Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) & Κυβερνοασφάλεια

Δρ. Φώτιος Γκιουλέκας
Μεταδιδάκτορας Πληροφορικής ΑΠΘ
Μέλος της Εθελοντικής Ομάδας ENISA E-Health Security Experts

ARISTOTLE UNIVERSITY OF THESSALONIKI

GOOGLE.ORG CYBERSECURITY SEMINARS

Σύνοψη

- Κανονισμοί και Πρότυπα Προστασίας Προσωπικών Δεδομένων
- Ο Γενικός Κανονισμός για την Προστασία Προσωπικών Δεδομένων (GDPR)
- Ορισμοί & Ορολογία
- Μέτρα Κυβερνοασφάλειας
- Μεθοδολογία Συμμόρφωσης & Εκτίμηση Αντικτύπου Προστασίας Δεδομένων (DPIA)
- Ψευδωνυμοποίηση

Νόμοι και Κανονισμοί Προστασίας Δεδομένων

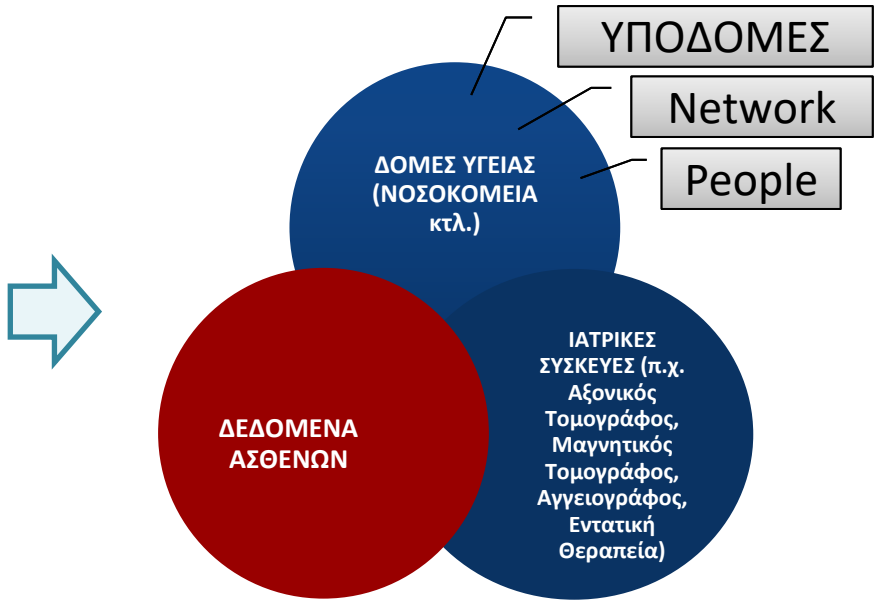
- Η συμμόρφωση με τους νόμους προστασίας δεδομένων αποτελεί κύρια ανησυχία για τους χρήστες εφαρμογών Cloud (Ιδιωτικού ή Δημοσίου Τομέα), κοινωνικών δικτύων κτλ. και ιδιαίτερα όταν πρόκειται για ευαίσθητα και προσωπικά δεδομένα
- Νόμοι όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (**GDPR**) στην Ευρωπαϊκή Ένωση (**ΕΕ**), ο Νόμος για την Ιδιωτικότητα των Καταναλωτών στην Καλιφόρνια (**California Consumer Privacy Act - CCPA**) και ο Νόμος για τη Μεταχείριση Υγειονομικών Πληροφοριών (**HIPAA**) στον τομέα της υγειονομικής περίθαλψης επιβάλλουν αυστηρές απαιτήσεις για την προστασία της ιδιωτικότητας και της ασφάλειας των δεδομένων

Υφίστανται Νομοθετικές Ρυθμίσεις & Πρότυπα για την Προστασία Προσωπικών Δεδομένων;

ΣΥΜΜΟΡΦΩΣΗ

- Οδηγίες & Κανονιστικό Πλαίσιο ΕΕ
  - Κανονισμός NIS2
  - Κανονισμός GDPR
  - Κανονισμός MDR & IVDR
- Εθνική Νομοθεσία
  - Ν.5160/2024
  - Νόμος 4624/2019, **Νόμος 5169/2025**
  - Θα εφαρμοστεί καθολικά το 2028
- Πρότυπα & Πιστοποιήσεις
  - Εθνική Στρατηγική Κυβερνοασφάλειας της ΕΑΚ – Αρχή Προστασίας Προσωπικών Δεδομένων
  - ISO/IEC 27001 - information security standard

ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ: π.χ. ΤΟΜΕΑΣ ΥΓΕΙΑΣ



Κανονισμοί ΕΕ & Εθνική Νομοθεσία

Κανονισμοί ΕΕ

- **Γενικός Κανονισμός για την Προστασία Δεδομένων – GDPR:** Κανονισμός 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32016R0679)

- **Network and Information Security - NIS 1:** Οδηγία 2016/1148 του Ευρωπαϊκού Κοινοβουλίου & του Συμβουλίου της 6ης Ιουλίου 2016 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016L1148)

- **Network and Information Security - NIS 2:** Οδηγία 2022/2555 του Ευρωπαϊκού Κοινοβουλίου & Του Συμβουλίου της 14ης Δεκεμβρίου 2022 σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση – κατάργηση της NIS 1 (https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32022L2555)

Εθνική Νομοθεσία

- **Νομοθεσία Προσωπικών Δεδομένων:**
  - **Νόμος 4624/2019, ΦΕΚ Α' 137/ 29.8.2019:** Ενσωμάτωση του Κανονισμού 2016/679/ΕΕ (https://www.dpa.gr/sites/default/files/2020-02/nomos_4624_2019.pdf)
  - **Νόμος 5169/2025, ΦΕΚ Α' 4/17.1.2025:** Κύρωση του από 10 Οκτωβρίου 2018 Τροποποιητικού Πρωτοκόλλου της Σύμβασης του Συμβουλίου της Ευρώπης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα. (https://ministryofjustice.gr/wp-content/uploads/2025/01/Nomos_5169_2025.pdf)

- **Ν. 4577, ΦΕΚ Α' 199/03.12.2018 - NIS 1:** Ενσωμάτωση στην Ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ (link)

- **Ν. 5160/2024, ΦΕΚ Α' 195/27.11.2024 - NIS 2:** Ενσωμάτωση στην Ελληνική νομοθεσία της Οδηγίας 2022/2555/ΕΕ (link)

- **ΚΥΑ 1689/2025, ΦΕΚ Β' 2186/06.05.2025:** Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας Βασικών και Σημαντικών Οντοτήτων (link)

- **ΚΥΑ 1990 /2025, ΦΕΚ Β ' 4241/04.08.2025 :** Δημιουργία ψηφιακής πλατφόρμας για την εγγραφή των βασικών και των σημαντικών οντοτήτων (link)

- **ΥΑ 1899/2025, ΦΕΚ Β' 4250/05.08.2025:** Καθορισμός προσόντων, καθηκόντων, ασυμβιβάστων και υποχρεώσεων των Υπεύθυνων Ασφαλείας Συστημάτων Πληροφορικής και Επικοινωνιών. (link)

Κανονισμοί ΕΕ - MDR & IVDR

- **Medical Device Regulation (MDR):** Κανονισμός (ΕΕ) 2017/745 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 5ης Απριλίου 2017, για τα ιατροτεχνολογικά προϊόντα
  - **Διέπει την κλινική έρευνα και τη διάθεση στην αγορά ιατροτεχνολογικών προϊόντων στην Ευρωπαϊκή Ένωση, ενισχύοντας τις απαιτήσεις ασφάλειας και επιδόσεων. Αντικατέστησε προηγούμενες οδηγίες και εισήγαγε αυστηρότερα μέτρα εποπτείας και συμμόρφωσης για τους κατασκευαστές και τα ιατροτεχνολογικά προϊόντα.**
  - **26/5/2021** τέθηκε σε ισχύ ο MDR, θα εφαρμοστεί καθολικά τέλη του **2028**
  - https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32016R0679

- **In Vitro Diagnostic Regulation (IVDR):** Εκτελεστικός κανονισμός (ΕΕ) 2017/2185 της Επιτροπής, της 23ης Νοεμβρίου 2017, σχετικά με τον κατάλογο των κωδικών και των τύπων τεχνολογικών προϊόντων στα οποία αυτοί αντιστοιχούν, με σκοπό τον προσδιορισμό του πεδίου εφαρμογής για το οποίο ορίζονται οι κοινοποιημένοι οργανισμοί στον τομέα των ιατροτεχνολογικών προϊόντων σύμφωνα με τον κανονισμό (ΕΕ) 2017/745 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και στον τομέα των in vitro διαγνωστικών ιατροτεχνολογικών προϊόντων σύμφωνα με τον κανονισμό (ΕΕ) 2017/746 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου
  - **Στόχος του είναι να εξασφαλίσει την ασφάλεια και την αποτελεσματικότητα αυτών των συσκευών μέσω αυστηρότερης εποπτείας και ταξινόμησης με βάση τα επίπεδα κινδύνου**
  - 26/5/2022 τέθηκε σε ισχύ ο IVDR, θα εφαρμοστεί καθολικά τέλη του **2028**
  - https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32016R0679

Ο Γενικός Κανονισμός για την Προστασία Προσωπικών Δεδομένων (GDPR)

- **Πεδίο Εφαρμογής**
- Ο ΓΚΠΔ καθορίζει λεπτομερώς τις απαιτήσεις για τη συλλογή, την αποθήκευση και τη διαχείριση προσωπικών δεδομένων από επιχειρήσεις και οργανισμούς **=> Κάθε επεξεργασία των Προσωπικών Δεδομένων Αυτοματοποιημένη και Μη**
- Στοχεύει στην προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών
- Οι απαιτήσεις ισχύουν για Ευρωπαϊκούς Οργανισμούς **Δημόσιους και Ιδιωτικούς** που επεξεργάζονται προσωπικά δεδομένα ατόμων στην ΕΕ, αλλά και για οργανισμούς εκτός της ΕΕ, οι οποίοι στοχεύουν σε άτομα εντός της επικράτειας της ΕΕ και προσφέρουν αγαθά ή υπηρεσίες σε αυτά ή ακόμα και αν παρακολουθούν τη διαδικτυακή τους συμπεριφορά
  - **Επομένως, η εξωεδαφική προσέγγιση της συμμόρφωσης με τον ΓΚΠΔ ορίζει ότι οι οργανισμοί, που δεν είναι εγκατεστημένοι στην ΕΕ, πρέπει να διορίσουν έναν εκπρόσωπο εντός της ΕΕ αν προσφέρουν υπηρεσίες εντός ΕΕ**

Χαρακτηρισμός Προσωπικών Δεδομένων

- Στον ΓΚΠΔ, καλείται «**Υποκείμενο των Δεδομένων**» το φυσικό πρόσωπο του οποίου τα προσωπικά δεδομένα συλλέγονται, διατηρούνται ή επεξεργάζονται,
- «**Δεδομένο Προσωπικού Χαρακτήρα**» συνιστά κάθε πληροφορία που αναφέρεται σε ένα ορισμένο πρόσωπο και με το οποίο μπορεί να προσδιοριστεί
- Τα προσωπικά δεδομένα διακρίνονται σε **Απλά** και **Ευαίσθητα**
- Ο νομοθέτης παρέχει στα ευαίσθητα προσωπικά δεδομένα **διευρυμένη προστασία, ορίζοντας αυστηρότερες προϋποθέσεις** για την πρόσβαση σε αυτά και την τήρηση αρχείων που να τα εμπεριέχουν

