

		Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου									
Αριθμός εγγράφου: PII23		Τίτλος εγγράφου: <b>Πολιτική εκτελούντος την επεξεργασία δεδομένων προσωπικού χαρακτήρα σε υπηρεσίες υπολογιστικού νέφους</b>									
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><b>Νομική σημείωση (πνευματικά δικαιώματα και περιορισμοί χρήσης)</b> (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: <a href="mailto:info@clarysec.com">info@clarysec.com</a></p>
--

## Ευθυγραμμισμένη με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο / Κανονιστική απαίτηση	Ρήτρα / Έλεγχος / Άρθρο	Εφαρμοσιμότητα	Τύπος κάλυψης	Σχόλιο
ISO/IEC 27701:2025	Clause 4.1; Clause 6.1.3	Processor	Supporting	Ρόλος PIMS και εφαρμοσιμότητα ελέγχων
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Processor	Primary	Τεκμηριωμένα τεκμήρια εκτελούντος την επεξεργασία σε περιβάλλον υπολογιστικού νέφους και επιχειρησιακός έλεγχος
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Processor	Supporting	Παρακολούθηση, μη συμμόρφωση και διορθωτικά μέτρα
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.5; Annex A.2.2.6; Annex A.2.2.7	Processor	Primary	Συμφωνίες πελατών, εντολές, υποστήριξη και αρχεία
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Υποστήριξη πελατών για υποχρεώσεις έναντι των υποκειμένων των δεδομένων προσωπικού χαρακτήρα
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Primary	Προσωρινά αρχεία, επιστροφή, μεταφορά, διάθεση και έλεγχοι μετάδοσης
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Supporting	Βάση διαβίβασης και τοποθεσίες
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Αρχεία κοινολόγησης και χειρισμός αιτημάτων κοινολόγησης
ISO/IEC 27701:2025	Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9	Processor	Primary	Κοινολόγηση υπεργολάβου επεξεργασίας, ανάθεση και ειδοποίηση αλλαγής
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9; Annex A.3.14; Annex A.3.24; Annex A.3.25	Processor	Supporting	Τεκμήρια πρόσβασης, αρχείων, αντιγράφων ασφαλείας και καταγραφής
GDPR	Article 28	Processor	Primary	Εκτελών την επεξεργασία, υπεργολάβος επεξεργασίας, συνδρομή, έλεγχος, διαγραφή και επιστροφή

GDPR	Article 30	Processor	Supporting	Αρχεία εκτελούντος την επεξεργασία
GDPR	Article 32; Article 33	Processor	Supporting	Ασφάλεια και γνωστοποίηση παραβίασης στον υπεύθυνο επεξεργασίας
GDPR	Article 44	Conditional	Referenced	Δρομολόγηση διεθνών διαβιβάσεων
ISO/IEC 29100:2020	Clause 5.3; Clause 5.5; Clause 5.6	Processor	Supporting	Περιορισμός σκοπού, ελαχιστοποίησης, χρήσης, διατήρησης και κοινολόγησης
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Processor	Supporting	Λογοδοσία, ασφάλεια πληροφοριών και συμμόρφωση
ISO/IEC 29151:2022	Clause 15.1.2; Clause 15.2.2; Clause 15.2.3; Annex A.7; Annex A.7.2	Processor	Supporting	Αξιολόγηση, παρακολούθηση, αλλαγές και έλεγχοι διατήρησης εκτελούντος την επεξεργασία
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 5.19; 5.20; 5.21; 5.22; 5.23	Processor	Supporting	Εφαρμοσιμότητα ελέγχων, επιχειρησιακός έλεγχος και έλεγχοι προμηθευτών/υπολογιστικού νέφους
ISO/IEC 27002:2022	Control 5.19; Control 5.20; Control 5.21; Control 5.22; Control 5.23; Control 8.10; Control 8.15; Control 8.16	Processor	Supporting	Έλεγχοι προμηθευτών, υπολογιστικού νέφους, διαγραφής, καταγραφής και παρακολούθησης
ISO/IEC 27018:2020	Annex A.2.1; Annex A.3.1	Processor	Primary	Υποστήριξη πελατών από εκτελούντα την επεξεργασία σε περιβάλλον υπολογιστικού νέφους και περιορισμός σκοπού
ISO/IEC 27018:2020	Annex A.6.1; Annex A.6.2; Annex A.8.1	Processor	Primary	Ειδοποίηση κοινολόγησης σε περιβάλλον υπολογιστικού νέφους, αρχεία κοινολόγησης και διαφάνεια υπεργολάβων επεξεργασίας
ISO/IEC 27018:2020	Annex A.10.1; Annex A.10.3; Annex A.11.11;	Processor	Primary	Διεπαφή παραβίασης υπολογιστικού νέφους, έξοδος, συμβατικά μέτρα,

