ΕΚΠΑΙΔΕΥΤΙΚΟ & ΠΡΑΚΤΙΚΟ ΒΟΗΘΗΜΑ · ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΥΓΕΙΑ

Πρακτικός Οδηγός Ορθής Χρήσης του ΓΚΠΔ (GDPR)

Κανονισμός (ΕΕ) 2016/679 & ελληνικό νομικό πλαίσιο

Σημείο αναφοράς για το προσωπικό οργανισμών παροχής υπηρεσιών υγείας

Σε ποιους απευθύνεται: ιατρικό, νοσηλευτικό, διοικητικό και τεχνικό προσωπικό — νοσοκομεία, κλινικές, κέντρα υγείας, κέντρα κοινωνικής πρόνοιας, διαγνωστικά κέντρα, ιατρεία, φαρμακεία.

Ισχύον δίκαιο αναφοράς: Καν. (ΕΕ) 2016/679 · Ν. 4624/2019 (κωδικοποιημένος, ενοπ. έκδ. 4.8.2025, με Ν. 5221/2025) · Ν. 3418/2005 · Καν. (ΕΕ) 2025/327 (EHDS).

Πώς να χρησιμοποιήσετε αυτόν τον οδηγό

Ο οδηγός είναι γραμμένος σε απλή γλώσσα και λειτουργεί ως σημείο αναφοράς για την καθημερινή σας εργασία. Δεν χρειάζεται να τον διαβάσετε από την αρχή ως το τέλος: ανατρέξτε στο κεφάλαιο που σας ενδιαφέρει τη στιγμή που το χρειάζεστε.

Αν βιάζεστε, **ξεκινήστε από τους «10 Βασικούς Κανόνες»** (Κεφ. 3) και τα «Σενάρια από την καθημερινότητα» (Κεφ. 16). Για γρήγορη απάντηση σε συγκεκριμένη ερώτηση, δείτε τις «60 Συχνές Ερωτήσεις» (Κεφ. 17) ή τους πίνακες γρήγορης αναφοράς (Κεφ. 18).

Τι σημαίνουν τα χρωματιστά πλαίσια

ΒΑΣΙΚΟΣ ΚΑΝΟΝΑΣ

Ένας βασικός κανόνας που αξίζει να θυμάστε.

ΣΩΣΤΗ ΠΡΑΚΤΙΚΗ

Μια ενδεδειγμένη, σωστή πρακτική.

ΠΡΟΣΟΧΗ

Ένα συχνό λάθος ή σημείο αυξημένου κινδύνου.

ΠΑΡΑΔΕΙΓΜΑ

Ένα ρεαλιστικό παράδειγμα από μονάδα υγείας.

ΝΟΜΙΚΗ ΒΑΣΗ

Η σχετική διάταξη του Κανονισμού ή του εθνικού νόμου, για όποιον θέλει να ανατρέξει στο κείμενο.

ΣΗΜΕΙΩΣΗ

Μια διευκρίνιση ή πρακτική επισήμανση.

ΔΕΝ ΥΠΟΚΑΘΙΣΤΑ ΝΟΜΙΚΗ ΣΥΜΒΟΥΛΗ

Σημαντικό: Το υλικό είναι εκπαιδευτικό και πληροφοριακό. Δεν υποκαθιστά την εξειδικευμένη νομική συμβουλή ούτε τις οδηγίες του Υπευθύνου Προστασίας Δεδομένων (DPO) του Οργανισμού σας. Σε κάθε αμφιβολία, απευθύνεστε στον DPO σας.

Περιεχόμενα

ΜΕΡΟΣ Α΄ — Τα βασικά σε απλά λόγια

1. Τι είναι ο ΓΚΠΔ και γιατί μας αφορά

Ο ΓΚΠΔ (Γενικός Κανονισμός Προστασίας Δεδομένων, στα αγγλικά GDPR) είναι ο ευρωπαϊκός νόμος που προστατεύει τα προσωπικά δεδομένα κάθε ανθρώπου. Ισχύει σε όλη την ΕΕ από τις **25 Μαΐου 2018**. Στην Ελλάδα τον συμπληρώνει ο Ν. 4624/2019.

Μας αφορά άμεσα γιατί σε μια μονάδα υγείας επεξεργαζόμαστε κάθε μέρα **δεδομένα υγείας** — μια από τις πιο ευαίσθητες κατηγορίες δεδομένων, με **ενισχυμένη προστασία**. «Επεξεργασία» είναι σχεδόν ό,τι κάνουμε με τα δεδομένα: συλλογή, καταχώριση, αποθήκευση, ανάκτηση, διαβίβαση, διαγραφή.

Τι κερδίζουμε — και τι διακυβεύεται

- **Εμπιστοσύνη:** ο ασθενής εμπιστεύεται τα δεδομένα του στον Οργανισμό.
- **Ασφάλεια:** λιγότερες διαρροές και περιστατικά.
- **Συμμόρφωση:** αποφυγή κυρώσεων. Παράβαση μπορεί να επιφέρει πειθαρχικές, αστικές και ποινικές συνέπειες, καθώς και πρόστιμα στον Οργανισμό.

> **ΣΗΜΕΙΩΣΗ**
>
> Ο ΓΚΠΔ και το **ιατρικό απόρρητο** λειτουργούν **παράλληλα**. Το ιατρικό απόρρητο δεσμεύει εσάς ως επαγγελματία· ο ΓΚΠΔ δεσμεύει τον Οργανισμό ως Υπεύθυνο Επεξεργασίας.

> **ΝΟΜΙΚΗ ΒΑΣΗ**
>
> Καν. (ΕΕ) 2016/679, άρθρα 4 & 9 · Ν. 4624/2019 · Ν. 3418/2005, άρθρο 13.

2. Οι λέξεις-κλειδιά που χρειάζεται να ξέρω

Δέκα όροι που επιστρέφουν συνέχεια. (Πλήρες γλωσσάρι στο τέλος του οδηγού.)

Όρος	Τι σημαίνει στην πράξη
Υπεύθυνος Επεξεργασίας (Controller)	Ο Οργανισμός (π.χ. το νοσοκομείο) που αποφασίζει γιατί και πώς γίνεται η επεξεργασία.
Εκτελών την Επεξεργασία (Processor)	Όποιος επεξεργάζεται για λογαριασμό του Οργανισμού (π.χ. πάροχος υπολογιστικού νέφους/cloud, εταιρεία πληροφοριακού συστήματος/HIS, μισθοδοσία).
Υπεύθυνος Προστασίας Δεδομένων (DPO / ΥΠΔ)	Ο Υπεύθυνος Προστασίας Δεδομένων του Οργανισμού — το πρώτο σας σημείο επαφής για κάθε θέμα δεδομένων.
Δεδομένα ειδικών κατηγοριών	Ευαίσθητα δεδομένα (υγείας, γενετικά κ.ά.). Η επεξεργασία τους κατ’ αρχήν απαγορεύεται, εκτός αν ισχύει εξαίρεση.
Νόμιμη βάση	Ο λόγος που μας επιτρέπει να επεξεργαστούμε δεδομένα. Χωρίς νόμιμη βάση, δεν επεξεργαζόμαστε.
Συγκατάθεση	Ελεύθερη, ρητή και ενημερωμένη συμφωνία του ασθενούς. Πάντα ανακλητή. Δεν είναι η βάση για τη θεραπεία.
Ελάχιστη αναγκαία πρόσβαση (need-to-know)	Βλέπω μόνο τα δεδομένα που χρειάζομαι για τη δουλειά μου — τίποτα παραπάνω.
Παραβίαση (breach)	Περιστατικό ασφάλειας: απώλεια, διαρροή ή μη εξουσιοδοτημένη πρόσβαση σε δεδομένα.
Ψευδωνυμοποίηση	Αφαιρώ τα στοιχεία ταυτότητας, αλλά μπορώ να τα επαναφέρω με «κλειδί». Παραμένουν προσωπικά δεδομένα.

Όρος	Τι σημαίνει στην πράξη
Ανωνυμοποίηση	Αφαιρώ οριστικά κάθε στοιχείο ταυτότητας. Τα δεδομένα παύουν να είναι προσωπικά.

3. Οι 10 Βασικοί Κανόνες του προσωπικού

Αν κρατήσετε μόνο μία σελίδα από τον οδηγό, ας είναι αυτή. Δέκα κανόνες που καλύπτουν το 90% της καθημερινότητας.

1. **Ελάχιστη αναγκαία πρόσβαση (need-to-know)** βλέπω μόνο τα δεδομένα που χρειάζομαι για τη δουλειά μου.
2. **Εχεμύθεια παντού** δεν συζητώ για ασθενείς σε διαδρόμους, ασανσέρ ή καφετέρια.
3. **Κλειδώνω την οθόνη** (Win+L) και δεν αφήνω έγγραφα εκτεθειμένα (πολιτική «καθαρού γραφείου»).
4. **Δεν μοιράζομαι κωδικούς** και χρησιμοποιώ πολυπαραγοντική ταυτοποίηση (MFA).
5. **Εγκεκριμένα κανάλια μόνο** όχι προσωπικό ηλεκτρονικό ταχυδρομείο (email), όχι WhatsApp/Viber για δεδομένα υγείας.
6. **Ταυτοποιώ πάντα** πριν δώσω πληροφορία ή αντίγραφο φακέλου.
7. **Θεραπεία = άρθρο 9(2)(η),** όχι συγκατάθεση· η συγκατάθεση είναι για το προαιρετικό.
8. **Αναφέρω άμεσα** κάθε ύποπτο περιστατικό ή παραβίαση στον DPO/μηχανογράφηση (μετράει το 72ωρο).
9. **Δεν κάνω κλικ** σε ύποπτα μηνύματα/συνδέσμους — επιβεβαιώνω πάντα τον αποστολέα.
10. **Όταν αμφιβάλλω, ρωτώ τον DPO** — προτού ενεργήσω.

