https://eyenet-vision.com/

Συνοπτική Νομοθεσία Προσωπικών Δεδομένων - Ελλάδα ΕΕ ΗΠΑ

Συνοπτική Επισκόπηση Νομοθεσίας Προσωπικών Δεδομένων

Ελλάδα • Ευρωπαϊκή Ένωση • Ηνωμένες Πολιτείες (ΗΠΑ)

Έργο αναφοράς: EyeNet Vision / PPL Meta Platform
Ημερομηνία: 8 Μαρτίου 2026
Σκοπός: Συνοπτική χαρτογράφηση νομικών απαιτήσεων και διαφορών ανά περίπτωση χρήσης της τεχνολογίας computer vision.

> Το παρόν είναι ενημερωτικό/στρατηγικό κείμενο και δεν αποτελεί νομική γνωμοδότηση.

Επιτελική Σύνοψη (1 σελίδα)

Η πλατφόρμα EyeNet διαθέτει ισχυρή βάση συμμόρφωσης (on-premises αρχιτεκτονική, offline λειτουργία, modular παραμετροποίηση), αλλά οι νομικές υποχρεώσεις διαφοροποιούνται σημαντικά ανά δικαιοδοσία και λειτουργία.
Στην **Ελλάδα/ΕΕ** εφαρμόζεται αυστηρό πλαίσιο GDPR με έμφαση σε νομιμότητα, αναλογικότητα, διαφάνεια και DPIA. Στις **ΗΠΑ** το πλαίσιο είναι πολιτειακό, με αυξημένο πρακτικό ρίσκο σε βιομετρικά δεδομένα και third-party διαβιβάσεις.

Τι είναι κρίσιμο για τη διοίκηση

- Οι λειτουργίες με **υψηλό νομικό κίνδυνο (High)** είναι κυρίως: ταυτοποίηση προσώπου, δημογραφικό profiling, cross-camera tracking, third-party webhooks/APIs και πολυμισθωτικά logs.
- Οι λειτουργίες **μεσαίου κινδύνου (Med)** απαιτούν αυστηρή τεκμηρίωση νομικής βάσης, data minimization και ανθρώπινη εποπτεία.
- Οι λειτουργίες **χαμηλού κινδύνου (Low)** παραμένουν νομικά κρίσιμες ως προς ασφάλεια, retention και λογοδοσία.

Επιχειρησιακή ετοιμότητα πλατφόρμας

- Υπάρχει δυνατότητα απενεργοποίησης μη αναγκαίων βιομετρικών λειτουργιών.
- Υπάρχει granular έλεγχος ανά κάμερα/κανάλι/ρόλο πρόσβασης.
- Υπάρχει τεχνική βάση για privacy-by-default (retention rules, audit trails, local processing).
- Υπάρχει υποστήριξη για compliant ενεργοποίηση ανά χώρα/πολιτεία.

Προαπαιτήσεις συμμόρφωσης πριν την παραγωγική λειτουργία

1. Ορισμός **jurisdiction matrix** (Ελλάδα, ΕΕ, πολιτείες ΗΠΑ) ανά πελάτη/εγκατάσταση.
2. Υποχρεωτικό **DPIA** για High-risk λειτουργίες πριν από production go-live.
3. Ενοποιημένη πολιτική **retention + access control + incident response**.
4. Υλοποίηση workflow έγκρισης για triggers, webhooks και νέες integrations.
5. Τριμηνιαίος έλεγχος συμμόρφωσης με ownership από Legal / DPO / IT / Ops.

KPI συμμόρφωσης για παρακολούθηση διοίκησης

- % λειτουργιών σε production με τεκμηριωμένη νομική βάση.
- % High-risk λειτουργιών με ολοκληρωμένο DPIA.
- Χρόνος απόκρισης σε αιτήματα δικαιωμάτων υποκειμένων.
- Ποσοστό incidents με πλήρη audit trail και κλείσιμο διορθωτικών ενεργειών.

Συμπέρασμα

Η EyeNet μπορεί να επιτύχει πλήρη και κλιμακούμενη νομική συμμόρφωση, εφόσον η ενεργοποίηση λειτουργιών γίνεται με risk-based διακυβέρνηση, αυστηρή τεκμηρίωση και συνεχές operational monitoring. Ο πίνακας της ενότητας 11 αποτελεί το πρακτικό εργαλείο εφαρμογής για workshops, pilots και production onboarding.

---

1) Σύντομο πλαίσιο ανά γεωγραφία

1.1 Ελλάδα

- Ισχύει ο **GDPR** και ο εφαρμοστικός ελληνικός νόμος **Ν. 4624/2019**.
- Αρμόδια αρχή: **ΑΠΔΠΧ** (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα).
- Ιδιαίτερη προσοχή σε:
  - επεξεργασία εικόνας σε χώρους εργασίας,
  - βιντεοεπιτήρηση,
  - χρήση βιομετρικών/ευαίσθητων δεδομένων,
  - αρχές αναλογικότητας και ελαχιστοποίησης.

1.2 Ευρωπαϊκή Ένωση

- Κύριο πλαίσιο: **GDPR** (Νομιμότητα, Διαφάνεια, Σκοπός, Ελαχιστοποίηση, Ακρίβεια, Περιορισμός χρόνου, Ασφάλεια, Λογοδοσία).
- Για video analytics, συνήθως απαιτούνται:
  - **DPIA** (Εκτίμηση Αντικτύπου),
  - σαφής νομική βάση (έννομο συμφέρον, συγκατάθεση, νομική υποχρέωση κ.λπ.),
  - αυστηρά μέτρα ασφάλειας,
  - πολιτική διατήρησης και δικαιώματα υποκειμένων.
- Τα βιομετρικά δεδομένα θεωρούνται ειδική κατηγορία και απαιτούν αυξημένη τεκμηρίωση/εξαίρεση.

1.3 ΗΠΑ

- Δεν υπάρχει ένα ενιαίο ομοσπονδιακό GDPR-equivalent· το πλαίσιο είναι **κατακερματισμένο**:
  - Πολιτειακοί νόμοι ιδιωτικότητας (π.χ. California CPRA, Virginia, Colorado κ.ά.).
  - Ειδικοί νόμοι για βιομετρικά (π.χ. **BIPA** στο Illinois).
  - Κλαδικές ρυθμίσεις (π.χ. για παιδιά, υγεία, χρηματοοικονομικά).
- Στις ΗΠΑ ο νομικός κίνδυνος συχνά σχετίζεται με:
  - έλλειψη notice/opt-out,
  - χρήση βιομετρικών χωρίς ρητή συναίνεση όπου απαιτείται,
  - ανεπαρκή ασφάλεια και παραβιάσεις.