	Annex A.11.12; Annex A.12.1			υπεργολαβίες και αρχεία τοποθεσιών
ISO/IEC 27036-2:2022	Clause 6.1.1; Clause 6.1.2	Processor	Supporting	Στρατηγική και διακυβέρνηση σχέσεων προμήθειας
ISO/IEC 27036-2:2022	Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5	Processor	Supporting	Σχεδιασμός, συμφωνία, διαχείριση, παρακολούθηση και τερματισμός σχέσης προμηθευτή
ISO/IEC 27555:2025	Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8	Processor	Supporting	Πλαίσιο διαγραφής και τεκμηρίωση
ISO/IEC 27555:2025	Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7	Processor	Supporting	Υλοποίηση διαγραφής και εξαιρέσεις

## 1. Πεδίο εφαρμογής

1.1 Η παρούσα πολιτική καθορίζει υποχρεωτικές απαιτήσεις ιδιωτικότητας για υπηρεσίες υπολογιστικού νέφους στις οποίες ο οργανισμός ενεργεί ως εκτελών την επεξεργασία ή ως υπεργολάβος επεξεργασίας δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων υπηρεσιών SaaS, PaaS, IaaS, φιλοξενούμενων εφαρμογών, διαχειριζόμενου υπολογιστικού νέφους, υποστήριξης υπολογιστικού νέφους, αποθήκευσης υπολογιστικού νέφους, αναλυτικών υπηρεσιών υπολογιστικού νέφους και υπηρεσιών υποδομής υπολογιστικού νέφους που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για λογαριασμό πελατών.

1.2 Η παρούσα πολιτική εφαρμόζεται στην επεξεργασία σε περιβάλλον υπολογιστικού νέφους που διενεργείται βάσει συμφωνιών πελατών, τεκμηριωμένων εντολών πελάτη, εντολών ανάντη εκτελούντος την επεξεργασία, ρυθμίσεων υπεργολάβου επεξεργασίας, διαμόρφωσης περιοχής υπολογιστικού νέφους, πρόσβασης υποστήριξης υπολογιστικού νέφους, διαχείρισης υπηρεσίας, αντιγράφων ασφαλείας, αναπαραγωγής, καταγραφής, παρακολούθησης, διαγραφής, επιστροφής, υποστήριξης παραβίασης, υποστήριξης ελέγχου και υποχρεώσεων συνδρομής προς πελάτες.

### 1.3 Η παρούσα πολιτική καλύπτει:

1.3.1 το πεδίο επεξεργασίας δεδομένων προσωπικού χαρακτήρα σε περιβάλλον υπολογιστικού νέφους και τα αρχεία εντολών·

1.3.2 τεκμήρια συμφωνιών πελατών και κοινής ευθύνης·

1.3.3 τεκμήρια απομόνωσης μισθωτών, πρόσβασης στο υπολογιστικό νέφος, διαχειριστικής πρόσβασης και καταγραφής·

1.3.4 διακυβέρνηση υπεργολάβων επεξεργασίας και εφοδιαστικής αλυσίδας υπολογιστικού νέφους·

1.3.5 τοποθεσία, απομακρυσμένη πρόσβαση και δρομολόγηση διεθνών διαβιβάσεων·

1.3.6 τεκμήρια επιστροφής, μεταφοράς, διαγραφής, διάθεσης και εξόδου·

1.3.7 συνδρομή προς πελάτες για δικαιώματα υποκειμένων των δεδομένων προσωπικού χαρακτήρα, DPIA, ελέγχους και απόκριση σε παραβιάσεις·

1.3.8 τεκμήρια παρακολούθησης, εξαιρέσεων, εφαρμογής και βελτίωσης.

