| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου | | | | | | | |
| Αριθμός εγγράφου:<br>PII08 | | | | | Τίτλος εγγράφου:<br>**Πολιτική προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό και εξ ορισμού** | | | | | | | |
| Έκδοση:<br>1.0 | | Ημερομηνία έναρξης ισχύος:<br>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 / Κανονιστική απαίτηση | Ρήτρα / Έλεγχος / Άρθρο | Εφαρμοσιμότητα | Τύπος κάλυψης | Σχόλιο |
|---|---|---|---|---|
| ISO/IEC 27701:2025 | Clause 6.1.2; Clause 6.1.3 | Both | Supporting | Σύνδεση με την αξιολόγηση κινδύνου ιδιωτικότητας και την αντιμετώπιση κινδύνου ιδιωτικότητας |
| ISO/IEC 27701:2025 | Clause 6.3; Clause 8.1 | Both | Primary | Προγραμματισμένες αλλαγές και επιχειρησιακός έλεγχος |
| ISO/IEC 27701:2025 | Clause 7.5 | Both | Supporting | Τεκμηριωμένα τεκμήρια σχεδιασμού προστασίας της ιδιωτικότητας |
| ISO/IEC 27701:2025 | Clause 9.1; Clause 10.2 | Both | Supporting | Παρακολούθηση και διορθωτικά μέτρα |
| ISO/IEC 27701:2025 | Annex A.1.2.2; Annex A.1.2.6; Annex A.1.2.9 | Controller | Supporting | Σκοποί, εναύσματα PIA και αρχεία |
| ISO/IEC 27701:2025 | Annex A.1.4.2; Annex A.1.4.3 | Controller | Primary | Περιορισμός συλλογής και επεξεργασίας |
| ISO/IEC 27701:2025 | Annex A.1.4.4; Annex A.1.4.5 | Controller | Supporting | Στόχοι ακρίβειας και ελαχιστοποίησης |
| ISO/IEC 27701:2025 | Annex A.1.4.6; Annex A.1.4.7 | Controller | Supporting | Αποταυτοποίηση, σχεδιασμός διαγραφής και προσωρινά αρχεία |
| ISO/IEC 27701:2025 | Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7 | Processor | Supporting | Συμφωνία πελάτη, υποστήριξη και αρχεία εκτελούντος την επεξεργασία |
| ISO/IEC 27701:2025 | Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4 | Processor | Supporting | Δυνατότητες σχεδιασμού εκτελούντος την επεξεργασία |
| ISO/IEC 27701:2025 | Annex A.3.27; Annex A.3.29 | Both | Supporting | Κύκλος ζωής ανάπτυξης και αρχές μηχανικής |

| | | | | |
|---|---|---|---|---|
| GDPR | Article 5(1)(b); Article 5(1)(c); Article 5(2) | Controller | Supporting | Περιορισμός σκοπού, ελαχιστοποίηση και λογοδοσία |
| GDPR | Article 24 | Controller | Supporting | Μέτρα υπευθύνου επεξεργασίας |
| GDPR | Article 25 | Controller | Primary | Προστασία δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού |
| GDPR | Article 28 | Both | Supporting | Εντολές και συνδρομή εκτελούντος την επεξεργασία |
| GDPR | Article 30 | Both | Supporting | Αρχεία επεξεργασίας |
| GDPR | Article 35 | Controller | Supporting | Σύνδεση εναυσμάτων DPIA |
| ISO/IEC 29100:2020 | Clause 4.7 | Both | Supporting | Έλεγχοι ιδιωτικότητας ήδη από τον σχεδιασμό |
| ISO/IEC 29100:2020 | Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6 | Both | Primary | Σκοπός, συλλογή, ελαχιστοποίηση και περιορισμός χρήσης |
| ISO/IEC 29100:2020 | Clause 5.7; Clause 5.10; Clause 5.12 | Both | Supporting | Ακρίβεια, λογοδοσία και συμμόρφωση |
| ISO/IEC 29151:2022 | Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8 | Both | Primary | Αρχές και έλεγχοι προστασίας δεδομένων προσωπικού χαρακτήρα |

## 1. Πεδίο εφαρμογής

1.1 Η παρούσα πολιτική καθορίζει απαιτήσεις για την ενσωμάτωση της προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό και της προστασίας της ιδιωτικότητας εξ ορισμού σε νέες και τροποποιημένες δραστηριότητες επεξεργασίας δεδομένων προσωπικού χαρακτήρα, έργα, προϊόντα, υπηρεσίες, συστήματα, εφαρμογές, ενσωματώσεις, δραστηριότητες προμηθειών και αλλαγές επιχειρησιακών διαδικασιών εντός του πεδίου εφαρμογής του PIMS.

