					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: PII24					Τίτλος εγγράφου: **Πολιτική ιδιωτικότητας για CCTV και παρακολούθηση φυσικών χώρων**							
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**

Ευθυγραμμισμένη με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο / Κανονισμός	Ρήτρα / Έλεγχος / Άρθρο	Εφαρμοσιμότητα	Τύπος κάλυψης	Σχόλιο
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Τεκμηριωμένοι και λειτουργικοί έλεγχοι
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Παρακολούθηση και διορθωτική ενέργεια
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9	Controller	Primary	Σκοπός, νομική βάση, έναυσμα κινδύνου και αρχεία
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Κατανομή σε εκτελούντα την επεξεργασία και σε από κοινού υπεύθυνους επεξεργασίας
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10	Controller	Supporting	Υποχρεώσεις και αιτήματα των υποκειμένων των δεδομένων προσωπικού χαρακτήρα
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	Συλλογή, επεξεργασία, ελαχιστοποίηση, διατήρηση και διάθεση
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Αρχεία κοινολογήσεων και αιτήματα
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Συμφωνίες εκτελούντων την επεξεργασία, εντολές, υποστήριξη και αρχεία
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Δικαιώματα εκτελούντος την επεξεργασία και υποστήριξη κοινολογήσεων
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Προστασία αρχείων και καταγραφή
GDPR	Article 5(1)(a); Article 5(1)(b);	Controller	Primary	Αρχές και λογοδοσία

	Article 5(1)(c); Article 5(1)(e); Article 5(2)			
GDPR	Article 6	Controller	Primary	Νομική βάση
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Διαφάνεια και ειδοποιήσεις
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21	Controller	Supporting	Αιτήματα άσκησης δικαιωμάτων
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Διακυβέρνηση, 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, 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 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Κίνδυνος ιδιωτικότητας και εναύσματα DPIA
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Έλεγχοι ιδιωτικότητας για την προστασία PII
ISO/IEC 29151:2022	Clause 9.2.3; Clause 9.4.2; Clause 11.1.3	Both	Supporting	Έλεγχοι πρόσβασης και φυσικής εισόδου
ISO/IEC 27002:2022	Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15	Both	Supporting	PII, παρακολούθηση φυσικών χώρων, περιορισμός πρόσβασης και καταγραφή

1. Πεδίο εφαρμογής

1.1 Η παρούσα πολιτική εφαρμόζεται σε CCTV, βιντεοπαρακολούθηση, παρακολούθηση επισκεπτών, αρχεία καταγραφής ελέγχου φυσικής πρόσβασης, αρχεία παρακολούθησης που τηρούνται από φύλακες, συστήματα παρακολούθησης εγκαταστάσεων και συναφείς δραστηριότητες παρακολούθησης φυσικών χώρων που συλλέγουν ή επεξεργάζονται με άλλον τρόπο PII.

1.2 Η παρούσα πολιτική εφαρμόζεται σε οργανισμούς που ενεργούν ως υπεύθυνοι επεξεργασίας PII για τις δικές τους εγκαταστάσεις και δραστηριότητες παρακολούθησης φυσικών χώρων.

1.3 Η παρούσα πολιτική εφαρμόζεται επίσης σε δραστηριότητες υποστήριξης από εκτελούντα την επεξεργασία ή υπεργολάβο επεξεργασίας, όταν ο οργανισμός λειτουργεί, φιλοξενεί, ανασκοπεί, αποθηκεύει, κοινολογεί, διαγράφει ή επεξεργάζεται με άλλον τρόπο υλικό βιντεοεπιτήρησης, δεδομένα επισκεπτών ή αρχεία καταγραφής φυσικής πρόσβασης για λογαριασμό πελάτη.

1.4 Η παρούσα πολιτική καλύπτει τον καθορισμό σκοπού παρακολούθησης, την έγκριση, τις ειδοποιήσεις και τη σήμανση, τους περιορισμούς πρόσβασης, την κοινολόγηση, τη διατήρηση, τη διαγραφή, την εξωτερική ανάθεση, την κλιμάκωση περιστατικών, τη δρομολόγηση αιτημάτων άσκησης δικαιωμάτων, την ανασκόπηση και τη διαχείριση τεκμηρίων.