1.4 Η παρούσα πολιτική δεν δημιουργεί χωριστό μητρώο συμβάσεων πελατών, μητρώο υπηρεσιών υπολογιστικού νέφους, μητρώο απομόνωσης μισθωτών, μητρώο πρόσβασης, μητρώο αρχείων καταγραφής, μητρώο διαγραφής, μητρώο αιτημάτων υποστήριξης, μητρώο ελεγκτικών τεκμηρίων, μητρώο παραβιάσεων, μητρώο υπεργολάβων επεξεργασίας ή επιτροπή διακυβέρνησης υπολογιστικού νέφους.

### 1.5 Η παρούσα πολιτική δεν αντικαθιστά:

1.5.1 την PII03 για το αποθετήριο επεξεργασίας και την κυριότητα νομικής βάσης·

1.5.2 την PII06 για την πλήρη ροή εργασίας δικαιωμάτων υποκειμένων των δεδομένων προσωπικού χαρακτήρα·

1.5.3 την PII07 για τη μεθοδολογία κινδύνου ιδιωτικότητας και DPIA·

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

1.5.5 την PII09 για γενικούς ελέγχους συλλογής, χρήσης, κοινολόγησης και κοινοχρησίας·

1.5.6 την PII10 για τη μεθοδολογία διατήρησης, διαγραφής και διάθεσης·

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

1.5.8 την PII13 για την αξιολόγηση μηχανισμού διεθνούς διαβίβασης·

1.5.9 την PII14 για την πλήρη αρχιτεκτονική ασφάλειας και ελέγχου πρόσβασης δεδομένων προσωπικού χαρακτήρα·

- 1.5.10 την PII15 για τη ροή εργασίας διαχείρισης περιστατικών και παραβιάσεων
- 1.5.11 την PII17 για τον έλεγχο τεκμηριωμένων πληροφοριών
- 1.5.12 την PII18 για τη διακυβέρνηση παρακολούθησης, ελέγχου και βελτίωσης του PIMS.

## **2. Σκοπός**

- 2.1 Σκοπός της παρούσας πολιτικής είναι να διασφαλίσει ότι οι υπηρεσίες εκτελούντος την επεξεργασία και υπεργολάβου επεξεργασίας δεδομένων προσωπικού χαρακτήρα σε περιβάλλον υπολογιστικού νέφους λειτουργούν βάσει τεκμηριωμένων εντολών πελάτη, σαφούς πεδίου επεξεργασίας, ελεγχόμενων ρυθμίσεων υπεργολάβων επεξεργασίας, κατάλληλων ευθυνών ασφάλειας υπολογιστικού νέφους, τεκμηριωμένης τοποθεσίας και δρομολόγησης διαβίβασης, υποχρεώσεων συνδρομής προς πελάτες, υποστήριξης παραβίασης, δυνατότητας διαγραφής/επιστροφής και τεκμηρίων έτοιμων για έλεγχο.
- 2.2 Η παρούσα πολιτική υποστηρίζει την ετοιμότητα για πιστοποίηση PIMS κατά ISO/IEC 27701:2025 για εκτελούντες την επεξεργασία και υπεργολάβους επεξεργασίας σε περιβάλλον υπολογιστικού νέφους, παραμένοντας παράλληλα ενσωματωμένη στο υφιστάμενο σύνολο πολιτικών PIMS και στα κανονικά αντικείμενα τεκμηρίων.