---

2) Τι σημαίνουν οι διαφορές για την πλατφόρμα EyeNet Vision

Η αξία του EyeNet (on-premises, offline, privacy-first) είναι θετική για συμμόρφωση, αλλά οι απαιτήσεις αλλάζουν ανά χρήση.

Κοινές απαιτήσεις (όλες οι αγορές)

- Privacy by Design / Privacy by Default.
- Περιορισμός σκοπού και δεδομένων (μόνο ό,τι είναι απαραίτητο).
- Πολιτική retention με σαφή χρονικά όρια.
- Τεχνικά μέτρα: κρυπτογράφηση, role-based access, audit logs.
- Διαδικασία για δικαιώματα υποκειμένων (πρόσβαση, διαγραφή, εναντίωση όπου ισχύει).

---

3) Ανάλυση ανά περίπτωση χρήσης (use case)

3.1 Intelligent Signage (δημογραφική στόχευση περιεχομένου)

Περιγραφή: Ανάλυση δημογραφικών χαρακτηριστικών για επιλογή περιεχομένου.

- **Ελλάδα/ΕΕ:**
  - Υψηλός κίνδυνος όταν γίνεται προφίλ/κατηγοριοποίηση προσώπων.
  - Απαιτείται σαφής ενημέρωση, DPIA και ισχυρή τεκμηρίωση νομικής βάσης.
  - Προτείνεται χρήση aggregate/ανωνυμοποιημένων στατιστικών και αποφυγή ταυτοποίησης.
- **ΗΠΑ:**

- Εξαρτάται από πολιτεία. Στην Καλιφόρνια απαιτείται διαφάνεια και δικαιώματα opt-out.
- Αν εμπλέκονται βιομετρικά/face templates, αυξάνεται σημαντικά ο νομικός κίνδυνος.

Ετοιμότητα πλατφόρμας (EyeNet):

- On-premises και offline επεξεργασία που μειώνει διασυνοριακές μεταφορές δεδομένων.
- Δυνατότητα λειτουργίας με aggregate analytics αντί για ταυτοποίηση προσώπων.
- Παραμετροποίηση retention και ρόλων πρόσβασης ανά εγκατάσταση.
- Audit trails για τεκμηρίωση λογοδοσίας και ελέγχων.

Ενέργειες χρήστη (πελάτη/φορέα):

- Να ορίσει νόμιμη βάση επεξεργασίας και να ολοκληρώσει DPIA πριν την παραγωγική χρήση.
- Να ενεργοποιήσει metadata/aggregate mode όπου είναι εφικτό.
- Να αναρτήσει σαφή ενημέρωση (notice/signage) στον χώρο λειτουργίας.
- Να θέσει σύντομο χρόνο διατήρησης και διαδικασία διαγραφής.

3.2 Gate Activity (ασφάλεια, crowd analytics, εντοπισμός απειλών)

Περιγραφή: Παρακολούθηση εισόδων/ροών σε σημεία πρόσβασης.

- **Ελλάδα/ΕΕ:**
  - Συνήθως στηρίζεται σε έννομο συμφέρον ασφάλειας με τεστ εξισορρόπησης.
  - Απαιτούνται signage notices, περιορισμένη γωνία λήψης, μικρός χρόνος διατήρησης.
  - Αυτοματοποιημένη λήψη αποφάσεων με σοβαρές συνέπειες απαιτεί πρόσθετες εγγυήσεις.
- **ΗΠΑ:**
  - Επιτρέπεται ευρύτερα σε ιδιωτικούς χώρους, αλλά απαιτείται σαφές notice.
  - Σε κάποιες πολιτείες η αναγνώριση προσώπου/βιομετρικά έχουν ειδικούς περιορισμούς.

Ετοιμότητα πλατφόρμας (EyeNet):

- Per-camera ρυθμίσεις για ανεξάρτητους κανόνες ανά σημείο πρόσβασης.
- Event-driven ειδοποιήσεις χωρίς ανάγκη πλήρους ταυτοποίησης ατόμων.
- Δυνατότητα περιορισμού περιοχών λήψης και κανόνων ενεργοποίησης.
- Κεντρική καταγραφή συμβάντων για έλεγχο συμμόρφωσης.

Ενέργειες χρήστη (πελάτη/φορέα):

- Να τεκμηριώσει έννομο συμφέρον και balancing test (ιδίως σε Ελλάδα/ΕΕ).
- Να ρυθμίσει κάμερες ώστε να αποφεύγεται υπερβολική κάλυψη μη αναγκαίων χώρων.
- Να εφαρμόσει σαφή signage πολιτική και εσωτερική διαδικασία πρόσβασης σε footage.
- Να ορίσει πρωτόκολλο χειρισμού alerts ώστε να αποφεύγονται αυτοματοποιημένες δυσμενείς αποφάσεις χωρίς ανθρώπινο έλεγχο.

3.3 Room & Gate Protection (παρουσίες, πρόσβαση, compliance)

Περιγραφή: Παρακολούθηση παρουσιών και ελέγχων πρόσβασης σε οργανισμούς.

- **Ελλάδα/ΕΕ:**
  - Εργασιακό περιβάλλον: αυξημένη προστασία εργαζομένων, αναλογικότητα και ελάχιστη παρεμβατικότητα.
  - Για βιομετρική πρόσβαση απαιτείται ισχυρή νομική βάση και εναλλακτικές μέθοδοι όπου είναι εφικτό.
- **ΗΠΑ:**
  - Μεγαλύτερη ευελιξία, αλλά υψηλός litigation risk όπου ισχύουν βιομετρικοί νόμοι (π.χ. BIPA).

Ετοιμότητα πλατφόρμας (EyeNet):

- Modular αρχιτεκτονική για ενεργοποίηση μόνο των απολύτως απαραίτητων λειτουργιών.
- Υποστήριξη πολιτικών πρόσβασης με ρόλους και καταγραφή ενεργειών διαχειριστών.
- Δυνατότητα εναλλακτικών σεναρίων χωρίς βιομετρικά χαρακτηριστικά.
- Παραμετροποίηση retention ανά τύπο συμβάντος (attendance, access, alerts).

Ενέργειες χρήστη (πελάτη/φορέα):

- Να υιοθετήσει πολιτική εργαζομένων/επισκεπτών με σαφή όρια χρήσης και σκοπό.
- Να εξετάσει αν υπάρχει λιγότερο παρεμβατική εναλλακτική πριν από βιομετρική χρήση.

- Να λάβει νομική επιβεβαίωση ανά δικαιοδοσία (ιδίως για εργατικό δίκαιο και BIPA-like νόμους).
- Να ορίσει υπεύθυνο συμμόρφωσης για αιτήματα πρόσβασης/διόρθωσης/διαγραφής.

3.4 Sentinel (monitoring προσωπικού ασφαλείας)

Περιγραφή: Έλεγχος παρουσίας/δραστηριότητας φυλάκων.