1.2 Η παρούσα πολιτική εφαρμόζεται σε πλαίσια υπευθύνου επεξεργασίας, από κοινού υπευθύνου επεξεργασίας, εκτελούντος την επεξεργασία και υπεργολάβου επεξεργασίας. Οι υποχρεώσεις εκτελούντος την επεξεργασία και υπεργολάβου επεξεργασίας εφαρμόζονται όταν ο οργανισμός σχεδιάζει, ρυθμίζει, αλλάζει ή λειτουργεί επεξεργασία για λογαριασμό πελάτη, υπευθύνου επεξεργασίας ή ανάντη εκτελούντος την επεξεργασία βάσει τεκμηριωμένων εντολών.

**1.3 Η παρούσα πολιτική καλύπτει:**

1.3.1 απαιτήσεις ιδιωτικότητας κατά την έναρξη έργου·

1.3.2 ελέγχους σχεδιασμού για σκοπό, ελαχιστοποίηση δεδομένων και εξ ορισμού ρυθμίσεις·

1.3.3 ανασκόπηση σχεδιασμού προστασίας της ιδιωτικότητας πριν από τη θέση σε λειτουργία·

1.3.4 ανασκόπηση σχεδιασμού προστασίας της ιδιωτικότητας που ενεργοποιείται από αλλαγές·

1.3.5 ελέγχους προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό στο πλαίσιο προμηθειών·

1.3.6 σύνδεση με τον κίνδυνο ιδιωτικότητας, τον έλεγχο αναγκαιότητας DPIA και τα τεκμήρια διορθωτικών μέτρων.

**1.4 Η παρούσα πολιτική δεν αντικαθιστά:**

1.4.1 την PII03 για το αποθετήριο επεξεργασίας, τους σκοπούς, τη νομική βάση και τα αρχεία ROPA·

1.4.2 την PII04 για το περιεχόμενο και τη δημοσίευση ειδοποιήσεων ιδιωτικότητας·

1.4.3 την PII05 για τους ελέγχους συγκατάθεσης και προτιμήσεων·

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

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

1.4.6 την PII09 για τους ελέγχους συλλογής, χρήσης, γνωστοποίησης και κοινοποίησης·

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

1.4.8 την PII11 για τη λειτουργία ακρίβειας και ποιότητας·

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

1.4.10 την PII13 για μηχανισμούς διεθνών μεταφορών·

1.4.11 την PII14 για την ασφάλεια δεδομένων προσωπικού χαρακτήρα και τη λειτουργία ελέγχου πρόσβασης·

1.4.12 την PII18 για την παρακολούθηση, τον έλεγχο, τα διορθωτικά μέτρα και τη διακυβέρνηση βελτίωσης σε επίπεδο PIMS.

## 2. Σκοπός

2.1 Σκοπός της παρούσας πολιτικής είναι να διασφαλίζει ότι οι απαιτήσεις ιδιωτικότητας αναγνωρίζονται, υλοποιούνται και τεκμηριώνονται πριν αρχίσει ή αλλάξει ουσιωδώς η επεξεργασία δεδομένων προσωπικού χαρακτήρα, και ότι τα συστήματα και οι διαδικασίες ρυθμίζονται εξ ορισμού ώστε να περιορίζουν τη συλλογή, χρήση, έκθεση, εξάρτηση από διατήρηση, εξάρτηση από γνωστοποίηση και δυνατότητα ταυτοποίησης των δεδομένων προσωπικού χαρακτήρα σε ό,τι είναι αναγκαίο για τον τεκμηριωμένο σκοπό.