1.5 Η παρούσα πολιτική δεν παρέχει συμβουλές εργατικού δικαίου, νομικό σχολιασμό σχετικά με συμβούλια εργαζομένων, διαδικασίες επιβολής του νόμου ή ειδικό μητρώο CCTV.

1.6 Τα ειδικά τεκμήρια παρακολούθησης τηρούνται στα κανονικά αντικείμενα τεκμηρίων PIMS που προσδιορίζονται στην παρούσα πολιτική.

2. Σκοπός

2.1 Σκοπός της παρούσας πολιτικής είναι η θέσπιση ελέγχων ιδιωτικότητας για CCTV και παρακολούθηση φυσικών χώρων, ώστε οι δραστηριότητες παρακολούθησης να έχουν καθορισμένο σκοπό, να είναι διαφανείς, αναλογικές, ελεγχόμενες ως προς την πρόσβαση, να διατηρούνται για καθορισμένα χρονικά διαστήματα, να κοινολογούνται μόνο μέσω εγκεκριμένων διαύλων και να υποστηρίζονται από ελέγξιμα τεκμήρια PIMS.

2.2 Η παρούσα πολιτική υποστηρίζει τη συνεπή διαχείριση υλικού βιντεοεπιτήρησης, αρχείων επισκεπτών, αρχείων καταγραφής φυσικής πρόσβασης και συναφών PII παρακολούθησης, χωρίς να δημιουργεί πρόσθετα μητρώα, επιτροπές, πίνακες ελέγχου ή μη κανονικούς ρόλους.

3. Στόχοι

3.1 Οι στόχοι της παρούσας πολιτικής είναι να:

3.1.1 καθορίζει τους σκοπούς παρακολούθησης και το πεδίο επεξεργασίας πριν από την έναρξη της παρακολούθησης·

3.1.2 τεκμηριώνει τις δραστηριότητες CCTV, φυσικής πρόσβασης, παρακολούθησης επισκεπτών και παρακολούθησης φυσικών χώρων στο REG02·

3.1.3 εντοπίζει δραστηριότητες παρακολούθησης που απαιτούν ανασκόπηση κινδύνου ιδιωτικότητας ή έλεγχο αναγκαιότητας DPIA στο REG04·

3.1.4 τηρεί τεκμήρια διαφανούς ειδοποίησης και σήμανσης στο REG07·

3.1.5 περιορίζει την πρόσβαση, την προβολή, την εξαγωγή, την κοινολόγηση και τη διατήρηση των PII παρακολούθησης·

3.1.6 δρομολογεί αιτήματα υποκειμένων των δεδομένων προσωπικού χαρακτήρα μέσω του REG06·

3.1.7 διαχειρίζεται τους εξωτερικούς παρόχους παρακολούθησης και τα τεκμήρια κοινοχρησίας δεδομένων μέσω του REG08·

3.1.8 κλιμακώνει ύποπτα περιστατικά PII που σχετίζονται με παρακολούθηση μέσω του REG10·

3.1.9 καταγράφει ανασκοπήσεις, εξαιρέσεις, μη συμμορφώσεις, διορθωτικές ενέργειες, ευρήματα ελέγχου και βελτιώσεις στο REG12.

4. Δηλώσεις πολιτικής

4.1 Απογραφή, σκοπός και έγκριση παρακολούθησης

4.1.1 [Controller] Το Process Owner / Business Owner πρέπει να καταγράφει κάθε δραστηριότητα CCTV, παρακολούθησης επισκεπτών, αρχείου καταγραφής ελέγχου φυσικής πρόσβασης ή παρακολούθησης φυσικών χώρων στο REG02 πριν από την έναρξη της δραστηριότητας.

