GDPR: COMPLIANCE & PHYSICAL SECURITY

DR. GEORGE STERGIOPOULOS
IT SECURITY CONSULTANT – SENIOR

ΦΥΣΙΚΗ ΑΣΦΑΛΕΙΑ

- Προστασία δικτύων, προσωπικού και υλικού από φυσικές συνθήκες και γεγονότα που μπορεί να προκαλέσουν σοβαρές ζημιές.
  - Περιλαμβάνει προστασία από μη εξουσιοδοτημένη πρόσβαση, πυρκαγιά, βανδαλισμούς, φυσικές καταστροφές και τρομοκρατία.

- Μέτρα ελέγχου φυσικής ασφάλειας
  - Εφαρμογή ελέγχων κατά την είσοδο και έξοδο από κτίριο ή αίθουσα, κατά περίπτωση.
  - πρόληψη της κλοπής κ.λπ.
  - προστασία εξοπλισμού και συσκευών.

ΣΥΝΟΠΤΙΚΑ

1) Η φυσική ασφάλεια εμπίπτει στον ΓΚΠΔ

2) Περιορισμένη επικοινωνία μεταξύ των επαγγελματιών προστασίας φυσικής ασφάλειας και του IT security.

3) Συμμόρφωση μπορεί να επιτευχθεί μέσω αναβαθμίσεων παρά μέσω ανακατασκευής και αντικατάστασης.

ΠΩΣ?

- Τρεις σημαντικές κατηγορίες φυσικής ασφάλειας:
  - Ε**μπόδια** στην είσοδο τοποθεσιών και πιθανών επιτιθέμενων.
    - Παραδείγματα: Χρήση συσκευών ασφαλείας έξυπνων καρτών, πολλαπλών κλειδαριών και ασφαλιστικών θυρίδων ασφαλείας.
  - **Συστήματα επιτήρησης** και ενημέρωσης: Κάμερες, συστήματα ανίχνευσης εισβολών, συναγερμοί και ανιχνευτές.
  - Στόχος ο **εντοπισμός** κακόβουλων πριν προκαλέσει ζημιά.

ΟΡΙΣΜΟΙ

- «Υπεύθυνος επεξεργασίας δεδομένων»:
  - Φυσικό ή νομικό πρόσωπο που αποφασίζει τη φύση και έκταση μιας πράξης επεξεργασίας δεδομένων (18), δηλαδή τη δράση που αφορά τα προσωπικά δεδομένα του υποκειμένου.

- «Εκτελών την επεξεργασία»
  - Επεξεργάζεται δεδομένα εξ ονόματος του υπευθύνου
    - Π.χ. προμηθευτής πληροφορικής
    - φορέας παροχής υπηρεσιών υπολογιστικού νέφους.

CCTV

- Δεδομένα CCTV (σε μόνιμη, συνεχή ή τακτική βάση) **αποτελούν προσωπικά δεδομένα**.

- Μη αποθήκευση ή περαιτέρω επεξεργασία δεν απαλλάσσει τον Υπεύθυνο επεξεργασίας από την υποχρέωσή να ειδοποιεί την Αρχή και να ενημερώνει το κοινό.

ΒΙΝΤΕΟΕΠΙΤΗΡΗΣΗ

- Οι διαμεσολαβητές μπορούν υπό προϋποθέσεις:
  - Να επεξεργάζονται προσωπικά δεδομένα σχετικά με υπαλλήλους,
  - Να διατηρούν δεδομένα σχετικά με πελάτες για δικά τους αρχεία ή
  - Να συλλέγουν εικόνες ανθρώπων, εργαζομένων ή κοινού, που καταγράφονται από κάμερες παρακολούθησης βίντεο (CCTV) **στις εγκαταστάσεις του**.
  - Ο διαμεσολαβητής = Εκτελών επεξεργασία αλλά **ίσως ενεργεί ως Υπεύθυνος επεξεργασίας**.

ΠΟΥ ΕΓΚΑΘΙΣΤΑΝΤΑΙ..

- Οι κάμερες CCTV μπορούν να εγκατασταθούν
  - στο χώρο εργασίας για λόγους ασφαλείας
  - για πρόληψη και διερεύνηση εγκλημάτων, κλοπών ή παραπτωμάτων.
  - στις περιοχές εισόδου και εξόδου, στις εξόδους έκτακτης ανάγκης και στους διαδρόμους
  - σε περιοχές όπου αποθηκεύονται αγαθά ή πολύτιμα αντικείμενα.

- CCTV gap analysis ιδιαίτερα σημαντική για χρήστες που βιντεοσκοπούν δημόσιους χώρους. (high risk GDPR)

..ΚΑΙ ΠΟΥ ΑΠΑΓΟΡΕΥΕΤΑΙ

- Σεβασμός ιδιωτικής ζωής εργαζομένων.
- Οι κάμερες **δεν πρέπει** να καταγράφουν:
  - υπαλλήλους στα γραφεία, με ορισμένες εξαιρέσεις (π.χ. εργαζόμενοι που χειρίζονται μετρητά - αλλά η κάμερα πρέπει να επικεντρωθεί στην ταμειακή μηχανή).
  - τουαλέτες, προσωπικό, αποδυτήρια ή γραφεία συνδικάτων.
- Πρόσβαση σε αρχεία CCTV περιορίζεται σε άτομα με **εξουσιοδοτημένα δικαιώματα** (π.χ. διαχειριστής ασφαλείας).
- **Εγκατάσταση σε ή βιντεοσκόπηση δημόσιων χώρων παρά μόνο σε ειδικές περιπτώσεις.**

CCTV & GDPR: ΔΙΚΑΙΩΜΑΤΑ

1. Δικαίωμα αντιγράφου υλικού CCTV στο οποίο βρίσκονται και / ή είναι σαφώς αναγνωρίσιμα (**data portability**).
2. Δικαίωμα ενημέρωσης.
3. Δικαίωμα προστασίας.
4. **Privacy by design.**
5. Αρχή της Αναλογικότητας & του σκοπού.
   – Επισημάνετε έναν κίνδυνο που ελαχιστοποιείται μέσω χρήσης CCTV.