> **ΤΟ ΜΟΤΟ**
> «Σεβασμός, Ασφάλεια, Διαφάνεια — σε κάθε δεδομένο ασθενούς.»

ΜΕΡΟΣ Β΄ — Οι κανόνες στην πράξη

4. Οι 7 αρχές — τι σημαίνουν για τη δουλειά μου

Κάθε επεξεργασία πρέπει να σέβεται ταυτόχρονα και τις επτά αρχές. Δείτε τι σημαίνει η καθεμία πρακτικά:

Αρχή	Στην πράξη
1. Νομιμότητα, αντικειμενικότητα, διαφάνεια	Επεξεργάζομαι μόνο με νόμιμη βάση, δίκαια και ενημερώνοντας τον ασθενή.
2. Περιορισμός σκοπού	Συλλέγω για συγκεκριμένο σκοπό· δεν χρησιμοποιώ τα δεδομένα για άσχετους σκοπούς.
3. Ελαχιστοποίηση	Συλλέγω μόνο όσα χρειάζονται — όχι «για παν ενδεχόμενο».
4. Ακρίβεια	Κρατώ τα δεδομένα σωστά & επικαιροποιημένα· διορθώνω ό,τι είναι λάθος.
5. Περιορισμός χρόνου	Διατηρώ μόνο όσο απαιτείται (βλ. χρόνους τήρησης ιατρικού αρχείου, Κεφ. 8).
6. Ακεραιότητα & εμπιστευτικότητα	Προστατεύω τα δεδομένα με κατάλληλα τεχνικά & οργανωτικά μέτρα ασφαλείας.
7. Λογοδοσία	Ο Οργανισμός όχι μόνο συμμορφώνεται, αλλά το αποδεικνύει εγγράφως.

ΠΑΡΑΔΕΙΓΜΑ

Δεδομένα που συλλέχθηκαν για τη θεραπεία ΔΕΝ χρησιμοποιούνται για εμπορική προώθηση (marketing) χωρίς ξεχωριστή νόμιμη βάση. Στον οδοντίατρο, π.χ., δεν καταγράφεται ψυχιατρικό ιστορικό αν δεν σχετίζεται με τη θεραπεία.

ΝΟΜΙΚΗ ΒΑΣΗ

Καν. (ΕΕ) 2016/679, άρθρο 5 παρ. 1–2.

5. Με ποιο δικαίωμα επεξεργαζόμαστε δεδομένα ασθενών

Για κάθε επεξεργασία χρειάζεται μια νόμιμη βάση. Για δεδομένα υγείας χρειάζονται ΔΥΟ βάσεις ταυτόχρονα: μία από το άρθρο 6 (γενική) ΚΑΙ μία από το άρθρο 9 (ειδικές κατηγορίες).

ΒΑΣΙΚΟΣ ΚΑΝΟΝΑΣ

Η θεραπεία και η φροντίδα στηρίζονται στο άρθρο 9(2)(η) (ιατρική διάγνωση/περίθαλψη) — ΟΧΙ στη συγκατάθεση. Η συγκατάθεση φυλάσσεται για το προαιρετικό (π.χ. ενημερωτικό δελτίο/newsletter, έρευνα).

Γρήγορος πίνακας: ποια βάση για ποιον σκοπό

Σκοπός επεξεργασίας	Άρθρο 6	Άρθρο 9
Παροχή θεραπείας / φροντίδας	**6(1)(ε) ή (β)**	**9(2)(η)**
Επείγον σε αναίσθητο ασθενή	**6(1)(δ)**	**9(2)(γ)**
Δήλωση στον ΕΟΔΥ / δημόσια υγεία	**6(1)(γ)**	**9(2)(θ)**
Κλινική μελέτη / έρευνα	**6(1)(α) ή (ε)**	**9(2)(α) ή (ι)**
Ενημ. δελτίο (newsletter) / προώθηση (marketing)	**6(1)(α)**	**9(2)(α) αν χρειάζεται**
CCTV ασφάλειας	**6(1)(ε)/(στ)**	**—**

Σκοπός επεξεργασίας	Άρθρο 6	Άρθρο 9

ΝΟΜΙΚΗ ΒΑΣΗ

Καν. (ΕΕ) 2016/679, άρθρα 6 & 9 · για εμπορική προώθηση (marketing) και Ν. 3471/2006 (e-Privacy).

6. Ειδικές κατηγορίες & ιατρικό απόρρητο

Τα **δεδομένα ειδικών κατηγοριών** (υγείας, γενετικά, βιομετρικά, φυλετική/εθνοτική καταγωγή, θρησκευτικές/πολιτικές πεποιθήσεις, συνδικαλισμός, σεξουαλική ζωή) έχουν ενισχυμένη προστασία. Η επεξεργασία τους κατ' αρχήν **απαγορεύεται**, εκτός αν συντρέχει εξαίρεση του άρθρου 9 παρ. 2.

Πρακτικά μέτρα για δεδομένα υγείας

- Αυστηρός έλεγχος πρόσβασης (ελάχιστη αναγκαία πρόσβαση/need-to-know, έλεγχος βάσει ρόλου/RBAC).
- Ψευδωνυμοποίηση όπου είναι δυνατόν.
- Ιδιαίτερη προσοχή σε γενετικά & δεδομένα ψυχικής υγείας — συχνά τηρούνται χωριστά από τον κύριο φάκελο.

ΣΗΜΕΙΩΣΗ

Το ιατρικό απόρρητο ισχύει **και μετά τον θάνατο** του ασθενούς. Άρση μόνο σε ρητά προβλεπόμενες περιπτώσεις (π.χ. συναίνεση, επιβολή νόμου, εκπλήρωση καθήκοντος).

ΝΟΜΙΚΗ ΒΑΣΗ

Καν. (ΕΕ) 2016/679, άρθρο 9 · Ν. 3418/2005, άρθρο 13 (ιατρικό απόρρητο).

7. Συγκατάθεση: πότε χρειάζεται, πότε ΟΧΙ

Η συγκατάθεση παρεξηγείται συχνά. Δεν χρειάζεται για τη θεραπεία — χρειάζεται για το προαιρετικό.

ΣΩΣΤΗ ΠΡΑΚΤΙΚΗ

Πότε ζητάμε συγκατάθεση:

για ενημερωτικό δελτίο (newsletter)/εμπορική προώθηση (marketing), για συμμετοχή σε έρευνα, για φωτογράφηση που δεν αφορά τη θεραπεία.

ΠΡΟΣΟΧΗ

Πότε ΔΕΝ στηριζόμαστε σε συγκατάθεση:

για την ίδια τη θεραπεία/φροντίδα (βάση 9(2)(η)) και για υποχρεώσεις του νόμου (π.χ. δηλώσεις δημόσιας υγείας).

Όταν ζητάμε συγκατάθεση, αυτή πρέπει να είναι **ελεύθερη, ειδική, ενημερωμένη και ρητή**, και ο ασθενής μπορεί να την **ανακαλέσει ανά πάσα στιγμή** τόσο εύκολα όσο την έδωσε.

ΣΗΜΕΙΩΣΗ

Ανήλικοι: το όριο των 15 ετών (άρθρο 21 Ν. 4624/2019) αφορά τη συγκατάθεση σε υπηρεσίες της κοινωνίας των πληροφοριών (π.χ. ψηφιακές εφαρμογές) — όχι τη συναίνεση σε ιατρική πράξη, για την οποία ισχύουν οι κανόνες της ιατρικής & αστικής νομοθεσίας για τους ανηλίκους.

ΝΟΜΙΚΗ ΒΑΣΗ

Καν. (ΕΕ) 2016/679, άρθρα 4 παρ. 11 & 7 · Ν. 4624/2019, άρθρο 21.

8. Ο ιατρικός φάκελος: τι περιέχει, πόσο τον κρατάμε, ποιος βλέπει

Ο ιατρικός φάκελος περιέχει στοιχεία ταυτότητας, ημερομηνίες επισκέψεων, διαγνώσεις, αγωγή και αποτελέσματα εξετάσεων. Πρόσβαση έχει μόνο όποιος τη χρειάζεται για τη φροντίδα του ασθενούς (ελάχιστη αναγκαία πρόσβαση, need-to-know).

Χρόνοι τήρησης (από την τελευταία επίσκεψη)

Φορέας	Χρόνος τήρησης
Ιδιωτικά ιατρεία & λοιπές μονάδες Π.Φ.Υ. ιδιωτικού τομέα	**10 έτη**
Κάθε άλλη περίπτωση (νοσοκομεία, κλινικές — δημόσια & ιδιωτικά)	**20 έτη**
Ανήλικοι	**Συνήθως μέχρι ενηλικίωση + ο προβλεπόμενος χρόνος**

> **ΝΟΜΙΚΗ ΒΑΣΗ**
>
> **Ν. 3418/2005, άρθρο 14 παρ. 4:** 10ετία για ιδιωτική Π.Φ.Υ., 20ετία για κάθε άλλη περίπτωση. Η διάκριση είναι «πρωτοβάθμια ιδιωτική φροντίδα έναντι κάθε άλλης περίπτωσης», όχι απλώς «δημόσιο έναντι ιδιωτικού».