4.1.2 [Controller] Το Privacy Lead / PIMS Manager πρέπει να επικυρώνει την καταχώριση REG02 ως προς τον σκοπό, τη νομική βάση, την παρακολουθούμενη τοποθεσία, τις κατηγορίες PII, τις κατηγορίες υποκειμένων των δεδομένων προσωπικού χαρακτήρα, τη διατήρηση, την ειδοποίηση, την πρόσβαση και τα πεδία κοινολόγησης πριν από την ενεργοποίηση νέας ή ουσιωδώς τροποποιημένης δραστηριότητας παρακολούθησης.

4.1.3 [Controller] Το Process Owner / Business Owner πρέπει να καταγράφει στο REG02 τις εγκεκριμένες παρακολουθούμενες ζώνες, τις εξαιρούμενες ζώνες και τα όρια συλλογής πριν ενεργοποιηθούν κάμερες, αισθητήρες, αρχεία επισκεπτών ή καταγραφή ελέγχου πρόσβασης.

4.1.4 [Conditional] Το Process Owner / Business Owner πρέπει να λαμβάνει απόφαση κινδύνου ιδιωτικότητας στο REG04 πριν ενεργοποιήσει παρακολούθηση που περιλαμβάνει συστηματική παρακολούθηση, ηχογράφηση, βιομετρική ταυτοποίηση, ανίχνευση με ενεργοποιημένη ανάλυση, ευαίσθητες τοποθεσίες, ευάλωτα άτομα ή μη εμφανή παρακολούθηση.

4.1.5 [Joint Controller] Το Privacy Lead / PIMS Manager πρέπει να καταγράφει την κατανομή ευθυνών για κοινή παρακολούθηση στο REG08 πριν από την έναρξη κοινής παρακολούθησης με εκμισθωτή, συνεργάτη εγκαταστάσεων, πελάτη ή άλλο από κοινού υπεύθυνο επεξεργασίας.

4.1.6 [Processor] Το Privacy Lead / PIMS Manager πρέπει να καταγράφει τις εντολές πελάτη για παρακολούθηση και τα επιτρεπόμενα όρια επεξεργασίας στο REG08 πριν από την επεξεργασία υλικού βιντεοεπιτήρησης, αρχείων επισκεπτών ή αρχείων καταγραφής φυσικής πρόσβασης για λογαριασμό πελάτη.

4.2 Ειδοποίηση και διαφάνεια

4.2.1 [Controller] Το Process Owner / Business Owner πρέπει να διασφαλίζει ότι τα τεκμήρια σήμανσης παρακολούθησης ή ισοδύναμης ειδοποίησης just-in-time καταγράφονται στο REG07 πριν οι παρακολουθούμενοι χώροι ανοίξουν σε υποκείμενα των δεδομένων προσωπικού χαρακτήρα.

4.2.2 [Controller] Το Privacy Lead / PIMS Manager πρέπει να συνδέει κάθε ειδοποίηση παρακολούθησης στο REG07 με τον αντίστοιχο σκοπό επεξεργασίας REG02 πριν από τη δημοσίευση ή την ουσιώδη αλλαγή.

4.2.3 [Processor] Το Privacy Lead / PIMS Manager πρέπει να παρέχει πληροφορίες υποστήριξης ειδοποιήσεων σχετικά με την παρακολούθηση στο REG08, όταν ο οργανισμός λειτουργεί υπηρεσίες παρακολούθησης βάσει εντολών πελάτη.

4.2.4 [Conditional] Το Process Owner / Business Owner πρέπει να καταγράφει εναλλακτικά μέτρα διαφάνειας στο REG07 και στο REG04 πριν ενεργοποιηθεί μη εμφανής ή επείγουσα παρακολούθηση.

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

9. Εξαιρέσεις

9.1 [All] Το Privacy Lead / PIMS Manager πρέπει να καταγράφει κάθε εξαίρεση από την παρούσα πολιτική στο REG12 πριν από τη χρήση της εξαίρεσης.

9.2 [Conditional] Το Data Protection Officer / Privacy Advisor πρέπει να τεκμηριώνει συμβουλές ιδιωτικότητας στο REG04 ή στο REG12 πριν από την έγκριση εξαιρέσεων που αφορούν μη εμφανή

παρακολούθηση, ηχογράφηση, βιομετρική ταυτοποίηση, παρακολούθηση με ενεργοποιημένη ανάλυση ή ευαίσθητες τοποθεσίες παρακολούθησης.