- **Ελλάδα/ΕΕ:**
  - Employee monitoring = υψηλή ευαισθησία.
  - Απαραίτητη σαφής πολιτική, περιορισμός σκοπού, και αποφυγή συνεχούς δυσανάλογης επιτήρησης.
- **ΗΠΑ:**
  - Συνήθως επιτρέπεται με πολιτική ενημέρωσης και συμβατικούς όρους, αλλά αλλάζει ανά πολιτεία.

Ετοιμότητα πλατφόρμας (EyeNet):

- Event-based monitoring αντί για συνεχή αδιάκριτη επιτήρηση.
- Χρονικοί κανόνες λειτουργίας ανά βάρδια/σημείο.
- Audit logs για τεκμηρίωση σκοπού ασφάλειας και εσωτερικών ελέγχων.
- Δυνατότητα περιορισμού ορατότητας δεδομένων μόνο σε εξουσιοδοτημένους ρόλους.

Ενέργειες χρήστη (πελάτη/φορέα):

- Να θεσπίσει γραπτή πολιτική employee monitoring με σαφή και αναλογικό σκοπό.
- Να ενημερώσει προσωπικό και συνεργάτες πριν από την ενεργοποίηση.
- Να αποφύγει χρήση για γενική αξιολόγηση απόδοσης πέρα από σκοπό ασφάλειας.
- Να κάνει περιοδικό έλεγχο αναλογικότητας και αναγκαιότητας.

3.5 Underage Detector (ηλικιακή συμμόρφωση σε POS)

Περιγραφή: Έλεγχος αν ο πελάτης είναι πιθανώς ανήλικος για ρυθμιζόμενα προϊόντα.

- **Ελλάδα/ΕΕ:**
  - Θετικό compliance use case όταν υλοποιείται ως age-threshold χωρίς ταυτοποίηση.
  - Προτείνεται “age estimation only”, χωρίς αποθήκευση εικόνων/προφίλ.
- **ΗΠΑ:**
  - Γενικά αποδεκτό ως compliance εργαλείο, αλλά απαιτεί clear notice και περιορισμένη διατήρηση.
  - Προσοχή σε πολιτείες με αυστηρούς κανόνες για βιομετρικά.

Ετοιμότητα πλατφόρμας (EyeNet):

- Σχεδιασμός για age-threshold χρήση χωρίς απαίτηση ταυτοποίησης προσώπου.
- Δυνατότητα λειτουργίας με ελάχιστα δεδομένα (decision output και βασικά logs).
- Τοπική επεξεργασία που περιορίζει μεταφορά προσωπικών δεδομένων.
- Παραμετροποίηση αυτόματης διαγραφής εικόνων/frames.

Ενέργειες χρήστη (πελάτη/φορέα):

- Να εφαρμόσει πολιτική “age estimation only” και να απενεργοποιήσει μη αναγκαίες λειτουργίες.
- Να αναρτήσει σαφή ενημέρωση στο POS για τον σκοπό συμμόρφωσης.
- Να εκπαιδεύσει προσωπικό ώστε το σύστημα να χρησιμοποιείται ως υποβοήθηση και όχι ως αποκλειστικό μέσο απόφασης.
- Να ελέγχει περιοδικά την ακρίβεια/μεροληψία και να τεκμηριώνει διορθωτικές ενέργειες.

3.6 Security Officer Agent (wearable / mobile field operations)

Περιγραφή: Φορητές κάμερες/έξυπνα γυαλιά για προσωπικό ασφαλείας σε κίνηση.

- **Ελλάδα/ΕΕ:**
  - Υψηλός κίνδυνος λόγω συνεχούς λήψης σε δημόσιους ή μικτούς χώρους.
  - Απαιτείται εκτενές DPIA, αυστηρός γεωγραφικός/χρονικός περιορισμός και policy ενεργοποίησης.
- **ΗΠΑ:**
  - Μεταβλητό πλαίσιο ανά πολιτεία· σημαντική η πολιτική διαφάνειας και ο έλεγχος πρόσβασης σε footage.

Ετοιμότητα πλατφόρμας (EyeNet):

- Modular ενεργοποίηση λειτουργιών wearable ανά σενάριο αποστολής.
- Δυνατότητα αυστηρών κανόνων ενεργοποίησης/παύσης καταγραφής.
- Κεντρική διαχείριση πρόσβασης και ιχνηλασιμότητα ενεργειών.
- On-premises αρχιτεκτονική που διευκολύνει έλεγχο κυριαρχίας δεδομένων.

Ενέργειες χρήστη (πελάτη/φορέα):

- Να εκπονήσει ειδικό DPIA για mobile/wearable λειτουργία πριν από παραγωγική χρήση.
- Να ορίσει σαφείς κανόνες πού/πότε επιτρέπεται η καταγραφή (γεωγραφικά και χρονικά).
- Να εφαρμόσει διαδικασία incident response για παράπονα και αιτήματα δικαιωμάτων.
- Να εξασφαλίσει εκπαίδευση προσωπικού για νόμιμη χρήση σε δημόσιους και μικτούς χώρους.

---

4) Κρίσιμες νομικές διαφορές (συμπέρασμα)

1. **ΕΕ/Ελλάδα:** πιο αυστηρό, αρχοκεντρικό πλαίσιο με προτεραιότητα στη νομιμότητα, αναλογικότητα και τεκμηρίωση (GDPR + DPIA).
2. **ΗΠΑ:** πιο αποκεντρωμένο, πολιτειακό μοντέλο με αυξημένο πρακτικό κίνδυνο σε βιομετρικά και class actions.
3. **Για EyeNet:** τα use cases ασφάλειας/συμμόρφωσης είναι ισχυρά, αλλά οι λειτουργίες δημογραφικής ανάλυσης, employee monitoring και wearable καταγραφής απαιτούν τη μεγαλύτερη νομική πειθαρχία.

---

5) Προτεινόμενο ελάχιστο πλάνο συμμόρφωσης για εμπορική ανάπτυξη

- Δημιουργία **jurisdiction matrix** (Ελλάδα, λοιπή ΕΕ, ανά πολιτεία ΗΠΑ).
- Τυποποιημένα **DPIA templates** ανά use case (Signage, Gate, Underage, Wearable).
- Ενεργοποίηση λειτουργιών με **feature flags ανά χώρα/πολιτεία**.
- Data retention standards ανά σενάριο (π.χ. metadata-only mode όπου εφικτό).
- Νομικός/τεχνικός έλεγχος πριν από κάθε νέο pilot σε ευαίσθητο κλάδο.