## 3. Στόχοι

### 3.1 Οι στόχοι της παρούσας πολιτικής είναι:

3.1.1 η ενσωμάτωση απαιτήσεων ιδιωτικότητας στις αποφάσεις έναρξης έργων, σχεδιασμού, προμηθειών, αλλαγών και θέσης σε λειτουργία·

3.1.2 η διασφάλιση ότι οι σχεδιασμοί επεξεργασίας δεδομένων προσωπικού χαρακτήρα συνδέονται με τεκμηριωμένους σκοπούς και αρχεία επεξεργασίας REG02·

3.1.3 η εφαρμογή ελαχιστοποίησης δεδομένων και εξ ορισμού ρυθμίσεων που προστατεύουν την ιδιωτικότητα πριν από την έναρξη επεξεργασίας·

3.1.4 η διασφάλιση ότι ενεργοποιείται ο έλεγχος κινδύνου ιδιωτικότητας και ο έλεγχος αναγκαιότητας DPIA χωρίς επανάληψη της μεθοδολογίας PII07·

3.1.5 η διασφάλιση ότι οι απαιτήσεις σχεδιασμού προμηθειών και εκτελούντων την επεξεργασία καταγράφονται χωρίς επανάληψη της διακυβέρνησης κύκλου ζωής της PII12·

3.1.6 η διασφάλιση ότι τα ανεπίλυτα ζητήματα σχεδιασμού κλιμακώνονται μέσω του REG12·

3.1.7 η διατήρηση τεκμηρίων σχεδιασμού έτοιμων για έλεγχο στα REG02, REG04, REG08 και REG12.

## 4. Δηλώσεις πολιτικής

### 4.1 Έναρξη έργου και απαιτήσεις ιδιωτικότητας

4.1.1 [Both] The Process Owner / Business Owner MUST καταγράφει καταχώριση σχεδιασμού προστασίας της ιδιωτικότητας στο REG04 πριν από την έναρξη οποιουδήποτε έργου, προϊόντος, υπηρεσίας, συστήματος, εφαρμογής, ενσωμάτωσης ή αλλαγής επιχειρησιακής διαδικασίας που περιλαμβάνει δεδομένα προσωπικού χαρακτήρα.

4.1.2 [Both] The Process Owner / Business Owner MUST συνδέει κάθε καταχώριση σχεδιασμού προστασίας της ιδιωτικότητας στο REG04 με υφιστάμενη ή προσχέδια δραστηριότητα επεξεργασίας REG02 πριν εγκριθούν οι λειτουργικές απαιτήσεις.

4.1.3 [Controller] The Privacy Lead / PIMS Manager MUST καταγράφει τις απαιτήσεις προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό του υπευθύνου επεξεργασίας στο REG04 πριν από την έγκριση λειτουργικού σχεδιασμού υπευθύνου επεξεργασίας.

4.1.4 [Processor] The Vendor / Procurement Owner MUST καταγράφει τις εντολές σχεδιασμού προστασίας της ιδιωτικότητας του πελάτη και τους συμβατικούς περιορισμούς σχεδιασμού στο REG08 πριν από την έγκριση σχεδιασμού υπηρεσίας εκτελούντος την επεξεργασία ή ουσιώδους αλλαγής υπηρεσίας.

4.1.5 [Conditional] The Data Protection Officer / Privacy Advisor MUST καταγράφει συμβουλή στο REG04 πριν από την έγκριση σχεδιασμού δεδομένων προσωπικού χαρακτήρα υψηλού κινδύνου, νέου, ευαίσθητου, αυτοματοποιημένου, μεγάλης κλίμακας ή ουσιωδώς τροποποιημένου.

4.1.6 [Both] The Information Security Lead MUST καταγράφει στο REG04, πριν από την έγκριση αρχιτεκτονικής, τις εξαρτήσεις ελέγχων ασφάλειας δεδομένων προσωπικού χαρακτήρα που υποστηρίζουν τον σχεδιασμό προστασίας της ιδιωτικότητας.

