παρακολούθηση και μέτρηση της πληρότητας αποθετηρίου επεξεργασίας, της επικύρωσης νομικής βάσης, της διασύνδεσης εντολών, της κατάστασης ανασκόπησης, της διασύνδεσης ελέγχου αναγκαιότητας DPIA και των εξαιρέσεων συμφιλώσης. Addressed by clauses [4.5.4; 4.5.5; 6.1.1; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 8.1.8].
- 13.2.8 **Clause 10.2** - Αντιστοιχίζεται στον χειρισμό μη συμμορφώσεων αποθετηρίου και νομικής βάσης, εξαιρέσεων, διορθωτικών ενεργειών, εφαρμογής απαιτήσεων και επαλήθευσης αποτελεσματικότητας. Addressed by clauses [9.1.1; 9.1.2; 9.1.4; 9.1.6; 10.1.1; 10.1.6; 10.1.7].
- 13.2.9 **Annex A.1.2.2** - Αντιστοιχίζεται στον προσδιορισμό και την τεκμηρίωση σκοπών επεξεργασίας υπευθύνου επεξεργασίας πριν συλλεχθεί, χρησιμοποιηθεί, γνωστοποιηθεί ή υποβληθεί με άλλον τρόπο σε επεξεργασία το PII. Addressed by clauses [4.1.2; 4.2.1; 4.2.8; 4.3.5].

- 13.2.10 **Annex A.1.2.3** - Αντιστοιχίζεται στον καθορισμό, την τεκμηρίωση, την επικύρωση και την απόδειξη νομικής βάσης για επεξεργασία από υπεύθυνο επεξεργασίας. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7].
- 13.2.11 **Annex A.1.2.6** - Αντιστοιχίζεται στον έλεγχο νέων και ουσιαδώς αλλαγμένων δραστηριοτήτων επεξεργασίας υπευθύνου επεξεργασίας για ανάγκη DPIA. Addressed by clauses [4.5.2; 4.5.3; 8.1.5].
- 13.2.12 **Annex A.1.2.8** - Αντιστοιχίζεται στην καταγραφή σκοπών επεξεργασίας από κοινού υπευθύνων επεξεργασίας και αναφορών κατανομής ευθυνών. Addressed by clauses [4.1.6; 4.3.5; 10.1.5].
- 13.2.13 **Annex A.1.2.9** - Αντιστοιχίζεται στη διατήρηση αρχείων υπευθύνου επεξεργασίας σχετικά με την επεξεργασία PII, συμπεριλαμβανομένων σκοπών, κατηγοριών, αποδεκτών, αναφορών διατήρησης, μεταφορών, νομικής βάσης, ελέγχου κινδύνου, ιδιοκτήτη, κατάστασης και τεκμηρίων ανασκόπησης. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.4.6; 4.5.1; 4.5.6; 7.1.2; 7.1.8].
- 13.2.14 **Annex A.2.2.2** - Αντιστοιχίζεται στη συμφωνία πελάτη εκτελούντος την επεξεργασία και στα τεκμήρια τεκμηριωμένων εντολών, συμπεριλαμβανομένων αντικειμένου, διάρκειας, σκοπού, κατηγοριών PII και κατηγοριών υποκειμένων των δεδομένων προσωπικού χαρακτήρα. Addressed by clauses [4.3.1; 4.3.2; 5.1.7; 10.1.3].
- 13.2.15 **Annex A.2.2.3** - Αντιστοιχίζεται στη διασφάλιση ότι οι σκοποί επεξεργασίας του εκτελούντος την επεξεργασία παραμένουν ευθυγραμμισμένοι με τεκμηριωμένες εντολές πελάτη. Addressed by clauses [4.3.1; 4.3.3; 4.3.4; 10.1.3].
- 13.2.16 **Annex A.2.2.7** - Αντιστοιχίζεται στη διατήρηση αρχείων εκτελούντος την επεξεργασία σχετικά με την επεξεργασία PII για λογαριασμό πελατών. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 8.1.3].

