

ΠΟΛΙΤΙΚΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

ο Το πλαίσιο εφαρμογής της παρούσας Πολιτικής

Η παρούσα Πολιτική ισχύει για όλα τα προσωπικά δεδομένα που επεξεργάζεται το Διαγνωστικό Κέντρο ΙΑΤΡΟΚΟΣΜΟΣ, ανεξάρτητα από την τοποθεσία στην οποία αποθηκεύονται τα προσωπικά δεδομένα (π.χ. PACS, PC, Server κτλ.) και ανεξάρτητα από το υποκείμενο των δεδομένων, είτε πρόκειται για τους υπαλλήλους και λοιπούς συνεργάτες του Διαγνωστικού Κέντρου, είτε πρόκειται για τους ίδιους τους ασθενείς. Όσοι επεξεργάζονται για λογαριασμό του προσωπικά δεδομένα που αφορούν εργαζόμενους και ασθενείς οφείλουν να μελετήσουν την παρούσα. Η μη συμμόρφωση με αυτή την Πολιτική μπορεί να οδηγήσει σε πειθαρχικές κυρώσεις.

Ο λόγος και ο τρόπος επεξεργασίας των προσωπικών δεδομένων είναι σε συμμόρφωση με:

1. Τον Γενικό Κανονισμό για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα (ΕΕ) 2016/679.
2. Τις διατάξεις του Νόμου 4624/2019 (ΦΕΚ 137/Α/29-8-2019): Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις.

Όλοι οι επικεφαλής των μονάδων είναι υπεύθυνοι για τη διασφάλιση ότι όλο το προσωπικό του Διαγνωστικού Κέντρου συμμορφώνεται με την παρούσα Πολιτική και θα πρέπει να εφαρμόσει τις κατάλληλες πρακτικές, διαδικασίες και ελέγχους για να εξασφαλίσει τη συμμόρφωση.

Η Υπεύθυνη Προστασίας Προσωπικών Δεδομένων (DPO) του ΙΑΤΡΟΚΟΣΜΟΥ είναι η **Δανάη Στεργίου**, στην οποία μπορείτε να απευθυνθείτε στο email: dpo@iatrocosmos.gr και τον αριθμό τηλεφώνου: 210-8211660.

ο Οι αρχές προστασίας των προσωπικών δεδομένων

Κάθε φορά που ο ΙΑΤΡΟΚΟΣΜΟΣ επεξεργάζεται προσωπικά δεδομένα θα πρέπει να ακολουθεί τις παρακάτω αρχές, οι οποίες ορίζονται στον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων. Το Διαγνωστικό Κέντρο είναι υπεύθυνο και πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωσή του με τις αρχές προστασίας προσωπικών δεδομένων που αναφέρονται παρακάτω.

Οι αρχές αυτές απαιτούν τα προσωπικά δεδομένα:

1. Να επεξεργάζονται νόμιμα, δίκαια και με διαφάνεια (*Νομιμότητα, δικαιοσύνη και διαφάνεια*).
2. Να συλλέγονται μόνο για καθορισμένους, ρητούς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία με τρόπο ασυμβίβαστο με τους σκοπούς αυτούς (*περιορισμός του σκοπού*).
3. Να είναι επαρκή, σχετικά και περιορισμένα σε ό, τι είναι απαραίτητο σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία (*ελαχιστοποίηση δεδομένων*).
4. Να είναι ακριβή και, όπου χρειάζεται, ενημερωμένα (*ακρίβεια*).
5. Να μην τηρούνται υπό μορφή που επιτρέπει τον προσδιορισμό των προσώπων στα οποία αναφέρονται τα προσωπικά δεδομένα για μεγαλύτερο χρονικό διάστημα από αυτό που είναι αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται αυτά σε επεξεργασία (*περιορισμός αποθήκευσης*).
6. Να υποβάλλονται σε επεξεργασία με τρόπο που διασφαλίζει την ασφάλειά τους, χρησιμοποιώντας κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και από τυχαία απώλεια, καταστροφή ή ζημία (*Ασφάλεια, ακεραιότητα και εμπιστευτικότητα*).