## **3. Στόχοι**

### **3.1 Οι στόχοι της παρούσας πολιτικής είναι να:**

- 3.1.1 Καθορίζει το πεδίο επεξεργασίας δεδομένων προσωπικού χαρακτήρα σε περιβάλλον υπολογιστικού νέφους πριν από την ένταξη πελάτη ή ουσιώδη αλλαγή.
- 3.1.2 Διασφαλίζει ότι οι εντολές πελάτη καταγράφονται, ανασκοπούνται και ακολουθούνται.
- 3.1.3 Διατηρεί τεκμήρια εκτελούντος την επεξεργασία και υπεργολάβου επεξεργασίας σε περιβάλλον υπολογιστικού νέφους στα κανονικά μητρώα PIMS.
- 3.1.4 Καθορίζει τεκμήρια κοινής ευθύνης, απομόνωσης μισθωτών, πρόσβασης, καταγραφής και τοποθεσίας χωρίς να αντιγράφει την πολιτική ασφάλειας δεδομένων προσωπικού χαρακτήρα.
- 3.1.5 Ελέγχει τεκμήρια ένταξης, αλλαγής, μετακυλιόμενων υποχρεώσεων και παρακολούθησης υπεργολάβων επεξεργασίας.
- 3.1.6 Υποστηρίζει πελάτες σε δικαιώματα υποκειμένων των δεδομένων προσωπικού χαρακτήρα, DPIA, αιτήματα ελέγχου και απόκριση σε παραβιάσεις.
- 3.1.7 Διασφαλίζει ότι κατά την έξοδο διατηρούνται τεκμήρια επιστροφής, διαγραφής, μεταφοράς και διάθεσης.
- 3.1.8 Παρακολουθεί τους ελέγχους εκτελούντος την επεξεργασία σε περιβάλλον υπολογιστικού νέφους και προωθεί διορθωτικά μέτρα μέσω του REG12.

## **4. Δηλώσεις πολιτικής**

### **4.1 Πεδίο επεξεργασίας σε περιβάλλον υπολογιστικού νέφους και εντολές πελάτη**

- 4.1.1 [Processor] The Privacy Lead / PIMS Manager MUST καταγράφει κάθε υπηρεσία επεξεργασίας δεδομένων προσωπικού χαρακτήρα σε περιβάλλον υπολογιστικού νέφους, τον ρόλο επεξεργασίας του πελάτη, την πηγή εντολών πελάτη, τις κατηγορίες δεδομένων προσωπικού χαρακτήρα, τις κατηγορίες υποκειμένων των δεδομένων προσωπικού χαρακτήρα, τον σκοπό υπηρεσίας, την τοποθεσία επεξεργασίας, την εξάρτηση από υπεργολάβο επεξεργασίας, την εξάρτηση διαγραφής και τη σημαία διαβίβασης στο REG02 και στο REG08 πριν από την ένταξη πελάτη ή ουσιώδη αλλαγή υπηρεσίας.
- 4.1.2 [Processor] The Process Owner / Business Owner MUST καταγράφει τις τεκμηριωμένες εντολές πελάτη για επεξεργασία δεδομένων προσωπικού χαρακτήρα σε περιβάλλον υπολογιστικού νέφους στο REG08 πριν από την έναρξη της επεξεργασίας.
- 4.1.3 [Subprocessor] The Process Owner / Business Owner MUST καταγράφει τις εντολές ανάντη εκτελούντος την επεξεργασία ή τις εγκεκριμένες από τον πελάτη εντολές στο REG08

πριν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα ως υπεργολάβος επεξεργασίας σε περιβάλλον υπολογιστικού νέφους.

- 4.1.4 [Processor] The Privacy Lead / PIMS Manager MUST καταγράφει την εφαρμοσιμότητα ελέγχων εκτελούντος την επεξεργασία σε περιβάλλον υπολογιστικού νέφους στο REG03 πριν από τη διάθεση ή ουσιώδη αλλαγή νέας υπηρεσίας επεξεργασίας δεδομένων προσωπικού χαρακτήρα σε περιβάλλον υπολογιστικού νέφους.
- 4.1.5 [Processor] The Data Protection Officer / Privacy Advisor MUST ανασκοπεί στο REG12 κάθε εντολή πελάτη που φαίνεται ασύμβατη με τεκμηριωμένες υποχρεώσεις πελάτη, απαιτήσεις PIMS ή εγκεκριμένο πεδίο υπηρεσίας πριν ο οργανισμός ενεργήσει βάσει της εντολής.
- 4.1.6 [Processor] The Process Owner / Business Owner MUST καταγράφει στο REG12 κάθε προτεινόμενη επεξεργασία δεδομένων προσωπικού χαρακτήρα πελάτη εκτός των τεκμηριωμένων εντολών πελάτη και λαμβάνει έγκριση από τον Privacy Lead / PIMS Manager πριν πραγματοποιηθεί η επεξεργασία.

