

Εφαρμογή του νέου Ευρωπαϊκού Κανονισμού 679/2016 για την προστασία προσωπικών δεδομένων

Επίτροπος Προστασίας
Δεδομένων Προσωπικού Χαρακτήρα

2 Μαρτίου 2018

1

Πρωτογενές Δίκαιο

Σύμβαση Ανθρωπίνων Δικαιωμάτων ΣΤΕ

- Άρθρο 8: ιδιωτική & οικογενειακή ζωή

Σύνταγμα ΚΔ

- Άρθρο 15: ιδιωτική & οικογενειακή ζωή

Χάρτης θεμελιωδών Δικαιωμάτων ΕΕ

- Άρθρο 7: ιδιωτική & οικογενειακή ζωή
- Άρθρο 8: προστασία προσωπικών δεδομένων

2

Υφιστάμενο Νομικό Πλαίσιο

- Κυρωτικοί Νόμοι της Σύμβασης 108 και του Πρόσθετου Πρωτοκόλλου της
- Ο περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου Νόμος του 2001 (Εναρμονιστικός - Οδηγία 95/46/ΕΚ)
- Κανονισμός (ΕΕ) 679/2016 που αντικαθιστά την Οδηγία 95/46/ΕΚ

3

Ο (Γενικός) Κανονισμός (ΕΕ) 679/2016

- Τέθηκε σε ισχύ στις 24/05/2016 και θα εφαρμοστεί στις 25/05/2018
- Καταργεί την Οδηγία 95/46/ΕΚ, η οποία μεταφέρθηκε στο Νόμο 138(Ι)2001 όπως τροποποιήθηκε

Σκοπός της αντικατάστασης του υφιστάμενου πλαισίου:

- Οι ραγδαίες τεχνολογικές εξελίξεις και η παγκοσμιοποίηση: η Οδηγία δεν ανταποκρινόταν επαρκώς στις ανάγκες της εποχής με smartphones, social media, internet banking
- Αυξανόμενη δημοσιοποίηση προσωπικών πληροφοριών και διάθεσή τους σε παγκόσμιο επίπεδο

4

Πεδίο εφαρμογής

- Στο έδαφος της Κυπριακής Δημοκρατίας
- Όταν εφαρμόζεται το κυπριακό δίκαιο δυνάμει διεθνούς δικαίου
- Διασυνοριακές υποθέσεις που αφορούν πρόσωπα σε περισσότερα κράτη μέλη (συνδεδεμένες εταιρείες)
- Σε επεξεργασία εκτός ΕΕ για υποκείμενα που βρίσκονται εντός ΕΕ
- Σε επεξεργασία που εκτελείται στην ΕΕ για υποκείμενα που βρίσκονται εκτός ΕΕ

5

- **Κύρια εγκατάσταση:** ορίζεται, όταν μια εταιρεία έχει εγκαταστάσεις σε πολλά κμ
- ❖ **Για υπεύθυνο επεξεργασίας:** ο τόπος λήψης αποφάσεων για τους σκοπούς και τα μέσα της επεξεργασίας και εξουσίας εφαρμογής των αποφάσεων αυτών, αλλιώς ο τόπος της κεντρικής διοίκησης στην ΕΕ
- ❖ **Για εκτελών την επεξεργασία:** ο τόπος της κεντρικής διοίκησης στην ΕΕ , αλλιώς ο τόπος όπου εκτελούνται οι κύριες δραστηριότητες επεξεργασίας

6

Ορισμοί

- **Δεδομένα που αφορούν στην υγεία:** προσωπικά δεδομένα που αφορούν στη σωματική ή ψυχική υγεία φυσικού προσώπου, π.χ. παροχή υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του
 - **γενετικά δεδομένα:** δεδομένα που κληρονομήθηκαν ή αποκτήθηκαν από ανάλυση βιολογικού δείγματος και παρέχουν μοναδικές πληροφορίες για την υγεία ή φυσιολογία π.χ. DNA
 - **βιομετρικά δεδομένα:** δεδομένα που προκύπτουν από ειδική τεχνική επεξεργασία και επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση φυσικού προσώπου π.χ. εικόνες προσώπου, δακτυλοσκοπικά δεδομένα
- ❖ Εμπίπτουν στις «ειδικές κατηγορίες προσωπικών δεδομένων»

7

- **Υπεύθυνος επεξεργασίας: το κάθε νοσοκομείο ξεχωριστά**
Καθορίζει τους σκοπούς της συλλογής και επεξεργασίας των προσωπικών δεδομένων, τα μέσα για την επίτευξη των σκοπών αυτών καθώς και την πολιτική και τα μέτρα ασφαλείας για τη διασφάλιση του απορρήτου και την προστασία των προσωπικών δεδομένων
- ΠΑΡΑΔΕΙΓΜΑΤΑ:** (α) υπεύθυνος επεξεργασίας του Αρχείου Μαγνητικού Τομογράφου του Αρεταίειου Νοσοκομείου είναι το ίδιο το Αρεταίειο
(β) υπεύθυνος επεξεργασίας του Μητρώου Γεννήσεων της Μονάδας Παρακολούθησης Υγείας είναι το Υπουργείο Υγείας
(γ) υπεύθυνος επεξεργασίας του αρχείου «παροχής ιατρικών υπηρεσιών» του Νοσοκομείου Λεμεσού είναι το ίδιο το Νοσοκομείο
- Για σκοπούς του Κανονισμού:
- Το κάθε νοσοκομείο ξεχωριστά (ως νομική οντότητα) συνιστά υπεύθυνο επεξεργασίας και υπεύθυνο για την εφαρμογή και τήρηση των προνοιών του Κανονισμού
 - Τα τμήματα/μονάδες δεν θεωρούνται ξεχωριστοί υπεύθυνοι επεξεργασίας

8

➤ **Εκτελών την επεξεργασία**

❖ Το φυσικό πρόσωπο ή νομική οντότητα **εκτός του υπεύθυνου επεξεργασίας** που επεξεργάζεται δεδομένα εκ μέρους και για λογαριασμό του