---

6) Σύντομη θέση για επενδυτικό/επιχειρηματικό υλικό

Η πλατφόρμα EyeNet Vision έχει δομικά χαρακτηριστικά (on-premises επεξεργασία, offline λειτουργία, modular αρχιτεκτονική) που διευκολύνουν τη συμμόρφωση σε Ελλάδα/ΕΕ/ΗΠΑ. Ωστόσο, η νομική βιωσιμότητα εξαρτάται από προσαρμογή ανά use case και ανά δικαιοδοσία, με αυξημένη προσοχή σε δημογραφική ανάλυση, βιομετρικά και φορητή συνεχόμενη καταγραφή.

---

7) Πίνακας Ελέγχου (Checklist) για Pilots / Onboarding ανά Use Case

> Οδηγία χρήσης: Συμπληρώνεται από τον πελάτη μαζί με τον υπεύθυνο υλοποίησης πριν το go-live.
> Συνιστάται έγκριση από DPO/νομικό σύμβουλο όπου απαιτείται.

7.1 Intelligent Signage

Α. Ετοιμότητα πλατφόρμας (να επιβεβαιωθεί από integrator/admin)

- ☐ Ενεργοποιήθηκε λειτουργία aggregate/στατιστικής ανάλυσης χωρίς ταυτοποίηση.
- ☐ Απενεργοποιήθηκαν μη αναγκαίες λειτουργίες βιομετρικής επεξεργασίας.
- ☐ Ρυθμίστηκαν role-based δικαιώματα πρόσβασης σε dashboards/αναφορές.
- ☐ Ενεργοποιήθηκαν audit logs και έλεγχος ιστορικού ενεργειών.
- ☐ Ορίστηκε retention policy με αυτόματη διαγραφή.

Β. Ενέργειες πελάτη (νομικές/οργανωτικές)

- ☐ Ορίστηκε νόμιμη βάση επεξεργασίας ανά χώρα λειτουργίας.
- ☐ Ολοκληρώθηκε DPIA (ιδίως σε Ελλάδα/ΕΕ).

- ☐ Τοποθετήθηκε ενημερωτική σήμανση (notice/signage) στους χώρους.
- ☐ Ενημερώθηκαν privacy notice και διαδικασίες δικαιωμάτων υποκειμένων.
- ☐ Καταγράφηκε υπεύθυνος επικοινωνίας για αιτήματα ιδιωτικότητας.

7.2 Gate Activity

Α. Ετοιμότητα πλατφόρμας (να επιβεβαιωθεί από integrator/admin)

- ☐ Έγινε per-camera παραμετροποίηση κανόνων σε κάθε σημείο εισόδου.
- ☐ Ρυθμίστηκαν περιοχές ενδιαφέροντος (ROI) για ελαχιστοποίηση περιττής λήψης.
- ☐ Τα alerts λειτουργούν event-driven χωρίς υποχρεωτική ταυτοποίηση προσώπου.
- ☐ Ενεργοποιήθηκε κεντρική καταγραφή συμβάντων και πρόσβασης.
- ☐ Ορίστηκαν χρονικά όρια αποθήκευσης βίντεο/μεταδεδομένων.

Β. Ενέργειες πελάτη (νομικές/οργανωτικές)

- ☐ Τεκμηριώθηκε έννομο συμφέρον και balancing test (Ελλάδα/ΕΕ).
- ☐ Εγκρίθηκαν σημεία τοποθέτησης καμερών ως αναλογικά και αναγκαία.
- ☐ Τοποθετήθηκε σαφής signage ενημέρωση σε όλες τις εισόδους.
- ☐ Ορίστηκε SOP ανθρώπινου ελέγχου πριν από κρίσιμες αποφάσεις.
- ☐ Ορίστηκαν διαδικασίες πρόσβασης σε footage μόνο από εξουσιοδοτημένους ρόλους.

7.3 Room & Gate Protection

Α. Ετοιμότητα πλατφόρμας (να επιβεβαιωθεί από integrator/admin)

- ☐ Ενεργοποιήθηκαν μόνο οι απολύτως απαραίτητες λειτουργίες attendance/access.
- ☐ Υπάρχει εναλλακτικό flow χωρίς βιομετρική ταυτοποίηση όπου απαιτείται.
- ☐ Ρυθμίστηκε granular access control για HR/Security/Admin.
- ☐ Ενεργοποιήθηκαν audit logs για ενέργειες διαχειριστών.
- ☐ Ορίστηκε διαφοροποιημένο retention ανά τύπο δεδομένων.

Β. Ενέργειες πελάτη (νομικές/οργανωτικές)

- ☐ Εκδόθηκε εσωτερική πολιτική για εργαζόμενους/επισκέπτες.
- ☐ Εξετάστηκε και τεκμηριώθηκε η λιγότερο παρεμβατική εναλλακτική.
- ☐ Έγινε νομικός έλεγχος για εργατική νομοθεσία και βιομετρικά.
- ☐ Ορίστηκε υπεύθυνος για αιτήματα πρόσβασης/διόρθωσης/διαγραφής.
- ☐ Έγινε εκπαίδευση χειριστών για ορθή και αναλογική χρήση.

7.4 Sentinel

Α. Ετοιμότητα πλατφόρμας (να επιβεβαιωθεί από integrator/admin)

- ☐ Η παρακολούθηση ρυθμίστηκε σε event-based και όχι συνεχές blanket mode.
- ☐ Ορίστηκαν χρονικά παράθυρα λειτουργίας ανά βάρδια.
- ☐ Περιορίστηκε η ορατότητα δεδομένων σε εξουσιοδοτημένους ρόλους.
- ☐ Ενεργοποιήθηκε λογοδοσία μέσω audit trail.
- ☐ Ρυθμίστηκε retention με σύντομο κύκλο διατήρησης.

Β. Ενέργειες πελάτη (νομικές/οργανωτικές)

- ☐ Εκδόθηκε γραπτή policy employee monitoring με σαφή σκοπό ασφάλειας.
- ☐ Ενημερώθηκαν εργαζόμενοι/συνεργάτες πριν την έναρξη.
- ☐ Αποκλείστηκε χρήση για γενική αξιολόγηση απόδοσης εκτός σκοπού.
- ☐ Ορίστηκε διαδικασία παραπόνων και επανεξέτασης περιστατικών.
- ☐ Προγραμματίστηκε περιοδικός έλεγχος αναλογικότητας.

7.5 Underage Detector

Α. Ετοιμότητα πλατφόρμας (να επιβεβαιωθεί από integrator/admin)

- ☐ Ενεργοποιήθηκε age estimation only (χωρίς αναγνώριση ταυτότητας).
- ☐ Απενεργοποιήθηκε αποθήκευση εικόνων όπου δεν είναι αναγκαία.
- ☐ Διατηρείται μόνο ελάχιστο compliance output/log.
- ☐ Ενεργοποιήθηκε τοπική επεξεργασία και κλειδωμένη πρόσβαση.