### 4.2 Ελαχιστοποίηση δεδομένων και σχεδιασμός ιδιωτικότητας εξ ορισμού

4.2.1 [Controller] The Process Owner / Business Owner MUST τεκμηριώνει τις ελάχιστες κατηγορίες δεδομένων προσωπικού χαρακτήρα, κατηγορίες υποκειμένων των δεδομένων προσωπικού χαρακτήρα, πηγές και σκοπούς στα REG02 και REG04 πριν από την έγκριση σχεδιασμού συλλογής ή εισαγωγής.

4.2.2 [Both] The System Owner / Application Owner MUST ρυθμίζει τις εξ ορισμού ρυθμίσεις επεξεργασίας στην ελάχιστη συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα που απαιτείται για τον τεκμηριωμένο σκοπό και καταγράφει τεκμήρια στο REG04 πριν από τη θέση σε λειτουργία.

4.2.3 [Controller] The Process Owner / Business Owner MUST τεκμηριώνει προαιρετικά πεδία δεδομένων προσωπικού χαρακτήρα, προαιρετικές επιλογές επεξεργασίας και ρυθμίσεις εξ ορισμού απενεργοποίησης στα REG02 και REG04 πριν από την έγκριση διεπαφής χρήστη, φόρμας ή ροής εργασιών.

4.2.4 [Both] The System Owner / Application Owner MUST τεκμηριώνει στο REG04, πριν από τη θέση σε λειτουργία, τις εξ ορισμού ρυθμίσεις έκθεσης ιδιωτικότητας για προβολές, αναφορές, εξαγωγές, διεπαφές και αυτοματοποιημένες ροές εργασιών.

4.2.5 [Both] The Process Owner / Business Owner MUST τεκμηριώνει στο REG04 τη σκοπιμότητα αποταυτοποίησης, ψευδωνυμοποίησης, συγκέντρωσης ή μη ταυτοποιήσιμης επεξεργασίας πριν εγκρίνει ταυτοποιήσιμα δεδομένα προσωπικού χαρακτήρα για δοκιμές, αναλύσεις, αναφορές ή δευτερεύουσα επιχειρησιακή χρήση.

4.2.6 [Both] The System Owner / Application Owner MUST τεκμηριώνει στο REG04, πριν από τη θέση σε λειτουργία, τη διαχείριση προσωρινών τεχνουργημάτων δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων προσωρινών αρχείων, caches, αρχείων καταγραφής ή εγγραφών σταδιοποίησης.

4.2.7 [Both] The Process Owner / Business Owner MUST δρομολογεί τις απαιτήσεις σχεδιασμού που ανήκουν στις PII10, PII11, PII13 ή PII14 προς τη σχετική διαδρομή τεκμηρίων πολιτικής στο REG04 εντός πέντε εργάσιμων ημερών από την αναγνώριση της εξάρτησης.

[ ... 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 σχεδιασμού προστασίας της ιδιωτικότητας

9.1.1 [Both] The Process Owner / Business Owner MUST αιτείται εξαίρεση σχεδιασμού προστασίας της ιδιωτικότητας στο REG12 πριν εγκρίνει σχεδιασμό ή αλλαγή που δεν μπορεί να ικανοποιήσει εφαρμοστέα απαίτηση σχεδιασμού προστασίας της ιδιωτικότητας.

9.1.2 [Both] The Privacy Lead / PIMS Manager MUST αξιολογεί στο REG12 τον αντίκτυπο, τους αντισταθμιστικούς ελέγχους και τη λήξη κάθε εξαίρεσης σχεδιασμού προστασίας της ιδιωτικότητας εντός πέντε εργάσιμων ημερών από το αίτημα.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST καταγράφει συμβουλή στο REG12 πριν από την έγκριση εξαίρεσης σχεδιασμού προστασίας της ιδιωτικότητας που αφορά επεξεργασία υψηλού κινδύνου, ευαίσθητη, αυτοματοποιημένη, μεγάλης κλίμακας, αμφισβητούμενη ή νομικά ουσιώδη.

9.1.4 [All] Top Management MUST εγκρίνει στο REG12 εξαίρεση σχεδιασμού προστασίας της ιδιωτικότητας που επηρεάζει επεξεργασία υψηλού αντικτύπου, πεδίο πιστοποίησης, ανεπίλυτο μείζονα κίνδυνο ή νομική υποχρέωση πριν από την έναρξη ισχύος της εξαίρεσης.