ΠΑΡΑΔΕΙΓΜΑΤΑ

- Εταιρεία καταστροφής ή φύλαξης φακέλων ιδιωτικών νοσοκομείων
- Το Ινστιτούτο Νευρολογίας και Γενετικής Κύπρου που επεξεργάζεται εξετάσεις μοριακής βιολογίας για το στίγμα θαλασσαιμίας εκ μέρους του Υπουργείου Υγείας και του Νοσοκομείου Μακάριος Γ΄
- ❖ Η σχετική ανάθεση γίνεται **ΥΠΟΧΡΕΩΤΙΚΑ ΓΡΑΠΤΩΣ** (Άρθρο 28)
- ❖ Επιλογή του κατάλληλου εκτελούντος ο οποίος θα πρέπει να παρέχει εχέγγυα απορρήτου και ασφάλειας των δεδομένων
- Εκτελών την επεξεργασία που επεξεργάζεται τα δεδομένα για δικούς του σκοπούς καθίσταται υπεύθυνος επεξεργασίας

9

Ενισχύει τις υφιστάμενες αρχές προστασίας των δεδομένων:

- ❖ **Διαφάνεια:** οι εσωτερικές διαδικασίες θα πρέπει να αποδεικνύεται ότι είναι διαφανείς
- ❖ **Αρχή του περιορισμού του σκοπού**
 - **Περαιτέρω επεξεργασία** για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς, εφόσον πληρούνται οι προϋποθέσεις του άρθρου 89
 - **Άρθρο 89:** υιοθέτηση τεχνικών και οργανωτικών μέτρων, π.χ. ψευδωνυμοποίηση ούτως ώστε να μην ταυτοποιούνται τα υποκείμενα, δεδομένου ότι, οι εν λόγω σκοποί μπορούν να εκπληρωθούν με τον τρόπο αυτό
 - Σε περίπτωση μη ταυτοποίησης των υποκειμένων, οι ερευνητές δεν έχουν υποχρέωση λήψης συγκατάθεσης για κάθε νέα χρήση των δεδομένων στην έρευνα

10

❖ **Ελαχιστοποίηση των δεδομένων:** συλλογή μόνο των αναγκαίων δεδομένων για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία

ΠΑΡΑΔΕΙΓΜΑΤΑ συλλογής υπερβολικών δεδομένων:

(α) η θρησκεία του ασθενή

(β) η αναγραφή της πάθησης του ασθενή στις συνταγές που εκδίδονται από ιατρούς

❖ **Διατήρηση / αποθήκευση:** μόνο για όσο διάστημα χρειάζεται για τους σκοπούς της επεξεργασίας

❖ **Ακεραιότητα και εμπιστευτικότητα:** προστασία και ασφάλεια των δεδομένων π.χ. από μη εξουσιοδοτημένη ή παράνομη επεξεργασία, απώλεια

❖ **Λογοδοσία:** ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με τις αρχές που διέπουν την επεξεργασία

11

Πότε είναι νόμιμη η επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων

❖ Κατά κανόνα απαγορεύεται η επεξεργασία τους

❖ **Επιτρέπεται όταν:**

(α) **υπάρχει συγκατάθεση**

- το άτομο την δίνει ελεύθερα
- είναι σε θέση να επιλέξει
- δεν διατρέχει τον κίνδυνο εξαπάτησης, εκφοβισμού, εξαναγκασμού ή σημαντικών αρνητικών επιπτώσεων εάν δεν συγκατατεθεί
- Ο υπεύθυνος επεξεργασίας **πρέπει να αποδείξει** ότι το άτομο έδωσε τη συγκατάθεσή του
- Μπορεί να ανακληθεί ανά πάσα στιγμή

(β) αφορά στον τομέα του εργατικού δικαίου, δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας

(γ) αφορά σε ζωτικό συμφέρον

12

- (δ) αφορά σε δραστηριότητες ιδρύματος, οργάνωσης ή άλλου μη κερδοσκοπικού φορέα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό στόχο – αφορά τα μέλη ή τα πρώην μέλη του ή πρόσωπα που έχουν τακτική επικοινωνία μαζί του και τα δεδομένα δεν κοινοποιούνται σε τρίτους
- (ε) αφορά σε δεδομένα που έχουν δημοσιοποιηθεί από το άτομο
- (στ) αφορά σε θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων
- (ζ) αφορά σε λόγους ουσιαστικού δημόσιου συμφέροντος
- (η) αφορά σε προληπτική ή επαγγελματική ιατρική, εκτίμηση ικανότητας εργασίας, ιατρική διάγνωση, υγειονομική ή κοινωνική περίθαλψη ή θεραπεία ή διαχείριση υγειονομικών και κοινωνικών συστημάτων δυνάμει νόμου ή σύμβασης με επαγγελματία στον τομέα της υγείας που τηρεί το επαγγελματικό απόρρητο

13

- (θ) αφορά σε λόγους δημόσιου συμφέροντος: π.χ. δημόσια υγεία, διασφάλιση υψηλών προτύπων ποιότητας και ασφάλειας της υγειονομικής περίθαλψης και φαρμάκων ή των ιατροτεχνολογικών προϊόντων
- (ι) αφορά σε σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, σε σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς

ΠΑΡΑΔΕΙΓΜΑ:

Η λήψη δεδομένων υγείας από φακέλους ασθενών χωρίς τη συγκατάθεση τους και/ή

η διεξαγωγή επιστημονικής έρευνας που αφορά δεδομένα υγείας τα οποία ο ερευνητής ΔΕΝ λαμβάνει απευθείας εθελοντικά από τους ασθενείς και/ή η διαβίβαση δεδομένων υγείας σε τρίτες χώρες,