- ☐ Ρυθμίστηκε αυτόματη διαγραφή προσωρινών frames.

Β. Ενέργειες πελάτη (νομικές/οργανωτικές)

- ☐ Τοποθετήθηκε ενημέρωση στο POS για τον σκοπό ηλικιακής συμμόρφωσης.
- ☐ Καθορίστηκε διαδικασία επιβεβαίωσης από υπάλληλο όπου απαιτείται.
- ☐ Τεκμηριώθηκε ότι το σύστημα είναι υποβοηθητικό και όχι αποκλειστικό.
- ☐ Έγινε αρχικός έλεγχος ακρίβειας/μεροληψίας πριν το go-live.
- ☐ Προγραμματίστηκε περιοδική επαναξιολόγηση μοντέλου και πολιτικών.

7.6 Security Officer Agent (Wearable)

Α. Ετοιμότητα πλατφόρμας (να επιβεβαιωθεί από integrator/admin)

- ☐ Ενεργοποιήθηκαν wearable λειτουργίες μόνο για εγκεκριμένα σενάρια.
- ☐ Ρυθμίστηκαν κανόνες ενεργοποίησης/παύσης καταγραφής.
- ☐ Εφαρμόστηκε αυστηρός έλεγχος πρόσβασης σε footage και metadata.
- ☐ Ενεργοποιήθηκε πλήρης ιχνηλασιμότητα ενεργειών χρηστών.
- ☐ Ρυθμίστηκαν πολιτικές retention ειδικά για mobile περιστατικά.

Β. Ενέργειες πελάτη (νομικές/οργανωτικές)

- ☐ Ολοκληρώθηκε ειδικό DPIA για φορητή/κινητή καταγραφή.
- ☐ Ορίστηκαν γεωγραφικά και χρονικά όρια χρήσης wearable.
- ☐ Εγκρίθηκαν SOP για δημόσιους/μικτούς χώρους και sensitive περιοχές.
- ☐ Εκπαιδεύτηκε το προσωπικό σε νόμιμη και αναλογική χρήση.
- ☐ Ορίστηκε διαδικασία incident response για αιτήματα/παράπονα.

---

8) Γρήγορο Gate πριν από Go-Live (όλα τα use cases)

- ☐ Έχει ολοκληρωθεί νομικός έλεγχος για τη συγκεκριμένη δικαιοδοσία.
- ☐ Έχουν ολοκληρωθεί DPIA/εκτιμήσεις αντικτύπου όπου απαιτούνται.
- ☐ Υπάρχουν ενεργά privacy notices και διαδικασία δικαιωμάτων υποκειμένων.
- ☐ Έχουν ελεγχθεί retention, πρόσβαση, κρυπτογράφηση, audit logs.
- ☐ Έχει οριστεί υπεύθυνος συμμόρφωσης και cadence επανελέγχου.

---

9) Νομικοί Περιορισμοί & Ρυθμίσεις Συμμόρφωσης ανά Λειτουργία EyeNet Vision

> Βάση χαρτογράφησης: έγγραφο λειτουργιών EyeNet Vision (v2.23.1).
> Στόχος: πρακτικός οδηγός για ρύθμιση κάθε functionality σε Ελλάδα/ΕΕ/ΗΠΑ.

9.1 Computer Vision & People Analytics

9.1.1 Real-time people tracking and identification

Νομικοί περιορισμοί

- Σε Ελλάδα/ΕΕ, η ταυτοποίηση προσώπου αποτελεί υψηλού κινδύνου επεξεργασία (συχνά βιομετρική).
- Απαιτείται ισχυρή νομική βάση, αυστηρή αναγκαιότητα/αναλογικότητα και DPIA.
- Σε πολιτείες ΗΠΑ με βιομετρικούς νόμους (π.χ. BIPA), απαιτείται ειδική συμμόρφωση και αυξημένη τεκμηρίωση.

Ρύθμιση για συμμόρφωση

- Απενεργοποίηση identification by default και χρήση detection-only όπου είναι εφικτό.
- Ενεργοποίηση αναγνώρισης μόνο σε εγκεκριμένα σενάρια με νομική κάλυψη.
- Σύντομο retention για ταυτοποιητικά δεδομένα και αυστηρός περιορισμός πρόσβασης.

9.1.2 Accurate counting and attendance monitoring

Νομικοί περιορισμοί

- Στο εργασιακό περιβάλλον απαιτείται ελάχιστη παρεμβατικότητα και σαφής σκοπός.
- Απαγορεύεται υπέρμετρη παρακολούθηση πέρα από νόμιμη επιχειρησιακή ανάγκη.

Ρύθμιση για συμμόρφωση

- Προτίμηση σε count-based metrics χωρίς ατομική ταυτοποίηση.
- Διαχωρισμός reporting σε aggregate επίπεδο ανά τμήμα/βάρδια.
- Ρητή πολιτική ενημέρωσης προσωπικού και περιοδικός έλεγχος αναλογικότητας.

9.1.3 3D route tracking and movement analysis

Νομικοί περιορισμοί

- Η συνεχής παρακολούθηση διαδρομών μπορεί να δημιουργεί προφίλ συμπεριφοράς.
- Σε ΕΕ απαιτείται ελαχιστοποίηση, περιορισμός σκοπού και τεκμηρίωση αναγκαιότητας.

Ρύθμιση για συμμόρφωση

- Χρήση ψευδωνυμοποίησης/anon IDs αντί πραγματικής ταυτότητας.
- Περιορισμός ανάλυσης σε ζώνες και χρονικά παράθυρα επιχειρησιακού ενδιαφέροντος.
- Αυτόματη διαγραφή ιστορικών διαδρομών μετά από μικρό προκαθορισμένο διάστημα.

9.1.4 Demographic analysis (age, gender, etc.)

Νομικοί περιορισμοί

- Υψηλή ευαισθησία για profiling, ειδικά σε δημόσιους χώρους.
- Απαιτείται σαφές notice, DPIA και αποφυγή δυσμενών αυτοματοποιημένων αποφάσεων.

Ρύθμιση για συμμόρφωση

- Ενεργοποίηση μόνο aggregate δημογραφικών στατιστικών.
- Απενεργοποίηση αποθήκευσης ατομικών δημογραφικών προφίλ.
- Ορισμός μηχανισμού ανθρώπινης εποπτείας για κρίσιμες επιχειρησιακές αποφάσεις.

9.2 Camera & Hardware Integration

9.2.1 Multi-source camera support (IP/WiFi/soft cameras)

Νομικοί περιορισμοί

- Κάθε νέα πηγή κάμερας επεκτείνει το πεδίο επεξεργασίας και τον κίνδυνο υπερσυλλογής.
- Απαιτείται σαφής χαρτογράφηση σκοπών και ευθύνης ανά σημείο λήψης.