## **4.2 Διαμόρφωση υπολογιστικού νέφους, απομόνωση μισθωτών, πρόσβαση και καταγραφή**

- 4.2.1 [Processor] The Information Security Lead MUST καταγράφει στο REG08 το όριο κοινής ευθύνης υπολογιστικού νέφους για πρόσβαση σε δεδομένα προσωπικού χαρακτήρα, διαχείριση, καταγραφή, αντίγραφα ασφαλείας, κρυπτογράφηση, διαχείριση ευπαθειών και διαγραφή πριν από την ένταξη πελάτη ή ουσιώδη αλλαγή υπηρεσίας.
- 4.2.2 [Processor] The System Owner / Application Owner MUST επικυρώνει στο REG12 τους ελέγχους απομόνωσης μισθωτών ή διαχωρισμού πελατών πριν από τη χρήση σε παραγωγή και μετά από ουσιώδη αλλαγή αρχιτεκτονικής.
- 4.2.3 [Processor] The System Owner / Application Owner MUST χορηγεί διαχειριστική πρόσβαση σε περιβάλλον υπολογιστικού νέφους σε δεδομένα προσωπικού χαρακτήρα πελάτη μόνο αφού καταγραφούν στο REG12 η εγκεκριμένη επιχειρησιακή ανάγκη, το πεδίο πρόσβασης, η διάρκεια πρόσβασης και η συχνότητα ανασκόπησης.
- 4.2.4 [Processor] The Information Security Lead MUST ανασκοπεί στο REG12 την προνομιούχα πρόσβαση σε περιβάλλον υπολογιστικού νέφους, την πρόσβαση υποστήριξης, την πρόσβαση σε δεδομένα προσωπικού χαρακτήρα πελάτη και την κάλυψη καταγραφής τουλάχιστον ανά τρίμηνο.
- 4.2.5 [Processor] The System Owner / Application Owner MUST επικυρώνει στο REG12 τον διαχωρισμό περιβαλλόντων παραγωγής, σταδιοποίησης, δοκιμών και υποστήριξης για δεδομένα προσωπικού χαρακτήρα πελάτη πριν από τη διάθεση και μετά από ουσιώδη αλλαγή περιβάλλοντος.
- 4.2.6 [Processor] The System Owner / Application Owner MUST καταγράφει τις τοποθεσίες αντιγράφων ασφαλείας, αναπαραγωγής, αποθήκευσης αρχείων καταγραφής και πρόσβασης υποστήριξης για δεδομένα προσωπικού χαρακτήρα πελατών σε περιβάλλον υπολογιστικού νέφους στο REG02, REG08 ή REG09 πριν από την ενεργοποίηση ή αλλαγή αυτών των τοποθεσιών.

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

## **9. Εξαιρέσεις**

- 9.1 [Processor] The Process Owner / Business Owner MUST ζητά εξαιρέση εκτελούντος την επεξεργασία σε περιβάλλον υπολογιστικού νέφους στο REG12 πριν από την ένταξη, διάθεση, ανανέωση ή συνεχιζόμενη χρήση όταν τα απαιτούμενα τεκμήρια εντολών πελάτη, υπεργολάβου επεξεργασίας, τοποθεσίας, πρόσβασης, καταγραφής, διαγραφής ή διεπαφής περιστατικών είναι ελλιπή.