CCTV & GDPR

- Σε περίπτωση μη συμμόρφωσης του Υπευθύνου, ο υπάλληλος (ή οποιοδήποτε υποκείμενο των δεδομένων) καταγγέλλει στην Αρχή.

- Ποινή κατά του οργανισμού σε περιπτώσεις που:
  - *παρακολούθηση CCTV δυσανάλογη του σκοπού.*
  - *πληροφορίες που παρέχονται στους υπαλλήλους ή πρόσωπα σχετικά με παρακολούθηση είναι ανεπαρκείς.*
  - *η περίοδος διατήρησης είναι υπερβολική*
  - *τα μέτρα ασφαλείας είναι ανεπαρκή*

CCTV & GDPR

- (Άρθρο 35 GDPR) Κάθε υπερβολική χρήση παρακολούθησης CCTV εργαζομένων θεωρείται υψηλού κινδύνου (άρθρου 29).

- Απαιτεί εκτίμηση επιπτώσεων στην προστασία δεδομένων ("DPIA").
  - *Επιτήρηση αναγκαία και ανάλογη με βάση κινδύνους για τα δικαιώματα των προσώπων στα οποία αναφέρονται τα δεδομένα*
  - *Επιλογή μέτρων προστασίας που θα εφαρμόσει ο υπεύθυνος επεξεργασίας.*

CCTV & GDPR

- Οι εργαζόμενοι και οποιοσδήποτε άλλο υποκείμενο προσ. δεδομένων (δηλ. Επισκέπτες, πελάτες, αν υπάρχουν, κ.λπ.) πρέπει **να ενημερώνονται**:
  - τη **φύση** και την **έκταση** της παρακολούθησης του CCTV ·
  - το **όνομα** του υπευθύνου · και
  - τη **διαδικασία** για την πρόσβαση στο βίντεο,
  - **προειδοποιητική ειδοποίηση** τοποθετημένης όπου έχει CCTV.
  - κάθε εργαζόμενος **ξεχωριστά** για χρήση CCTV στη σύμβαση εργασίας ή σε εσωτερικό σημείωμα.

CCTV & GDPR

- Θέσπιση από **κατάλληλα τεχνικά και οργανωτικά μέτρα** για περιορισμό κάθε **κινδύνου** για τα δικαιώματα ιδιωτικού απορρήτου ενός εργαζομένου σε περίπτωση παραβίασης των δεδομένων, όπως απαιτείται από το GDPR.

- Προσωπικά δεδομένα σε λιγότερο ευαίσθητη μορφή ή να ψευδονομηθούν.
  - Π.χ. Δεδομένα βίντεο από κάμερες παρακολούθησης που μπορεί να ταυτοποιούν ανθρώπους που στέκονται ή κινούνται να θολώνουν.

- Κρυπτογράφηση

CCTV & GDPR

- Δεδομένα CCTV να χρησιμοποιούνται και να διατηρούνται μόνο για την εκπλήρωση του αρχικού σκοπού.
- **Έντονη**, **σαφής** και **επαρκής** σήμανση σε περιοχές με κάμερες CCTV.
- Πολιτικές προστασίας δεδομένων σχετικές με τη χρήση κάμερας CCTV:
  - τους σκοπούς της επιτήρησης του CCTV
  - τις συνθήκες υπό τις οποίες θα πραγματοποιηθεί η παρακολούθηση
  - τη φύση της παρακολούθησης,
  - πώς θα χρησιμοποιηθούν τα προσωπικά δεδομένα των ατόμων,
  - πόσο χρόνο θα διατηρηθεί το βίντεο, καθώς και
  - την επίπτωση στα δικαιώματα των ατόμων.

ΜΕΤΡΑ ΦΥΣΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

- Μέτρα φυσικής ασφάλειας κατά ISO 27001:
  - φυσικός έλεγχος πρόσβασης,
  - ασφάλεια υλικού,
  - προστασία από πηγές κινδύνου πλην του ανθρώπου κ.λπ.
- Privacy by design:
  - κρυπτογράφηση
  - αυτοματοποιημένη επεξεργασία βίντεο που καταγράφουν δημόσιους χώρους.

ΜΕΤΡΑ ΦΥΣΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

- **Αξιοποιείστε GDPR-compliant υπηρεσίες cloud** για μείωση εύρους και όγκου δραστηριοτήτων.

- Συστήματα CCTV εγγενώς **ευάλωτα σε επιθέσεις στον κυβερνοχώρο** όταν συνδέονται με το Internet ή το σύννεφο.
  - ***περιορισμό της πρόσβασης*** σε αυτά και
  - ύπαρξη ***ισχυρών συστημάτων*** για την αποφυγή επιθέσεων μέσω του Διαδικτύου, κακόβουλο λογισμικό.