9.1.5 [Both] The Privacy Lead / PIMS Manager MUST ορίζει στο REG12 ημερομηνία λήξης που δεν υπερβαίνει τις 90 ημέρες για κάθε εγκεκριμένη εξαίρεση σχεδιασμού προστασίας της ιδιωτικότητας πριν από την έγκριση.

9.1.6 [Both] The Privacy Lead / PIMS Manager MUST κλείνει ή επαναξιολογεί κάθε εξαίρεση σχεδιασμού προστασίας της ιδιωτικότητας στο REG12 εντός πέντε εργάσιμων ημερών από τη λήξη.

## 10. Εφαρμογή

### 10.1 Εφαρμογή και διαχείριση μη συμμορφώσεων

10.1.1 [Both] The Privacy Lead / PIMS Manager MUST καταγράφει την απουσία ανασκόπησης σχεδιασμού προστασίας της ιδιωτικότητας, την απουσία τεκμηρίων ελαχιστοποίησης, την

ανεπίλυτη αστοχία ρυθμίσεων εξ ορισμού ή τη μη εξουσιοδοτημένη θέση σε λειτουργία ως μη συμμόρφωση στο REG12 εντός πέντε εργάσιμων ημερών από την αναγνώριση.

10.1.2 [Both] The System Owner / Application Owner MUST αποτρέπει τη θέση σε λειτουργία συστήματος επεξεργασίας δεδομένων προσωπικού χαρακτήρα όταν η ανασκόπηση σχεδιασμού προστασίας της ιδιωτικότητας REG04 είναι ελλιπής και καταγράφει την απόφαση στο REG12 πριν από τη θέση σε λειτουργία.

10.1.3 [Both] The Vendor / Procurement Owner MUST αποτρέπει την ένταξη προμηθευτή ή την υπογραφή σύμβασης όταν απουσιάζουν τα απαιτούμενα τεκμήρια σχεδιασμού προστασίας της ιδιωτικότητας REG08 και καταγράφει την απόφαση στο REG12 πριν από την ένταξη ή την υπογραφή.

10.1.4 [Both] The Process Owner / Business Owner MUST αναστέλλει τη χρήση νέου ή τροποποιημένου σχεδιασμού επεξεργασίας δεδομένων προσωπικού χαρακτήρα έως ότου ολοκληρωθούν η ανασκόπηση REG04, οι επικαιροποιήσεις REG02 και οι απαιτούμενες εξαιρέσεις REG12.

10.1.5 [All] Top Management MUST απαιτεί διορθωτικό μέτρο στο REG12 εντός 10 εργάσιμων ημερών για επαναλαμβανόμενη, παρατεταμένη ή υψηλού αντικτύπου αστοχία σχεδιασμού προστασίας της ιδιωτικότητας.

10.1.6 [All] The Internal Audit / Compliance Reviewer MUST επαληθεύει την αποτελεσματικότητα διορθωτικών μέτρων για μη συμμορφώσεις σχεδιασμού προστασίας της ιδιωτικότητας στο REG12 στον επόμενο προγραμματισμένο έλεγχο PIMS ή εντός 60 ημερών από το κλείσιμο, όποιο συμβεί πρώτο.

## 11. Ανασκόπηση και συντήρηση

### 11.1 Ανασκόπηση πολιτικής και ελέγχων σχεδιασμού

11.1.1 [All] The Privacy Lead / PIMS Manager MUST ανασκοπεί την παρούσα πολιτική στο REG12 ετησίως και εντός 30 ημερών από ουσιώδη νομική αλλαγή ή ουσιώδη αλλαγή επεξεργασίας, τεχνολογίας, πεδίου πιστοποίησης ή ελέγχου PIMS.

11.1.2 [Both] The Process Owner / Business Owner MUST ανασκοπεί ετησίως τις ενεργές δραστηριότητες επεξεργασίας REG02 για αλλαγές εξαρτήσεων σχεδιασμού προστασίας της ιδιωτικότητας και εντός 30 ημερών από ουσιώδη αλλαγή επεξεργασίας.