Χαρακτηρισμός Προσωπικών Δεδομένων

- **Απλά Προσωπικά Δεδομένα**
- Ταυτοποιούν ή δύνανται να Ταυτοποιήσουν άμεσα ή έμμεσα ένα φυσικό πρόσωπο π.χ.:
  - Ονοματεπώνυμο
  - Ημερομηνία γέννησης
  - Διεύθυνση κατοικίας
  - Αριθμός ταυτότητας, Διαβατηρίου, ΑΦΜ ή ΑΜΚΑ
  - Διεύθυνση email
  - Αρ. Τηλεφώνου
  - Διεύθυνση IP
  - Φωτογραφία προσώπου
  - Φυσικά χαρακτηριστικά
- Δεν αφορούν σε στοιχεία εταιρειών, Νομικών Προσώπων, ζώων, ούτε σε δεδομένα στατιστικής (π.χ. συγκεντρωτικά στοιχεία) από τα οποία δεν μπορούν πλέον να προσδιοριστούν τα υποκείμενα

- **Ευαίσθητα ή Ειδικές Κατηγορίες Προσωπικών Δεδομένων**
- Αφορούν την προσωπικότητα, τις πεποιθήσεις ή την υγεία και η επεξεργασία τους χρήζει ιδιαίτερης προσοχής, γιατί μπορούν να προκαλέσουν διακρίσεις ή σοβαρές συνέπειες για το άτομο π.χ.:
  - Φυλετική ή εθνική καταγωγή
  - Πολιτικές απόψεις
  - Θρησκευτικές ή φιλοσοφικές πεποιθήσεις
  - Συμμετοχή σε συνδικαλιστική οργάνωση
  - Δεδομένα υγείας (Διάγνωση, Ιατρικές Εξετάσεις, κτλ.)
  - Γενετικά και βιομετρικά δεδομένα (για ταυτοποίηση)
  - Σεξουαλική ζωή - σεξουαλικό προσανατολισμό
  - ***Ποινικό Μητρώο (Ποινικά Δεδομένα)***

Επεξεργασία Προσωπικών Δεδομένων

- **Κάθε πράξη ή σειρά πράξεων που πραγματοποιείται** με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η:
  - Συλλογή
  - Καταχώριση
  - Οργάνωση
  - Διάρθρωση
  - Αποθήκευση
  - Προσαρμογή ή η μεταβολή
  - Ανάκτηση
  - Αναζήτηση πληροφοριών
  - Χρήση
  - Κοινολόγηση με διαβίβαση
  - Διάδοση ή κάθε άλλη μορφή διάθεσης
  - Συσχέτιση ή ο συνδυασμός
  - Περιορισμός
  - Διαγραφή ή η καταστροφή

Αρχές που Διέπουν το Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (Άρθρο 5)

Νομιμότητα, αντικειμενικότητα και διαφάνεια (awfulness, fairness and transparency)

Υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων

Περιορισμός του σκοπού (purpose limitation)

Συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς

Ελαχιστοποίηση των δεδομένων(data minimisation)

Κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία

Αρχές που Διέπουν το Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (Άρθρο 5)

Ακρίβεια (accuracy)

Είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται (όσο το δυνατό άμεσα)

Περιορισμός της περιόδου αποθήκευσης (storage limitation)

Διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται

Ακεραιότητα και εμπιστευτικότητα (integrity and confidentiality)

Κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία

Λογοδοσία (accountability)

Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωση

Δικαιώματα Χρήστη

Διαφανής Ενημέρωση και ρυθμίσεις (αρ. 12)

- **Οι πληροφορίες στο Υποκείμενο παρέχονται με σαφή**, **κατανοητό** και **εύκολα προσβάσιμο** τρόπο, σε **απλή και κατανοητή γλώσσα**, είτε με **γραπτή μορφή είτε** με **ηλεκτρονικά μέσα** (π.χ. email, ιστοσελίδα). Η ενημέρωση γίνεται **εντός 1 μηνός** από την αίτηση του χρήστη κάθε καθυστέρηση πρέπει να αιτιολογείται. Ενημερώνουν για το σκοπό της συλλογής των δεδομένων, την αποθήκευσή τους, τη διατήρησή τους και το είδος τους

Δικαίωμα Ενημέρωσης (αρ. 13 & 14)

- Όταν τα δεδομένα συλλέγονται απευθείας από το υποκείμενο (π.χ. Online form, αίτηση κτλ), πρέπει ο υπεύθυνος να ενημερώσει από την αρχή για το σκοπό και την νομική βάση της επεξεργασίας.
- Όταν τα δεδομένα συλλέγονται χωρίς τη συμμετοχή του υποκειμένου (π.χ. μια διαφημιστική εταιρεία λαμβάνει από 3η πηγή email), τότε πρέπει αυτό να ενημερωθεί εντός 1 μηνός
- Εξαιρέσεις ισχύουν αν έχει γίνει ήδη η ενημέρωση, υφίσταται νομική υποχρέωση που απαγορεύει ή είναι δυσανάλογη η προσπάθεια ενημέρωσης με τα δεδομένα (π.χ. χιλιάδες email από Χρυσό Οδηγό ή ΓΕΜΗ)

Δικαιώματα Χρήστη

Δικαίωμα Πρόσβασης (αρ. 15)

Εφόσον δεν υπάρχει Νόμιμη Εξαίρεση (π.χ. εθνικό συμφέρον), πρέπει ο οργανισμός να σου επιβεβαιώσει αν τηρεί ή επεξεργάζεται τα δεδομένα σου καθώς και ποια είναι αυτά εντός 1 μήνα

Δικαίωμα Διόρθωσης (αρ. 16)

Αν τα προσωπικά δεδομένα που διατηρεί ένας οργανισμός είναι Λανθασμένα ή Ελλιπή, τότε το υποκείμενο μπορεί να ζητήσει τη διόρθωσή τους χωρίς καθυστέρηση

Δικαιώματα Χρήστη

Δικαίωμα Διαγραφής/Δικαίωμα στη «Λήθη» (αρ. 17)

Π.χ. διαγραφή από newsletter & διαγραφή των δεδομένων που σχετίζονται με τη συμμετοχή στη συνδρομή σε αυτό. Εξαίρεση οι λόγοι δημοσίου συμφέροντος, δημόσιας υγείας, νομικές αξιώσεις, δημοσιοποίηση πληροφοριών – ενημέρωση κοινού

Δικαίωμα Περιορισμού της Επεξεργασίας (αρ. 18)

Επιτρέπει στο υποκείμενο να ζητήσει αναστολή ή περιορισμό της επεξεργασίας των δεδομένων του, όταν αμφισβητεί την ακρίβεια ή την ανάγκη της επεξεργασίας. Ισχύει όταν τα δεδομένα δεν είναι πλέον απαραίτητα για τον αρχικό σκοπό, αλλά απαιτούνται για άσκηση δικαιωμάτων άλλων προσώπων ή νομικές αξιώσεις

Δικαίωμα Εναντίωσης (αρ. 21)

Το υποκείμενο μπορεί αντιταχθεί στην επεξεργασία των προσωπικών δεδομένων σε συγκεκριμένες περιπτώσεις, όπως όταν τα δεδομένα επεξεργάζονται για σκοπούς **άμεσης εμπορικής προώθησης**

Δικαιώματα Χρήστη

Δικαίωμα στην ανθρώπινη παρέμβαση σχετική με την αυτοματοποιημένη Λήψη Αποφάσεων, Κατάρτιση Προφίλ (αρ. 22)

Εάν μια απόφαση που επηρεάζει τον χρήστη βασίζεται αποκλειστικά σε αυτοματοποιημένα συστήματα (π.χ. αλγόριθμους ή τεχνητή νοημοσύνη), το υποκείμενο των δεδομένων μπορεί να ζητήσει ανθρώπινη παρέμβαση για να αναθεωρηθεί η απόφαση π.χ. η κατάρτιση προφίλ για αγοραστικές συνήθειες που μπορεί να οδηγήσει σε διακρίσεις ή αρνητικές συνέπειες για το άτομο.

Δικαίωμα Ενημέρωσης σε Περιστατικό Παραβίασης (αρ. 34)

Αν η παραβίαση αφορά ευαίσθητα δεδομένα, η ενημέρωση προς τα υποκείμενα είναι υποχρεωτική, ενώ σε άλλες περιπτώσεις (όταν δεν υπάρχει κίνδυνος) μπορεί να μην απαιτείται η ενημέρωση. Ο οργανισμός είναι υποχρεωμένος να ενημερώσει τα άτομα που επηρεάζονται, εκτός εάν η παραβίαση δεν ενέχει κανένα κίνδυνο για τα δικαιώματά τους και τις ελευθερίες τους εντός 72 ωρών.

Υπεύθυνος Επεξεργασίας (άρθρα 25 & 26)

- Ο «**Υπεύθυνος επεξεργασίας**» (**controller**) είναι το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, ο οργανισμός ή η υπηρεσία που καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας των προσωπικών δεδομένων
- Αυτός που αποφασίζει γιατί και πώς θα συλλεχθούν και θα χρησιμοποιηθούν τα δεδομένα
- Σε ένα **νοσοκομείο**, ο **υπεύθυνος επεξεργασίας** είναι συνήθως το **ίδιο το νοσοκομείο** (ως νομικό πρόσωπο), δηλαδή η **διοίκηση** που το λειτουργεί **και καθορίζει τους σκοπούς** (π.χ. παροχή υγειονομικής περίθαλψης) και τα **μέσα επεξεργασίας** (π.χ. ιατρικοί φάκελοι, ηλεκτρονικό σύστημα) των προσωπικών δεδομένων των ασθενών

- Δύο ή περισσότεροι οργανισμοί είναι «**Κοινοί υπεύθυνοι επεξεργασίας**» (**joint controllers)** όταν **συνεργάζονται στενά** και **αποφασίζουν μαζί** για τη συλλογή και χρήση των δεδομένων.
- **Παράδειγμα: Νοσοκομείο & ΗΔΙΚΑ (Ηλεκτρονική Διακυβέρνηση Κοινωνικής Ασφάλισης ΑΕ)**
- Το νοσοκομείο καταχωρεί τα ιατρικά δεδομένα του ασθενή (π.χ. συνταγές, εξετάσεις)
- Η ΗΔΙΚΑ διαχειρίζεται τα δεδομένα μέσω της ηλεκτρονικής πλατφόρμας συνταγογράφησης και άλλων πληροφοριακών συστημάτων (π.χ. Αποθετήριο Εξετάσεων, παρέχει το H-Cloud για τη φιλοξενία του πληροφοριακού συστήματος του Νοσοκομείου)

Ο Εκτελών την Επεξεργασία (άρθρο 28)