Ρύθμιση για συμμόρφωση

- Camera inventory με σκοπό, τοποθεσία, ιδιοκτήτη και βάση νομιμότητας.
- Πρότυπο ρυθμίσεων privacy-by-default για κάθε νέο camera onboarding.
- Υποχρεωτικός έλεγχος ROI masking πριν ενεργοποίηση παραγωγής.

9.2.2 Camera health monitoring

Νομικοί περιορισμοί

- Τα logs υγείας δεν πρέπει να περιέχουν περιττά προσωπικά δεδομένα.

Ρύθμιση για συμμόρφωση

- Διατήρηση τεχνικών logs χωρίς αναγνωρίσιμα πρόσωπα.
- Περιορισμός metadata σε ό,τι είναι αναγκαίο για SLA/συντήρηση.

9.3 Intelligent Triggers & Automated Actions

9.3.1 Camera-level trigger configuration

Νομικοί περιορισμοί

- Κίνδυνος μη αναλογικών κανόνων ανά κάμερα που επηρεάζουν άτομα χωρίς επαρκή αιτιολόγηση.

Ρύθμιση για συμμόρφωση

- Trigger approval workflow με τεκμηρίωση σκοπού/αναγκαιότητας.
- Πρότυπα trigger templates ανά use case και δικαιοδοσία.

9.3.2 Real-time event detection (count, dwell, velocity, direction, demographics)

Νομικοί περιορισμοί

- Η συνδυαστική ανάλυση συμπεριφοράς μπορεί να οδηγεί σε προφίλ υψηλού κινδύνου.

Ρύθμιση για συμμόρφωση

- Ενεργοποίηση μόνο απολύτως αναγκαίων event types.
- Καταγραφή νομικής βάσης ανά event type σε configuration registry.

9.3.3 Complex condition logic (AND/OR)

Νομικοί περιορισμοί

- Σύνθετοι κανόνες μπορεί να παράγουν δυσμενή αποτελέσματα χωρίς διαφάνεια.

Ρύθμιση για συμμόρφωση

- Διατήρηση explainable rule descriptions ανά trigger.
- Υποχρεωτικός human-in-the-loop έλεγχος για υψηλής επίπτωσης συμβάντα.

9.3.4 Automated action execution & multi-channel notifications

Νομικοί περιορισμοί

- Κίνδυνος υπερκοινοποίησης προσωπικών δεδομένων μέσω push/email/SMS.

Ρύθμιση για συμμόρφωση

- Data minimization στα μηνύματα (π.χ. event ID αντί εικόνας όταν αρκεί).
- Κρυπτογράφηση/ασφαλή κανάλια και role-based distribution lists.

9.3.5 Third-party triggers (webhooks, external systems)

Νομικοί περιορισμοί

- Μεταφορά δεδομένων σε τρίτους απαιτεί συμβατική και νομική κάλυψη.

Ρύθμιση για συμμόρφωση

- Data Processing Agreements με τρίτους και περιορισμός πεδίων webhook payload.
- Allowlist endpoints και υποχρεωτική αυθεντικοποίηση/υπογραφή κλήσεων.

9.3.6 Custom workflows

Νομικοί περιορισμοί

- Αυξημένος κίνδυνος function creep (χρήση πέρα από τον αρχικό σκοπό).

Ρύθμιση για συμμόρφωση

- Change management με legal/privacy review πριν από κάθε νέο workflow.
- Περιοδικός έλεγχος για απενεργοποίηση workflows που δεν είναι πλέον αναγκαία.

9.4 Video & Data Management

9.4.1 Local storage, offline operation, no cloud dependency

Νομικοί περιορισμοί

- Η τοπική αποθήκευση μειώνει μεταφορές, αλλά δεν αίρει υποχρεώσεις GDPR/πολιτειακών νόμων.
- Απαιτείται ασφάλεια αρχείων, πρόσβαση βάσει ρόλου και πολιτική retention.

Ρύθμιση για συμμόρφωση

- File-level encryption, key management και διακριτοί admin ρόλοι.
- Αυτόματη διαγραφή βάσει πολιτικής ανά data class (video, snapshots, logs).
- Τακτικός έλεγχος backup/restore με privacy-safe διαδικασίες.

9.5 Intelligent Communications

9.5.1 Push/In-app/Email/SMS/Webhooks/Audit delivery tracking

Νομικοί περιορισμοί

- Κάθε κανάλι αποτελεί ξεχωριστή ροή δεδομένων με υποχρεώσεις ασφάλειας και διαφάνειας.

Ρύθμιση για συμμόρφωση

- Channel policy ανά τύπο συμβάντος (τι επιτρέπεται να αποστέλλεται και πού).
- Masking προσωπικών στοιχείων στα notifications by default.
- Καταγραφή παραδόσεων χωρίς περιττό περιεχόμενο προσωπικών δεδομένων.

9.6 Analytics & Insights

9.6.1 Dashboards, trends, behavioral patterns, reporting

Νομικοί περιορισμοί

- Κίνδυνος επαναταυτοποίησης από ιστορικά/συνδυαστικά reports.
- Υποχρέωση ακρίβειας, περιορισμού σκοπού και fairness σε μοντέλα συμπερασμάτων.

Ρύθμιση για συμμόρφωση

- Dashboards σε aggregate επίπεδο με ελάχιστη granular πληροφορία.
- Thresholds ανωνυμοποίησης (π.χ. ελάχιστος αριθμός ατόμων ανά report bucket).
- Περιοδικός έλεγχος bias/accuracy και τεκμηρίωση διορθωτικών ενεργειών.

9.7 Deployment Architecture

9.7.1 On-prem/edge, modular microservices, service discovery

Νομικοί περιορισμοί

- Απαιτείται σαφής κατανομή ρόλων controller/processor σε πολυ-οντοτικές εγκαταστάσεις.
- Κίνδυνος ανεξέλεγκτης πρόσβασης μεταξύ υπηρεσιών αν δεν υπάρχουν όρια.

Ρύθμιση για συμμόρφωση

- Service-to-service authentication, network segmentation και least privilege.
- Data flow mapping ανά microservice με καταγραφή σκοπού και retention.
- Tenant isolation για περιβάλλοντα πολλαπλών πελατών.

9.8 Security & Access Control

9.8.1 RBAC, encryption, private VPN, audit trails

Νομικοί περιορισμοί

- Η ασφάλεια είναι νομική υποχρέωση (τεχνικά και οργανωτικά μέτρα).
- Παραβιάσεις ασφάλειας ενεργοποιούν υποχρεώσεις γνωστοποίησης.

Ρύθμιση για συμμόρφωση

- Υποχρεωτικό MFA για διαχειριστές και περιοδική αναθεώρηση δικαιωμάτων.
- Κρυπτογράφηση σε ανάπαυση/μεταφορά και rotation κλειδιών.
- Incident response plan με SLA ειδοποίησης και διαδικασία καταγραφής παραβιάσεων.