9.3 [All] To Top Management πρέπει να εγκρίνει στο REG12 εξαιρέσεις που υπερβαίνουν τις 90 ημέρες πριν από την παράταση πέραν της αρχικής περιόδου εξαίρεσης.

9.4 [All] To Privacy Lead / PIMS Manager πρέπει να ανασκοπεί ανοικτές εξαιρέσεις παρακολούθησης στο REG12 τουλάχιστον μηνιαίως έως το κλείσιμο.

10. Εφαρμογή

10.1 [All] To Privacy Lead / PIMS Manager πρέπει να καταγράφει αστοχίες ελέγχων παρακολούθησης ως μη συμμορφώσεις στο REG12 εντός πέντε εργάσιμων ημερών από την επιβεβαίωση.

10.2 [Both] To Information Security Lead πρέπει να αναστέλλει μη εξουσιοδοτημένη πρόσβαση σε σύστημα παρακολούθησης εντός μίας εργάσιμης ημέρας από την επιβεβαίωση και να καταγράφει την ενέργεια στο REG10 ή στο REG12.

10.3 [All] To Top Management πρέπει να αναθέτει την ευθύνη διορθωτικής ενέργειας στο REG12 εντός 10 εργάσιμων ημερών για επαναλαμβανόμενες ή ουσιώδεις παραβιάσεις πολιτικής.

10.4 [Conditional] To Incident Response Coordinator πρέπει να εκκινεί τη ροή εργασίας περιστατικών PII στο REG10 σε περίπτωση ύποπτης μη εξουσιοδοτημένης κοινολόγησης, απώλειας ή διακύβευσης PII παρακολούθησης.

11. Ανασκόπηση και συντήρηση

11.1 [All] To Privacy Lead / PIMS Manager πρέπει να ανασκοπεί την παρούσα πολιτική και τα σχετικά τεκμήρια παρακολούθησης στο REG12 τουλάχιστον ετησίως.

11.2 [Controller] To Process Owner / Business Owner πρέπει να επανεπικυρώνει κάθε ενεργό σκοπό παρακολούθησης, ειδοποίηση, πεδίο τοποθεσίας και καταχώριση διατήρησης στα REG02 και REG07 τουλάχιστον ετησίως.

11.3 [Both] To System Owner / Application Owner πρέπει να επανεπικυρώνει τους ελέγχους πρόσβασης, καταγραφής, διαγραφής και εξαγωγής του συστήματος παρακολούθησης στο REG12 τουλάχιστον ετησίως και μετά από ουσιώδη αλλαγή συστήματος.

11.4 [Conditional] To Vendor / Procurement Owner πρέπει να επανεπικυρώνει τα τεκμήρια εξωτερικά ανατεθειμένων παρόχων παρακολούθησης στο REG08 τουλάχιστον ετησίως και πριν από την ανανέωση σύμβασης.

11.5 [All] To Privacy Lead / PIMS Manager πρέπει να επικαιροποιεί τα σχετικά τεκμήρια REG02, REG04, REG07, REG08, REG10 ή REG12 εντός 30 ημερολογιακών ημερών μετά από εγκεκριμένες αλλαγές πολιτικής.