13.3 **GDPR**

- 13.3.1 **Article 5(1)(a)** - Αντιστοιχίζεται στον σκοπό επεξεργασίας υπευθύνου επεξεργασίας, στην επικύρωση νομικής βάσης και στα τεκμήρια λογοδοσίας πριν αρχίσει η επεξεργασία. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.8].
- 13.3.2 **Article 5(1)(b)** - Αντιστοιχίζεται στην εξειδίκευση σκοπού, στην αξιολόγηση συμβατότητας σκοπών επεξεργασίας και στην αποτροπή μη τεκμηριωμένης επεξεργασίας για νέο σκοπό. Addressed by clauses [4.2.1; 4.2.8; 4.3.3].
- 13.3.3 **Article 5(1)(c)** - Αντιστοιχίζεται στην καταγραφή κατηγοριών PII, κατηγοριών υποκειμένων των δεδομένων προσωπικού χαρακτήρα και δεδομένων πηγής πριν από την επεξεργασία για την υποστήριξη ανασκόπησης ελαχιστοποίησης. Addressed by clauses [4.1.2; 4.4.1; 4.4.6].
- 13.3.4 **Article 5(1)(e)** - Αντιστοιχίζεται στην καταγραφή κανόνα διατήρησης ή αναφοράς διατήρησης για κάθε δραστηριότητα επεξεργασίας. Addressed by clauses [4.4.4; 8.1.6].
- 13.3.5 **Article 5(2)** - Αντιστοιχίζεται σε τεκμήρια λογοδοσίας για αποθετήριο επεξεργασίας, επικύρωση νομικής βάσης, ανασκόπηση, συμφιλίωση, δειγματοληψία ελέγχου και διορθωτικές ενέργειες. Addressed by clauses [4.1.1; 4.2.2; 4.5.4; 4.5.5; 6.1.2; 10.1.1; 10.1.7].
- 13.3.6 **Article 6** - Αντιστοιχίζεται στην τεκμηρίωση και επικύρωση νομικής βάσης για επεξεργασία από υπεύθυνο επεξεργασίας, συμπεριλαμβανομένων της διασύνδεσης συγκατάθεσης, της αναφοράς αξιολόγησης έννομου συμφέροντος και της συμβατότητας σκοπών επεξεργασίας. Addressed by clauses [4.2.2; 4.2.4; 4.2.5; 4.2.8].
- 13.3.7 **Article 9** - Αντιστοιχίζεται στην καταγραφή προϋπόθεσης επεξεργασίας ειδικών κατηγοριών και συμβουλής ιδιωτικότητας πριν από την επεξεργασία ειδικών κατηγοριών PII. Addressed by clauses [4.2.3; 4.2.6; 9.1.3].

- 13.3.8 **Article 10** - Αντιστοιχίζεται στην καταγραφή της βάσης εξουσιοδότησης για δεδομένα ποινικών καταδικών ή αδικημάτων πριν από την επεξεργασία. Addressed by clauses [4.2.3; 4.2.7; 9.1.3].
- 13.3.9 **Article 24** - Αντιστοιχίζεται στη διακυβέρνηση, ανασκόπηση, λογοδοσία και εποπτεία από τη διοίκηση των αρχείων αποθετηρίου επεξεργασίας και νομικής βάσης από τον υπεύθυνο επεξεργασίας. Addressed by clauses [4.2.2; 5.1.1; 6.1.2; 10.1.6; 11.1.4].
- 13.3.10 **Article 26** - Αντιστοιχίζεται σε τεκμήρια σκοπού επεξεργασίας από κοινού υπευθύνων επεξεργασίας και κατανομής ευθυνών. Addressed by clauses [4.1.6; 4.3.5; 10.1.5].
- 13.3.11 **Article 28** - Αντιστοιχίζεται στους ελέγχους εντολών, συμφωνιών, διασύνδεσης σχέσεων και ένταξης εκτελούντων την επεξεργασία και υπερβολάβων επεξεργασίας. Addressed by clauses [4.1.6; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 5.1.7; 7.1.7; 10.1.3; 10.1.5].
- 13.3.12 **Article 30** - Αντιστοιχίζεται στα αρχεία δραστηριοτήτων επεξεργασίας υπευθύνου επεξεργασίας και εκτελούντος την επεξεργασία, συμπεριλαμβανομένων σκοπών επεξεργασίας, κατηγοριών PII, κατηγοριών υποκειμένων των δεδομένων προσωπικού χαρακτήρα, αποδεκτών, μεταφορών, αναφορών διατήρησης και αρχείων εντολών πελάτη. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.3.1; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.1; 4.5.6; 7.1.2].
- 13.3.13 **Article 35** - Αντιστοιχίζεται στη διασύνδεση ελέγχου αναγκαιότητας DPIA για νέες, ουσιωδώς αλλαγμένες ή υψηλού κινδύνου δραστηριότητες επεξεργασίας υπευθύνου επεξεργασίας. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].