9.9 Scalability & Expandability

9.9.1 Scaling across sites, unlimited cameras, APIs/plugins/integrations

Νομικοί περιορισμοί

- Η κλιμάκωση αυξάνει τον κίνδυνο ασυνέπειας συμμόρφωσης μεταξύ τοποθεσιών.

- APIs/plugins μπορεί να εισάγουν μη εγκεκριμένες ροές προσωπικών δεδομένων.

Ρύθμιση για συμμόρφωση

- Standard baseline privacy profile που εφαρμόζεται αυτόματα σε κάθε νέο site.
- API governance (scopes, rate limits, payload minimization, key rotation).
- Vendor/plugin due diligence πριν από κάθε νέα ενσωμάτωση.

9.10 Support & Monitoring

9.10.1 Remote diagnostics, centralized logs, multi-tenant support

Νομικοί περιορισμοί

- Remote support μπορεί να επιτρέπει πρόσβαση σε προσωπικά δεδομένα εκτός αναγκαιότητας.
- Centralized logs πρέπει να αποφεύγουν υπερσυγκέντρωση αναγνωρίσιμων πληροφοριών.

Ρύθμιση για συμμόρφωση

- Just-in-time support access με έγκριση πελάτη και πλήρη καταγραφή συνεδρίας.
- Redaction προσωπικών στοιχείων στα logs και αυστηρό retention.
- Διακριτή διαχείριση tenant IDs και πολιτική πρόσβασης ανά πελάτη.

9.11 Technical Architecture Highlights (εξειδικευμένες λειτουργίες)

9.11.1 Multi-camera correlation & cross-zone tracking

Νομικοί περιορισμοί

- Αυξημένος κίνδυνος προφίλ και επαναταυτοποίησης σε μεγάλης κλίμακας παρακολούθηση.

Ρύθμιση για συμμόρφωση

- Ενεργοποίηση correlation μόνο με τεκμηριωμένη ανάγκη ασφαλείας.
- Χρήση ανωνυμοποιημένων αναγνωριστικών και μικρού retention για συσχετίσεις.

9.11.2 Historical comparison triggers

Νομικοί περιορισμοί

- Μακροχρόνια ιστορικά δεδομένα αυξάνουν ρίσκο σκοπού πέραν του αρχικού.

Ρύθμιση για συμμόρφωση

- Data windows περιορισμένης διάρκειας και auto-pruning.
- Τεκμηρίωση γιατί απαιτείται ιστορική σύγκριση για τον συγκεκριμένο σκοπό.

9.11.3 Digital signage dynamic demographic targeting

Νομικοί περιορισμοί

- Κίνδυνος διακριτικής μεταχείρισης/προφίλ με βάση ευαίσθητα χαρακτηριστικά.

Ρύθμιση για συμμόρφωση

- Απαγόρευση rules που στοχεύουν ευαίσθητες ή προστατευόμενες κατηγορίες.
- Χρήση broad audience segments με ελάχιστη λεπτομέρεια και χωρίς αποθήκευση ατομικού ιστορικού.

---

10) Ελάχιστο Operational Policy για ενεργοποίηση λειτουργιών

- ☐ Κάθε functionality έχει ορισμένο σκοπό, νομική βάση και ιδιοκτήτη (owner).
- ☐ Κάθε functionality έχει privacy-by-default preset και τεκμηριωμένο exception process.
- ☐ Κάθε functionality περνά νομικό/τεχνικό έλεγχο πριν το production enablement.
- ☐ Υπάρχει επανέλεγχος ανά τρίμηνο για αναγκαιότητα, ακρίβεια και αναλογικότητα.
- ☐ Οι αλλαγές σε triggers/workflows/integrations καταγράφονται σε compliance changelog.

---

11) Επιχειρησιακή ετοιμότητα πλατφόρμας Eyenet για πλήρη νομική

συμμόρφωση

Α/Α	Λειτουργία	Νομικός περιορισμός	Risk Level	Ρύθμιση για αντιμετώπιση περιορισμού	Διαθέσιμο;	Owner
1	Real-time people tracking & identification	Υψηλός κίνδυνος βιομετρικής/ ταυτοποίησης (GDPR, πολιτειακοί βιομετρικοί νόμοι ΗΠΑ)	High	`identification off by default`, ενεργοποίηση μόνο με νομική βάση + DPIA, σύντομο retention	ΝΑΙ	Legal + DPO + IT
2	3D route tracking & movement analysis	Κίνδυνος συμπεριφορικού προφίλ και επαναταυτοποίησης	High	Ψευδωνυμοποίηση IDs, περιορισμός σε ζώνες/χρόνο, auto-delete ιστορικού	ΝΑΙ	DPO + IT
3	Demographic analysis (age, gender)	Profiling υψηλής ευαισθησίας, ανάγκη διαφάνειας και DPIA	High	Μόνο aggregate δημογραφικά, χωρίς ατομικά προφίλ, human oversight	ΝΑΙ	Legal + DPO
4	Third-party application triggers (webhooks)	Διαβίβαση δεδομένων σε τρίτους χωρίς επαρκή συμβατική κάλυψη	High	DPA με τρίτους, payload minimization, endpoint allowlist, υπογραφή/ αυθεντικοποίηση	ΝΑΙ	Legal + IT
5	Behavioral pattern recognition	Συμπερασματική επεξεργασία υψηλής επίπτωσης	High	Ενεργοποίηση μόνο όπου αναγκαίο, fairness/bias checks, ανθρώπινη επιβεβαίωση	ΝΑΙ	DPO + Ops
6	REST APIs / plugin integrations	Νέες μη ελεγχόμενες ροές προσωπικών δεδομένων	High	API governance (scopes, rate limits), vendor due diligence, contract controls	ΝΑΙ	IT + Legal
7	Centralized logging & multi-tenant support	Υπερσυγκέντρωση δεδομένων και κίνδυνος tenant leakage	High	Tenant isolation, log redaction, tenant-based access policies	ΝΑΙ	IT + DPO
8	Multi-camera correlation / cross-zone tracking	Υψηλός κίνδυνος παρακολούθησης μεγάλης κλίμακας	High	Ενεργοποίηση μόνο σε ειδικές περιπτώσεις ασφάλειας, anon IDs, σύντομο retention	ΝΑΙ	Legal + DPO + IT
9	Digital signage dynamic content switching	Κίνδυνος διακριτικής μεταχείρισης με βάση προφίλ κοινού	High	Απαγόρευση ευαίσθητων categories, broad segmentation, no individual history	ΝΑΙ	Legal + DPO + Ops
10	Demographic-based targeting in signage	Αυξημένη υποχρέωση διαφάνειας και μη διάκρισης	High	Notice/signage, aggregate-only λειτουργία, legal review ανά αγορά	ΝΑΙ	Legal + DPO
11	Accurate counting & attendance monitoring	Κίνδυνος υπέρμετρης παρακολούθησης σε χώρους εργασίας	Med	Aggregate counting χωρίς ταυτοποίηση, πολιτική εργαζομένων, περιοδικός έλεγχος αναλογικότητας	ΝΑΙ	DPO + Ops
12	Multi-source camera support (IP/WiFi/soft)	Επέκταση πεδίου επεξεργασίας χωρίς έλεγχο σκοπού	Med	Camera inventory με σκοπό/βάση νομιμότητας, privacy presets, ROI masking πριν go-live	ΝΑΙ	IT + Ops
13	Camera-level trigger configuration	Μη αναλογικοί κανόνες ανά κάμερα χωρίς αιτιολόγηση	Med	Trigger approval workflow + τεκμηρίωση σκοπού/νομικής βάσης ανά trigger	ΝΑΙ	Ops + DPO
14	Real-time event detection (count/dwell/velocity/direction/demographics)	Συνδυαστική ανάλυση αυξάνει κίνδυνο profiling	Med	Ενεργοποίηση μόνο αναγκαίων event types, καταγραφή νομικής βάσης ανά event	ΝΑΙ	DPO + IT
15	Complex condition logic (AND/OR)	Πιθανές δυσμενείς αυτοματοποιημένες εκβάσεις χωρίς διαφάνεια	Med	Explainable rules, υποχρεωτικό human-in-the-loop σε high-impact ενέργειες	ΝΑΙ	Ops + Legal
16	Multi-channel notifications (push/in-app/email/SMS)	Υπερκοινοποίηση προσωπικών δεδομένων σε πολλαπλά κανάλια	Med	Data minimization στα μηνύματα, role-based recipients, ασφαλή κανάλια	ΝΑΙ	IT + Ops