12. Συναφείς πολιτικές

12.1 PII02 - Πολιτική ρόλων, αρμοδιοτήτων και λογοδοσίας για την ιδιωτικότητα

12.2 PII03 - Πολιτική απογραφής επεξεργασίας PII και νομικής βάσης

12.3 PII04 - Πολιτική ειδοποιήσεων ιδιωτικότητας και διαφάνειας

12.4 PII06 - Πολιτική διαχείρισης δικαιωμάτων υποκειμένων των δεδομένων προσωπικού χαρακτήρα

12.5 PII07 - Πολιτική αξιολόγησης κινδύνου ιδιωτικότητας και DPIA

12.6 PII08 - Πολιτική προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό και εξ ορισμού

12.7 PII09 - Πολιτική συλλογής, χρήσης, κοινολόγησης και κοινοχρησίας PII

12.8 PII10 - Πολιτική διατήρησης, διαγραφής και διάθεσης PII

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

12.10 PII13 - Πολιτική διεθνών διαβιβάσεων PII

12.11 PII14 - Πολιτική ασφάλειας PII και ελέγχου πρόσβασης

12.12 PII15 - Πολιτική διαχείρισης περιστατικών και παραβιάσεων PII

12.13 PII17 - Πολιτική τεκμηριωμένων πληροφοριών και διαχείρισης τεκμηρίων PIMS

12.14 PII18 - Πολιτική παρακολούθησης, ελέγχου και βελτίωσης PIMS

12.15 PII19 - Πολιτική ιδιωτικότητας εργαζομένων

12.16 PII21 - Πολιτική ιδιωτικότητας για τεχνητή νοημοσύνη και αυτοματοποιημένη λήψη αποφάσεων

12.17 PII23 - Πολιτική εκτελούντος την επεξεργασία PII σε υπηρεσίες νέφους

13. Πρότυπα και πλαίσια αναφοράς

13.1 Η παρούσα πολιτική έχει αντιστοιχιστεί στα ακόλουθα πρότυπα και κανονιστικές απαιτήσεις.

13.2 Η αντιστοίχιση εξηγεί πώς η πολιτική υποστηρίζει τις αναφερόμενες απαιτήσεις και προσδιορίζει τις εσωτερικές ρήτρες που τις υλοποιούν ή τις υποστηρίζουν.

13.3 ISO/IEC 27701:2025

13.3.1 **Clause 7.5; Clause 8.1** - Αντιστοιχίζεται σε τεκμήρια παρακολούθησης, επιχειρησιακό σχεδιασμό, ελέγχους ενεργοποίησης, αρχεία σκοπού, σύνδεση ειδοποιήσεων, διαμόρφωση πρόσβασης, διαμόρφωση διατήρησης και έλεγχο αλλαγών για δραστηριότητες CCTV και παρακολούθησης φυσικών χώρων. Addressed by clauses [4.1.1; 4.1.2; 4.2.2; 4.3.1; 4.4.1; 6.2; 7.1; 11.5].

13.3.2 **Clause 9.1; Clause 10.2** - Αντιστοιχίζεται στη μέτρηση ελέγχων παρακολούθησης, την ανασκόπηση παρόχων, την ανασκόπηση πρόσβασης, τα ευρήματα ελέγχου, τις μη συμμορφώσεις, τις διορθωτικές ενέργειες, την κλιμάκωση εκπρόθεσμων ενεργειών και τα τεκμήρια βελτίωσης. Addressed by clauses [4.6.4; 6.4; 6.5; 6.6; 8.1; 8.7; 10.1; 11.1].

13.3.3 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9** - Αντιστοιχίζεται στον καθορισμό σκοπού παρακολούθησης από τον υπεύθυνο επεξεργασίας, την τεκμηρίωση νομικής βάσης, τις αποφάσεις για εναύσματα κινδύνου ιδιωτικότητας και τα αρχεία δραστηριοτήτων επεξεργασίας παρακολούθησης στα REG02 και REG04. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.4.1; 6.2; 7.1; 11.2].

13.3.4 **Annex A.1.2.7; Annex A.1.2.8** - Αντιστοιχίζεται στην κατανομή εξωτερικά ανατεθειμένων παρόχων παρακολούθησης, την κατανομή ευθυνών κοινής παρακολούθησης και τα τεκμήρια εκτελούντος την επεξεργασία ή από κοινού υπεύθυνου επεξεργασίας στο REG08. Addressed by clauses [4.1.5; 4.6.1; 4.6.2; 5.7; 6.2; 7.6].

13.3.5 **Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10** - Αντιστοιχίζεται στις υποχρεώσεις έναντι υποκειμένων των δεδομένων προσωπικού χαρακτήρα που σχετίζονται με παρακολούθηση, στη δρομολόγηση αιτημάτων, στη διαφύλαξη που απαιτείται για την αξιολόγηση αιτημάτων και στα τεκμήρια διακυβέρνησης για την υποστήριξη δικαιωμάτων. Addressed by clauses [4.5.1; 4.5.2; 5.2; 7.2; 11.5].