Πρόσβαση & αντίγραφα

- Ο ασθενής δικαιούται αντίγραφο του φακέλου του. Το πρώτο αντίγραφο παρέχεται δωρεάν.
- Ταυτοποιούμε πάντα τον αιτούντα πριν δώσουμε οτιδήποτε.
- Πολλά στοιχεία ο ασθενής τα βρίσκει ήδη στον Ατομικό Ηλεκτρονικό Φάκελο Υγείας (ΑΗΦΥ — myHealth / gov.gr).

9. Τα δικαιώματα των ασθενών & πώς απαντάμε

Ο ασθενής έχει συγκεκριμένα δικαιώματα. Όλα ασκούνται με τυποποιημένη, απλή διαδικασία.

Δικαίωμα	Βάση	Τι σημαίνει
Ενημέρωση	Άρθρα 13–14	Να γνωρίζει πώς χρησιμοποιούμε τα δεδομένα του.
Πρόσβαση	Άρθρο 15	Να λάβει αντίγραφο των δεδομένων του.
Διόρθωση	Άρθρο 16	Να διορθωθούν λανθασμένα στοιχεία.
Διαγραφή / Λήθη	Άρθρο 17	Διαγραφή — υπό προϋποθέσεις (όχι όταν ισχύει υποχρέωση τήρησης).
Περιορισμός	Άρθρο 18	Προσωρινό «πάγωμα» της επεξεργασίας.
Φορητότητα	Άρθρο 20	Λήψη & μεταφορά των δεδομένων σε κοινό μορφότυπο.
Εναντίωση	Άρθρο 21	Αντίρρηση σε ορισμένες επεξεργασίες.
Καταγγελία	Άρθρο 77	Προσφυγή στην ΑΠΔΠΧ.

Η διαδικασία σε 5 βήματα

1. Ταυτοποιώ τον αιτούντα με ασφάλεια.
2. Καταγράφω το αίτημα στο μητρώο αιτημάτων.
3. Προωθώ στον DPO ή στην αρμόδια υπηρεσία.
4. Απαντώ εντός 1 μηνός (παράταση έως 2 μήνες για πολύπλοκα αιτήματα, με ενημέρωση).
5. Το πρώτο αντίγραφο δωρεάν· τυχόν εγγραφή σε ενημερωτικό δελτίο (newsletter) διαγράφεται με την ανάκληση.

ΝΟΜΙΚΗ ΒΑΣΗ

Καν. (ΕΕ) 2016/679, άρθρα 12–22 & 77.

ΜΕΡΟΣ Γ΄ — Ασφάλεια & περιστατικά

10. Ασφάλεια δεδομένων στην καθημερινότητα

Η ασφάλεια είναι συνδυασμός τεχνολογίας και ανθρώπινης συμπεριφοράς. Το πιο ισχυρό σύστημα παρακάμπτεται με ένα κλικ σε μήνυμα «ψαρέματος» (phishing).

ΣΩΣΤΗ ΠΡΑΚΤΙΚΗ

ΝΑΙ — κάνετε

- Κλειδώνετε την οθόνη (Win+L) όταν απομακρύνεστε.
- Ισχυροί κωδικοί + MFA — ποτέ διαμοιρασμός.
- Μόνο εγκεκριμένα αποθηκευτικά μέσα (USB) & κανάλια.
- Αναφέρετε άμεσα κάθε ύποπτο περιστατικό στον DPO/IT.

ΠΡΟΣΟΧΗ

ΟΧΙ — αποφεύγετε

- Έντυπα με δεδομένα σε κοινόχρηστους χώρους.
- Συζήτηση για ασθενείς σε ασανσέρ/καφετέρια/διαδρόμους.
- Αποστολή δεδομένων υγείας μέσω προσωπικού ηλεκτρονικού ταχυδρομείου (email) ή WhatsApp/Viber.
- Άνοιγμα ύποπτων μηνυμάτων/συνδέσμων («ψάρεμα», phishing) ή φωτογραφία ασθενών.

ΠΑΡΑΔΕΙΓΜΑ — «ΨΑΡΕΜΑ» (PHISHING)

Νοσηλεύτρια λαμβάνει email «από τη Διοίκηση» που ζητά κατεπείγον αρχείο ασθενών. Σωστά: δεν κάνει κλικ, επιβεβαιώνει τηλεφωνικά, αναφέρει σε μηχανογράφηση (IT) & DPO.

ΝΟΜΙΚΗ ΒΑΣΗ

Καν. (ΕΕ) 2016/679, άρθρο 32 (ασφάλεια επεξεργασίας).

11. Παραβίαση δεδομένων: η πρώτη ώρα & το 72ωρο

Η ταχύτητα είναι κρίσιμη. Το **72ωρο γνωστοποίησης** στην ΑΠΔΠΧ μετράει από τη στιγμή που ο Οργανισμός **λαμβάνει γνώση** της παραβίασης — όχι από την επιβεβαίωση.

Τι κάνω την πρώτη 1 ώρα

1. Σταματώ τη ζημιά: αποσυνδέω/απομονώνω (χωρίς να σβήσω συστήματα — χάνονται ίχνη).
2. Ειδοποιώ DPO & IT αμέσως — το 72ωρο τρέχει.
3. Δεν διαγράφω τίποτα και δεν «διορθώνω» μόνος μου.
4. Καταγράφω τι, πότε, πώς το αντιλήφθηκα και ποια δεδομένα αφορά.
5. Ακολουθώ τις οδηγίες του DPO για αξιολόγηση & γνωστοποίηση.

ΣΗΜΕΙΩΣΗ

Αν η παραβίαση συνεπάγεται **υψηλό κίνδυνο** για τα δικαιώματα των προσώπων, ενημερώνονται και τα ίδια τα υποκείμενα (οι ασθενείς). Αν τα δεδομένα ήταν κρυπτογραφημένα, ο κίνδυνος συχνά μειώνεται.

ΝΟΜΙΚΗ ΒΑΣΗ

Καν. (ΕΕ) 2016/679, άρθρα 33 (γνωστοποίηση στην ΑΠΔΠΧ) & 34 (ενημέρωση υποκειμένων).

12. DPIA, ΑΔΕ, DPO — ποιος κάνει τι

Εργαλείο / Ρόλος	Τι είναι	Ποιος
ΑΔΕ (RoPA)	Αρχείο όλων των δραστηριοτήτων επεξεργασίας του Οργανισμού. Υποχρεωτικό.	Υπεύθυνος + DPO
DPIA (ΕΑΠΔ)	Εκτίμηση αντικτύπου, υποχρεωτική σε επεξεργασίες υψηλού κινδύνου (π.χ. νέο πληροφοριακό σύστημα/HIS, μεγάλη κλίμακα).	Υπεύθυνος, με συμβουλή DPO
DPO (ΥΠΔ)	Υπεύθυνος Προστασίας Δεδομένων. Ανεξάρτητος, αναφέρεται στη διοίκηση. Υποχρεωτικός στους φορείς υγείας.	Ορίζεται από τον Οργανισμό

ΒΑΣΙΚΟΣ ΚΑΝΟΝΑΣ

Προστασία ήδη από τον σχεδιασμό (Privacy by Design) — πριν, όχι μετά. Η εκτίμηση κινδύνου (DPIA) γίνεται στον σχεδιασμό κάθε νέας επεξεργασίας υψηλού κινδύνου. Αν παραμένει υψηλός κίνδυνος, προηγείται διαβούλευση με την ΑΠΔΠΧ.

ΝΟΜΙΚΗ ΒΑΣΗ

Καν. (ΕΕ) 2016/679, άρθρα 24–25, 30, 35–39 · Ν. 4624/2019, άρθρο 6 (DPO δημόσιων φορέων).

ΜΕΡΟΣ Δ΄ — Ειδικά θέματα

13. Έρευνα & κλινικές μελέτες

Η επεξεργασία για έρευνα έχει δικούς της κανόνες και συνήθως πρόσθετες εγγυήσεις.

- Νόμιμη βάση: άρθρο 6(1)(α) ή (ε) + άρθρο 9(2)(α) ή (ι).
- Απαιτούνται: ψευδωνυμοποίηση/ανωνυμοποίηση όπου είναι εφικτό, έγκριση Επιτροπής Ηθικής (IRB), ενημερωμένη συγκατάθεση, πρωτόκολλο, DPIA και καταχώριση στο ΑΔΕ.
- Για φάρμακα/κλινικές δοκιμές ισχύει και ο Καν. (ΕΕ) 536/2014.

ΒΑΣΙΚΟΣ ΚΑΝΟΝΑΣ

Πρώτα η Ηθική & η ενημερωμένη συγκατάθεση, μετά η συλλογή δεδομένων. Καμία ερευνητική χρήση δεδομένων ασθενών χωρίς το κατάλληλο πλαίσιο.

ΝΟΜΙΚΗ ΒΑΣΗ

Καν. (ΕΕ) 2016/679, άρθρα 6, 9 παρ. 2 (ι) & 89 · Ν. 4624/2019, άρθρο 30.

14. Τηλεϊατρική & ηλεκτρονικά συστήματα υγείας

Η τηλεϊατρική απαιτεί κρυπτογραφημένη πλατφόρμα, ταυτοποίηση ασθενούς, νόμιμη βάση, ενημέρωση και τήρηση του περιστατικού στον φάκελο — όπως κάθε ιατρική πράξη.