- **Εκτελών την Επεξεργασία** (**Processor**) είναι το φυσικό ή νομικό πρόσωπο που **επεξεργάζεται προσωπικά δεδομένα για λογαριασμό του Υπευθύνου Επεξεργασίας**, **χωρίς** να καθορίζει **ούτε τον σκοπό** ούτε τα **μέσα** της επεξεργασίας
- Π.χ. Ένα νοσοκομείο συνεργάζεται με ιδιωτική εταιρεία πληροφορικής για την τεχνική υποστήριξη και την παροχή το Πληροφοριακού Συστήματος του ηλεκτρονικού φακέλου ασθενούς
- Το νοσοκομείο είναι υπεύθυνος επεξεργασίας
- Η εταιρεία πληροφορικής είναι ο εκτελών την επεξεργασία

- Ο εκτελών πρέπει:
  - Να επεξεργάζεται δεδομένα μόνο με γραπτές εντολές
  - Να διασφαλίζει εμπιστευτικότητα και ασφάλεια
  - Να μην αναθέτει υπεργολαβία χωρίς άδεια
  - Να βοηθά τον υπεύθυνο με αιτήματα πολιτών (π.χ. διαγραφή, πρόσβαση)
  - Να διαγράφει ή επιστρέφει τα δεδομένα μετά τη λήξη της συνεργασίας

Υπεύθυνος Προστασίας Δεδομένων - DPO

- Ο **DPO** (**Data Protection Officer** – **Υπεύθυνος Προστασίας Δεδομένων**) είναι το πρόσωπο που έχει την ευθύνη να **επιβλέπει τη συμμόρφωση ενός οργανισμού με τον ΓΚΠΔ** και να λειτουργεί ως **σημείο επαφής** μεταξύ της επιχείρησης, των υποκειμένων των δεδομένων και της Αρχής Προστασίας Δεδομένων
- Σύμφωνα με **Άρθρο 37** του Κανονισμού, ο ορισμός DPO είναι **υποχρεωτικός** όταν επεξεργασία γίνεται από δημόσια αρχή (π.χ. νοσοκομείο, Δήμος), η **κύρια δραστηριότητα περιλαμβάνει συστηματική και εκτεταμένη παρακολούθηση ατόμων** και η επεξεργασία αφορά ευαίσθητα δεδομένα (π.χ. υγείας, δημοτολόγιο) σε μεγάλη κλίμακα

- Ο DPO μπορεί να είναι **εσωτερικός εργαζόμενος** ή **εξωτερικός συνεργάτης** και πρέπει να έχει **εξειδικευμένες γνώσεις** και **Πιστοποίηση** στον τομέα της προστασίας δεδομένων με αρμοδιότητες για την:
  - Ενημέρωση & συμβουλευτική για την εφαρμογή του GDPR
  - Παρακολούθηση συμμόρφωσης του οργανισμού (π.χ. πολιτικές, εκπαιδεύσεις)
  - Έλεγχος DPIA (Εκτίμησης Αντικτύπου στην Προστασία Δεδομένων)
  - Επικοινωνία με την Αρχή Προστασίας Δεδομένων.
  - Υποστήριξη υποκειμένων των δεδομένων (σε αιτήματα πρόσβασης, διαγραφής κ.λπ.)

- Δεν εγκρίνει ή απορρίπτει επεξεργασίες
- Δε φέρει νομική ευθύνη για παραβιάσεις
- Δεν αποφασίζει για σκοπούς και μέσα

Συγκατάθεση του Υποκειμένου των Δεδομένων

- Κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν

- Ρητή υποχρέωση του υπευθύνου επεξεργασίας να μπορεί να αποδείξει ότι έχει λάβει έγκυρη συγκατάθεση
- Η δυνατότητα ανάκλησης της συγκατάθεσης είναι απαραίτητη

Αρχή Προστασίας Προσωπικών Δεδομένων

- Αποτελεί την Ανεξάρτητη Δημόσια Αρχή που συγκροτείται από κάθε κράτος μέλος
- Ο ΓΚΠΔ προσδιορίζει ότι πρέπει να υπάρχει (τουλάχιστον) μια σε κάθε κράτος μέλος
- Τα κράτη μέλη οφείλουν να προσδιορίσουν το πλήρες καθεστώς λειτουργίας και ανεξαρτησίας
- Η Αρχή Προστασίας Προσωπικών Δεδομένων προβλέπεται στο Σύνταγμα και το καθεστώς της διέπεται και από το ν. 3051/2002
- Εχει ως αποστολή της την εποπτεία της εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων, του ν. 4624/2019, του ν. 3471/2006 και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και την ενάσκηση των αρμοδιοτήτων που της ανατίθενται κάθε φορά

- https://www.dpa.gr/

Online Toolkits

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΕΝΗΜΕΡΩΣΗ ΣΕ ΠΕΡΙΠΤΩΣΗ ΠΑΡΑΒΙΑΣΗΣ ΔΕΔΟΜΕΝΩΝ

- **Υποχρέωση** να ενημερώνεται η **Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)** όταν υπάρχει **παραβίαση δεδομένων προσωπικού χαρακτήρα**, **εντός 72 ωρών** από τη στιγμή που ο υπεύθυνος επεξεργασίας την αντιληφθεί — σύμφωνα με το **Άρθρο 33 του ΓΚΠΔ**
- https://www.dpa.gr/el/foreis/asfaleia_dedomenwn/gnwstopoiisi_paraviasis
- **Το Άρθρο 34 του ΓΚΠΔ προβλέπει** όταν η παραβίαση ενδέχεται να θέσει σε **υψηλό κίνδυνο** τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων τα οποία αφορά το περιστατικό, τότε ο υπεύθυνος επεξεργασίας οφείλει να ανακοινώνει αμελλητί την παραβίαση και στα πρόσωπα αυτά.

- Η Αρχή δύναται σε κάθε περίπτωση να δώσει εντολή στον υπεύθυνο επεξεργασίας να ενημερώσει τα φυσικά πρόσωπα για το περιστατικό (**άρθρο 58 παρ. 2 ε' ΓΚΠΔ**).
- **ΠΡΟΣΟΧΗ**
- **Αν η παραβίαση προέκυψε ως απότοκο Κυβερνοεπίθεσης τότε ο οργανισμός οφείλει να ενημερώσει και την Εθνική Αρχή Κυβερνοασφάλειας αρχικά εντός 24 ωρών**
- **Εφόσον έχει θέσει σε κίνδυνο τη Διαθεσιμότητα, Αυθεντικότητα, Ακεραιότητα, Εμπιστευτικότητα**
- **https://cyber.gov.gr/kyvernoepitheseis/anafora-symvanton/**
- **incident[@]cyber.gov.gr**

ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟ ΑΣΦΑΛΕΙΑΣ

Τί ορίζεται Παραβίαση Προσωπικών Δεδομένων;

Η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία

Σχηματική Αναπαράσταση

Παραβίαση Προσωπικών Δεδομένων βάσει CIA

Ποιος Κοινοποιεί;

Ο Υπεύθυνος Επεξεργασίας & ο Εκτελών την Επεξεργασία

Πότε Κοινοποιεί;

Εντός 72 ωρών

Ποιόν Κοινοποιεί;

Την ΑΧΠΔ & Τα φυσικά πρόσωπα για την αυτοπροστασία τους (ΕΑΚ μόνο σε περίπτωση Κυβερνοεπίθεσης)

Τί Κοινοποιεί;

1. Χρονοδιάγραμμα Περιστατικού
2. Πληροφορίες για τη Φύση του Περιστατικού (CIA)
3. Είδος Προσωπικών Δεδομένων
4. Πρόσωπα που αφορά
5. Ληφθέντα ή Προτεινόμενα Μέτρα

Παραδείγματα

- Ransomware προσβάλει Η/Υ και κρυπτογραφεί τα αρχεία με προσωπικά δεδομένα
- Δεν υφίσταται backup για τα δεδομένα αυτά
- Η ανάλυση έδειξε ότι αυτή ήταν η μόνη περίπτωση κυβερνοεπίθεσης
  - Ενημερώνω την ΑΧΠΔ; => ΝΑΙ
  - Ενημερώνω τα Φυσικά Πρόσωπα; => ΝΑΙ
  - Ενημερώνω την ΕΑΚ; => ΝΑΙ

https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_el.pdf

- Το Αρχείο backup με προσωπικά δεδομένα αποθηκεύεται κρυπτογραφημένα με ισχυρό αλγόριθμο κρυπτογράφησης σε USB stick
- Πραγματοποιήθηκε κλοπή του USB stick
  - Ενημερώνω την ΑΧΠΔ; => ΟΧΙ
  - Ενημερώνω τα Φυσικά Πρόσωπα; => ΟΧΙ
  - Ενημερώνω την ΕΑΚ; => ΔΙΑΚΡΙΤΙΚΗ ΕΥΧΕΡΕΙΑ – ΑΝΑΛΟΓΩΣ ΜΕ ΤΗΝ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΤΟΥ ΟΡΓΑΝΙΣΜΟΥ
  - Ενημερώνω την Ελληνική Αστυνομία; => ΝΑΙ

Ειδικές Περιπτώσεις - Ι

- Απλά δεδομένα προσωπικού χαρακτήρα, όπως ο ΑΜΚΑ ή το ονοματεπώνυμο, εφόσον αναφέρονται σε ασθενείς θεωρούνται και αυτά ευαίσθητα δεδομένα προσωπικού χαρακτήρα, ως τμήμα του ιατρικού φακέλου του ασθενούς, δηλαδή ως πληροφορίες που αφορούν την κατάσταση της υγείας του υποκειμένου τους
- Ο Κώδικας Ιατρικής Δεοντολογίας ορίζει το χρόνο τήρησης των ιατρικών δεδομένων (άρ. 14 παρ. 4 Ν. 3418/2005) (α) στα ιδιωτικά ιατρεία και τις λοιπές μονάδες πρωτοβάθμιας φροντίδας υγείας του ιδιωτικού τομέα, για μία δεκαετία από την τελευταία επίσκεψη του ασθενή και β) σε κάθε άλλη περίπτωση, για μία εικοσαετία από την τελευταία επίσκεψη του ασθενή)
- Χαρακτηριστικές περιπτώσεις λειτουργίας συστημάτων βιντεοεπιτήρησης για τον ιατρικούς σκοπούς είναι η επιτήρηση βαριά ψυχικά ή νοητικά ασθενούς που μπορεί να προκαλέσει βλάβη στην υγεία του ή σε τρίτους ή η επιτήρηση ασθενών σε Μονάδες Εντατικής Θεραπείας.
- Ο υπεύθυνος επεξεργασίας οφείλει να έχει λάβει την άδεια της Αρχής για την επεξεργασία ευαίσθητων δεδομένων με σκοπό την παροχή υπηρεσιών υγείας. Στην άδεια αυτή πρέπει να περιλαμβάνονται και τα δεδομένα που λαμβάνονται από το σύστημα βιντεοεπιτήρησης.