επιτρέπεται ΜΟΝΟ όταν ισχύει ΤΟΥΛΑΧΙΣΤΟΝ μία από τις εξαιρέσεις των παραγράφων: (ζ – ουσιαστικό δημόσιο συμφέρον), (η – για προληπτική/επαγγελματική ιατρική, παροχή υγειονομικής περίθαλψης κλπ), (θ – δημόσιο συμφέρον στον τομέα της δημόσιας υγείας), (ι- επιστημονική έρευνα η οποία υπόκειται σε κατάλληλες εγγυήσεις π.χ. χρήση ψευδωνύμων και ελαχιστοποίηση των δεδομένων)

14

Νέες υποχρεώσεις υπεύθυνου επεξεργασίας

1. Φέρει το βάρος της αποδείξεως όσον αφορά στην παροχή συγκατάθεσης

- Καταργείται η σιωπηρή συγκατάθεση
- Δήλωση συγκατάθεσης: σε απλή και κατανοητή γλώσσα
- Απόδειξη λήψης συγκατάθεσης
- Οι ασθενείς έχουν την επιλογή να συγκατατίθενται ξεχωριστά για τη συμμετοχή σε ιατρική ή επιστημονική έρευνα

2. Εφαρμογή αρχής «Privacy by design»: ο αρχικός σχεδιασμός υπηρεσίας ή προϊόντος θα πρέπει να δημιουργεί φιλικές συνθήκες για την προστασία των δεδομένων

3. Εφαρμογή αρχής «Privacy by default»: εφαρμογή κατάλληλων μέτρων που θα διασφαλίζουν ότι εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα που είναι απαραίτητα για το σκοπό της επεξεργασίας

15

4. Υποχρέωση γνωστοποίησης παραβιάσεων ασφάλειας

Ο υπεύθυνος επεξεργασίας σε περίπτωση παραβίασης προσωπικών δεδομένων γνωστοποιεί αμέσως και όχι περὶ των **72 ωρών** από τη στιγμή που αποκτά γνώση του γεγονότος, την παραβίαση στην ΑΠΔΠΧ, εκτός αν η παραβίαση δεν ενδέχεται να προκαλέσει κίνδυνο. Μετά τις 72 ώρες, λογοδοτεί στην ΑΠΔΠΧ

5. Υποχρέωση ανακοίνωσης παραβιάσεων ασφάλειας

Η παραβίαση ιατρικών δεδομένων ανακοινώνεται αμέσως στο επηρεαζόμενο άτομο όταν υπάρχει ψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες του

• Η ανακοίνωση δεν απαιτείται, εάν:

- (α) είχαν ήδη εφαρμοστεί κατάλληλα μέτρα προστασίας στα δεδομένα που αφορά η παραβίαση όπως π.χ. κρυπτογράφηση
- (β) λήφθηκαν στη συνέχεια μέτρα που διασφαλίζουν ότι δεν υπάρχει κίνδυνος πλέον
- (γ) προϋποθέτει δυσανάλογες προσπάθειες (γίνεται όμως δημόσια ανακοίνωση ή παρόμοιο μέτρο για ενημέρωση των επηρεαζόμενων προσώπων)

16

6. Υποχρέωση δέσμευσης του εκτελούντα την επεξεργασία με σύμβαση ή άλλη δεσμευτική πράξη

- Συνάπτεται συμφωνία/σύμβαση μεταξύ του υπεύθυνου επεξεργασίας και του εκτελούντα, η οποία καθορίζει τις υποχρεώσεις/ευθύνες του
- Ο εκτελών επεξεργάζεται τα δεδομένα μόνο βάσει καταγεγραμμένων εντολών του υπεύθυνου
- Θέτει στη διάθεση του υπεύθυνου κάθε απαραίτητη πληροφορία
- **Ο εκτελών:**
 - Τηρεί αρχείο καταγραφής δραστηριοτήτων επεξεργασίας
 - Συνεργάζεται με την ΑΠΔΠΧ
 - Λαμβάνει κατάλληλα τεχνικά και οργανωτικά μέτρα για τη διασφάλιση της επεξεργασίας
 - Ενημερώνει τον υπεύθυνο επεξεργασίας σε περίπτωση παραβίασης
 - Διορίζει ΥΠΔ
 - Υπόκειται στον έλεγχο της εποπτικής αρχής και κυρώσεις

17

7. Ορισμός Υπεύθυνου Προστασίας Δεδομένων:

- ❖ Όταν οι βασικές δραστηριότητες επεξεργασίας απαιτούν **τακτική και συστηματική παρακολούθηση των υποκειμένων σε μεγάλη κλίμακα (π.χ. νοσοκομεία) ή μεγάλης κλίμακας επεξεργασίας ειδικών κατηγοριών δεδομένων (π.χ. δεδομένα υγείας, γενετικά δεδομένα)**

8. Τήρηση αρχείου δραστηριοτήτων: αντικαθιστά την υφιστάμενη γνωστοποίηση

- ❖ Το κάθε νοσοκομείο έχει υποχρέωση να τηρεί εσωτερικά (σε γραπτή ή ηλεκτρονική μορφή) όλα τα αρχεία των δραστηριοτήτων επεξεργασίας που ήδη γνωστοποίησε στο Γραφείο μου και οποιαδήποτε άλλα νέα αρχεία συσταθούν *(εκτός του προσωπικού)*
- ❖ **Για ιδιωτικά νοσοκομεία:** βάσει του περί Ιδιωτικών Νοσηλευτηρίων (Έλεγχος Ίδρυσης και Λειτουργίας) Νόμου του 2001. Παραδείγματα:
 - ❖ Μητρώο Ασθενών
 - ❖ Βιβλίο χειρουργείου
 - ❖ Μητρώο εργαστηριακών εξετάσεων
- ❖ **Για Δημόσια νοσοκομεία: παραδείγματα**
 - ❖ Αρχείο Μητρώου Αιμοδοτών / Μητρώου Εμβολιασμών
 - ❖ Αρχείο Μητρώου Χειρουργικών Επεμβάσεων
 - ❖ Αρχείο Μητρώου Ευρωπαϊκής Κάρτας