Τα ελληνικά συστήματα ηλε-υγείας

- **ΑΗΦΥ (Ν. 4600/2019):** Ατομικός Ηλεκτρονικός Φάκελος Υγείας για κάθε κάτοχο ΑΜΚΑ — προσβάσιμος μέσω myHealth & gov.gr.
- **Ηλεκτρονική συνταγογράφηση:** συνταγές & παραπεμπτικά (ηλεκτρονική συνταγογράφηση, e-prescription).

Ευρωπαϊκός Χώρος Δεδομένων Υγείας (EHDS)

Ο **Καν. (ΕΕ) 2025/327 (EHDS)** τέθηκε σε ισχύ στις 26.3.2025 και εφαρμόζεται σταδιακά. Στόχος: ο πολίτης να έχει πρόσβαση στα δεδομένα υγείας του σε όλη την ΕΕ (πρωτογενής χρήση) και να αξιοποιούνται με εγγυήσεις για έρευνα/δημόσια υγεία (δευτερογενής χρήση).

Ορόσημο	Τι ισχύει
26.3.2025	Έναρξη ισχύος (με μεταβατική περίοδο).
≈2027 – 2029	Σταδιακή εφαρμογή· βασικές κατηγορίες πρωτογενούς χρήσης.
2029 – 2031	Διεύρυνση κατηγοριών & δευτερογενής χρήση.

ΣΗΜΕΙΩΣΗ

Τι σημαίνει για εμάς: ο EHDS δεν αντικαθιστά τον ΓΚΠΔ — τον συμπληρώνει. Οι μονάδες υγείας θα προσαρμόζονται σταδιακά σε διαλειτουργικά συστήματα. Παρακολουθείτε τις οδηγίες του DPO.

15. Μέσα κοινωνικής δικτύωσης & φωτογραφίες

ΠΡΟΣΟΧΗ

Δεν αναρτώνται φωτογραφίες ή στοιχεία ασθενών σε προσωπικά ή εταιρικά μέσα κοινωνικής δικτύωσης (social media) χωρίς ρητή, ειδική και έγγραφη συγκατάθεση για τον συγκεκριμένο σκοπό.

Ακόμη και «αθώες» αναρτήσεις (π.χ. φωτογραφία από επιτυχημένη επέμβαση όπου διακρίνεται ο ασθενής) συνιστούν επεξεργασία δεδομένων υγείας. Εναλλακτικά: πλήρης ανωνυμοποίηση ώστε να μην είναι αναγνωρίσιμος ο ασθενής.

> **ΝΟΜΙΚΗ ΒΑΣΗ**
>
> Καν. (ΕΕ) 2016/679, άρθρο 9 παρ. 2 (α) (ειδική συγκατάθεση).

ΜΕΡΟΣ Ε΄ — Γρήγορη αναφορά

16. Σενάρια από την καθημερινότητα

Πέντε συνηθισμένες καταστάσεις και η ενδεδειγμένη αντίδραση.

1. Το τηλεφώνημα του «συγγενή»

Η ΚΑΤΑΣΤΑΣΗ

Τηλεφωνεί κάποιος δηλώνοντας συγγενής ασθενούς και ζητά τη διάγνωση.

ΥΠΟΔΕΙΓΜΑΤΙΚΗ ΑΠΑΝΤΗΣΗ

Δεν δίνουμε πληροφορίες υγείας τηλεφωνικά χωρίς ταυτοποίηση & νόμιμη βάση. Εξηγούμε ευγενικά ότι οι πληροφορίες δίνονται μόνο στον ίδιο τον ασθενή ή σε νόμιμα εξουσιοδοτημένο πρόσωπο, με κατάλληλη ταυτοποίηση.

2. Το «κατεπείγον» email του Διοικητή

Η ΚΑΤΑΣΤΑΣΗ

Email που ζητά άμεσα αρχείο Excel με ΑΜΚΑ & διαγνώσεις 300 ασθενών «για το Υπουργείο».

ΥΠΟΔΕΙΓΜΑΤΙΚΗ ΑΠΑΝΤΗΣΗ

Πιθανό «ψάρεμα» (phishing) ή απάτη εταιρικού email (BEC). Δεν απαντώ, δεν στέλνω, δεν κάνω κλικ. Επιβεβαιώνω τον αποστολέα από διαφορετικό κανάλι (τηλέφωνο). Αναφέρω σε μηχανογράφηση (IT) & DPO.

3. Η εύρεση του χαμένου φακέλου

Η ΚΑΤΑΣΤΑΣΗ

Βρίσκω σε κοινόχρηστο εκτυπωτή έντυπο με εξετάσεις ασθενούς άλλου τμήματος.

ΥΠΟΔΕΙΓΜΑΤΙΚΗ ΑΠΑΝΤΗΣΗ

Δεν το διαβάζω. Το παραδίδω στον αρμόδιο/προϊστάμενο. Ενημερώνω τον DPO (πιθανή έκθεση δεδομένων). Προτείνω ασφαλή εκτύπωση (secure-print) στους κοινόχρηστους εκτυπωτές.

4. Το αίτημα διαγραφής

Η ΚΑΤΑΣΤΑΣΗ

Πρώην ασθενής ζητά «να διαγράψετε εντελώς τον ιατρικό μου φάκελο».

ΥΠΟΔΕΙΓΜΑΤΙΚΗ ΑΠΑΝΤΗΣΗ

Καταγράφω & ταυτοποιώ. Εξηγώ ότι ο φάκελος δεν διαγράφεται όσο ισχύει η νόμιμη υποχρέωση τήρησης (10/20ετία). Απαντώ αιτιολογημένα εντός 1 μηνός. Τυχόν εγγραφή σε newsletter διαγράφεται.

5. Η φωτογραφία στα μέσα κοινωνικής δικτύωσης

Η ΚΑΤΑΣΤΑΣΗ

Συνάδελφος θέλει να αναρτήσει στο Instagram φωτογραφία από επέμβαση όπου διακρίνεται ο ασθενής.

ΥΠΟΔΕΙΓΜΑΤΙΚΗ ΑΠΑΝΤΗΣΗ

> Δεν αναρτάται χωρίς ρητή έγγραφη συγκατάθεση για τον σκοπό αυτό. Εναλλακτικά πλήρης ανωνυμοποίηση. Η φροντίδα δεν καλύπτει τη δημοσιοποίηση.

17. -- 60 Συχνές Ερωτήσεις & Απαντήσεις

Άμεσες απαντήσεις για την καθημερινή λειτουργία, με τη νομική βάση κάθε απάντησης. Οργανωμένες σε 7 ενότητες.

Α. Γενικά για τον ΓΚΠΔ

1. Τι είναι ο ΓΚΠΔ και γιατί με αφορά ως εργαζόμενο σε μονάδα υγείας;

Είναι το ευρωπαϊκό πλαίσιο προστασίας προσωπικών δεδομένων. Σας αφορά διότι καθημερινά επεξεργάζεστε δεδομένα υγείας (ειδική κατηγορία) με ενισχυμένη προστασία. Παράβαση επιφέρει πειθαρχικές, αστικές και ποινικές κυρώσεις, καθώς και πρόστιμα στον Οργανισμό.

Νομική βάση: *Καν. (ΕΕ) 2016/679, άρθρο 9 · Ν. 4624/2019*

2. Από πότε ισχύει ο ΓΚΠΔ;

Από τις 25/5/2018. Στην Ελλάδα συμπληρώνεται από τον Ν. 4624/2019, που θεσπίζει τα εθνικά μέτρα εφαρμογής.

Νομική βάση: *Καν. 2016/679 (έναρξη ισχύος 25.5.2018) · Ν. 4624/2019*

3. Τι σημαίνει «προσωπικό δεδομένο»;

Κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο: όνομα, ΑΜΚΑ, διάγνωση, αποτέλεσμα εξέτασης, διεύθυνση IP, φωτογραφία.

Νομική βάση: *Καν. 2016/679, άρθρο 4 παρ. 1*

4. Τι είναι τα «δεδομένα ειδικών κατηγοριών»;

Δεδομένα ενισχυμένης προστασίας: φυλετική/εθνοτική καταγωγή, πολιτικά φρονήματα, θρησκεία, συνδικαλισμός, γενετικά, βιομετρικά, δεδομένα υγείας και σεξουαλικής ζωής. Η επεξεργασία τους κατ' αρχήν απαγορεύεται, εκτός αν συντρέχει εξαίρεση.

Νομική βάση: *Καν. 2016/679, άρθρο 9 παρ. 1–2*

5. Ποιες είναι οι βασικές αρχές επεξεργασίας;

Επτά: νομιμότητα / αντικειμενικότητα / διαφάνεια, περιορισμός σκοπού, ελαχιστοποίηση δεδομένων, ακρίβεια, περιορισμός χρόνου διατήρησης, ακεραιότητα & εμπιστευτικότητα και — οριζόντια — λογοδοσία.

Νομική βάση: *Καν. 2016/679, άρθρο 5 παρ. 1–2*

6. Τι σημαίνει «λογοδοσία (accountability)»;

Ο Οργανισμός όχι μόνο συμμορφώνεται, αλλά αποδεικνύει εγγράφως τη συμμόρφωσή του: πολιτικές, ΑΔΕ, DPIA, εκπαιδεύσεις, αρχεία συγκαταθέσεων και συμβάσεις ανάθεσης (DPA).