Α/Α	Λειτουργία	Νομικός περιορισμός	Risk Level	Ρύθμιση για αντιμετώπιση περιορισμού	Διαθέσιμο;	Owner
17	Custom workflows	Function creep (χρήση πέραν αρχικού σκοπού)	Med	Change management με legal/privacy review και περιοδικό cleanup workflows	ΝΑΙ	Ops + DPO
18	Local video/data storage (on-prem, no cloud)	Υποχρέωση ασφάλειας/retention παραμένει πλήρως	Med	File encryption, RBAC, auto-retention rules, ελεγχόμενο backup/restore	ΝΑΙ	IT
19	Intelligent communications audit tracking	Logs επικοινωνίας μπορεί να αποκαλύπτουν προσωπικά δεδομένα	Med	Masking/redaction σε logs, retention limits, πρόσβαση μόνο σε εξουσιοδοτημένους	ΝΑΙ	IT + DPO
20	Real-time dashboards & historical analytics	Κίνδυνος επαναταυτοποίησης μέσω granular reports	Med	Aggregate dashboards, ελάχιστα thresholds ανωνυμοποίησης, περιορισμένο export	ΝΑΙ	DPO + Ops
21	Action execution monitoring & statistics	Δευτερογενής χρήση logs πέρα από αρχικό σκοπό	Med	Σαφής πολιτική σκοπού για monitoring δεδομένα, διαχωρισμός operational vs personal logs	ΝΑΙ	DPO + Ops
22	On-prem/edge deployment architecture	Ασάφεια ρόλων controller/processor σε σύνθετες εγκαταστάσεις	Med	Contractual role mapping, data-flow mapping, τεκμηριωμένη κατανομή ευθυνών	ΝΑΙ	Legal + DPO
23	Microservices architecture & service discovery	Κίνδυνος lateral access μεταξύ υπηρεσιών	Med	Service-to-service auth, network segmentation, least privilege ανά service	ΝΑΙ	IT
24	User access management (RBAC)	Μη εξουσιοδοτημένη πρόσβαση σε προσωπικά δεδομένα	Med	Role matrices, periodic access recertification, αρχή ελάχιστου δικαιώματος	ΝΑΙ	IT + DPO
25	Scaling across sites / unlimited cameras	Ασυνέπεια συμμόρφωσης μεταξύ τοποθεσιών	Med	Baseline compliance profile ανά νέο site + τοπικό legal override	ΝΑΙ	Ops + DPO
26	Remote diagnostics & troubleshooting	Πρόσβαση support σε προσωπικά δεδομένα πέραν αναγκαιότητας	Med	Just-in-time access με έγκριση πελάτη, session logging, προσωρινά δικαιώματα	ΝΑΙ	IT + Ops
27	Installation identification / multi-tenant identifiers	Πιθανή συσχέτιση δεδομένων μεταξύ πελατών	Med	Pseudonymous tenant IDs, διαχωρισμός περιβαλλόντων, περιορισμός cross-tenant queries	ΝΑΙ	IT + DPO
28	Context-aware triggers (time/day/occupancy)	Έμμεσο profiling συμπεριφορών	Med	Ελάχιστα απαιτούμενα context signals, disable μη αναγκαίων παραμέτρων	ΝΑΙ	DPO + Ops
29	Historical comparison triggers	Μακροχρόνια διατήρηση αυξάνει νομικό ρίσκο	Med	Μικρά data windows, auto-pruning, τεκμηρίωση σκοπού ιστορικής σύγκρισης	ΝΑΙ	DPO + IT
30	Camera health monitoring	Τεχνικά logs μπορεί να περιέχουν περιττά προσωπικά δεδομένα	Low	Μόνο τεχνικά health metadata, χωρίς εικόνα/PII όπου δεν απαιτείται	ΝΑΙ	IT
31	Offline operation	Μειωμένη εξάρτηση από cloud αλλά πλήρης ευθύνη τοπικής ασφάλειας	Low	Local hardening, ασφαλής πρόσβαση διαχειριστών, καταγραφή ενεργειών	ΝΑΙ	IT
32	File-level encryption	Νομική απαίτηση για κατάλληλα τεχνικά μέτρα ασφάλειας	Low	Encryption at rest/in transit, key rotation, έλεγχος διαχείρισης κλειδιών	ΝΑΙ	IT
33	Optional private VPN for communications	Κίνδυνος διαρροής δεδομένων σε απομακρυσμένη πρόσβαση	Low	Υποχρεωτικό secure tunnel για remote πρόσβαση, logging και policy πρόσβασης	ΝΑΙ	IT
34	Trigger/action audit trails	Υποχρέωση λογοδοσίας και δυνατότητα ελέγχου συμβάντων	Low	Αμετάβλητα logs, χρονοσήμανση, περιορισμένη πρόσβαση, policy retention	ΝΑΙ	IT + DPO