Πηγή: https://www.moh.gov.gr/articles/gdpr/5667-syxnes-erwthseis

Ειδικές Περιπτώσεις - ΙΙ

- Η συγκατάθεση του υποκειμένου είναι απλώς μία από τις δυνατές νομικές βάσεις για την επεξεργασία δεδομένων του προσωπικού χαρακτήρα και καταρχήν δεν απαιτείται στον τομέα παροχής υπηρεσιών υγείας (Αρ. 6 & 9). **Γενική Αρχή: Η ΕΠΕΞΕΡΓΑΣΙΑ ΧΩΡΙΣ ΝΟΜΙΚΗ ΒΑΣΗ ΠΑΡΑΒΙΑΖΕΙ ΤΟΝ ΓΚΠΔ**
- **Στον τομέα παροχής υπηρεσιών υγείας κατεξοχήν ενδεδειγμένες (ως ειδικές) νομικές βάσεις για την επεξεργασία δεδομένων των υποκειμένων (κυρίως των ασθενών, αλλά όχι μόνο αυτών) είναι**:
  - η παροχή ιατρικών υπηρεσιών κατά το άρθρο 9 παρ. 2 στοιχ. (η΄) του ΓΚΠΔ, είτε η εν λόγω παροχή ιατρικών υπηρεσιών στηρίζεται ειδικότερα σε νομικές ρυθμίσεις για την παροχή υπηρεσιών φροντίδας υγείας από φορείς του Δημοσίου τομέα είτε σε σύμβαση παροχής ιατρικών υπηρεσιών από φορέα του ιδιωτικού τομέα
  - η εκπλήρωση δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας κατά το άρθρο 9 παρ. 2 στοιχ. (θ΄) του ΓΚΠΔ, και όχι η συγκατάθεση του υποκειμένου (ιδίως του ασθενούς)

Πηγή: https://www.moh.gov.gr/articles/gdpr/5667-syxnes-erwthseis

Πότε δεν Εφαρμόζεται ο ΓΚΠΔ

- Σε Δημόσιες αρχές με εξαίρεση την επεξεργασία για σκοπούς πρόληψης, διερεύνησης κλπ. εγκλημάτων και δημόσιας ασφάλειας (Οδηγία 2016/680/ΕΕ)
- Σε Δικαστήρια με εξαίρεση την άσκηση δικαιοδοτικής αρμοδιότητας
- Όταν δεν καταλαμβάνεται η επεξεργασία για αποκλειστικά προσωπικούς/οικιακούς σκοπούς
- Όταν τα υποκείμενα που δε βρίσκονται εν ζωή
- Όταν το υποκείμενο των δεδομένων είναι νομικό πρόσωπο
- Όταν η επεξεργασία γίνεται από πρόσωπο που ενεργεί για σκοπούς εκτός του εμπορικού, επιχειρηματικού ή επαγγελματικού του πεδίου

Συσχέτιση με Κυβερνοασφάλεια – Άρθρο 25 ΓΚΠΔ

- **Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού (Data protection by design and by default)**
- ο υπεύθυνος επεξεργασίας εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, **κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων**, όπως η ελαχιστοποίηση των δεδομένων, και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία κατά τρόπο, ώστε να πληρούνται οι απαιτήσεις του παρόντος κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων
- Εφαρμόζει κατάλληλα **τεχνικά και οργανωτικά μέτρα** για να διασφαλίζει ότι, εξ ορισμού, υφίστανται επεξεργασία **μόνο τα δεδομένα προσωπικού χαρακτήρα** που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας
- Αυτή η υποχρέωση ισχύει για το εύρος των δεδομένων προσωπικού χαρακτήρα που συλλέγονται, τον βαθμό της επεξεργασίας τους, την περίοδο αποθήκευσης και την προσβασιμότητά τους
- Ειδικότερα, τα εν λόγω μέτρα διασφαλίζουν ότι, εξ ορισμού, τα δεδομένα προσωπικού χαρακτήρα δεν καθίστανται προσβάσιμα χωρίς την παρέμβαση του φυσικού προσώπου σε αόριστο αριθμό φυσικών προσώπων

Συσχέτιση με Κυβερνοασφάλεια – Άρθρο 25 ΓΚΠΔ

- **Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού (Data protection by design and by default)**
- ο υπεύθυνος επεξεργασίας εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η **ψευδωνυμοποίηση**, **αρχεία καταγραφής (logs)** σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων, και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία κατά τρόπο, ώστε να πληρούνται οι απαιτήσεις του παρόντος κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων
- Εφαρμόζει κατάλληλα **τεχνικά και οργανωτικά μέτρα** για να διασφαλίζει ότι, εξ ορισμού, υφίστανται επεξεργασία **μόνο τα δεδομένα προσωπικού χαρακτήρα** που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας
- Αυτή η υποχρέωση ισχύει για το εύρος των δεδομένων προσωπικού χαρακτήρα που συλλέγονται, τον βαθμό της επεξεργασίας τους, την περίοδο αποθήκευσης και την προσβασιμότητά τους
- Ειδικότερα, τα εν λόγω μέτρα διασφαλίζουν ότι, εξ ορισμού, τα **δεδομένα προσωπικού χαρακτήρα δεν καθίστανται προσβάσιμα χωρίς την παρέμβαση του φυσικού προσώπου σε αόριστο αριθμό φυσικών προσώπων**

Ορισμοί

Protection by Design

- Ενσωματωμένα εξαρχής μέτρα και τεχνικές ασφάλειας σε νέες τεχνολογίες, προϊόντα, υπηρεσίες
- Χρήση προστασίας δεδομένων κατά την επεξεργασία

Protection by Default

- Μέτρα για τήρηση περιορισμών επεξεργασίας πάντα
- Εφαρμογή τους καθολικά, σε κάθε επεξεργασία

Παραδείγματα

- **Προστασία δεδομένων ήδη από τον σχεδιασμό**
- Χρήση ψευδωνυμοποίησης (αντικατάσταση προσωπικά ταυτοποιήσιμου υλικού με τεχνητά αναγνωριστικά στοιχεία) και κρυπτογράφησης (κωδικοποίηση μηνυμάτων έτσι ώστε μόνο όσοι είναι εξουσιοδοτημένοι να μπορούν να τα διαβάζουν)
- **Νοσοκομεία:** Η υιοθέτηση νέου Πληροφοριακού Συστήματος Ηλεκτρονικού Φακέλου Ασθενούς, θα πρέπει από την αρχή να:
  - ✓ Ορίσει ποιοι ρόλοι έχουν πρόσβαση σε ποια δεδομένα
  - ✓ Κρυπτογραφήσει τα δεδομένα
  - ✓ Αποθηκεύει μόνο τα απολύτως απαραίτητα στοιχεία για κάθε χρήση

- **Προστασία δεδομένων εξ ορισμού**
- Μια πλατφόρμα κοινωνικής δικτύωσης θα πρέπει να ενθαρρύνεται να ορίζει τις ρυθμίσεις των προφίλ των χρηστών έτσι ώστε να προστατεύουν όσο το δυνατόν περισσότερο το ιδιωτικό απόρρητο, για παράδειγμα, περιορίζοντας από την αρχή την προσβασιμότητα στα προφίλ των χρηστών έτσι ώστε να μην είναι προσβάσιμα εξ ορισμού από αόριστο αριθμό ατόμων
- **Νοσοκομεία:** Ηλ. Σύστημα Ραντεβού Ασθενών:
  - ✓ Μόνο τα βασικά δεδομένα συλλέγονται
  - ✓ Δεν εμφανίζονται ευαίσθητα δεδομένα - Οι υπάλληλοι της γραμματείας βλέπουν μόνο το όνομα και την ώρα του ραντεβού, όχι ποια είναι η ιατρική κατάσταση του ασθενούς
  - ✓ Ασφαλής διαχείριση στοιχείων επικοινωνίας:

https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_el

Παράδειγμα – Τηλεϊατρικής

- **Καθορισμός όρων, προϋποθέσεων και διαδικασίας διαχείρισης Εφαρμογής Τηλεϊατρικής κατ' εφαρμογή της παρ. 3 του άρθρου 5 του Κώδικα Ιατρικής Δεοντολογίας (Ν. 3418/2005, Α'287)**
- **Άρθρο 8 - Μέτρα για την προστασία και την ασφάλεια των δεδομένων προσωπικού χαρακτήρα**
- Οι εφαρμογές τηλεϊατρικής θα πρέπει να διαθέτουν τις απαραίτητες λειτουργικότητες σε ό,τι αφορά την εξ αποστάσεως παρακολούθηση και υποστήριξη των ασθενών διασφαλίζοντας την ασφάλεια, την προστασία, την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, καθώς και κάθε άλλο ζήτημα που αφορά την ομαλή λειτουργία τους

https://www.kodiko.gr/nomothesia/document/1127019/yp.-apofasi-7686-2025

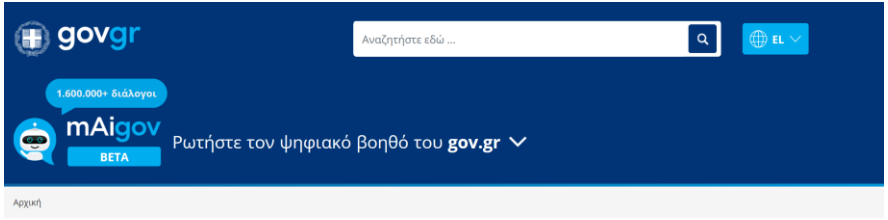
- Η επεξεργασία των δεδομένων **προσωπικού χαρακτήρα των συμβεβλημένων ιατρών από τον δικαιούχο λειτουργίας των εφαρμογών τηλεϊατρικής**, ως υπεύθυνο επεξεργασίας, θεμελιώνεται στο στοιχ. (β) της παρ. 1 του άρθρου 6 του ΓΚΠΔ (GDPR) («β) **η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης**»)
- Πληροφορίες από τα ιατρικά αρχεία που τηρούν οι ιατροί που παρέχουν υπηρεσίες τηλεϊατρικής υπό την έννοια της παρούσας, ως υπεύθυνοι επεξεργασίας, δύνανται να χορηγηθούν για σκοπούς αρχειοθέτησης για το δημόσιο συμφέρον ή για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς υπό τους όρους και τις προϋποθέσεις της παρ. 1 του άρθρου 89 του ΓΚΠΔ (GDPR) και σχετικών εθνικών ρυθμίσεων, τηρουμένων ιδίως των όρων **της ανωνυμοποίησης ή της ψευδωνυμοποίησης**

Ιστοσελίδες & ΓΚΠΔ

- **Η Πολιτική Ασφάλειας ή Απορρήτου** είναι ένα κρίσιμο έγγραφο που περιγράφει πώς μια ιστοσελίδα ή πλατφόρμα διαχειρίζεται τα προσωπικά δεδομένα των χρηστών της σύμφωνα με τους κανονισμούς του ΓΚΠΔ
- Η πολιτική αυτή πρέπει να διασφαλίζει ότι η ιστοσελίδα προστατεύει τα δεδομένα των χρηστών, ενημερώνει για τις διαδικασίες που ακολουθεί και προσφέρει τη δυνατότητα στους χρήστες να ασκήσουν τα δικαιώματά τους πρέπει να είναι εμφανής στην ιστοσελίδα και να ενημερώνει τους χρήστες για:
  - ✓ Στοιχεία Υπευθύνου Επεξεργασίας (Επιχείρησης)
  - ✓ Στοιχεία DPO
  - ✓ Περιγραφή των Προσωπικών Δεδομένων που συλλέγονται
  - ✓ Σκοποί Συλλογής και Επεξεργασίας των Προσωπικών Δεδομένων
  - ✓ Διάρκεια αποθήκευσης των Προσωπικών Δεδομένων
  - ✓ Η Νόμιμη βάση Επεξεργασίας
  - ✓ Διαχείριση Cookies ή Καταγραφής IP (Δυνατότητα του χρήστη να αποδεχτεί ή να απορρίψει τα cookies)
  - ✓ Κρυπτογράφηση των δεδομένων με SSL
  - ✓ Που διαβιβάζονται τα Προσωπικά Δεδομένα που συλλέγονται και για ποιο λόγο
  - ✓ Μέτρα προστασίας (περίπτωση eshop)
  - ✓ Λόγοι αποκάλυψής Προσωπικών Δεδομένων
  - ✓ Τα Δικαιώματα των Υποκειμένων
  - ✓ Αναθεωρήσεις και αριθμό Έκδοσης
  - ✓ Διαχείριση Παραβιάσεων Δεδομένων