Νομική βάση: *Καν. 2016/679, άρθρο 5 παρ. 2 & άρθρο 24*

7. Ποια αρχή εποπτεύει την εφαρμογή στην Ελλάδα;

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) — Λεωφ. Κηφισίας 1-3, Αθήνα, www.dpa.gr. Προς αυτήν υποβάλλονται γνωστοποιήσεις παραβιάσεων και καταγγελίες.

Νομική βάση: *Καν. 2016/679, άρθρα 51 & 57 · Ν. 4624/2019, άρθρο 9*

8. Ποια η σχέση του ΓΚΠΔ με το ιατρικό απόρρητο;

Συμπληρωματική. Το ιατρικό απόρρητο δεσμεύει ατομικά τον επαγγελματία υγείας· ο ΓΚΠΔ δεσμεύει τον Οργανισμό ως Υπεύθυνο Επεξεργασίας. Εφαρμόζονται παράλληλα.

Νομική βάση: *Ν. 3418/2005, άρθρο 13 · Καν. 2016/679, άρθρο 9 παρ. 2 (η)*

Β. Δικαιώματα ασθενών

9. Ποια δικαιώματα έχει ο ασθενής βάσει ΓΚΠΔ;

Ενημέρωσης, πρόσβασης, διόρθωσης, διαγραφής, περιορισμού, φορητότητας, εναντίωσης, μη υπαγωγής σε αποκλειστικά αυτοματοποιημένη απόφαση, καθώς και καταγγελίας στην ΑΠΔΠΧ.

Νομική βάση: *Καν. 2016/679, άρθρα 12–22 & 77*

10. Πώς υποβάλλεται αίτημα άσκησης δικαιώματος;

Εγγράφως — με έντυπο, email ή ταχυδρομικά — προς τον Υπεύθυνο Επεξεργασίας ή τον DPO, με προηγούμενη ταυτοποίηση του αιτούντος.

Νομική βάση: *Καν. 2016/679, άρθρο 12 παρ. 1–2 & παρ. 6*

11. Σε πόσο χρόνο απαντάμε σε αίτημα;

Εντός 1 μηνός. Δυνατή παράταση κατά 2 μήνες για ιδιαίτερα πολύπλοκα ή πολυάριθμα αιτήματα, με ενημέρωση του αιτούντος εντός του πρώτου μήνα.

Νομική βάση: *Καν. 2016/679, άρθρο 12 παρ. 3*

12. Χρεώνουμε για αντίγραφο ιατρικού φακέλου;

Το πρώτο αντίγραφο παρέχεται δωρεάν· για επιπλέον αντίγραφα επιτρέπεται εύλογο διοικητικό τέλος. Πολλά στοιχεία ο ασθενής τα βρίσκει ήδη δωρεάν στον ΑΗΦΥ (myHealth / gov.gr).

Νομική βάση: *Καν. 2016/679, άρθρο 15 παρ. 3 · Ν. 3418/2005, άρθρο 14*

13. Μπορεί ο ασθενής να ζητήσει διαγραφή του φακέλου του;

Όχι, όσο ισχύει η έννομη υποχρέωση τήρησης (10ετία στην ιδιωτική Π.Φ.Υ. / 20ετία σε κάθε άλλη περίπτωση). Εφαρμόζεται η ρητή εξαίρεση από το δικαίωμα διαγραφής.

Νομική βάση: *Καν. 2016/679, άρθρο 17 παρ. 3 (β) · Ν. 3418/2005, άρθρο 14 παρ. 4*

14. Μπορεί συγγενής να ζητήσει τον φάκελο ασθενούς;

Όχι αυτοδικαίως. Απαιτείται εξουσιοδότηση του ασθενούς, ιδιότητα νόμιμου εκπροσώπου, έννομο συμφέρον μετά θάνατον (κληρονόμοι) ή εισαγγελική παραγγελία.

Νομική βάση: *Ν. 3418/2005, άρθρο 14 παρ. 8 · Καν. 2016/679, άρθρο 15*

15. Τι κάνουμε αν ζητήσει αντίγραφο δικηγόρος;

Απαιτείται ειδικό πληρεξούσιο (όχι γενικό), με ρητή εξουσιοδότηση παραλαβής ιατρικών δεδομένων του εντολέα.

Νομική βάση: *Ν. 3418/2005, άρθρο 14 · Καν. 2016/679, άρθρο 12 παρ. 6*

16. Πώς ενημερώνουμε τον ασθενή για την επεξεργασία;

Με Ενημέρωση Ιδιωτικότητας (Ενημέρωση Ιδιωτικότητας) αναρτημένη στην ιστοσελίδα, διαθέσιμη στην υποδοχή και ενσωματωμένη στο έντυπο εισαγωγής.

Νομική βάση: *Καν. 2016/679, άρθρα 13–14*

17. Δικαιούται διόρθωση εσφαλμένης διάγνωσης;

Δικαιούται διόρθωση τυπικών στοιχείων. Η ιατρική κρίση αλλάζει μόνο από τον ιατρό· ο ασθενής μπορεί να καταχωρίσει αντίθετη άποψη στον φάκελο.

Νομική βάση: *Καν. 2016/679, άρθρο 16*

18. Ζητά «να ξεχαστεί» από ενημερωτικό δελτίο (newsletter) — τι κάνουμε;

Άμεση διαγραφή / εναντίωση στη λίστα εμπορική προώθηση (marketing) (απόλυτο δικαίωμα). Δεν επηρεάζεται ο ιατρικός φάκελος, ο οποίος τηρείται βάσει έννομης υποχρέωσης.

Νομική βάση: *Καν. 2016/679, άρθρο 21 παρ. 2–3 & άρθρο 17 · Ν. 3471/2006, άρθρο 11*

Γ. Ιατρικός φάκελος

19. Ποιος έχει πρόσβαση στον ιατρικό φάκελο;

Μόνο εξουσιοδοτημένο προσωπικό που τον χρειάζεται για τη φροντίδα (αρχή ελάχιστη αναγκαία πρόσβαση (need-to-know)) — όχι όλο το νοσοκομείο. Στα συστήματα (HIS, ΑΗΦΥ) κάθε πρόσβαση καταγράφεται (καταγραφή ενεργειών (logging)).

Νομική βάση: *Καν. 2016/679, άρθρο 5 παρ. 1 (στ) & άρθρο 32 · Ν. 3418/2005, άρθρο 13*

20. Πόσο χρόνο φυλάσσεται ο ιατρικός φάκελος;

Ιδιωτική Π.Φ.Υ.: 10 έτη. Κάθε άλλη περίπτωση (νοσοκομεία / κλινικές): 20 έτη από την τελευταία επίσκεψη του ασθενούς.

Νομική βάση: *Ν. 3418/2005, άρθρο 14 παρ. 4 · Καν. 2016/679, άρθρο 5 παρ. 1 (ε)*

21. Επιτρέπεται συζήτηση για ασθενή στον διάδρομο;

Όχι — παραβιάζει την εμπιστευτικότητα. Οι συζητήσεις γίνονται σε γραφεία ή αίθουσες με κλειστή πόρτα, χωρίς τρίτους που δεν εμπλέκονται στη φροντίδα.

Νομική βάση: *Καν. 2016/679, άρθρο 5 παρ. 1 (στ) · Ν. 3418/2005, άρθρο 13*

22. Επιτρέπεται φωτογραφία ασθενούς για εκπαίδευση;

Μόνο με ρητή έγγραφη συγκατάθεση για τον συγκεκριμένο σκοπό, ή εφόσον η εικόνα είναι πλήρως ανωνυμοποιημένη.

Νομική βάση: *Καν. 2016/679, άρθρο 9 παρ. 2 (α)*

23. Επιτρέπεται αποστολή αποτελεσμάτων με email;

Μόνο κρυπτογραφημένα (π.χ. PDF με κωδικό) στο email που δήλωσε ο ίδιος ο ασθενής. Καλύτερη λύση: ο ασθενής βλέπει ασφαλώς τα αποτελέσματα μέσω ΑΗΦΥ / myHealth (gov.gr).

Νομική βάση: *Καν. 2016/679, άρθρο 32*

24. Επιτρέπεται αποστολή με WhatsApp / Viber;

Αποθαρρύνεται για επαγγελματική χρήση δεδομένων υγείας. Χρησιμοποιούνται μόνο τα εγκεκριμένα κανάλια του Οργανισμού.

Νομική βάση: *Καν. 2016/679, άρθρο 32 & άρθρο 5 παρ. 1 (στ)*

25. Πώς διαχειριζόμαστε έντυπο ιατρικό φάκελο;

Σε κλειδωμένα ντουλάπια, με ελεγχόμενη πρόσβαση και αρχείο δανεισμού· καταστροφή με καταστροφέα εγγράφων (shredder) ή πιστοποιημένο φορέα και πρωτόκολλο καταστροφής.

Νομική βάση: *Καν. 2016/679, άρθρο 32 & άρθρο 5 παρ. 1 (στ)*

26. Τι κάνουμε με «λάθος φάκελο» στα χέρια μας;

Δεν τον διαβάζουμε. Τον επιστρέφουμε άμεσα στον αρμόδιο και ενημερώνουμε τον DPO αν υπάρχει υπόνοια διαρροής ή έκθεσης δεδομένων.