ο Τα δικαιώματά των υποκειμένων των προσωπικών δεδομένων

Τα υποκείμενα των προσωπικών δεδομένων, είτε πρόκειται για τους εργαζόμενους του Κέντρου, είτε

πρόκειται για τους ασθενείς-εξεταζόμενους που επισκέπτονται τον ΙΑΤΡΟΚΟΣΜΟ, έχουν δικαίωμα :

- **Πρόσβασης στα δεδομένα τους:** Αυτό σημαίνει ότι τα υποκείμενα δικαιούνται να υποβάλουν αίτημα πρόσβασης στα προσωπικά τους δεδομένα και να πληροφορηθούν τον τρόπο με τον οποίο τα χειρίζεται το Διαγνωστικό Κέντρο.
- **Διόρθωσης των δεδομένων τους σε περίπτωση ανακρίβειας:** Αυτό σημαίνει ότι τα υποκείμενα δικαιούνται να προβούν σε διόρθωση ή συμπλήρωση των προσωπικών τους πληροφοριών, όταν αυτές είναι ανακριβείς ή ελλιπείς.
- **Διαγραφής των δεδομένων τους σε συγκεκριμένες περιπτώσεις:** Αυτό σημαίνει ότι τα υποκείμενα μπορούν να ζητήσουν τη διαγραφή ορισμένων ή όλων των προσωπικών τους δεδομένων σε συγκεκριμένες περιστάσεις, εφόσον δεν υπάρχει νόμιμος λόγος συνέχισης της επεξεργασίας από τον ΙΑΤΡΟΚΟΣΜΟ και υπό την προϋπόθεση ότι δεν θίγονται τα συμφέροντα του Διαγνωστικού Κέντρου.
- **Περιορισμού της επεξεργασίας των δεδομένων τους:** Αυτό σημαίνει ότι τα υποκείμενα μπορούν να ζητήσουν να περιοριστεί η επεξεργασία των προσωπικών τους δεδομένων και πιο συγκεκριμένα ο ΙΑΤΡΟΚΟΣΜΟΣ δικαιούται να αποθηκεύει τα δεδομένα τους, χωρίς όμως να προχωράει σε περαιτέρω επεξεργασία.
- **Εναντίωσης στην επεξεργασία των δεδομένων τους:** Αυτό σημαίνει ότι τα υποκείμενα μπορούν να εναντιωθούν στην κάθε είδους επεξεργασία των προσωπικών τους πληροφοριών.
- **Διαβίβασης των δεδομένων τους σε άλλον πάροχο υπηρεσιών υγείας:** Αυτό σημαίνει ότι τα υποκείμενα έχουν το δικαίωμα φορητότητας των δεδομένων τους, υπό την έννοια ότι δικαιούνται να λαμβάνουν και να μεταφέρουν ένα ηλεκτρονικό αντίγραφο των δεδομένων τους εύκολα και με τρόπο ασφαλή και να ζητούν από το Διαγνωστικό Κέντρο να τα μεταφέρει σε άλλον υπεύθυνο επεξεργασίας.
- **Καταγγελίας στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.) σε περίπτωση ατυχούς συμβάντος παραβίασης των δεδομένων τους.**

Ο ΙΑΤΡΟΚΟΣΜΟΣ θα απαντήσει στα ως άνω αιτήματα των υποκειμένων εντός μηνός από την παραλαβή τους, εξαιρετικά δε αυτή η προθεσμία μπορεί να παραταθεί κατά 3 ακόμα μήνες, εφόσον απαιτείται επιπλέον χρόνος.

Σε περίπτωση που τα υποκείμενα των δεδομένων χρειάζονται διευκρινίσεις ή περαιτέρω πληροφορίες σχετικά με τα ανωτέρω δικαιώματά τους, μπορούν να απευθύνονται στη Γραμματεία του Διαγνωστικού Κέντρου ή να επικοινωνούν με τον Υπεύθυνο Προστασίας Δεδομένων του (στοιχεία επικοινωνίας παρακάτω).

ο Τα προσωπικά δεδομένα που επεξεργάζεται το Διαγνωστικό Κέντρο

Ο ΙΑΤΡΟΚΟΣΜΟΣ συλλέγει και χρησιμοποιεί τα απλά και ευαίσθητα προσωπικά δεδομένα των εργαζομένων του κυρίως για τη διαχείριση της σύμβασης εργασίας τους και της σχέσης τους με αυτόν. Η εν λόγω συλλογή και χρήση των δεδομένων των εργαζομένων από το Διαγνωστικό Κέντρο γίνεται για νόμιμους σκοπούς, όπως είναι η βελτίωση της αποδοτικότητας και αποτελεσματικότητας των εργασιών του ΙΑΤΡΟΚΟΣΜΟΥ, η διερεύνηση πιθανών παραβιάσεων νόμιμων ή συμβατικών υποχρεώσεων από τους εργαζόμενους ή από τα μέλη του προσωπικού του, καθώς επίσης και η αξιολόγηση της ικανότητας εργασίας των εργαζομένων.