13.3.6 **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 στον περιορισμό συλλογής παρακολούθησης, στα όρια επεξεργασίας, στην ελαχιστοποίηση, στις περιόδους διατήρησης, στη διαγραφή, στην αντικατάσταση, στις δεσμεύσεις διατήρησης και στον έλεγχο εξαχθέντων αντιγράφων. Addressed by clauses [4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 7.3; 7.5; 8.4].

13.3.7 **Annex A.1.5.4; Annex A.1.5.5** - Αντιστοιχίζεται σε αρχεία εξωτερικής κοινολόγησης, διαχείριση αιτημάτων κοινολόγησης, ελαχιστοποίηση πριν από κοινολόγηση και κοινολογήσεις

που συνδέονται με περιστατικά και αφορούν PII παρακολούθησης. Addressed by clauses [4.3.4; 4.5.4; 7.8; 10.4].

13.3.8 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7** - Αντιστοιχίζεται σε εντολές πελάτη προς τον εκτελούντα την επεξεργασία, επιτρεπόμενα όρια επεξεργασίας, υποστήριξη ειδοποιήσεων, εντολές διατήρησης και διαγραφής, συνδρομή για δικαιώματα και αρχεία εκτελούντος την επεξεργασία για εξωτερικά ανατεθειμένες υπηρεσίες παρακολούθησης. Addressed by clauses [4.1.6; 4.2.3; 4.4.5; 4.5.3; 4.6.3].

13.3.9 **Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Αντιστοιχίζεται στην υποστήριξη του εκτελούντος την επεξεργασία για τις υποχρεώσεις πελάτη, στην εξουσιοδότηση κοινολόγησης, στα αρχεία κοινολόγησης, στην κοινοποίηση αιτημάτων κοινολόγησης και στη διαχείριση νομικά δεσμευτικών κοινολογήσεων για PII παρακολούθησης. Addressed by clauses [4.3.5; 4.5.3; 4.6.2; 4.6.3].

13.3.10 **Annex A.3.14; Annex A.3.25** - Αντιστοιχίζεται στην προστασία αρχείων παρακολούθησης, στην περιορισμένη πρόσβαση, στην ανασκόπηση προνομιούχας πρόσβασης, στην καταγραφή πρόσβασης, στον περιορισμό μη εξουσιοδοτημένης πρόσβασης και στα τεκμήρια καταγραφής για συστήματα παρακολούθησης. Addressed by clauses [4.3.2; 4.3.3; 4.5.5; 5.4; 7.4; 10.2; 11.3].

13.4 GDPR

13.4.1 **Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)** - Αντιστοιχίζεται σε νομιμότητα, δικαιοσύνη, διαφάνεια, περιορισμό σκοπού, ελαχιστοποίηση δεδομένων, περιορισμό αποθήκευσης και τεκμήρια λογοδοσίας για δραστηριότητες παρακολούθησης. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.1; 4.4.2; 4.4.3; 6.1; 8.1; 11.2].

13.4.2 Article 6 - Αντιστοιχίζεται στην τεκμηρίωση νομικής βάσης για CCTV, παρακολούθηση επισκεπτών, αρχεία καταγραφής φυσικής πρόσβασης και άλλες δραστηριότητες παρακολούθησης φυσικών χώρων. Addressed by clauses [4.1.2; 4.1.4; 7.1].

13.4.3 **Article 12; Article 13; Article 14** - Αντιστοιχίζεται σε διαφανείς ειδοποιήσεις παρακολούθησης, τεκμήρια σήμανσης, σύνδεση ειδοποιήσεων με σκοπούς επεξεργασίας, πληροφορίες υποστήριξης ειδοποιήσεων από εκτελούντα την επεξεργασία και εναλλακτικά μέτρα διαφάνειας. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 7.2; 8.2; 11.2].