18

9. Ενισχυμένη ασφάλεια και εφαρμογή πολιτικών ασφάλειας

- ❖ Ψευδωνυμοποίηση και κρυπτογράφηση των δεδομένων των ασθενών
- ❖ Εκτίμηση του ενδεχόμενου επιπέδου ασφαλείας, λαμβάνοντας υπόψη τους κινδύνους που απορρέουν από την επεξεργασία (π.χ. από απώλεια, πρόσβαση στον εξυπηρετητή από hackers, κλοπή εγγράφων, διαρροή δεδομένων κ.λ.π.)
- ❖ Η τήρηση εγκεκριμένου κώδικα δεοντολογίας ή εγκεκριμένου μηχανισμού πιστοποίησης είναι στοιχείο συμμόρφωσης

Παραδείγματα:

- ❖ Να μην τοποθετούνται φάκελοι ασθενών σε διαδρόμους
- ❖ Το αρχείο με τους ιατρικούς φακέλους (σε χάρτινη μορφή) να κλειδώνεται σε ασφαλή χώρο (με επιτήρηση)

19

10. Διενέργεια εκτίμησης αντικτύπου (impact assessment):

τα νοσοκομεία που επεξεργάζονται δεδομένα υγείας ασθενών *(θεωρείται επεξεργασία που παρουσιάζει υψηλό κίνδυνο για τα δικαιώματα και ελευθερίες των ασθενών)* οφείλουν όπως, ΠΡΙΝ από την επεξεργασία, διενεργήσουν εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων

11. Τήρηση Κωδίκων Δεοντολογίας και εξασφάλιση πιστοποιήσεων, σφραγίδων και σημάτων προστασίας δεδομένων

Αφορούν στα ιδιωτικά νοσοκομεία αλλά **ΔΕΝ** αφορούν άμεσα στα δημόσια νοσοκομεία

20

12. Άδεια της Επιτροπής για διαβίβαση προσωπικών δεδομένων

εάν το νοσοκομείο επιλέξει ως νομική βάση για τη διαβίβαση συμβατικές ρήτρες που θα ετοιμάσει **και θα εγκριθούν από το Γραφείο μου.** Εάν από τη διαβίβαση επηρεάζονται και πολίτες κρατών μελών, οι συμβατικές ρήτρες θα εγκριθούν στα πλαίσια του μηχανισμού συνεκτικότητας*.

➤ **ΔΕΝ απαιτείται άδεια** για διαβίβαση σε τρίτη χώρα, όταν αυτή:

- Εξασφαλίζει ικανοποιητικό επίπεδο προστασίας (με Απόφαση της Ευρωπαϊκής Επιτροπής)
- Δεν εξασφαλίζει μεν ικανοποιητικό επίπεδο προστασίας αλλά διαθέτει ως νομική βάση για τη διαβίβαση:
 - (α) νομικά δεσμευτικό μέσο μεταξύ δημόσιων αρχών π.χ. πολυμερής συμφωνία, FATCA ή
 - (β) δεσμευτικούς εταιρικούς κανόνες (για ομίλους επιχειρήσεων) ή

* *Θεσπίζεται μηχανισμός συνεκτικότητας για τη συνεργασία μεταξύ των εποπτικών αρχών, ιδιαίτερα όταν μια εποπτική αρχή θεσπίζει μέτρο που επηρεάζει ουσιωδώς σημαντικό αριθμό υποκειμένων των δεδομένων σε περισσότερα κμ.*

21

(γ) τυποποιημένες ρήτρες που εκδίδονται από την Επιτροπή ή

(δ) τυποποιημένες ρήτρες που **εκδίδονται από το Γραφείο μου και** εγκρίνονται από την Επιτροπή ή

(ε) κώδικα δεοντολογίας, **ο οποίος εγκρίνεται από το Γραφείο μου** ή από το Συμβούλιο Προστασίας Δεδομένων, εάν ο Κώδικας αναφέρεται σε επεξεργασίες σε διάφορα κμ ή

(στ) μηχανισμό πιστοποίησης, **ο οποίος εγκρίνεται από το Γραφείο μου** ή τον εθνικό οργανισμό πιστοποίησης ή και από τους δύο

- ΔΕΝ εξασφαλίζει ικανοποιητικό επίπεδο προστασίας, ΔΕΝ διαθέτει καμία από τις πιο πάνω νομικές βάσεις, αλλά πληρούνται συγκεκριμένες προϋποθέσεις

Π.χ. για λόγους δημοσίου συμφέροντος, για άσκηση νομικών αξιώσεων, για προστασία ζωτικού συμφέροντος κλπ

ΣΗΜ: Σε κάθε περίπτωση, το νοσοκομείο θα διενεργεί εκτίμηση ανικτύπου για επεξεργασίες που παρουσιάζουν υψηλό κίνδυνο και σχετίζονται με αξιολόγηση προσωπικών πτυχών, αφορούν σε δεδομένα μεγάλης κλίμακας ή σε παρακολούθηση δημοσίου χώρου

22

Ενίσχυση των δικαιωμάτων των πολιτών

➤ Συγκατάθεση:

- ❖ **Κείμενο συγκατάθεσης:** κατανοητό, με σαφή και απλή διατύπωση και ξεχωριστό από άλλα θέματα
- ❖ δικαίωμα ανάκλησης συγκατάθεσης ανά πάσα στιγμή
- ❖ ελεύθερη συγκατάθεση στα πλαίσια σύμβασης: το άτομο είναι σε θέση να επιλέξει και δεν διατρέχει τον κίνδυνο εξαπάτησης, εκφοβισμού, εξαναγκασμού ή σημαντικών αρνητικών επιπτώσεων εάν δεν συγκατατεθεί