Νομική βάση: *Καν. 2016/679, άρθρο 5 παρ. 1 (στ) & άρθρο 33*

27. Μπορούμε να καταγράψουμε χειρουργείο σε βίντεο;

Για εκπαίδευση ή τεκμηρίωση: μόνο με συγκατάθεση, ψευδωνυμοποίηση όπου είναι εφικτό, ασφαλή αποθήκευση, ορισμένο χρόνο διατήρησης και DPIA σε μεγάλη κλίμακα.

Νομική βάση: *Καν. 2016/679, άρθρο 9 παρ. 2 (α) & άρθρο 35*

28. Ασθενείς σε ΜΕΘ που δεν μπορούν να συναινέσουν;

Επεξεργασία βάσει ζωτικών συμφερόντων. Όταν ο ασθενής ανακτήσει τις αισθήσεις του, ενημερώνεται για την επεξεργασία.

Νομική βάση: *Καν. 2016/679, άρθρο 9 παρ. 2 (γ) & άρθρο 6 παρ. 1 (δ)*

Δ. Συγκατάθεση & νόμιμες βάσεις

29. Χρειάζεται «συγκατάθεση ΓΚΠΔ» για θεραπεία;

ΟΧΙ. Η νόμιμη βάση είναι η παροχή υγειονομικής περίθαλψης. Η ιατρική συναίνεση σε θεραπεία είναι διαφορετική έννοια από τη συγκατάθεση ΓΚΠΔ.

Νομική βάση: *Καν. 2016/679, άρθρο 9 παρ. 2 (η) & άρθρο 6 παρ. 1 (ε)/(β) · Ν. 3418/2005*

30. Πότε χρειάζεται συγκατάθεση ΓΚΠΔ;

Για προαιρετικές επεξεργασίες: ενημερωτικό δελτίο (newsletter), εμπορική προώθηση (marketing), έρευνα, φωτογραφίσεις, χρήση εικόνας, μη αναγκαία αρχεία εντοπισμού (cookies).

Νομική βάση: *Καν. 2016/679, άρθρο 6 παρ. 1 (α) & άρθρο 9 παρ. 2 (α) · Ν. 3471/2006*

31. Πώς πρέπει να είναι η συγκατάθεση;

Ελεύθερη, ειδική, ρητή, σε πλήρη επίγνωση, αποδεικνύσιμη και εξίσου εύκολα ανακλητέα.

Νομική βάση: *Καν. 2016/679, άρθρο 4 παρ. 11 & άρθρο 7*

32. Επιτρέπονται προ-συμπληρωμένα προσυμπληρωμένα πεδία επιλογής (checkboxes);

Όχι — απαιτείται θετική ενέργεια του υποκειμένου (ρητή συγκατάθεση (opt-in)). Η σιωπή ή τα προ-επιλεγμένα πεδία δεν συνιστούν έγκυρη συγκατάθεση.

Νομική βάση: *Καν. 2016/679, άρθρο 4 παρ. 11 & άρθρο 7 (αιτ. σκέψη 32)*

33. Τι ισχύει για συγκατάθεση ανηλίκου;

Για υπηρεσίες Κοινωνίας της Πληροφορίας: έως 15 ετών συναινούν οι γονείς, άνω των 15 ο ίδιος. Για ιατρικές πράξεις: συναίνεση γονέων μαζί με την ώριμη κρίση του ανηλίκου.

Νομική βάση: *Ν. 4624/2019, άρθρο 21 · Καν. 2016/679, άρθρο 8 · Ν. 3418/2005, άρθρο 12*

34. Μπορεί να ανακαλέσει τη συγκατάθεση;

Ναι, ανά πάσα στιγμή και εξίσου εύκολα όπως τη χορήγησε. Η ανάκληση δεν θίγει τη νομιμότητα της επεξεργασίας που προηγήθηκε.

Νομική βάση: *Καν. 2016/679, άρθρο 7 παρ. 3*

35. Σχέση «ιατρικής συναίνεσης» και «συγκατάθεσης ΓΚΠΔ»;

Διακριτές έννοιες: η ιατρική συναίνεση αφορά την εκτέλεση ιατρικής πράξης· η συγκατάθεση ΓΚΠΔ αφορά την επεξεργασία δεδομένων. Συχνά συνυπάρχουν, με σαφή διαχωρισμό.

Νομική βάση: *Ν. 3418/2005, άρθρα 11–12 · Καν. 2016/679, άρθρο 7*

36. Νόμιμη βάση δήλωσης κρούσματος στον ΕΟΔΥ;

Έννομη υποχρέωση σε συνδυασμό με δημόσιο συμφέρον στη δημόσια υγεία — όχι συγκατάθεση.

Νομική βάση: *Καν. 2016/679, άρθρο 6 παρ. 1 (γ) & άρθρο 9 παρ. 2 (θ)*

Ε. Ασφάλεια & παραβιάσεις

37. Πού γνωστοποιείται μια παραβίαση δεδομένων;

Στην ΑΠΔΠΧ εντός 72 ωρών από τη γνώση της και, εφόσον υπάρχει υψηλός κίνδυνος για τα δικαιώματα των προσώπων, και στα ίδια τα υποκείμενα.

Νομική βάση: *Καν. 2016/679, άρθρα 33–34*

38. Τι θεωρείται παραβίαση δεδομένων;

Κάθε περιστατικό που οδηγεί σε καταστροφή, απώλεια, αλλοίωση ή μη εξουσιοδοτημένη πρόσβαση / κοινολόγηση: λογισμικό λύτρων (ransomware), κλοπή φορητό υπολογιστή (laptop), λάθος αποστολή email, χαμένος φάκελος.

Νομική βάση: *Καν. 2016/679, άρθρο 4 παρ. 12*

39. Τι κάνω αν χάσω USB με δεδομένα ασθενών;

Άμεση ειδοποίηση DPO και προϊσταμένου, με καταγραφή του περιστατικού. Αν τα δεδομένα ήταν μη κρυπτογραφημένα, πιθανή γνωστοποίηση στην ΑΠΔΠΧ και ενημέρωση των ασθενών.

Νομική βάση: *Καν. 2016/679, άρθρα 33–34 & άρθρο 32 παρ. 1 (α)*

40. Τι είναι το «ψάρεμα» (phishing);

Ηλεκτρονική απάτη με ψεύτικα μηνύματα για κλοπή κωδικών ή εγκατάσταση κακόβουλου λογισμικού. Σήματα: επείγουσα γλώσσα, ορθογραφικά λάθη, ύποπτος αποστολέας ή σύνδεσμοι.

Νομική βάση: *Καν. 2016/679, άρθρο 32*

41. Πώς προστατεύω τον κωδικό μου;

Ισχυρός κωδικός (12+ χαρακτήρες), MFA, μη διαμοιρασμός, άμεση αλλαγή σε υποψία διαρροής και χρήση διαχειριστή κωδικών.

Νομική βάση: *Καν. 2016/679, άρθρο 32 παρ. 1*

42. Επιτρέπεται τηλεργασία με δεδομένα ασθενών;

Μόνο εφόσον το επιτρέπει η πολιτική του Οργανισμού: μέσω VPN, σε εταιρικό εξοπλισμό, σε ιδιωτικό χώρο και με κλείδωμα οθόνης.

Νομική βάση: *Καν. 2016/679, άρθρο 32 & άρθρο 5 παρ. 1 (στ)*

43. Τι κάνουμε με παλιά αρχεία προς καταστροφή;

Έντυπα: καταστροφέα εγγράφων (shredder) ή πιστοποιημένος φορέας με πρωτόκολλο καταστροφής. Ηλεκτρονικά: ασφαλής διαγραφή (ασφαλή διαγραφή (wiping)) ή φυσική καταστροφή των δίσκων.

Νομική βάση: *Καν. 2016/679, άρθρο 5 παρ. 1 (ε) & άρθρο 32*

44. Βλέπω συνάδελφο να ψάχνει φακέλους που δεν τον αφορούν;

Ενημερώνω τον DPO ή τον προϊστάμενο. Η μη εξουσιοδοτημένη πρόσβαση αποτελεί πειθαρχικό και ποινικό αδίκημα.

Νομική βάση: *Ν. 4624/2019, άρθρο 38 · Καν. 2016/679, άρθρο 32*

ΣΤ. DPO · ΑΔΕ · DPIA

45. Ποιος είναι ο DPO και ποιος ο ρόλος του;

Ο Υπεύθυνος Προστασίας Δεδομένων. Συμβουλεύει, παρακολουθεί τη συμμόρφωση και συνεργάζεται με την ΑΠΔΠΧ. Είναι ανεξάρτητος και αναφέρεται στην ανώτατη διοίκηση.

Νομική βάση: *Καν. 2016/679, άρθρα 37–39*

46. Είναι υποχρεωτικός ο DPO σε νοσοκομείο;

Ναι. Τα δημόσια νοσοκομεία (ΝΠΔΔ) έχουν πάντοτε υποχρέωση· συχνά ο DPO ορίζεται σε επίπεδο φορέα ή Υ.Πε. Τα ιδιωτικά που επεξεργάζονται ειδικές κατηγορίες σε μεγάλη κλίμακα επίσης υποχρεούνται.

Νομική βάση: *Καν. 2016/679, άρθρο 37 παρ. 1 (β)–(γ)*

47. Ο DPO εσωτερικός ή εξωτερικός;

Και τα δύο επιτρέπονται. Σε μικρότερες κλινικές επιλέγεται συχνά εξωτερικός DPO (υπηρεσία παρόχου).

Νομική βάση: *Καν. 2016/679, άρθρο 37 παρ. 6*

48. Τι είναι το ΑΔΕ;

Αρχείο Δραστηριοτήτων Επεξεργασίας — η καταγραφή όλων των επεξεργασιών του φορέα. Είναι υποχρεωτικό για τις μονάδες υγείας.