13.4.4 **Article 15; Article 16; Article 17; Article 18; Article 21** - Αντιστοιχίζεται σε πρόσβαση, διόρθωση, διαγραφή, περιορισμό, εναντίωση, δρομολόγηση αιτημάτων, διαφύλαξη που απαιτείται για την αξιολόγηση αιτημάτων και συνδρομή προς τον πελάτη σχετικά με παρακολούθηση. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 7.8; 11.5].

13.4.5 **Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39** - Αντιστοιχίζεται στη διακυβέρνηση υπεύθυνου επεξεργασίας, στην κατανομή από κοινού υπεύθυνων επεξεργασίας, στη διακυβέρνηση εκτελούντος την επεξεργασία, στα αρχεία επεξεργασίας, στην ασφάλεια συστημάτων παρακολούθησης, στην ανασκόπηση κινδύνου ιδιωτικότητας, στα εναύσματα DPIA και στις συμβουλές ιδιωτικότητας. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 4.3.2; 4.3.3; 4.5.4; 4.6.1; 4.6.2; 4.6.4; 5.1; 5.3; 6.3; 8.5; 10.4].

13.5 ISO/IEC 29100:2020

13.5.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Αντιστοιχίζεται στον προσδιορισμό σκοπού, στον περιορισμό συλλογής, στην ελαχιστοποίηση δεδομένων, στον περιορισμό χρήσης, στον περιορισμό διατήρησης και στον περιορισμό κοινολόγησης για PII παρακολούθησης. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.4; 4.4.1; 4.4.2; 4.4.4; 7.8].

13.5.2 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12** - Αντιστοιχίζεται στη διαφάνεια, στη συμμετοχή φυσικών προσώπων, στη λογοδοσία, στην ασφάλεια πληροφοριών, στην ανασκόπηση συμμόρφωσης, στην ανασκόπηση πρόσβασης, στη δρομολόγηση

δικαιωμάτων, στην κλιμάκωση περιστατικών και στα τεκμήρια διορθωτικών ενεργειών. Addressed by clauses [4.2.1; 4.2.2; 4.3.2; 4.3.3; 4.5.1; 4.5.4; 6.1; 8.7; 10.1].

13.6 ISO/IEC 29134:2020

13.6.1 **Clause 5.1; Clause 6.2** - Αντιστοιχίζεται στον κίνδυνο ιδιωτικότητας και στον έλεγχο εναυσμάτων DPIA για συστηματική, μη εμφανή, ακουστική, βιομετρική, με ενεργοποιημένη ανάλυση, σε ευαίσθητες τοποθεσίες, με ευάλωτα άτομα ή άλλη υψηλότερου κινδύνου παρακολούθηση φυσικών χώρων. Addressed by clauses [4.1.4; 4.2.4; 5.3; 6.3; 7.5; 9.2].

13.7 ISO/IEC 29151:2022

13.7.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10** - Αντιστοιχίζεται σε ελέγχους προστασίας PII για σκοπό, συλλογή, ελαχιστοποίηση, διατήρηση, κοινολόγηση και συμμετοχή υποκειμένων των δεδομένων προσωπικού χαρακτήρα σε περιβάλλοντα παρακολούθησης. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.4.1; 4.4.3; 4.5.1; 7.2; 8.2].

13.7.2 **Clause 9.2.3; Clause 9.4.2; Clause 11.1.3** - Αντιστοιχίζεται στην παροχή πρόσβασης, στον περιορισμό πρόσβασης σε πληροφορίες και στους ελέγχους φυσικής εισόδου που σχετίζονται με πρόσβαση σε σύστημα παρακολούθησης και αρχεία ελέγχου φυσικής πρόσβασης. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.5.5; 5.4; 7.4; 10.2; 11.3].

13.8 ISO/IEC 27002:2022

13.8.1 Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15 - Αντιστοιχίζεται στην ιδιωτικότητα και προστασία PII, στη φυσική είσοδο, στην παρακολούθηση φυσικής ασφάλειας, στην προνομιούχα πρόσβαση, στον περιορισμό πρόσβασης σε πληροφορίες και στους ελέγχους καταγραφής για συστήματα CCTV και παρακολούθησης φυσικών χώρων. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.5.5; 5.4; 7.3; 7.4; 8.3; 10.2; 11.3].