11.1.3 [Both] The System Owner / Application Owner MUST ανασκοπεί τα τεκμήρια ρύθμισης ιδιωτικότητας εξ ορισμού στο REG04 ετησίως και εντός 30 ημερών από ουσιώδη αλλαγή συστήματος.

11.1.4 [Both] The Vendor / Procurement Owner MUST ανασκοπεί τις υποχρεώσεις σχεδιασμού προστασίας της ιδιωτικότητας προμηθευτών, εκτελούντων την επεξεργασία, υπεργολάβων επεξεργασίας και τρίτων μερών στο REG08 πριν από την ανανέωση και εντός 30 ημερών από ουσιώδη αλλαγή σχέσης.

11.1.5 [Conditional] The Data Protection Officer / Privacy Advisor MUST ανασκοπεί τον αντίκτυπο ουσιωδών αλλαγών πολιτικής στην ιδιωτικότητα στο REG12 πριν από την έγκριση.

11.1.6 [All] Top Management MUST εγκρίνει ουσιώδεις αλλαγές στην παρούσα πολιτική στο REG12 πριν από τη δημοσίευση.

## 12. Συναφείς πολιτικές

12.1 PII01 - Πολιτική Συστήματος Διαχείρισης Πληροφοριών Ιδιωτικότητας

12.2 PII02 - Πολιτική ρόλων, αρμοδιοτήτων και λογοδοσίας ιδιωτικότητας

12.3 PII03 - Πολιτική αποθετηρίου 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 PII09 - Πολιτική συλλογής, χρήσης, γνωστοποίησης και κοινοποίησης δεδομένων προσωπικού χαρακτήρα

12.9 PII10 - Πολιτική διατήρησης, διαγραφής και διάθεσης δεδομένων προσωπικού χαρακτήρα

12.10 PII11 - Πολιτική ακρίβειας και ποιότητας δεδομένων προσωπικού χαρακτήρα

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

12.12 PII13 - Πολιτική διεθνών μεταφορών δεδομένων προσωπικού χαρακτήρα

12.13 PII14 - Πολιτική ασφάλειας δεδομένων προσωπικού χαρακτήρα 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 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 6.1.2; Clause 6.1.3** - Αντιστοιχίζεται στον έλεγχο κινδύνου ιδιωτικότητας, στη σύνδεση ενεργειών αντιμετώπισης, στην ανάλυση εξαρτήσεων σχεδιασμού, στην κλιμάκωση και στα διορθωτικά μέτρα χωρίς επανάληψη της πλήρους μεθοδολογίας κινδύνου ιδιωτικότητας και DPIA. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.5; 5.1.3; 7.1.7].

13.2.2 **Clause 6.3; Clause 8.1** - Αντιστοιχίζεται σε προγραμματισμένες αλλαγές ιδιωτικότητας, έναρξη έργου, επιχειρησιακή ανασκόπηση σχεδιασμού προστασίας της ιδιωτικότητας, έλεγχο θέσης σε λειτουργία και ανασκόπηση ουσιωδών αλλαγών. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.3; 4.3.5; 4.5.1; 4.5.3; 4.5.4; 4.5.6; 7.1.2; 7.1.5; 10.1.2].

13.2.3 **Clause 7.5** - Αντιστοιχίζεται σε τεκμηριωμένα τεκμήρια σχεδιασμού προστασίας της ιδιωτικότητας που διατηρούνται στα REG02, REG04, REG08 και REG12. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.2; 4.4.3; 5.1.2; 5.1.5; 5.1.6; 5.1.7; 7.1.1; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1; Clause 10.2** - Αντιστοιχίζεται σε μετρικές σχεδιασμού προστασίας της ιδιωτικότητας, δειγματοληψία τεκμηρίων, καταγραφή μη συμμορφώσεων, διορθωτικά μέτρα και επαλήθευση αποτελεσματικότητας. Addressed by clauses [4.3.6; 4.4.5; 4.5.5; 6.1.1; 6.1.2; 6.1.4; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 10.1.1; 10.1.5; 10.1.6].