Παραδείγματα

- https://www.gov.gr/info/politiki-aporritou



Σχετικά με το gov.gr

Γενικοί Όροι & Πολιτικές Χρήσης

Πολιτική Προστασίας Προσωπικών Δεδομένων

Δήλωση προσβασιμότητας

Πολιτική χρήσης mAIgov

Πολιτική Προστασίας Προσωπικών Δεδομένων

Πολιτική Προστασίας Προσωπικών Δεδομένων
της Ενιαίας Ψηφιακής Πύλης της Δημόσιας Διοίκησης: www.gov.gr

1. ΕΙΣΑΓΩΓΗ

Στην Ευρωπαϊκή Ένωση εφαρμόζεται από τις 25 Μαΐου 2018 ο Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων – Κανονισμός ΕΕ 2016/679 (στο εξής «ΓΚΠΔ»). Για το κείμενο του Κανονισμού μπορείτε να επιλέξετε την διεύθυνση URL: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016R0679.

Η παρούσα Πολιτική Προστασίας Προσωπικών Δεδομένων (εφεξής η «Πολιτική Δεδομένων» ή «ΠΠΠΔ») αφορά την Ενιαία Ψηφιακή Πύλη της Δημόσιας Διοίκησης (εφεξής "η Πύλη") του Υπουργείου Ψηφιακής Διακυβέρνησης (εφεξής "το Υπουργείο"), που λειτουργεί υπό το όνομα χώρου: www.gov.gr.

Το Υπουργείο αποδίδει ιδιαίτερη σημασία στην προστασία των προσωπικών δεδομένων των πολιτών, αλλά και οιωνδήποτε προσώπων επισκέπτονται τον παρόντα διαδικτυακό τόπο. Για το λόγο αυτό έχει εκπονήσει την παρούσα Πολιτική Προστασίας Δεδομένων προκειμένου να ενημερώσει τα ανωτέρω πρόσωπα σχετικά με τον τρόπο συλλογής, χρήσης και κοινοποίησης των προσωπικών τους δεδομένων.

2. ΟΡΙΣΜΟΙ ΓΙΑ ΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ

(Σημ.: Οι ορισμοί ακολουθούν το άρ. 4 του ΓΚΠΔ)

«**Προσωπικά Δεδομένα**»: κάθε πληροφορία μέσω της οποίας είναι ταυτοποιήσιμο ή μπορεί

- https://www.auth.gr/gdpr/

Προσωπικά Δεδομένα

Σας ενημερώνουμε ότι έχει οριστεί Υπεύθυνη Προστασίας Δεδομένων (ΥΠΔ /DPO) για το ΑΠΘ η κα Κορνηλία Βικελίδου (ΑΔΑ: ΨΥ5Φ46Ψ8ΧΒ-0Σ7), κατεφαρμογή των διατάξεων των άρθρων 37 έως και 39 του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία δεδομένων.

Στοιχεία επικοινωνίας:
Email: data.protection(at)auth.gr
Τηλ: 2310996200

Σχετικά έγγραφα:

Πολιτική Προστασίας ΑΠΘ

Δήλωση ΑΠΘ για την τηλεκπαίδευση

Πολιτική για τη διενέργεια εξετάσεων με χρήση εξ αποστάσεως μεθόδων αξιολόγησης

Εκτίμηση Ελλείψεων – GAP Analysis

- Αποτελεί απαραίτητο εργαλείο για τη συμμόρφωση του οργανισμού με ΓΚΠΔ
- Είναι μια κρίσιμη διαδικασία για τον εντοπισμό και την αποκατάσταση των διαφορών (ή "κενού") που μπορεί να υπάρχουν μεταξύ των πρακτικών και διαδικασιών ενός οργανισμού και των απαιτήσεων του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR).
- Αναλύει την υφιστάμενη κατάσταση του οργανισμού σχετικά με τη συμμόρφωση με το GDPR και εντοπίζει τις αδυναμίες ή ελλείψεις που πρέπει να καλυφθούν προκειμένου να διασφαλιστεί η πλήρης συμμόρφωση με τον κανονισμό

- Περιλαμβάνει κυρίως την αξιολόγηση του τρόπου με τον οποίο πραγματοποιούνται:
- **Χαρτογράφηση Δεδομένων και Επεξεργασία**
- **Συγκατάθεση και Δικαιώματα Υποκειμένων Δεδομένων**
- **Πολιτικές Απορρήτου και Επικοινωνία**
- **Ασφάλεια Δεδομένων και Αντίδραση σε Παραβίαση**
- **Μεταφορά Δεδομένων και Τρίτα Μέρη**
- **Αξιολογήσεις Επιπτώσεων στην Προστασία Δεδομένων**
- **Υπεύθυνος Προστασίας Δεδομένων (DPO) και Λογοδοσία**

Εκτίμηση Αντικτύπου σχετικά με την προστασία δεδομένων (Άρθρο 35)

- Όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους

- Απαιτείται στις περιπτώσεις:
  - συστηματικής και εκτενούς αξιολόγησης πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο
  - μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων
  - συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα

Εκτίμηση Αντικτύπου σχετικά με την προστασία δεδομένων (Άρθρο 35)

- Ο υπεύθυνος επεξεργασίας έχει την υποχρέωση **εκτίμησης των κινδύνων** για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και τον **προσδιορισμό των ενδεδειγμένων μέτρων** για τη **μείωση αυτών σε αποδεκτό επίπεδο** προκειμένου για την απόδειξη της συμμόρφωσης προς τον ΓΚΠΔ
- Εκτίμηση Αντικτύπου Προσωπικών Δεδομένων (ΕΑΠΔ)
- Data Protection Impact Assessment (DPIA)
- Στόχος η αντιμετώπιση των Κινδύνων με μέτρα για την
  - Μείωση
  - Διατήρηση
  - Αποφυγή
  - Μετάθεση

Η μελέτη ΕΑΠΔ περιέχει τουλάχιστον τα ακόλουθα (άρθρο 35 παρ. 7 του ΓΚΠΔ):

- **συστηματική περιγραφή** των πράξεων επεξεργασίας και των σκοπών της επεξεργασίας,
- εκτίμηση της **αναγκαιότητας και της αναλογικότητας** των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς,
- εκτίμηση **των κινδύνων** για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων,
- τα **προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων**, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφαλείας, ώστε να διασφαλίζεται η προστασία των δεδομένων και να αποδεικνύεται η συμμόρφωση προς τον ΓΚΠΔ

Διαδικασία

- Ορισμός της διαδικασίας επεξεργασίας και των λειτουργιών που λαμβάνουν χώρα (π.χ.)

PROCESSING OPERATION DESCRIPTION	EMPLOYEES PAYROLL MANAGEMENT	
Personal Data Processed	Contact information (last and first name, address, telephone number,) social security number, taxation Identifier, date of employment, salary information	
Processing Purpose	Payroll management (payment of salaries, benefits and social security contributions)	
Data Subject	Employees	
Processing Means	Human Resources IT System	
Recipients of the Data	External	Financial Institutions
	External	Social Insurance Schemes
Data Processor Used	In-house (no data processor)	

- Τομείς και Επίπεδα Ασφαλείας που πρέπει να τηρηθούν

https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

Διαδικασία

- Διαχείριση Κινδύνων Ασφαλείας

LEVEL OF IMPACT	DESCRIPTION
Low	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc.).
Very high	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

Διαδικασία

- Διαστασιοποίηση Απειλών και της Πιθανότητας Εμφάνισης
  - Network & technical resources
  - Processes/Procedures related to the processing of personal data
  - Parties/People involved in the processing of personal data
  - Business sector and scale of processing

- Εκτίμηση της Πιθανότητας Εμφάνισης Απειλής:
  - **Χαμηλή (1):** Η απειλή έχει χαμηλή πιθανότητα να πραγματοποιηθεί
  - **Μεσαία (2):** Η απειλή έχει βάσιμη πιθανότητα να πραγματοποιηθεί
  - **Υψηλή (3):** Η απειλή είναι πολύ πιθανόν να πραγματοποιηθεί

ASSESSMENT AREA	PROBABILITY	
	LEVEL	SCORE
NETWORK AND TECHNICAL RESOURCES	☐ Low	1
	☐ Medium	2
	☐ High	3
PROCESSES/PROCEDURES RELATED TO THE PROCESSING OF PERSONAL DATA	☐ Low	1
	☐ Medium	2
	☐ High	3
PARTIES/PEOPLE INVOLVED IN THE PROCESSING OF PERSONAL DATA	☐ Low	1
	☐ Medium	2
	☐ High	3
BUSINESS SECTOR AND SCALE OF PROCESSING	☐ Low	1
	☐ Medium	2
	☐ High	3

https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

Διαδικασία

- Αξιολόγηση του Ρίσκου

IMPACT LEVEL

THREAT OCCURRENCE PROBABILITY	Low	Medium	High / Very High
Low			
Medium			
High			

Legend

Low Risk *Medium Risk* *High Risk*

https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

Εργαλεία Ανοικτού Λογισμικού για DPIA

- **CNIL** της Γαλλικής Αρχής (https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment) έχει ως στόχο να βοηθήσει τους υπευθύνους επεξεργασίας να διενεργήσουν ΕΑΠΔ, είναι διαθέσιμο και στην ελληνική γλώσσα

- Πληροφορίες στην ΑΧΠΔ (https://www.dpa.gr/foreis/ektimisi_adiktipou_kai_diavouleush/ektimisi_adiktipou)

Αρχείο Δραστηριότητας Επεξεργασίας

Δεν εφαρμόζεται σε επιχείρηση ή οργανισμό που απασχολεί λιγότερα από 250 άτομα, εκτός εάν η διενεργούμενη επεξεργασία ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων

Υπεύθυνος επεξεργασίας					
Όνομα και στοιχεία επικοινωνίας		Υπεύθυνος Προστασίας Δεδομένων (εφόσον υπάρχει)		Εκπρόσωπος (εφόσον υπάρχει)	
Όνομα		Ονοματεπώνυμο		Ονοματεπώνυμο	
Ταχυδρομική Διεύθυνση		Ταχυδρομική Διεύθυνση		Ταχυδρομική Διεύθυνση	
Ηλεκτρονική Διεύθυνη		Ηλεκτρονική Διεύθυνη		Ηλεκτρονική Διεύθυνη	
Τηλέφωνο		Τηλέφωνο		Τηλέφωνο	