Νομική βάση: *Καν. 2016/679, άρθρο 30*

49. Ποιος συντάσσει το ΑΔΕ;

Ο Υπεύθυνος Επεξεργασίας, με τη συνδρομή των τμημάτων και την επίβλεψη του DPO. Επικαιροποιείται τουλάχιστον ετησίως.

Νομική βάση: *Καν. 2016/679, άρθρο 30 παρ. 1 & άρθρο 24*

50. Τι είναι το DPIA;

Εκτίμηση Αντικτύπου — αξιολόγηση κινδύνων για νέες επεξεργασίες υψηλού κινδύνου (νέο HIS, διαγνωστικό AI, βιομετρικά).

Νομική βάση: *Καν. 2016/679, άρθρο 35 · Απόφ. ΑΠΔΠΧ 65/2018*

51. Ποιος εγκρίνει το DPIA;

Συντάσσεται από τον Υπεύθυνο, με συμβουλή του DPO, και εγκρίνεται από τη Διοίκηση. Αν παραμένει υψηλός κίνδυνος, απαιτείται προηγούμενη διαβούλευση με την ΑΠΔΠΧ.

Νομική βάση: *Καν. 2016/679, άρθρα 35–36*

52. Σύμβαση με εξωτερικό εργαστήριο;

Ναι — σύμβαση ανάθεσης (DPA) με υποχρεώσεις εμπιστευτικότητας, ασφάλειας, ελέγχου υπεργολάβων και επιστροφής / διαγραφής δεδομένων στο τέλος.

Νομική βάση: *Καν. 2016/679, άρθρο 28*

Ζ. Έρευνα · τηλεϊατρική · ειδικά

53. Επεξεργασία για κλινική μελέτη;

Απαιτείται έγκριση Επιτροπής Ηθικής, ΕΟΦ (για φάρμακα), πρωτόκολλο, Ενημερωμένη Συγκατάθεση, ψευδωνυμοποίηση, DPIA και καταχώριση στο ΑΔΕ.

Νομική βάση: *Καν. 2016/679, άρθρο 9 παρ. 2 (ι)/(α) & άρθρο 89 · Ν. 4624/2019, άρθρο 30*

54. Δεδομένα ασθενών για δημοσίευση άρθρου;

Μόνο πλήρως ανωνυμοποιημένα ή με ρητή συγκατάθεση. Σε εικόνες, κάλυψη των χαρακτηριστικών αναγνώρισης.

Νομική βάση: *Καν. 2016/679, άρθρο 9 παρ. 2 (α) & αιτ. σκέψη 26*

55. Τι ισχύει για την τηλεϊατρική;

Απαιτείται κρυπτογραφημένη πλατφόρμα, ταυτοποίηση ασθενούς, ενημέρωση ιδιωτικότητας, DPA με τον πάροχο και καταχώριση στο ΑΔΕ.

Νομική βάση: *Καν. 2016/679, άρθρο 9 παρ. 2 (η), άρθρο 28 & άρθρο 32*

56. Επιτρέπεται καταγραφή τηλεσυνεδρίας;

Μόνο με ρητή συγκατάθεση πριν την έναρξη, ασφαλή αποθήκευση και προκαθορισμένο χρόνο διατήρησης.

Νομική βάση: *Καν. 2016/679, άρθρο 9 παρ. 2 (α) & άρθρο 5 παρ. 1 (ε)*

57. Τι ισχύει για CCTV σε νοσοκομείο;

Βάση το δημόσιο συμφέρον / ασφάλεια. ΟΧΙ σε χώρους νοσηλείας, εξεταστήρια ή τουαλέτες. Πινακίδες ενημέρωσης, τήρηση έως ~15 ημέρες με αυτόματη διαγραφή· συνιστάται DPIA.

Νομική βάση: *Καν. 2016/679, άρθρο 6 παρ. 1 (ε) & άρθρο 13 · κατευθυντήριες ΑΠΔΠΧ βιντεοεπιτήρησης*

58. Φορετές συσκευές (φορετές συσκευές (wearables)) / εφαρμογές υγείας σε εργαζομένους;

Μόνο με πραγματικά ελεύθερη συγκατάθεση (δύσκολο λόγω της εργασιακής σχέσης), DPIA και διαχωρισμό των δεδομένων από τον εργοδότη (μόνο συγκεντρωτικά (aggregated)).

Νομική βάση: *Ν. 4624/2019, άρθρο 27 · Καν. 2016/679, άρθρο 9 & άρθρο 35*

59. Αναφορά παράνομης συμπεριφοράς (αναφορά παρατυπιών (whistleblowing));

Εσωτερικό κανάλι (για φορείς >50 εργαζομένων), εμπιστευτικότητα της ταυτότητας του αναφέροντος, καταγραφή, διερεύνηση και προστασία από αντίποινα.

Νομική βάση: *Ν. 4990/2022 · Καν. 2016/679, άρθρα 5–6*

60. Ποιοι οι κίνδυνοι κυρώσεων σε παραβίαση;

Διοικητικά πρόστιμα ΑΠΔΠΧ (έως 20 εκατ. € ή 4%· έως 10 εκατ. € για δημόσιους φορείς), αστική αποζημίωση, ποινικές και πειθαρχικές κυρώσεις, καθώς και βλάβη φήμης.

Νομική βάση: *Καν. 2016/679, άρθρα 82–84 · Ν. 4624/2019, άρθρα 38–39*

18. Πίνακες γρήγορης αναφοράς

Α. Νόμιμη βάση ανά σκοπό (άρθρα 6 & 9)

Σκοπός	Άρθρο 6	Άρθρο 9
Θεραπεία / φροντίδα	**6(1)(ε) ή (β)**	**9(2)(η)**
Επείγον σε αναίσθητο	**6(1)(δ)**	**9(2)(γ)**
Δημόσια υγεία / ΕΟΔΥ	**6(1)(γ)**	**9(2)(θ)**
Έρευνα / κλινική μελέτη	**6(1)(α) ή (ε)**	**9(2)(α) ή (ι)**
Προώθηση (marketing) / ενημ. δελτίο	**6(1)(α)**	**9(2)(α) αν χρειάζεται**
CCTV ασφάλειας	**6(1)(ε)/(στ)**	—

Β. Χρόνοι τήρησης ιατρικού αρχείου

Φορέας	Χρόνος (από τελευταία επίσκεψη)
Ιδιωτική Π.Φ.Υ. (ιατρεία & λοιπές μονάδες ιδιωτικού τομέα)	**10 έτη**
Κάθε άλλη περίπτωση (νοσοκομεία, κλινικές)	**20 έτη**
Ανήλικοι	**Έως ενηλικίωση + προβλεπόμενος χρόνος**

Γ. Προθεσμίες-κλειδιά

Ενέργεια	Προθεσμία
Γνωστοποίηση παραβίασης στην ΑΠΔΠΧ	**72 ώρες από τη γνώση**
Απάντηση σε αίτημα δικαιώματος	**1 μήνας (+2 για πολύπλοκα)**
Πρώτο αντίγραφο φακέλου	**Δωρεάν**

19. Λίστα ελέγχου προσωπικού

Δέκα σημεία αυτοελέγχου. Αν απαντάτε «ναι» σε όλα, είστε σε καλό δρόμο.

- □ Βλέπω μόνο τα δεδομένα που χρειάζομαι (need-to-know).
- □ Κλειδώνω την οθόνη και δεν αφήνω έγγραφα εκτεθειμένα.
- □ Δεν μοιράζομαι κωδικούς· χρησιμοποιώ MFA.
- □ Δεν συζητώ για ασθενείς σε κοινόχρηστους χώρους.
- □ Χρησιμοποιώ μόνο εγκεκριμένα κανάλια & μέσα.
- □ Ταυτοποιώ πάντα πριν δώσω πληροφορία ή αντίγραφο.
- □ Γνωρίζω ότι η θεραπεία στηρίζεται στο 9(2)(η), όχι στη συγκατάθεση.
- □ Αναφέρω άμεσα κάθε ύποπτο περιστατικό (72ωρο).
- □ Δεν κάνω κλικ σε ύποπτα emails/links.
- □ Όταν αμφιβάλλω, ρωτώ τον DPO πριν ενεργήσω.

20. Κυρώσεις — τι διακυβεύεται

Είδος	Ύψος / συνέπεια
Διοικητικό πρόστιμο (ιδιωτικοί)	έως 20 εκατ. € ή 4% του τζίρου

Είδος	Ύψος / συνέπεια
Διοικητικό πρόστιμο (δημόσιοι φορείς)	έως 10 εκατ. € (άρθρο 39 Ν. 4624/2019)
Ποινικές κυρώσεις	φυλάκιση & χρηματική ποινή έως 300.000 € (άρθρο 38 Ν. 4624/2019)
Αστική αποζημίωση	στον θιγόμενο (άρθρο 82 ΓΚΠΔ)
Πειθαρχικές & βλάβη φήμης	εσωτερικές συνέπειες & απώλεια εμπιστοσύνης

ΣΗΜΕΙΩΣΗ

Στους δημόσιους φορείς δεν εφαρμόζεται το ποσοστό επί τζίρου· ισχύει το ανώτατο όριο των 10 εκατ. € του άρθρου 39 Ν. 4624/2019.