13.2.5 **Annex A.1.2.2; Annex A.1.2.6; Annex A.1.2.9** - Αντιστοιχίζεται στην τεκμηρίωση σκοπών επεξεργασίας, αρχείων επεξεργασίας, σύνδεσης σχεδιασμού προστασίας της ιδιωτικότητας και εναυσμάτων ελέγχου κινδύνου ιδιωτικότητας ή DPIA για επεξεργασία υπευθύνου επεξεργασίας. Addressed by clauses [4.1.2; 4.2.1; 4.3.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3** - Αντιστοιχίζεται στον περιορισμό συλλογής και επεξεργασίας δεδομένων προσωπικού χαρακτήρα μέσω ελάχιστων απαιτήσεων δεδομένων βάσει σκοπού, προαιρετικής επεξεργασίας με εξ ορισμού απενεργοποίηση και ελάχιστων εξ ορισμού ρυθμίσεων επεξεργασίας. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.5.4; 7.1.5; 11.1.3].

13.2.7 **Annex A.1.4.4; Annex A.1.4.5** - Αντιστοιχίζεται στη δρομολόγηση εξαρτήσεων ακρίβειας, στους στόχους ελαχιστοποίησης, στη σκοπιμότητα αποταυτοποίησης και στα τεκμήρια

σχεδιασμού για την ελαχιστοποίηση ταυτοποιήσιμων δεδομένων προσωπικού χαρακτήρα. Addressed by clauses [4.2.5; 4.2.7; 4.3.2; 4.5.2; 7.1.3; 11.1.2].

13.2.8 **Annex A.1.4.6; Annex A.1.4.7** - Αντιστοιχίζεται στην αναγνώριση στο στάδιο σχεδιασμού της αποταυτοποίησης, της εξάρτησης από διαγραφή, των προσωρινών τεχνουργημάτων δεδομένων προσωπικού χαρακτήρα και της δρομολόγησης σε ελέγχους κύκλου ζωής χωρίς επανάληψη της εκτέλεσης διατήρησης ή διάθεσης. Addressed by clauses [4.2.5; 4.2.6; 4.2.7; 4.3.3; 4.5.4; 7.1.5; 11.1.3].

13.2.9 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7** - Αντιστοιχίζεται σε εντολές πελάτη προς εκτελούντα την επεξεργασία, πληροφορίες υποστήριξης πελάτη, αρχεία σχεδιασμού εκτελούντος την επεξεργασία και αλλαγές σχεδιασμού υπηρεσίας εξουσιοδοτημένες από τον πελάτη. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.6; 5.1.7; 7.1.4; 11.1.4].

13.2.10 **Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4** - Αντιστοιχίζεται σε δυνατότητες σχεδιασμού εκτελούντος την επεξεργασία για προσωρινά αρχεία, εξάρτηση από επιστροφή ή διάθεση και εξάρτηση από έλεγχο διαβίβασης, οι οποίες καταγράφονται ως τεκμήρια σχεδιασμού χωρίς επανάληψη διαδικασιών επιχειρησιακής διαγραφής ή ελέγχων ασφάλειας. Addressed by clauses [4.2.6; 4.2.7; 4.4.3; 4.4.4; 4.4.6; 7.1.4; 7.1.6; 11.1.4].

13.2.11 **Annex A.3.27; Annex A.3.29** - Αντιστοιχίζεται σε απαιτήσεις ιδιωτικότητας στον κύκλο ζωής ανάπτυξης, σε αρχές μηχανικής, σε σημεία ελέγχου προστασίας δεδομένων προσωπικού χαρακτήρα και σε τεκμήρια ρύθμισης ιδιωτικότητας εξ ορισμού. Addressed by clauses [4.1.6; 4.3.3; 4.3.4; 4.4.4; 4.5.1; 4.5.4; 5.1.4; 5.1.6; 7.1.5; 7.1.6; 10.1.2; 11.1.3].

**13.3 GDPR**

13.3.1 **Article 5(1)(b); Article 5(1)(c); Article 5(2)** - Αντιστοιχίζεται στον περιορισμό σκοπού, στον σχεδιασμό ελάχιστων δεδομένων προσωπικού χαρακτήρα, στη σύνδεση αρχείων επεξεργασίας, στην εξ ορισμού ελαχιστοποίηση, στα τεκμήρια και στη λογοδοσία. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.2; 4.5.2; 5.1.5; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Αντιστοιχίζεται σε μέτρα υπευθύνου επεξεργασίας, ανασκόπηση διακυβέρνησης, έγκριση εξαιρέσεων, διορθωτικά μέτρα και συντήρηση πολιτικής για την εφαρμογή προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό. Addressed by clauses [4.1.3; 4.5.6; 5.1.1; 6.1.2; 9.1.2; 9.1.4; 10.1.5; 11.1.6].