- **Συγκατάθεση γονέων:** ο υπεύθυνος επεξεργασίας επαληθεύει ότι η συγκατάθεση για τη συμμετοχή των παιδιών τους σε σχέση με τις υπηρεσίες της κοινωνίας των πληροφοριών (π.χ. *e-government, e-commerce, eBay, Amazon, gambling*) παρέχεται από το πρόσωπο που έχει τη γονική μέριμνα, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία
 - ΔΕΝ ισχύει στα δημόσια νοσοκομεία

23

➤ Δικαίωμα ενημέρωσης:

- ❖ Σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση, ιδίως όταν πρόκειται για πληροφορία απευθυνόμενη σε παιδιά
- ❖ Όταν η επεξεργασία ειδικών κατηγοριών δεδομένων **βασίστηκε στη συγκατάθεση του ατόμου** (π.χ. *ασθενής συγκατατέθηκε στην παροχή δεδομένων του για σκοπούς ιατρικής έρευνας*), πρέπει να ενημερωθεί ότι μπορεί να ανακαλέσει τη συγκατάθεση του ανά πάσα στιγμή
- ❖ Όταν ειδικές κατηγορίες δεδομένων **δεν έχουν συλλεγεί από το ίδιο το άτομο** (π.χ. *φαρμακευτική εταιρεία συλλέγει προσωπικά δεδομένα από νοσοκομείο*), το άτομο πρέπει να ενημερωθεί ότι μπορεί να ανακαλέσει τη συγκατάθεση του ανά πάσα στιγμή, χωρίς να θίγεται η νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση πριν από την ανάκλησή της

24

➤ **Δικαίωμα πρόσβασης:** Επιβεβαίωση του ατόμου εάν προσωπικά του δεδομένα τυγχάνουν επεξεργασίας

- ❖ Το υποκείμενο δικαιούται να λάβει ατελώς, σε έντυπη ή ηλεκτρονική μορφή, πληροφορίες που αφορούν στην υγεία του, **τις οποίες το ίδιο ή άλλο πρόσωπο** έδωσε στον υπεύθυνο επεξεργασίας

ΠΑΡΑΔΕΙΓΜΑ: πρόσβαση στον ιατρικό του φάκελο και λήψη αντίγραφου κάθε πληροφορίας (*δεδομένου ότι δεν επηρεάζονται δυσμενώς τα δικαιώματα οι ελεύθερες τρίτων*), όπως π.χ. ιατρικές εξετάσεις, απόφαση ιατροσυμβουλίου κ.λ.π.

- ❖ Δεν υπάρχει χρέωση (*μόνο για διοικητικά έξοδα σε περίπτωση πολλών αντιγράφων*)
- ❖ Πληροφορίες / έγγραφα που περιέχονται στο φάκελο του ασθενή δίνονται ΜΟΝΟ στον ίδιο ή στους γονείς/κηδεμόνες του (για ανήλικους) ή στους εξουσιοδοτημένους δικηγόρους του αν σχετίζονται με υπόθεση που εκκρεμεί στο δικαστήριο
- ❖ **Κατ' εξαίρεση δίνονται σε:** ποινικούς ανακριτές / Δικηγόρους που υπερασπίζονται την Κυπριακή Δημοκρατία ή Αστυνομία σε περιπτώσεις διεξαγωγής ανακρίσεων

25

➤ **Δικαίωμα διόρθωσης:**

- ❖ Διόρθωση των ανακριβών δεδομένων, χωρίς αδικαιολόγητη καθυστέρηση

➤ **Δικαίωμα στη φορητότητα:**

- ❖ Λήψη δεδομένων σε ψηφιακή μορφή (σε μορφή αναγνώσιμη, τόσο από τον άνθρωπο όσο και από το μηχανογραφημένο σύστημα του άλλου οργανισμού) και αποθήκευση τους για περαιτέρω προσωπική χρήση
- ❖ η αποθήκευση μπορεί να γίνεται σε ιδιωτική συσκευή ή ιδιωτικό υπολογιστικό σύννεφο, χωρίς, κατ' ανάγκη, διαβίβαση των δεδομένων σε άλλο υπεύθυνο επεξεργασίας
- ❖ **ΙΣΧΥΕΙ ΣΤΑ ΙΔΙΩΤΙΚΑ ΝΟΣΟΚΟΜΕΙΑ** αλλά **ΌΧΙ** στα δημόσια

26

➤ **Δικαίωμα στη λήθη (διαγραφή των δεδομένων):** Το δικαίωμα στη λήθη ενισχύει το δικαίωμα διαγραφής:

- ❖ Αφορά στο δικαίωμα διαγραφής δεδομένων στο διαδίκτυο, που το άτομο δεν επιθυμεί τη δημοσίευσή τους διότι του προκαλούν βλάβη και δεν είναι πλέον χρήσιμα για την ενημέρωση του κοινού
- ❖ Το υποκείμενο έχει δικαίωμα διαγραφής δεδομένων υγείας που τον αφορούν όταν, μεταξύ άλλων, **ανακαλέσει τη συγκατάθεση** του για την επεξεργασία των εν λόγω δεδομένων και δεν υπάρχει άλλη νομική βάση για την επεξεργασία
- ❖ **ΔΕΝ μπορεί να ασκηθεί το δικαίωμα** όταν η επεξεργασία είναι απαραίτητη:
 - για σκοπούς δημοσίου συμφέροντος στον τομέα της δημόσιας υγείας
 - για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον (π.χ. αρχειοθέτησης μίας επιδημιολογικής έρευνας), για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς

27

➤ **Δικαίωμα εναντίωσης (αντίρρησης):**

Το υποκείμενο έχει δικαίωμα να αντιταχθεί / εναντιωθεί όταν προσωπικά του δεδομένα υφίστανται επεξεργασία **για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς**, εκτός εάν η επεξεργασία είναι απαραίτητη για λόγους δημοσίου συμφέροντος.