Αρχείο Δραστηριοτήτων Επεξεργασίας (Άρ. 30 του Κανονισμού					
Αρμόδιο Τμήμα	Σκοπός της επεξεργασίας	Όνομα και στοιχεία επικοινωνίας του από κοινού υπευθύνου επεξεργασίας (αν υπάρχει)	Κατηγορίες υποκειμένων των δεδομένων	Κατηγορίες δεδομένων προσωπικού χαρακτήρα	Κατηγορίες αποδεκτών

Νομιμότητα επεξεργασίας και δικαιώματα υποκειμένων των δεδομένων					
Βάση για τη νομιμότητα της επεξεργασίας, σύμφωνα με το άρ. 6 του Κανονισμού	Βάση για τη νομιμότητα της επεξεργασίας ειδικών κατηγοριών δεδομένων, σύμφωνα με το άρ. 9 του Κανονισμού	Έννομο συμφέρον για την επεξεργασία (εφόσον η βάση για τη νομιμότητα είναι το άρ. 6 παρ. 2 στοιχ. στ')	Δικαιώματα των υποκειμένων των δεδομένων	Πραγματοποίηση αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένου προφίλ (εάν έχει εφαρμογή)	Πηγή των δεδομένων

	Συγκατάθεση - Τήρηση δεδομένων		Εκτίμηση αντικτύπου στην προστασία δεδομένων προσωπικού χαρακτήρα				Περιστατικά παραβίασης δεδομένων προσωπικού χαρακτήρα	
	Τρόπος λήψης συγκατάθεσης - Τρόπος απόδειξης λήψης αυτής	Τόπος τήρησης των δεδομένων προσωπικού χαρακτήρα	Απαιτείται η εκπόνηση αντικτύπου στην προστασία προσωπικών δεδομένων;	Στάδιο (πρόοδος) στο οποίο βρίσκεται η εκπόνηση αντικτύπου	Χρειάστηκε προηγούμενη διαβούλευση με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα;	Σύνδεσμος (Link) στην εκπονηθείσα εκτίμηση αντικτύπου	Έχει λάβει χώρα περιστατικό παραβίασης δεδομένων προσωπικού χαρακτήρα;	Σύνδεσμος (Link) στο σχετικό αρχείο καταγραφής περιστατικών παραβίασης

Ασφάλεια της Επεξεργασίας (Άρθρο 32)

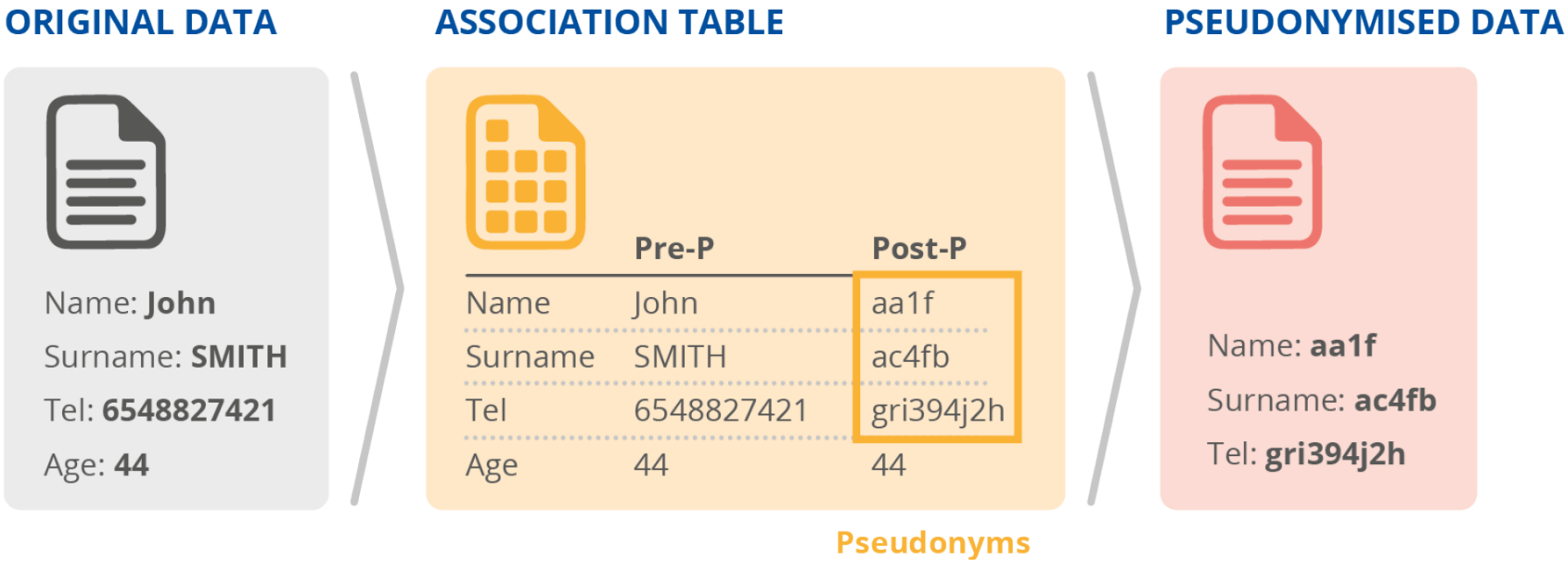
- Λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και **τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων**, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία **εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων**, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση:
  - της **ψευδωνυμοποίησης** και της **κρυπτογράφησης** δεδομένων προσωπικού χαρακτήρα,
  - της δυνατότητας διασφάλισης του **απορρήτου**, της **ακεραιότητας**, της **διαθεσιμότητας** και της **αξιοπιστίας** των **συστημάτων** και των **υπηρεσιών επεξεργασίας** σε συνεχή βάση,
  - της **δυνατότητας αποκατάστασης της διαθεσιμότητας** και της **πρόσβασης** σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος,
  - **διαδικασίας** για την τακτική δοκιμή, **εκτίμηση και αξιολόγηση της αποτελεσματικότητας** των **τεχνικών και των οργανωτικών μέτρων** για τη διασφάλιση της ασφάλειας της επεξεργασίας

Ψευδωνυμοποίηση (Άρθρο 4)

- «**Ψευδωνυμοποίηση**»: η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο

- «**Σύστημα Αρχειοθέτησης**»: κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε κατανεμημένο σε λειτουργική ή γεωγραφική βάση

Ψευδωνυμοποίηση – Παράδειγμα



https://www.enisa.europa.eu/publications/deploying-pseudonymisation-techniques

Βασικές τεχνικές ψευδωνυμοποίησης

Technique	Pseudonym Generator
Counter	Monotonic counter which starts at a certain value and is increased each time a new pseudonym is necessary
Random number	Random value extracted between a minimum and a maximum boundary each time a new pseudonym is necessary
Hash function	One-way (non-reversible) cryptographic function transforming input personal data in fixed-length values
Hash-based message authentication code (HMAC)	One-way (non-reversible) cryptographic function adding a key that makes it less predictable than a hash function
Encryption	Two-way (reversible) cryptographic function transforming an input personal data in values that can be re-transformed in its original format using a key

EXAMPLE

Progressive counter starting from
13, 14, 15

Random values between 0000 and 9999
9701, 3069, 1454

MD5 has for "John"
527bd5b5de689e2c32ae974c6229ff785

MD5 has for "John" and key "1337"
fbc76bcf46a35e9c21168cd54e5d31ff

AES encryption for "John" and key "1337"
WMaDIYzlmXQFO92cs5hNQ==

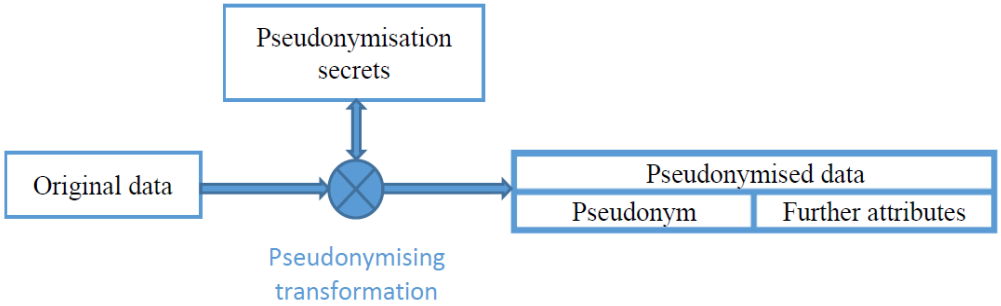
https://www.enisa.europa.eu/publications/deploying-pseudonymisation-techniques

European Data Protection Board

Guidelines 01/2025 on Pseudonymisation Adopted on 16 January 2025

https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf

- Για να είναι η ψευδωνυμοποίηση αποτελεσματική, τα ψευδωνυμοποιημένα δεδομένα **δεν πρέπει να περιέχουν άμεσα αναγνωριστικά (π.χ. αριθμούς εθνικής ταυτότητας) όποτε αυτά τα άμεσα αναγνωριστικά θα μπορούσαν να χρησιμοποιηθούν στο πεδίο της ψευδωνυμοποίησης για να αποδοθούν εύκολα τα δεδομένα στα υποκείμενα των δεδομένων. Για το σκοπό αυτό, τα αναγνωριστικά αυτά αφαιρούνται κατά τη διάρκεια της διαδικασίας ψευδωνυμοποίησης**. Ωστόσο, τα άμεσα αναγνωριστικά μπορεί να αντικατασταθούν με νέα αναγνωριστικά που μπορούν να αποδοθούν στα υποκείμενα των δεδομένων μόνο με τη χρήση πρόσθετων πληροφοριών. Τέτοια αναγνωριστικά ονομάζονται ψευδώνυμα.
- Ο **Μετασχηματισμός βάσει ψευδωνυμοποίησης υλοποιεί αυτή την αντικατάσταση**. Στο βαθμό που είναι αναγκαίο για να έχει η ψευδωνυμοποίηση το επιθυμητό αποτέλεσμα, τροποποιεί επίσης άλλες ιδιότητες, π.χ. με αφαίρεση, γενίκευση και προσθήκη θορύβου