13.4 ISO/IEC 29100:2020

- 13.4.1 **Clause 5.3** - Αντιστοιχίζεται στη νομιμότητα σκοπού, στην εξειδίκευση σκοπού, στη διασύνδεση νομικής βάσης και στα τεκμήρια συμβατότητας σκοπών επεξεργασίας. Addressed by clauses [4.2.1; 4.2.2; 4.2.8; 4.3.1; 4.3.3].
- 13.4.2 **Clause 5.4** - Αντιστοιχίζεται στον περιορισμό συλλογής μέσω τεκμηρίωσης κατηγοριών PII, κατηγοριών υποκειμένων των δεδομένων προσωπικού χαρακτήρα, πηγών και αιτιολόγησης πριν αρχίσει η επεξεργασία. Addressed by clauses [4.1.2; 4.4.1; 4.4.6].
- 13.4.3 **Clause 5.5** - Αντιστοιχίζεται στην ελαχιστοποίηση δεδομένων μέσω απαιτήσεων πεδίων αποθετηρίου, τεκμηρίωσης κατηγοριών, τεκμηρίωσης αποδεκτών και ανασκόπησης τρεχουσών καταχωρίσεων επεξεργασίας. Addressed by clauses [4.1.2; 4.4.1; 4.4.2; 4.5.4; 8.1.6].
- 13.4.4 **Clause 5.6** - Αντιστοιχίζεται στον περιορισμό χρήσης, διατήρησης, γνωστοποίησης και μεταφοράς μέσω τεκμηριωμένων σκοπών, κατηγοριών αποδεκτών, αναφορών διατήρησης, διασύνδεσης μεταφοράς και ελέγχων αλλαγής σκοπού. Addressed by clauses [4.2.1; 4.2.8; 4.4.2; 4.4.4; 4.4.5].
- 13.4.5 **Clause 5.10** - Αντιστοιχίζεται στη λογοδοσία μέσω ιδιοκτησίας, διακυβέρνησης αποθετηρίου, ανασκόπησης, συμφιλίωσης, δειγματοληψίας ελέγχου, χειρισμού εξαιρέσεων και τεκμηρίων διορθωτικών ενεργειών. Addressed by clauses [4.1.1; 4.1.3; 4.5.4; 4.5.5; 5.1.5; 6.1.1; 8.1.1; 10.1.1].

13.5 ISO/IEC 29151:2022

- 13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7** - Αντιστοιχίζεται σε ελέγχους προστασίας PII για νομιμότητα σκοπού, περιορισμό συλλογής, ελαχιστοποίηση δεδομένων και περιορισμό χρήσης, διατήρησης και γνωστοποίησης. Addressed by clauses [4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.4; 4.4.6; 4.5.4; 8.1.6].

13.6 ISO/IEC 29134:2020

- 13.6.1 **Clause 5.1; Clause 6.2** - Αντιστοιχίζεται στη χρήση αλλαγών αποθετηρίου επεξεργασίας για την ενεργοποίηση αξιολόγησης κινδύνου ιδιωτικότητας και ελέγχου αναγκαιότητας DPIA

πριν προχωρήσει νέα ή ουσιωδώς αλλαγμένη επεξεργασία. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].