➤ **Δικαίωμα εναντίωσης στην αυτοματοποιημένη λήψη αποφάσεων και στη δημιουργία προφίλ:**

Δικαίωμα του ατόμου να μην υπόκειται σε απόφαση που λαμβάνεται με αυτοματοποιημένα μέσα, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία το επηρεάζει σημαντικά

- ❖ **Εξαιρεση:** Το άτομο δικαιούται να αντιταχθεί στα προσωπικά του δεδομένα που τυγχάνουν επεξεργασίας για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, **ΕΚΤΟΣ ΕΑΝ Η ΕΠΕΞΕΡΓΑΣΙΑ ΑΣΚΕΙΤΑΙ ΓΙΑ ΛΟΓΟΥΣ ΔΗΜΟΣΙΟΥ ΣΥΜΦΕΡΟΝΤΟΣ**

28

Προετοιμασία για τη σωστή εφαρμογή του νέου Κανονισμού

- Ακριβής γνώση των δεδομένων που συλλέγονται και τυγχάνουν επεξεργασίας, ποιοι εμπλέκονται, ποιες διαδικασίες ακολουθούνται
- Καθορισμός και διαχωρισμός των αναγκών για διασφάλιση λήψης των απαιτούμενων συγκαταθέσεων και ότι δεν συλλέγονται υπερβολικά δεδομένα
- Κατάρτιση διαδικασιών για τήρηση Αρχείου Δραστηριοτήτων της επεξεργασίας
- Υιοθέτηση συστήματος διοίκησης για τακτική αναθεώρηση, αξιολόγηση και βελτίωση των μέτρων ασφάλειας
- Υιοθέτηση:
 - εσωτερικής διαδικασίας αναφοράς της παραβίασης
 - εσωτερικού «πλάνου ανταπόκρισης» (response plan) σε περίπτωση παραβίασης
 - διαδικασία γνωστοποίησης ενδεχόμενης παράβασης στην ΑΠΔΠΧ, εντός 72 ωρών

29

- Αναθεώρηση των συμβολαίων/συμβάσεων που συνάπτονται με πελάτες, υπαλλήλους, εκτελούντες την επεξεργασία
- Συστηματικός έλεγχος για συμμόρφωση με τον Κανονισμό
- Αξιολόγηση των κινδύνων και το είδος της βλάβης που πιθανόν να οδηγήσει σε παραβίαση προσωπικών δεδομένων
- Λήψη μέτρων για περιορισμό ή ακόμα αποφυγή κινδύνου παραβίασης
- Τρόποι αντιμετώπισης ενδεχόμενων παραβιάσεων και διαμόρφωση στρατηγικής για συμμόρφωση

30

Άλλα σημαντικά θέματα και ορθές πρακτικές

31

Ανησυχίες

- Οι αυστηρές προϋποθέσεις παροχής συγκατάθεσης ενδεχομένως να μειώσουν και/ή δυσχεράνουν την πραγματοποίηση ιατρικών ερευνών: τίθεται το ερώτημα κατά πόσο μπορεί να ληφθεί έγκυρη συγκατάθεση, καθώς δεν είναι δυνατόν να προβλεφθούν ή κατανοηθούν οι πιθανές συνέπειες της συγκατάθεσης
- Η λήψη ειδικής συγκατάθεσης για κάθε συσχετισμό ή επαναχρησιμοποίηση ιατρικών, γενετικών ή βιομετρικών δεδομένων μπορεί να προϋποθέτει δυσανάλογη προσπάθεια ή να είναι αδύνατη και/ή να οδηγήσει σε δαπανηρές και χρονοβόρες διαδικασίες
- Η πλήρης ανωνυμοποίηση των δεδομένων, για αποφυγή επιλογής οποιασδήποτε νομικής βάσης της επεξεργασίας π.χ. συγκατάθεση, είναι δύσκολο να διασφαλιστεί, ιδίως όταν:
 - ιατρικά δεδομένα επαναχρησιμοποιούνται για άλλους σκοπούς
 - η επεξεργασία αφορά γονιδιωματικά δεδομένα (genome data)
 - η συλλογή δεδομένων από διάφορες πηγές καθιστά εφικτή την επαναταυτοποίηση

32

- Επομένως, θα πρέπει να ληφθούν τα κατάλληλα τεχνικά και οργανωτικά μέτρα **που να αποδεικνύουν συμμόρφωση με τον Κανονισμό**, όπως:
 - ψευδωνυμοποίηση και ελαχιστοποίηση των δεδομένων
 - προστασία των δεδομένων από το στάδιο σχεδιασμό και εξ ορισμού
 - υιοθέτηση διαδικασιών ανακοίνωσης ενδεχόμενων παραβιάσεων στα επηρεαζόμενα πρόσωπα
 - υιοθέτηση διαδικασιών που να διασφαλίζουν ότι οι οργανισμοί θα μπορούν να αντιδράσουν και να γνωστοποιήσουν τυχόν παραβίαση δεδομένων εντός της καθορισμένης προθεσμίας
 - υιοθέτηση διαδικασιών για εκτίμηση και αξιολόγηση της αποτελεσματικότητας των ληφθέντων μέτρων
 - υιοθέτηση διαδικασιών ικανοποίησης των δικαιωμάτων των υποκειμένων
- ❖ Κάτι τέτοιο προϋποθέτει χρόνο, κόστος και επιλογή εξειδικευμένου προσωπικού

33

Συστάσεις Επιτρόπου ημερ. 26.07.2016 προς Υπ. Υγείας με αφορμή τους ελέγχους/επισκέψεις που πραγματοποίησε από Δεκ. 2015 – Ιούλιο 2016:

Γεν. Νοσ. Λευκωσίας	Γεν. Νοσ. Αμμοχώστου	Νοσ. Λάρνακας
Επαρχιακό Νοσ. Λεμεσού	Επαρχιακό Νοσ. Πάφου	Μακάριο Νοσ.