Επίσης, το Διαγνωστικό Κέντρο συλλέγει τα προσωπικά δεδομένα των ασθενών (δημογραφικά στοιχεία, στοιχεία πληρωμής και ασφάλισης, ιατρικό ιστορικό) για να τους παρέχει τις ιατρικές υπηρεσίες που επιθυμούν. Στο πλαίσιο αυτό, το Διαγνωστικό Κέντρο μπορεί να επεξεργαστεί, για σκοπούς ιατρικής διάγνωσης, στοιχεία προηγούμενων εξετάσεων και παθήσεων που παρέχουν οι ασθενείς – εξεταζόμενοι, εφόσον βέβαια το επιθυμούν. Περαιτέρω, το Διαγνωστικό Κέντρο αποθηκεύει, κατόπιν ρητής συναίνεσης των ανωτέρω ασθενών-εξεταζόμενων, στοιχεία επικοινωνίας οικείων τους, τα οποία και θα χρησιμοποιηθούν μόνο σε περίπτωση έκτακτης ανάγκης. Σε περίπτωση που οι ασθενείς επισκέπτονται το διαγνωστικό κέντρο κατόπιν παραπομπής Ιδιώτη Ιατρού, το Διαγνωστικό Κέντρο ενημερώνει τον τελευταίο για τα αποτελέσματα των εξετάσεων των ασθενών, μόνο εφόσον αυτό κρίνεται απαραίτητο για σκοπούς ορθής ιατρικής γνωμάτευσης.

• Λειτουργικές ανάγκες του Διαγνωστικού Κέντρου

ΚΑΤΗΓΟΡΙΑ

ΕΙΔΟΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

ΝΟΜΙΜΟΠΟΙΗΤΙΚΗ

ΒΑΣΗ

Μέτοχοι	Ονοματεπώνυμο, θέση, τηλέφωνο, email, ΑΦΜ, ΑΜΚΑ, ΑΔΤ, φωτοτυπία ΑΤ, μετοχές	νόμιμη υποχρέωση
Διοίκηση - Μέλη ΔΣ	Ονοματεπώνυμο, θέση, τηλέφωνο, email, ΑΦΜ, ΑΜΚΑ, ΑΔΤ, φωτοτυπία ΑΤ	νόμιμη υποχρέωση
Εργαζόμενοι (Διοικητικοί)	Ονοματεπώνυμο, Διεύθυνση, τηλέφωνο, email, φορολογικά στοιχεία, ΑΜΚΑ, Αρ. Αστυνομικής Ταυτότητας / Διαβατηρίου / φωτοτυπία ΑΤ/ Τίτλοι Σπουδών/ Αξιολογήσεις	νόμιμη υποχρέωση
Εξωτερικοί Συνεργάτες/ Τρίτα Νομικά ή Φυσικά Πρόσωπα	Ονοματεπώνυμο, Διεύθυνση/Επαγ. Έδρα, τηλέφωνο, email, φορολογικά στοιχεία, ΑΜΚΑ, Αρ. Αστυνομικής Ταυτότητας / Διαβατηρίου / φωτοτυπία ΑΤ/ έγγραφα συναφή με τη συνεργασία	νόμιμη υποχρέωση

• **Εκτέλεση των ιατρικών πράξεων**

ΚΑΤΗΓΟΡΙΑ	ΕΙΔΟΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ	ΝΟΜΙΜΟΠΟΙΗΤΙΚΗ ΒΑΣΗ
Εξεταζόμενοι	Ονοματεπώνυμο, πατρώνυμο, επάγγελμα, διεύθυνση, τηλέφωνο, email, ΑΦΜ, ΑΜΚΑ, ΑΔΤ, αποτελέσματα εξετάσεων, στοιχεία ασφαλίσεως, στοιχεία οικείων	νόμιμη υποχρέωση
Ιατροί	Ονοματεπώνυμο, θέση, τηλέφωνο, email, ΑΦΜ, ΑΜΚΑ, ΑΔΤ, φωτοτυπία ΑΤ, άδεια ασκήσεως επαγγέλματος, ιατρική ειδικότητα, στοιχεία ασφαλιστικού φορέα, στοιχεία οικογενειακής καταστάσεως	νόμιμη υποχρέωση

ο **Η νομιμοποιητική βάση για την επεξεργασία των προσωπικών δεδομένων**

Ο ΙΑΤΡΟΚΟΣΜΟΣ θα επεξεργάζεται τα προσωπικά δεδομένα των εργαζομένων του εφόσον αυτό είναι απαραίτητο για την εκτέλεση της σύμβασής τους και για λόγους συμμόρφωσης με τις νόμιμες υποχρεώσεις του Διαγνωστικού Κέντρου. Επιπλέον, το Διαγνωστικό Κέντρο θα λαμβάνει και θα αποθηκεύει στοιχειώδη προσωπικά δεδομένα των ασθενών (π.χ. δημογραφικά στοιχεία) για τον προγραμματισμό της επίσκεψής τους στο Διαγνωστικό Κέντρο, καθώς και όσα προσωπικά δεδομένα κρίνονται απαραίτητα για την παροχή των ιατρικών υπηρεσιών που επιθυμούν. Ως εκ τούτου, η συμφωνία παροχής ιατρικών υπηρεσιών αποτελεί τη νομιμοποιητική βάση για την επεξεργασία των δεδομένων τους.