- 9.2 [Processor] The Data Protection Officer / Privacy Advisor MUST ανασκοπεί στο REG12 αιτήματα εξαίρεσης εκτελούντος την επεξεργασία σε περιβάλλον υπολογιστικού νέφους που είναι σημαντικά για την ιδιωτικότητα πριν από την έγκριση, όταν η εξαίρεση επηρεάζει εντολές πελάτη, συνδρομή προς υποκείμενα των δεδομένων προσωπικού χαρακτήρα, διαβιβάσεις, υπερβολάβους επεξεργασίας, διαγραφή, υποστήριξη παραβίασης ή δεδομένα προσωπικού χαρακτήρα υψηλού αντικτύπου.
- 9.3 [Processor] Top Management MUST εγκρίνει εξαιρέσεις εκτελούντος την επεξεργασία σε περιβάλλον υπολογιστικού νέφους υψηλού κινδύνου ή ουσιώδεις εξαιρέσεις στο REG12 πριν η εξαίρεση τεθεί σε ισχύ.
- 9.4 [Processor] The Privacy Lead / PIMS Manager MUST αναθέτει ημερομηνία λήξης, ιδιοκτήτη αποκατάστασης, ημερομηνία ανασκόπησης και σημείωση υπολειπόμενου κινδύνου στο REG12 για κάθε εγκεκριμένη εξαίρεση εκτελούντος την επεξεργασία σε περιβάλλον υπολογιστικού νέφους πριν από την έγκριση.

## 10. Εφαρμογή

- 10.1 [Processor] The Privacy Lead / PIMS Manager MUST αποκλείει την ένταξη πελάτη, τη διάθεση υπηρεσίας, την ανανέωση ή τη συνεχιζόμενη επεξεργασία όταν λείπουν τα απαιτούμενα τεκμήρια REG02, REG03, REG08, REG09, REG10 ή REG12 πριν αρχίσει ή συνεχιστεί η επεξεργασία.
- 10.2 [Processor] The System Owner / Application Owner MUST απενεργοποιεί μη εγκεκριμένη πρόσβαση σε περιβάλλον υπολογιστικού νέφους, μη εγκεκριμένη χρήση περιοχής, μη εγκεκριμένη αναπαραγωγή, μη εγκεκριμένη πρόσβαση υποστήριξης ή μη εγκεκριμένη ροή δεδομένων υπερβολάβου επεξεργασίας εντός μίας εργάσιμης ημέρας από απόφαση εφαρμογής και καταγράφει την ολοκλήρωση στο REG08 ή στο REG12.
- 10.3 [Processor] The Vendor / Procurement Owner MUST αναστέλλει νέα επεξεργασία δεδομένων προσωπικού χαρακτήρα από μη εγκεκριμένο ή μη συμμορφούμενο υπερβολάβο επεξεργασίας σε περιβάλλον υπολογιστικού νέφους έως ότου ολοκληρωθούν τα τεκμήρια διορθωτικών ενεργειών στο REG08.
- 10.4 [Processor] The Incident Response Coordinator MUST κλιμακώνει μη τηρηθείσες προθεσμίες ειδοποίησης περιστατικών πελάτη στο REG10 και στο REG12 εντός μίας εργάσιμης ημέρας από την αναγνώριση.
- 10.5 [Processor] The Internal Audit / Compliance Reviewer MUST επαληθεύει την αποτελεσματικότητα διορθωτικών ενεργειών για μείζονες ή επαναλαμβανόμενες μη συμμορφώσεις εκτελούντος την επεξεργασία σε περιβάλλον υπολογιστικού νέφους στο REG12 εντός 60 ημερών από το κλείσιμο της διορθωτικής ενέργειας.

## 11. Ανασκόπηση και συντήρηση

- 11.1 [Processor] The Privacy Lead / PIMS Manager MUST ανασκοπεί την παρούσα πολιτική στο REG12 ετησίως και εντός 30 ημερών από ουσιώδη αλλαγή στις υποχρεώσεις εκτελούντος την επεξεργασία σε περιβάλλον υπολογιστικού νέφους, στην αρχιτεκτονική υπολογιστικού νέφους, στη διακυβέρνηση υπερβολάβων επεξεργασίας, στη συνδρομή προς πελάτες, στη δυνατότητα διαγραφής ή στις απαιτήσεις πιστοποίησης.
- 11.2 [Processor] The Vendor / Procurement Owner MUST ανασκοπεί τα αρχεία υπερβολάβων επεξεργασίας σε περιβάλλον υπολογιστικού νέφους και εξαρτήσεων υπηρεσιών υπολογιστικού νέφους στο REG08 τουλάχιστον ετησίως και πριν από την ανανέωση.
- 11.3 [Processor] The System Owner / Application Owner MUST ανασκοπεί τεκμήρια απομόνωσης μισθωτών, προνομιάς πρόσβασης, καταγραφής, αντιγράφων ασφαλείας, αναπαραγωγής και διαγραφής στο REG12 τουλάχιστον ετησίως και μετά από ουσιώδη αλλαγή αρχιτεκτονικής.