European Data Protection Board

Guidelines 01/2025 on Pseudonymisation Adopted on 16 January 2025

https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf

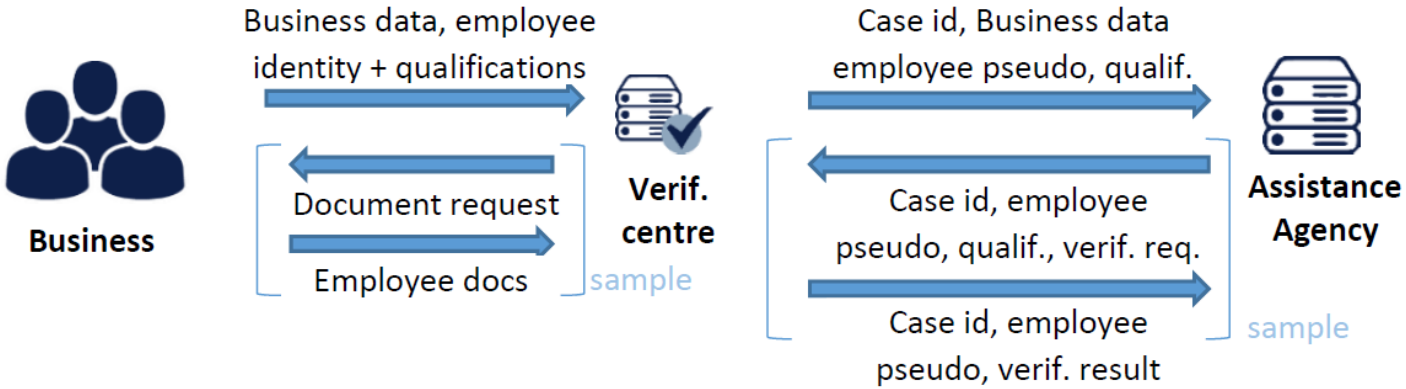
- Η διαδικασία ψευδωνυμοποίησης περιλαμβάνει τακτικά μυστικά δεδομένα. Ο υπεύθυνος επεξεργασίας μπορεί να επιλέξει αυτά τα δεδομένα πριν από την εκτέλεση της διαδικασίας. Μπορεί επίσης να τα επιλέξει ή να τα δημιουργήσει κατά τη διάρκεια της εκτέλεσης της διαδικασίας. Τα δεδομένα αυτά είναι συχνά είτε κρυπτογραφικά κλειδιά (για κρυπτογράφηση ή μονόδρομες λειτουργίες) είτε πίνακες που αντιστοιχούν τα ψευδώνυμα με τα προσωπικά δεδομένα που αντικαθιστούν («**κωδικές λέξεις ψευδωνυμοποίησης - pseudonymisation secrets**»)

Τα οφέλη της ψευδωνυμοποίησης υπό το πρίσμα ορισμένων από τις σχετικές αρχές και διατάξεις του GDPR

GDPR Article	GDPR Provisions
Art. 5(1)(c)	Data minimisation
Art. 5(1)(b)	Purpose limitation
Art. 5(1)(f)	Confidentiality
Art. 5(1)(d)	Accuracy
Art. 89(1)	Safeguard for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
Art. 32(1)	Security of processing
Art. 6(1)(f)	Lawfulness of processing for the purposes of legitimate interests
Art. 6(4)	Processing for a purpose other than that for which the personal data have been collected (further processing)
Art. 46	Transfers subject to appropriate safeguards
Art. 5(1)(a)	Fairness

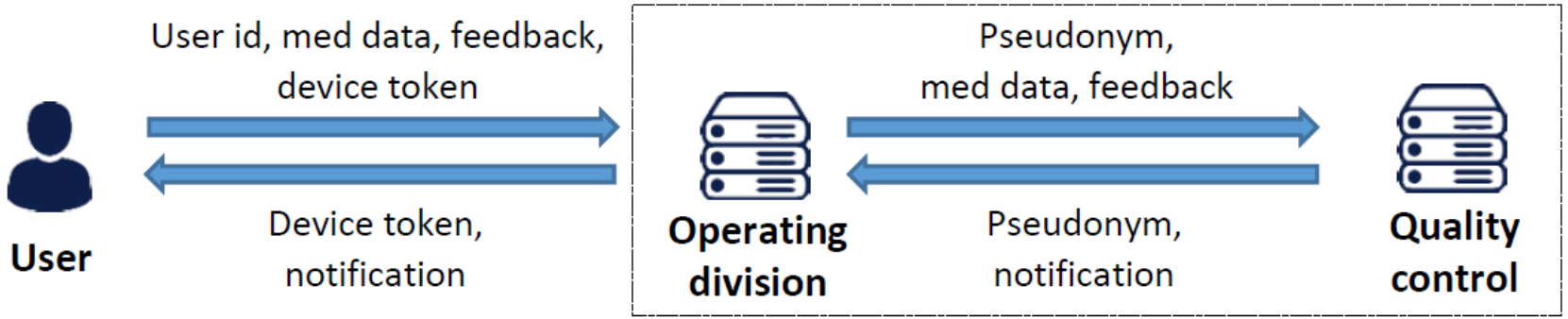
Παράδειγμα Ψευδωνυμοποίησης

- Διαχωρισμός λειτουργιών που επιτρέπει την ελαχιστοποίηση των δεδομένων, τον περιορισμό του σκοπού και την εμπιστευτικότητα



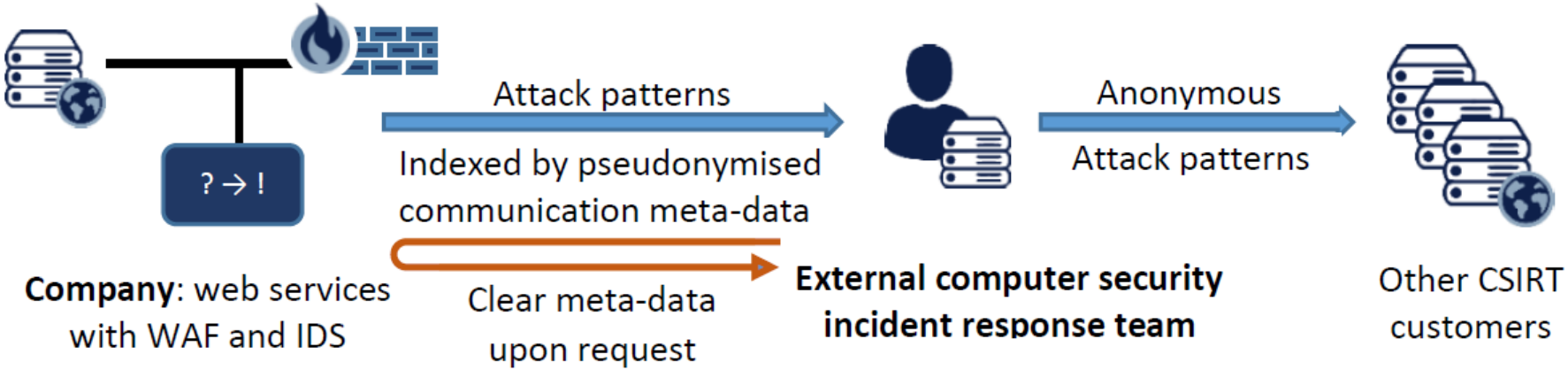
Παράδειγμα Ψευδωνυμοποίησης

- Ελαχιστοποίηση Δεδομένων και Εμπιστευτικότητα στην Εσωτερική Ανάλυση (Εντός Οργανισμού)

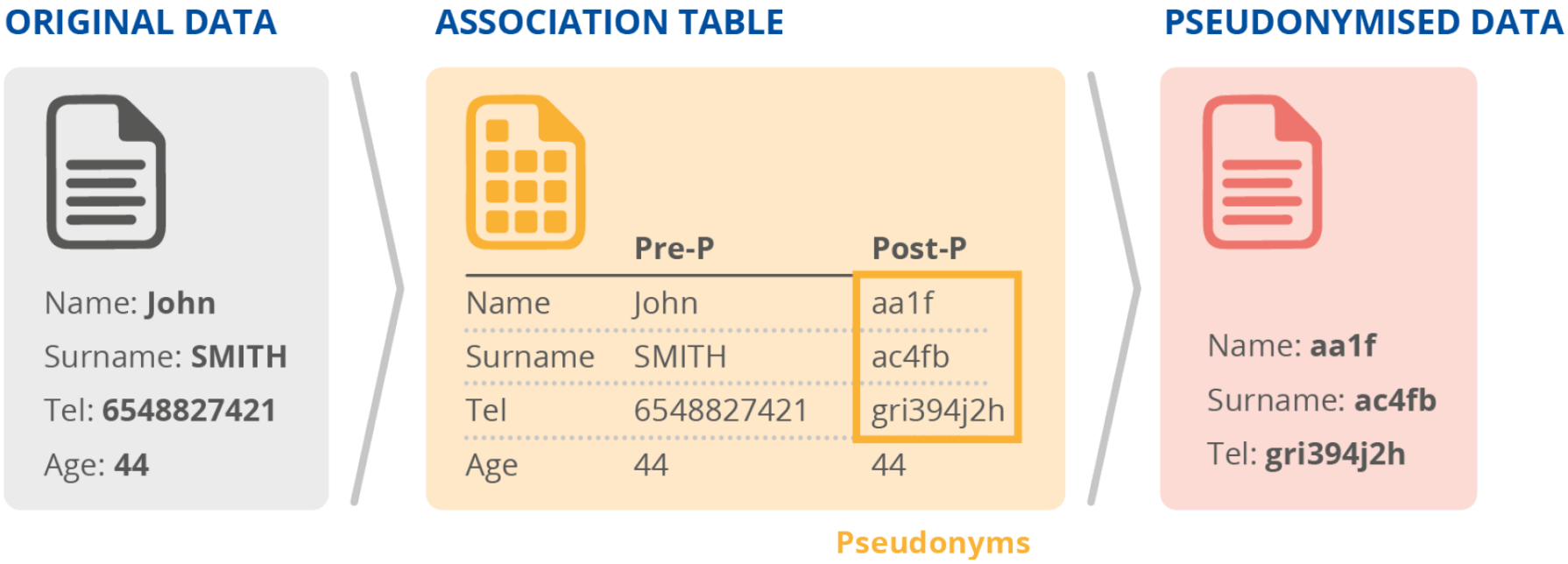


Παράδειγμα Ψευδωνυμοποίησης

- Μείωση κινδύνου ως παράγοντας στην εξισορρόπηση συμφερόντων και στην εξακρίβωση της συμβατότητας των επιδιωκόμενων σκοπών



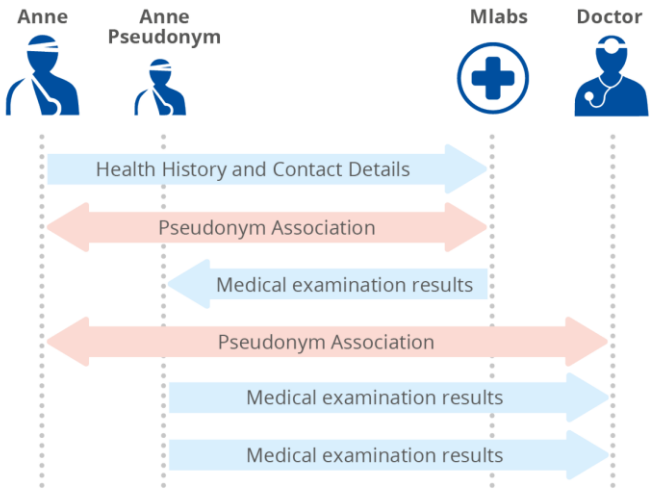
Ψευδωνυμοποίηση – Παράδειγμα



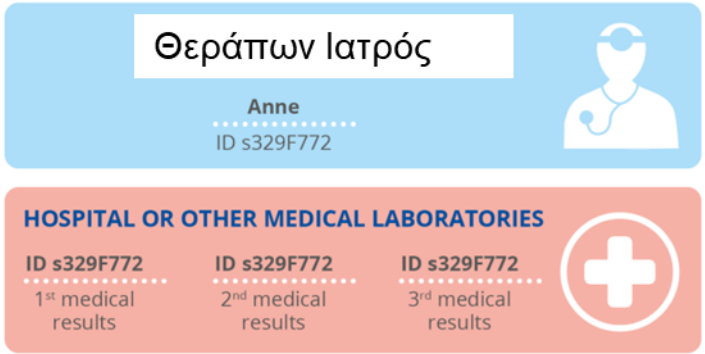
https://www.enisa.europa.eu/publications/deploying-pseudonymisation-techniques