1. Εγκατάσταση ηλεκτρονικού συστήματος φύλαξης ιατρικών δεδομένων ασθενών
2. Μέχρι την εγκατάσταση του ηλεκτρονικού συστήματος, να γίνεται σωστή αρχειοθέτηση και φύλαξη των ιατρικών φακέλων σε χάρτινη μορφή
3. Να μη δίνονται στους ασθενείς οι ιατρικοί φάκελοι *(για φύλαξη ή διακίνηση)* – για αποφυγή απώλειας τους και αφαίρεσης/αλλοίωσης του περιεχομένου τους
4. Τήρηση **ενημερωμένων** ιατρικών αρχείων (στοιχεία ταυτότητας του ασθενή, θεραπεία, προηγούμενο ιατρικό ιστορικό, διάγνωση, θεραπευτική αγωγή) – Α. 17 του Νόμου 1(Ι)/2005 και άρθρο 4(1)(δ) του Νόμου 138(Ι)/2001.
Παραβίαση του άρθρου 17 του Νόμου 1(Ι)/2005 από παροχέα υπηρεσίας υγείας είναι ένοχος αδικήματος
5. Ικανοποίηση του δικαιώματος πρόσβασης των ασθενών στους ιατρικούς φακέλους τους και/ή παροχής λήψης αντιγράφου *(εφόσον αυτό δεν προϋποθέτει δυσανάλογη προσπάθεια)*

34

Παροχή πληροφοριών για ασθενείς σε συγγενικά και φιλικά πρόσωπα

- Οι λειτουργοί εγγράφων και οι τηλεφωνητές επιτρέπεται να δίνουν πληροφορίες ασθενών που νοσηλεύονται στο νοσοκομείο, ΜΟΝΟ σε άτομο που ο ίδιος ο ασθενής επέλεξε να ενημερώνεται εκ μέρους του και/ή σε άτομο που έχει τέτοιο δικαίωμα βάσει νόμου (π.χ. γονείς ανηλίκων)
- Η πληροφόρηση για το που βρίσκεται ο θάλαμος και το δωμάτιο που βρίσκεται ο ασθενής (*οπότεν τεκμαίρεται ότι ο ασθενής έχει δημοσιοποιήσει τη διαμονή του στο νοσοκομείο*) ΔΕΝ συνιστά επεξεργασία ευαίσθητων δεδομένων, αλλά απλή καθοδήγηση

35

Ηχογράφηση τηλεφωνικών συνδιαλέξεων

Ισχύουν οι διατάξεις για το Απόρρητο των επικοινωνιών (άρθρο 99) του Νόμου 112(Ι)/2004

Παρέμβαση στις επικοινωνίες επιτρεπτή αν:

- εξασφαλίζεται η συγκατάθεση των επικοινωνούντων ή
- προβλέπεται από νομοθεσία (πρωτογενή /δευτερογενή) και με άδεια του Δικαστηρίου ή
- αν πρόκειται για νόμιμη επαγγελματική πρακτική επιτρέπεται η καταγραφή συνδιαλέξεων με σκοπό την εξασφάλιση αποδεικτικών στοιχείων κάποιας εμπορικής συναλλαγής και/ή οποιασδήποτε άλλης επικοινωνίας επαγγελματικού χαρακτήρα

36

Ισχύουν και οι διατάξεις του Νόμου 138(Ι)/2001, δυνάμει των οποίων:

- Προτού αρχίσει η τηλεφωνική συνομιλία, υπάρχει προειδοποιητική σήμανση ότι η συνομιλία ηχογραφείται,
- Στο περιεχόμενο της προειδοποιητικής σήμανσης, να αναφέρονται τα ακόλουθα:
 - η ταυτότητα του υπεύθυνου επεξεργασίας,
 - ο σκοπός της ηχογράφησης,
 - εάν η ηχογραφημένη συνομιλία θα κοινοποιηθεί σε τρίτους και ότι
 - το φυσικό πρόσωπο μπορεί να έχει πρόσβαση στο περιεχόμενο της ηχογραφημένης τηλεφωνικής συνομιλίας

37

Εγκατάσταση Κλειστού Κυκλώματος Βιντεοπαρακολούθησης

- Επιτρέπεται μόνο αν δεν υπάρχει λιγότερο παρεμβατικός τρόπος για την πραγματοποίηση του σκοπού π.χ. προστασία του χώρου από διαρρήξεις /κλοπές
- **Επιτρέπεται η εγκατάσταση και λειτουργία καμερών:**
 - στις εισόδους/εξόδους των νοσοκομείων
 - στο χώρο υποδοχής
 - για έλεγχο και παρακολούθηση του δωματίου νεογνών
 - για έλεγχο του ρολογιού ηλεκτρονικής καταγραφής της προσέλευσης /αναχώρησης από την εργασία
 - στην είσοδο/έξοδο στις ηλεκτρονικές μπάρες στο χώρο στάθμευσης ασθενοφόρων
 - στα δωμάτια νοσηλείας ανήλικων χρηστών εξαρτησιογόνων ουσιών και στο εξεταστικό δωμάτιο (υπό όρους)
 - σε χώρους που υπάρχουν ταμεία / φυλάγονται απόρρητα έγγραφα / φάκελοι ασθενών *(η κάμερα θα εστιάζει ΑΠΟΚΛΕΙΣΤΙΚΑ στο σημείο του ταμείου/χώρου φύλαξης εγγράφων – ΟΧΙ στους υπαλλήλους)*
 - απέναντι από τους ανελκυστήρες / σκάλες / εξόδους κινδύνων
 - στις εισόδους κλιμακοστασίων
 - για έλεγχο του ταμείου στην καφετέρια
 - χώρο του νεκροτομείου

38

➤ **ΔΕΝ επιτρέπεται η εγκατάσταση και λειτουργία κάμερας:**

- θαλάμους ασθενών
- θαλάμους εξέτασης
- θαλάμους ιατρικών επεμβάσεων
- στους χώρους έξω από τα εξεταστήρια
- διαδρόμους (έξω από τα δωμάτια των ασθενών)
- γραφεία ιατρών / νοσηλευτών
- χώρους αναμονής
- τουαλέτες
- ασανσέρ
- καφετέρια