- 11.4 [Processor] The Privacy Lead / PIMS Manager MUST ανασκοπεί τα αρχεία τοποθεσίας υπολογιστικού νέφους και δρομολόγησης διαβίβασης REG09 τουλάχιστον ετησίως και εντός 15 εργάσιμων ημερών από ουσιώδη αλλαγή τοποθεσίας, πρόσβασης υποστήριξης, αντιγράφων ασφαλείας ή υπεργολάβου επεξεργασίας.
- 11.5 [Processor] The Privacy Lead / PIMS Manager MUST επικαιροποιεί το REG03 εντός 15 εργάσιμων ημερών από εγκεκριμένες αλλαγές πολιτικής που επηρεάζουν την εφαρμοσιμότητα ελέγχων εκτελούντος την επεξεργασία σε περιβάλλον υπολογιστικού νέφους.
- 11.6 [All] Top Management MUST εγκρίνει ουσιώδεις αναθεωρήσεις της παρούσας πολιτικής στο REG12 πριν από τη δημοσίευση.

## 12. Συναφείς πολιτικές

- 12.1 Η παρούσα πολιτική υποστηρίζεται από τις ακόλουθες συναφείς πολιτικές:
- 12.2 PII01 - Πολιτική Συστήματος Διαχείρισης Πληροφοριών Ιδιωτικότητας
- 12.3 PII02 - Πολιτική ρόλων, αρμοδιοτήτων και λογοδοσίας ιδιωτικότητας
- 12.4 PII03 - Πολιτική αποθετηρίου επεξεργασίας δεδομένων προσωπικού χαρακτήρα και νομικής βάσης
- 12.5 PII06 - Πολιτική διαχείρισης δικαιωμάτων υποκειμένων των δεδομένων προσωπικού χαρακτήρα
- 12.6 PII07 - Πολιτική αξιολόγησης κινδύνου ιδιωτικότητας και DPIA
- 12.7 PII08 - Πολιτική προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό και εξ ορισμού
- 12.8 PII09 - Πολιτική συλλογής, χρήσης, κοινολόγησης και κοινοχρησίας δεδομένων προσωπικού χαρακτήρα
- 12.9 PII10 - Πολιτική διατήρησης, διαγραφής και διάθεσης δεδομένων προσωπικού χαρακτήρα
- 12.10 PII12 - Πολιτική διαχείρισης ιδιωτικότητας εκτελούντων την επεξεργασία, υπεργολάβων επεξεργασίας και τρίτων μερών
- 12.11 PII13 - Πολιτική διεθνούς διαβίβασης δεδομένων προσωπικού χαρακτήρα
- 12.12 PII14 - Πολιτική ασφάλειας και ελέγχου πρόσβασης δεδομένων προσωπικού χαρακτήρα
- 12.13 PII15 - Πολιτική διαχείρισης περιστατικών και παραβιάσεων δεδομένων προσωπικού χαρακτήρα
- 12.14 PII17 - Πολιτική τεκμηριωμένων πληροφοριών και διαχείρισης τεκμηρίων PIMS
- 12.15 PII18 - Πολιτική παρακολούθησης, ελέγχου και βελτίωσης PIMS
- 12.16 PII20 - Πολιτική ιδιωτικότητας παιδιών
- 12.17 PII21 - Πολιτική ιδιωτικότητας για AI και αυτοματοποιημένη λήψη αποφάσεων
- 12.18 PII22 - Πολιτική ιδιωτικότητας μάρκετινγκ και cookies
- 12.19 PII24 - Πολιτική ιδιωτικότητας CCTV και φυσικής παρακολούθησης

## 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 - Clause 4.1; Clause 6.1.3. Addressed by clauses [4.1.1; 4.1.4; 5.2; 7.1; 11.5].
- 13.3 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.3.1; 4.4.1; 4.6.1; 4.7.1; 4.8.1; 7.1; 7.2; 7.3].
- 13.4 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.3.5; 4.6.6; 4.8.1; 4.8.2; 4.8.4; 6.1; 6.2; 8.1; 8.2; 8.3; 8.4; 8.5; 10.5; 11.1].