21. Χρήσιμες επαφές & βασικό νομικό πλαίσιο

Πρώτα σημεία επαφής

DPO του Οργανισμού: το πρώτο σημείο επαφής για κάθε ερώτημα, περιστατικό ή αίτημα. (Συμπληρώστε τα στοιχεία του φορέα σας: ονοματεπώνυμο, τηλέφωνο, e-mail, ώρες επικοινωνίας.)

ΑΠΔΠΧ — Αρχή Προστασίας Δεδομένων	Στοιχεία
Διεύθυνση	Λεωφ. Κηφισίας 1-3, Τ.Κ. 115 23, Αθήνα
Τηλέφωνο	+30 210 6475600
E-mail	contact@dpa.gr
Ιστότοπος	www.dpa.gr

ΣΗΜΕΙΩΣΗ

Τα στοιχεία επικοινωνίας δημόσιων αρχών ενδέχεται να μεταβληθούν. Επιβεβαιώνετε πάντα από τον επίσημο ιστότοπο www.dpa.gr πριν από κάθε επίσημη υποβολή.

Λοιπές πηγές & αρχές

Φορέας	Αντικείμενο	Ιστότοπος
EDPB	Ευρωπαϊκές κατευθυντήριες γραμμές	edpb.europa.eu
Ευρωπαϊκή Επιτροπή	Αποφάσεις επάρκειας — διαβιβάσεις	commission.europa.eu
ΕΟΔΥ	Δημόσια υγεία — υποχρεωτικές δηλώσεις	eody.gov.gr
Υπουργείο Υγείας	Τομεακό πλαίσιο υγείας	moh.gov.gr

Βασικό νομικό πλαίσιο αναφοράς

Νομοθέτημα	Αντικείμενο
Καν. (ΕΕ) 2016/679 (ΓΚΠΔ)	Γενικός Κανονισμός Προστασίας Δεδομένων.
Ν. 4624/2019 (κωδ. με Ν. 5221/2025)	Εθνικά μέτρα εφαρμογής ΓΚΠΔ — εποπτεία ΑΠΔΠΧ, ποινικές κυρώσεις (άρ. 38), όριο 15 ετών (άρ. 21).
Ν. 3418/2005 (ΚΙΔ)	Κώδικας Ιατρικής Δεοντολογίας — ιατρικό απόρρητο (άρ. 13), τήρηση αρχείου (άρ. 14).
Ν. 3471/2006	Προστασία ηλεκτρονικών επικοινωνιών (e-Privacy) — εμπορική προώθηση (marketing), αρχεία εντοπισμού (cookies).
Ν. 2690/1999 (ΚΔΔ)	Κώδικας Διοικητικής Διαδικασίας — πρόσβαση σε έγγραφα.

Νομοθέτημα	Αντικείμενο
Ν. 4990/2022	Προστασία προσώπων που αναφέρουν παραβιάσεις (whistleblowing).
Ν. 4727/2020	Ψηφιακή Διακυβέρνηση.
Ν. 4600/2019	ΑΗΦΥ — Ατομικός Ηλεκτρονικός Φάκελος Υγείας.
Καν. (ΕΕ) 2025/327 (EHDS)	Ευρωπαϊκός Χώρος Δεδομένων Υγείας.

ΣΗΜΕΙΩΣΗ

Ισχύον δίκαιο κατά τη σύνταξη: ο Ν. 4624/2019 ισχύει σε κωδικοποιημένη (ενοποιημένη) μορφή, με τελευταία τροποποίηση από τον Ν. 5221/2025 (αφορά κυρίως τη Γραμματεία της ΑΠΔΠΧ).

22. Γλωσσάρι όρων

Όρος	Επεξήγηση
ΓΚΠΔ / ΓΚΠΔ	Γενικός Κανονισμός Προστασίας Δεδομένων, Καν. (ΕΕ) 2016/679 — το βασικό ευρωπαϊκό νομοθέτημα.
Προσωπικά Δεδομένα	Κάθε πληροφορία για ταυτοποιημένο/ταυτοποιήσιμο πρόσωπο (όνομα, ΑΜΚΑ, e-mail, αναγνωριστικά).
Ειδικές Κατηγορίες	Ευαίσθητα δεδομένα — υγείας, γενετικά, βιομετρικά κ.ά. — με ενισχυμένη προστασία (άρθρο 9).
Δεδομένα Υγείας	Δεδομένα για τη σωματική/ψυχική υγεία και την παροχή υπηρεσιών υγείας.
Υπεύθυνος Επεξεργασίας	Υπεύθυνος Επεξεργασίας (Controller) — καθορίζει σκοπούς & τρόπο επεξεργασίας (π.χ. το νοσοκομείο).
Εκτελών την Επεξεργασία	Εκτελών την Επεξεργασία (Processor) — επεξεργάζεται για λογαριασμό του Υπευθύνου (υπολογιστικό νέφος (cloud), HIS, μισθοδοσία).
DPO (ΥΠΔ)	Υπεύθυνος Προστασίας Δεδομένων — Υπεύθυνος Προστασίας Δεδομένων· υποχρεωτικός στους φορείς υγείας.
DPIA (ΕΑΠΔ)	Εκτίμηση Αντικτύπου — υποχρεωτική για επεξεργασίες υψηλού κινδύνου (άρθρο 35).
ΑΔΕ / RoPA	Αρχείο Δραστηριοτήτων Επεξεργασίας — καταγραφή όλων των επεξεργασιών (άρθρο 30).
ΑΠΔΠΧ / DPA	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα — η εθνική εποπτική αρχή.
EDPB	Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων — εκδίδει κατευθυντήριες γραμμές σε επίπεδο ΕΕ.
Συγκατάθεση	Ελεύθερη, ειδική, ρητή & εν πλήρει επιγνώσει δήλωση βούλησης· πάντα ανακλητή.
Νόμιμη Βάση	Μία από τις βάσεις του άρθρου 6 (& 9 για ειδικές κατηγορίες) που νομιμοποιεί την επεξεργασία.
Προστασία ήδη από τον σχεδιασμό & εξ ορισμού	Ενσωμάτωση προστασίας ήδη από τον σχεδιασμό & εξ ορισμού (άρθρο 25).
Ψευδωνυμοποίηση	Επεξεργασία ώστε τα δεδομένα να μην αποδίδονται σε πρόσωπο χωρίς πρόσθετες πληροφορίες.
Ανωνυμοποίηση	Μη αναστρέψιμη αφαίρεση κάθε στοιχείου ταυτοποίησης· τα δεδομένα παύουν να είναι προσωπικά.
Ενημέρωση Ιδιωτικότητας	Ενημέρωση Ιδιωτικότητας — ενημέρωση των υποκειμένων για την επεξεργασία (άρθρα 13–14).
Δικαίωμα στη Λήθη	Δικαίωμα στη λήθη — διαγραφή δεδομένων υπό προϋποθέσεις (άρθρο 17).
Φορητότητα	Λήψη των δεδομένων σε δομημένο, κοινό μορφότυπο & διαβίβασή τους (άρθρο 20).
Λογοδοσία	Υποχρέωση συμμόρφωσης & απόδειξής της (άρθρο 5§2).
Ελάχιστη αναγκαία πρόσβαση (ελάχιστη αναγκαία πρόσβαση (need-to-know))	Αρχή ελάχιστης πρόσβασης: κάθε εργαζόμενος βλέπει μόνο όσα χρειάζεται.
RBAC	Έλεγχος Πρόσβασης βάσει Ρόλου — έλεγχος πρόσβασης βάσει ρόλου/θέσης.
MFA	Ταυτοποίηση Πολλαπλών Παραγόντων — ταυτοποίηση πολλαπλών παραγόντων (κωδικός + OTP).

Όρος	Επεξήγηση
Κρυπτογράφηση	Μετατροπή δεδομένων σε μη αναγνώσιμη μορφή χωρίς το κλειδί αποκρυπτογράφησης.
HIS / EHR	Πληροφοριακό Σύστημα Νοσοκομείου / Ηλεκτρονικός Φάκελος Υγείας.
DPA (σύμβαση)	Σύμβαση Ανάθεσης Επεξεργασίας — σύμβαση ανάθεσης Υπευθύνου–Εκτελούντος (άρθρο 28).
SCCs	Τυποποιημένες Συμβατικές Ρήτρες — τυποποιημένες ρήτρες για διαβιβάσεις εκτός ΕΟΧ.
BCRs	Δεσμευτικοί Εταιρικοί Κανόνες — δεσμευτικοί εταιρικοί κανόνες για διαβιβάσεις εντός ομίλου.
Παραβίαση (Παραβίαση)	Παραβίαση ασφάλειας με απώλεια/διαρροή/μη εξουσιοδοτημένη πρόσβαση· 72ωρο (άρθρο 33).
«Ψάρεμα» («ψάρεμα» (phishing))	Απάτη μέσω πλαστών μηνυμάτων για υποκλοπή κωδικών ή δεδομένων.
Λογισμικό λύτρων (λογισμικό λύτρων (ransomware))	Κακόβουλο λογισμικό που κρυπτογραφεί αρχεία & απαιτεί λύτρα — συχνό σε φορείς υγείας.
Αναφορά παρατυπιών (αναφορά παρατυπιών (whistleblowing))	Αναφορά παρατυπιών μέσω εσωτερικών διαύλων (Ν. 4990/2022) με προστασία αναφέροντος.

— Σεβασμός · Ασφάλεια · Διαφάνεια —

σε κάθε δεδομένο ασθενούς και εργαζομένου