39

➤ Τα υποκείμενα των δεδομένων **θα πρέπει να ενημερώνονται** μέσω προειδοποιητικών πινακίδων, οι οποίες θα πρέπει να είναι:

- ευδιάκριτες
- επαρκείς σε αριθμό
- εμφανείς
- σε σημείο πριν τα υποκείμενα των δεδομένων εισέλθουν στο χώρο που γίνεται η οπτικογράφηση

40

Εγκατάσταση συστημάτων δακτυλικών αποτυπωμάτων για σκοπούς ελέγχου της ώρας προσέλευσης/ αναχώρησης των υπαλλήλων από την εργασία

- **Είναι βιομετρικό δεδομένο:** καθολικό, μοναδικό, μόνιμο δεδομένο όπως είναι φωτογραφία, DNA, ίριδα, παλάμη, φωνή κτλ
- **Δεν επιτρέπεται**
- **Επιτρέπεται** σε κτίρια υψίστης ασφάλειας και χώρους με ιδιαίτερες απαιτήσεις ασφαλείας και εφόσον δεν υπάρχει άλλο λιγότερο επαχθές μέσο για την επίτευξη **των σκοπών ασφαλείας** των εγκαταστάσεων / εξοπλισμού / προσώπων (π.χ. στρατιωτικές /αμυντικές εγκαταστάσεις, εργαστήρια υψηλού κινδύνου, χώροι αεροδρομίων, κ.α)
- Ο υπεύθυνος επεξεργασίας θα πρέπει να σταθμίζει τους κινδύνους, την έκταση των κινδύνων αυτών και τις υπάρχουσες εναλλακτικές δυνατότητες αντιμετώπισης των κινδύνων και από την άλλη, τις προσβολές της προσωπικότητας και της ιδιωτικότητας του ατόμου από τη χρήση τέτοιων μεθόδων
- **Απόφαση εναντίον Απολλώνειου Νοσοκομείου**

41

Ορθή χρήση αρχείου του προσωπικού

- Οι προσωπικοί φάκελοι των υπαλλήλων (που περιέχουν προσόντα και ατομικές εκθέσεις), θα πρέπει να διατηρούνται σε ασφαλές μέρος (σε χώρους που κλειδώνουν)
- Πρόσβαση στους προσωπικούς φακέλους να έχει μόνο εξουσιοδοτημένο προσωπικό
- Απαγορεύεται η διάδοση προσωπικών δεδομένων που αφορούν ένα υπάλληλο σε άλλο

42

Αναγραφή πάθησης των ασθενών στα πιστοποιητικά ασθενείας

- Ο εργοδότης δικαιούται να γνωρίζει την πάθηση/ασθένεια των υπαλλήλων του:
 - Για να μπορέσει να εκπληρώσει τις υποχρεώσεις του / εκτελέσει τα καθήκοντα του στον τομέα του εργατικού δικαίου αφού έχει την ευθύνη για την ασφάλεια και την υγεία τους (μεταδοτικές ασθένειες, επικίνδυνες εργασίες κ.λ.π.)
 - Βάσει Κανονισμού της δημόσιας υπηρεσίας, ο εργοδότης μπορεί να μην ικανοποιηθεί από το ιατρικό πιστοποιητικό και να ζητήσει να εξεταστεί ο υπάλληλος από ιατροσυμβούλιο

43

Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

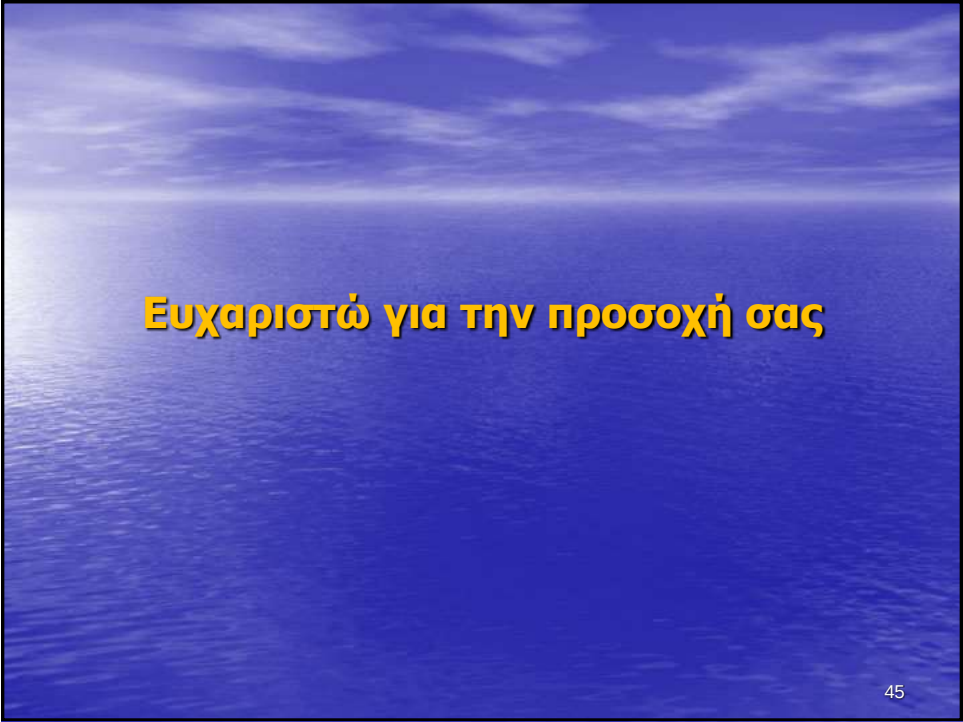
Ιάσονος 1, 1082 Λευκωσία
Τ.Θ. 23378, 1682 Λευκωσία

Τηλ: 22818456, Φαξ: 22304565

E-mail: commissioner@dataprotection.gov.cy

www.dataprotection.gov.cy

44



Ευχαριστώ για την προσοχή σας

45