- 13.5 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.5; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.2; 4.1.3; 4.1.5; 4.1.6; 4.3.1; 4.7.5; 7.2].
- 13.6 ISO/IEC 27701:2025 - Annex A.2.3.2. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5].
- 13.7 ISO/IEC 27701:2025 - Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].
- 13.8 ISO/IEC 27701:2025 - Annex A.2.5.2; Annex A.2.5.3. Addressed by clauses [4.2.6; 4.4.4; 4.5.1; 4.5.2; 7.5; 11.4].
- 13.9 ISO/IEC 27701:2025 - Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.5.3; 4.5.4; 4.7.2; 4.7.5].
- 13.10 ISO/IEC 27701:2025 - Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6].
- 13.11 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9; Annex A.3.14; Annex A.3.24; Annex A.3.25. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.7.3; 5.4; 5.6; 11.3].
- 13.12 GDPR - Article 28. Addressed by clauses [4.1.2; 4.1.3; 4.3.1; 4.3.2; 4.3.4; 4.4.2; 4.4.3; 4.4.5; 4.6.1; 4.6.3; 4.6.5; 4.7.2].
- 13.13 GDPR - Article 30. Addressed by clauses [4.1.1; 4.1.3; 4.4.1; 4.8.1; 7.1].
- 13.14 GDPR - Article 32; Article 33. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 7.6].
- 13.15 GDPR - Article 44. Addressed by clauses [4.2.6; 4.4.4; 4.5.1; 4.5.2; 7.5; 11.4].
- 13.16 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.1.6; 4.2.6; 4.5.1; 4.6.1; 4.6.3].
- 13.17 ISO/IEC 29100:2020 - Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.4; 4.3.5; 4.8.1; 4.8.4; 6.1; 8.5; 10.5].
- 13.18 ISO/IEC 29151:2022 - Clause 15.1.2; Clause 15.2.2; Clause 15.2.3; Annex A.7; Annex A.7.2. Addressed by clauses [4.4.1; 4.4.6; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.8.3].
- 13.19 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 5.19; 5.20; 5.21; 5.22; 5.23. Addressed by clauses [4.1.4; 4.2.1; 4.4.1; 4.4.3; 4.4.6; 4.8.1; 4.8.3; 6.1; 7.1; 11.5].
- 13.20 ISO/IEC 27002:2022 - Control 5.19; Control 5.20; Control 5.21; Control 5.22; Control 5.23; Control 8.10; Control 8.15; Control 8.16. Addressed by clauses [4.2.1; 4.2.4; 4.4.1; 4.4.3; 4.4.6; 4.6.1; 4.6.3; 4.7.3; 4.8.3; 11.3].
- 13.21 ISO/IEC 27018:2020 - Annex A.2.1; Annex A.3.1. Addressed by clauses [4.1.2; 4.1.6; 4.3.1; 4.3.2; 4.3.3; 4.3.5].
- 13.22 ISO/IEC 27018:2020 - Annex A.6.1; Annex A.6.2; Annex A.8.1. Addressed by clauses [4.4.1; 4.4.2; 4.4.5; 4.5.3; 4.5.4].
- 13.23 ISO/IEC 27018:2020 - Annex A.10.1; Annex A.10.3; Annex A.11.11; Annex A.11.12; Annex A.12.1. Addressed by clauses [4.2.6; 4.4.3; 4.4.4; 4.6.1; 4.6.3; 4.6.5; 4.7.1; 4.7.2; 4.7.5].
- 13.24 ISO/IEC 27036-2:2022 - Clause 6.1.1; Clause 6.1.2. Addressed by clauses [4.1.1; 4.2.1; 4.4.1; 4.4.6; 6.1; 7.2].
- 13.25 ISO/IEC 27036-2:2022 - Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.4.6; 4.8.2; 4.8.3; 10.3; 11.2].
- 13.26 ISO/IEC 27555:2025 - Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].
- 13.27 ISO/IEC 27555:2025 - Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7. Addressed by clauses [4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6; 9.1; 9.4].