Ψευδωνυμοποίηση – Παράδειγμα

- Ανταλλαγή δεδομένων υγείας ασθενών



Με την ολοκλήρωση των ιατρικών εξετάσεων, η Mlabs θα συσχετίσει τα αποτελέσματα των εξετάσεων με τον Κωδικό Ασθενούς (Patient_ID) της, αντί με τα προσωπικά της στοιχεία. Όταν η Άννα ζητήσει ένα αντίγραφο των αποτελεσμάτων της, η Mlabs θα πρέπει να αναζητήσει τον Κωδικό Ασθενούς που της έχει ανατεθεί και στη συνέχεια να πραγματοποιήσει τον συσχετισμό, καθώς ο Κωδικός Ασθενούς και τα προσωπικά στοιχεία αποθηκεύονται ξεχωριστά



https://www.enisa.europa.eu/publications/deploying-pseudonymisation-techniques

Προσοχή

Job	Sex	Age	Disease
Engineer	Male	35	Hepatitis
Engineer	Male	38	Hepatitis
Lawyer	Male	38	HIV
Writer	Female	30	Flu
Writer	Female	30	HIV
Dancer	Female	30	HIV
Dancer	Female	30	HIV

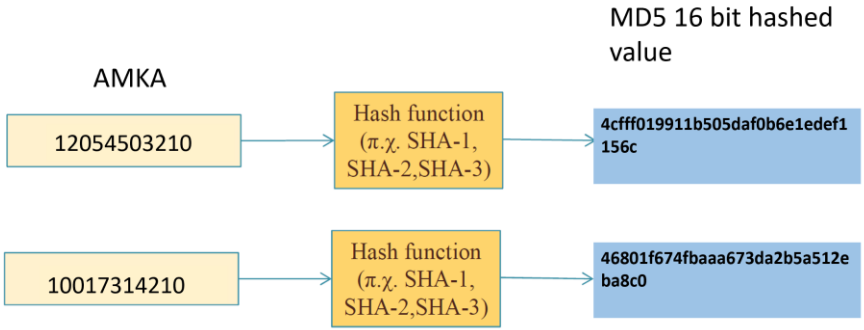
- Μπορεί εύκολα να ταυτοποιηθεί ο ασθενής λόγω της ύπαρξης της ηλικίας και του επαγγέλματος

- Χρήση Γενίκευσης αποτρέπει την ταυτοποίηση

Job	Sex	Age	Disease
Professional	Male	[35-40)	Hepatitis
Professional	Male	[35-40)	Hepatitis
Professional	Male	[35-40)	HIV
Artist	Female	[30-35)	Flu
Artist	Female	[30-35)	HIV
Artist	Female	[30-35)	HIV
Artist	Female	[30-35)	HIV

Προσοχή στην Κρυπτογράφηση και Συσχέτιση

- Πολλοί υπεύθυνοι επεξεργασίας καταγράφουν το hash value ενός μοναδικού αναγνωριστικού π.χ. ΑΜΚΑ, θεωρώντας ότι δεν καθίσταται εφικτή η εύρεση του αρχικού αναγνωριστικού δηλαδή του υποκειμένου λόγω του ότι μία κρυπτογραφική συνάρτηση κατακερματισμού (hash function) εκτελεί μια μη αναστρέψιμη διαδικασία



- **Είναι λάθος** γιατί αν ο πίνακας με τις hash values και τα λοιπά μη ψευδωνυποιημένα δεδομένα υποπέσει σε κακόβουλη επίθεση τότε εύκολα αν κάποιος γνωρίζει τον ΑΜΚΑ μπορεί να εκτελέσει τη hash faction και να συσχετίσει το υποκείμενο με τα προσωπικά του δεδομένα => απαιτείται ή πλήρης κρυπτογράφηση όλων των δεδομένων ή ψευδωνυνομοποίηση

Συμμόρφωση ή Διοικητικά Πρόστιμα - Ι

- **Βασικά Πρόστιμα (Άρθρο 83, Παράγραφος 4)**:
- Τα πρόστιμα μπορεί να φτάσουν έως το 2% του ετήσιου κύκλου εργασιών ή 10 000 000 EUR (όποιο από τα δύο είναι μεγαλύτερο).
- Παραδείγματα παραβάσεων που οδηγούν σε αυτά τα πρόστιμα:
  - Μη τήρηση της υποχρέωσης για τήρηση αρχείων επεξεργασίας δεδομένων
  - Μη εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων ασφαλείας
  - Μη τήρηση των προϋποθέσεων για την ανάθεση εκτελούντων την επεξεργασία

- **Σοβαρά Πρόστιμα (Άρθρο 83, Παράγραφος 5)**:
- Επισύρονται διοικητικά πρόστιμα έως **20 000 000 EUR** ή, σε περίπτωση επιχειρήσεων, έως το 4 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών (όποιο από τα δύο είναι μεγαλύτερο)
- Παραδείγματα παραβάσεων που οδηγούν σε αυτά τα πρόστιμα:
  - Διαβίβαση δεδομένων προσωπικού χαρακτήρα σε αποδέκτη σε τρίτη χώρα ή σε διεθνή οργανισμό
  - μη συμμόρφωση προς εντολή ή προς προσωρινό ή οριστικό περιορισμό της επεξεργασίας ή προς αναστολή της κυκλοφορίας δεδομένων

- **Σχέδιο Συμμόρφωσης**

I. Πολιτική ασφάλειας
II. Οργανωτικά μέτρα
III. Σχέδιο ανάκαμψης
IV. Τεχνικά μέτρα

Συμμόρφωση ή Διοικητικά Πρόστιμα - ΙΙ

"The 7th edition of **DLA Piper**'s ***GDPR Fines and Data Breach Survey*** highlights another significant year in data protection enforcement. Total fines issued in **2024** amounted to **€1.2 billion**, bringing the cumulative value of penalties under the GDPR to **€5.88 billion** since its implementation in May 2018" (link)

Πρόστιμα για παραβιάσεις του **ΓΚΠΔ** εντός του **2025**: **3.000.000.000 €** - Ενδεικτικά:

- **Meta –1.200.000.000 €**
  - ❑ **Παράβαση:** Παράνομες **μεταφορές δεδομένων** στις Η.Π.Α.
  - ✓ **Μάθημα:** Οι Τυπικές Συμβατικές Ρήτρες δεν επαρκούν από μόνες τους. Οι εταιρίες πρέπει να **διεξάγουν εκτιμήσεις κινδύνου, να εφαρμόζουν τεχνικά μέτρα προστασίας** και να διατηρούν συνεχή εποπτεία.
- **Amazon –746.000.000 €**
  - ❑ **Παράβαση:** Στοχευμένη διαφήμιση **χωρίς έγκυρη συγκατάθεση**.
  - ✓ **Μάθημα:** Η **συγκατάθεση πρέπει να είναι ελεύθερη**, τεκμηριωμένη και εύκολη στην ανάκληση.
- **TikTok – 530.000.000€**
  - ❑ **Παράβαση:** Πρόσβαση σε **δεδομένα χρηστών της ΕΕ από προσωπικό στην Κίνα** -έλλειψη διαφάνειας
  - ✓ **Μάθημα:** Σαφής **ενημέρωση για την αποθήκευση, την πρόσβαση και τη συμμετοχή τρίτων χωρών** στην επεξεργασία δεδομένων
- **Marina Salud Hospital – 500.000€**
  - ❑ **Παράβαση:** Διαμοιρασμός **ευαίσθητων ιατρικών δεδομένων** με υπεργολάβους χωρίς **έγκυρες συμβάσεις**.
  - ✓ **Μάθημα:** Συμβάσεις **επεξεργασίας δεδομένων με όλους τους προμηθευτές** και πλήρη διαφάνεια στην αλυσίδα της επεξεργασίας
- **Vodafone – 45.200.000€**
  - ❑ **Παράβαση:** Ανεπαρκής **ταυτοποίηση κατά την αλλαγή SIM** - **έλλειψη εποπτείας επί των εκτελούντων την επεξεργασία**
  - ✓ **Μάθημα:** Εφαρμογή **ισχυρών μεθόδους ταυτοποίησης** και **διενέργεια τακτικών ελέγχων συμμόρφωσης** στους εκτελούντες την επεξεργασία

Πηγή: https://www.gdprregister.eu/gdpr/gdpr-fines-2025-dpo-lessons/

Παράδειγμα Περιστατικού – Κλινική Vastaamo - Φιλανδία 2020

- **Περιστατικό:** Κλάπηκαν αρκετές δεκάδες χιλιάδες ιατρικά / θεραπευτικά αρχεία ασθενών (~**33.000** ασθενείς)
  - Ο εισβολέας χρησιμοποίησε παλιά στοιχεία πρόσβασης (όνομα χρήστη/κωδικό) που δεν είχαν απενεργοποιηθεί ή ήταν κοινά
  - Αφού απέκτησε πρόσβαση, αντέγραψε δεδομένα και 33.000 φακέλους ασθενών
  - Όταν αρνήθηκε η κλινική να πληρώσει λύτρα ύψους 400.000€ ξεκίνησε ο εκβιασμός των ασθενών από τον εισβολέα ζητώντας λύτρα σε Bitcoin (200 – 500 €)

- Αίτια:
  - Βάση Δεδομένων με απουσία μηχανισμών ελέγχου πρόσβασης
  - Απουσία firewall
  - Server δημόσια προσβάσιμος χωρίς επαρκή έλεγχο ταυτότητας
  - Ιατρικά δεδομένα μη κρυπτογραφημένα

ΠΑΡΑΒΙΑΣΗ ΓΚΠΔ

- Η Κλινική Vastaamo δεν είχε επαρκή τεχνικά και οργανωτικά μέτρα προστασίας, όπως απαιτεί το αρ. 32 του ΓΚΠΔ, δεν ενημέρωσε τις αρχές εγκαίρως για την παραβίαση (παρά μόνο 1,5–2 χρόνια μετά), δεν ενημέρωσε εγκαίρως τα θύματα, γεγονός που αύξησε την ψυχολογική και νομική ζημία

ΣΥΝΕΠΕΙΕΣ

- Επιβλήθηκε διοικητικό πρόστιμο ύψους **608.000€** από την Φινλανδική Αρχή Προστασίας Δεδομένων
- Τα θύματα απαίτησαν αποζημίωση από την Κλινική
- Η Κλινική Vastaamo **κήρυξε πτώχευση** από την απόφαση του Επαρχιακού Δικαστηρίου του Ελσίνκι τον Φεβρουάριο του 2021
- Ο εισβολέας καταδικάστηκε τον Απρίλιο του 2024 με ποινή φυλάκισης 6 ετών και 3 μηνών

Πηγή: https://www.bbc.com/news/articles/c97znd00q7mo

Ερωτήσεις;

ARISTOTLE UNIVERSITY OF THESSALONIKI

GOOGLE.ORG CYBERSECURITY SEMINARS