13.3.3 **Article 25** - Αντιστοιχίζεται στην έναρξη έργου, στις απαιτήσεις ιδιωτικότητας στο στάδιο σχεδιασμού, στις ρυθμίσεις ιδιωτικότητας εξ ορισμού, στην ελαχιστοποίηση, στους ελέγχους σχεδιασμού προμηθειών, στην ανασκόπηση θέσης σε λειτουργία και στην ανασκόπηση που ενεργοποιείται από αλλαγές. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.5; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 10.1.2].

13.3.4 **Article 28** - Αντιστοιχίζεται σε εντολές εκτελούντος την επεξεργασία, υποστήριξη σχεδιασμού εκτελούντος την επεξεργασία, τεκμήρια σχεδιασμού προστασίας της ιδιωτικότητας προμηθευτή και αλλαγές σχεδιασμού εξουσιοδοτημένες από τον πελάτη. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.5; 4.4.6; 5.1.7; 7.1.4; 10.1.3; 11.1.4].

13.3.5 **Article 30** - Αντιστοιχίζεται στη σύνδεση αρχείων επεξεργασίας, στις επικαιροποιήσεις REG02, στις εξαρτήσεις σχεδιασμού δραστηριοτήτων επεξεργασίας και στα τεκμήρια αρχείων επεξεργασίας. Addressed by clauses [4.1.2; 4.2.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].

13.3.6 **Article 35** - Αντιστοιχίζεται σε εναύσματα ελέγχου κινδύνου ιδιωτικότητας και ελέγχου αναγκαιότητας DPIA στο στάδιο σχεδιασμού, σε συμβουλή υψηλού κινδύνου και σε ελέγχους μετά την υλοποίηση χωρίς επανάληψη της μεθοδολογίας DPIA. Addressed by clauses [4.1.5; 4.3.1; 4.3.6; 5.1.3; 6.1.3; 9.1.3].

**13.4 ISO/IEC 29100:2020**

13.4.1 **Clause 4.7** - Αντιστοιχίζεται στον προσδιορισμό ελέγχων ιδιωτικότητας κατά τη φάση σχεδιασμού, στη σύνδεση με κίνδυνο ιδιωτικότητας και στα τεκμήρια σχεδιασμού για την υλοποίηση ελέγχων. Addressed by clauses [4.1.1; 4.1.3; 4.1.5; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.5.1].

13.4.2 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Αντιστοιχίζεται στον καθορισμό σκοπού, στον περιορισμό συλλογής, στην ελαχιστοποίηση δεδομένων, στον περιορισμό χρήσης και στις εξ ορισμού ρυθμίσεις επεξεργασίας. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.4.2; 4.5.2].

13.4.3 **Clause 5.7; Clause 5.10; Clause 5.12** - Αντιστοιχίζεται στη δρομολόγηση εξαρτήσεων ακρίβειας, στα τεκμήρια λογοδοσίας, στην παρακολούθηση σχεδιασμού προστασίας της ιδιωτικότητας, στον έλεγχο και στα διορθωτικά μέτρα. Addressed by clauses [4.2.7; 4.3.6; 4.5.5; 6.1.1; 6.1.4; 8.1.1; 8.1.2; 10.1.1; 10.1.6].

**13.5 ISO/IEC 29151:2022**

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8** - Αντιστοιχίζεται στη νομιμότητα σκοπού, στον περιορισμό συλλογής, στην ελαχιστοποίηση δεδομένων, στον περιορισμό χρήσης και γνωστοποίησης, στην εξάρτηση από διατήρηση, στη διαχείριση προσωρινών αρχείων και στους ελέγχους σχεδιασμού εξαρτήσεων ακρίβειας. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.4.2; 4.5.2; 4.5.4; 7.1.3; 7.1.5].