ο **Η ευθύνη του Διαγνωστικού Κέντρου**

Ο ΙΑΤΡΟΚΟΣΜΟΣ πρέπει να εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα με αποτελεσματικό τρόπο για να εξασφαλίσει την τήρηση των αρχών προστασίας προσωπικών δεδομένων. Το Διαγνωστικό Κέντρο είναι υπεύθυνο και πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωσή του με τις αρχές προστασίας αυτών των δεδομένων.

Επομένως, το Διαγνωστικό Κέντρο πρέπει να εφαρμόσει επαρκείς ελέγχους και μέτρα για την τεκμηρίωση και την εξασφάλιση της συμμόρφωσης με το GDPR, συμπεριλαμβανομένων των εξής:

1. διορισμός ενός υπεύθυνου προστασίας προσωπικών δεδομένων με τα κατάλληλα προσόντα.
2. εφαρμογή της προστασίας δεδομένων προσωπικού χαρακτήρα κατά την επεξεργασία αυτών των δεδομένων και ολοκλήρωση μιας αξιολόγησης αντικτύπου προστασίας δεδομένων (DPIA), καθώς το Διαγνωστικό Κέντρο επεξεργάζεται προσωπικά δεδομένα υγείας και συνεπώς η επεξεργασία παρουσιάζει υψηλό κίνδυνο για την ιδιωτική ζωή των υποκειμένων των δεδομένων.
3. ενσωμάτωση της προστασίας των προσωπικών δεδομένων στις πολιτικές και τις διαδικασίες του Διαγνωστικού Κέντρου, χειρισμός των προσωπικών δεδομένων από το Διαγνωστικό και παραγωγή απαιτούμενων εγγράφων, όπως ειδοποιήσεις περί απορρήτου, αρχεία επεξεργασίας και καταγραφές παραβιάσεων προσωπικών δεδομένων.

4. εκπαίδευση του προσωπικού σχετικά με την τήρηση του νόμου περί προστασίας δεδομένων και τήρηση αναλόγως του μητρώου.

5. τακτικός έλεγχος των μέτρων προστασίας της ιδιωτικής ζωής και διενέργεια περιοδικών αναθεωρήσεων και ελέγχων για την αξιολόγηση της συμμόρφωσης, συμπεριλαμβανομένης της χρήσης αποτελεσμάτων δοκιμών για την απόδειξη της προσπάθειας βελτίωσης της συμμόρφωσης, για την πλήρη εναρμόνιση με τη νομοθεσία.

ο Οι αρμοδιότητες της Διοίκησης

Η Διοίκηση του ΙΑΤΡΟΚΟΣΜΟΥ είναι αρμόδια να λαμβάνει τα απαραίτητα μέτρα προκειμένου να διασφαλίσει πλήρως την ιδιωτικότητα των υποκειμένων και την ασφάλεια των προσωπικών τους δεδομένων σύμφωνα με την ευρωπαϊκή και εθνική νομοθεσία.

ο Οι αρμοδιότητες του Υπευθύνου Προστασίας Προσωπικών Δεδομένων

Ο Υπεύθυνος Προστασίας Δεδομένων του ΙΑΤΡΟΚΟΣΜΟΥ έχει τα εξής καθήκοντα:

- προώθηση μιας κουλτούρας προστασίας των δεδομένων σε όλα τα επίπεδα του Διαγνωστικού Κέντρου και αρωγή κατά την υλοποίηση των θεμελιωδών στοιχείων του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR)·
- παροχή συμβουλευτικής καθοδήγησης στη Διοίκηση σε σχέση με το:
 - αν υφίσταται υποχρέωση για την εκπόνηση εκτίμησης αντικτύπου ως προς την Προστασία των Δεδομένων (DPIA) για κάποια συγκεκριμένη δραστηριότητα του Κέντρου
 - ποια μεθοδολογία ενδείκνυται να ακολουθείται κατά τη διενέργεια της εκτίμησης του αντικτύπου ως προς την Προστασία των Δεδομένων (DPIA)
 - αν θα πρέπει να διενεργείται η DPIA ενδοεταιρικά ή αν θα πρέπει να ανατίθεται σε εξωτερικούς συνεργάτες
 - αν η DPIA έχει πραγματοποιηθεί σωστά και αν τα συμπεράσματά της τελούν σε συμμόρφωση με τον Γενικό Κανονισμό για την Προστασία των Δεδομένων (GDPR)
- προσδιορισμός των μέτρων προστασίας (που περιλαμβάνουν τεχνικά και οργανωτικά μέτρα) τα οποία είναι ενδεδειγμένο να εφαρμόζονται, ώστε να μετριάζονται οι ενδεχόμενοι κίνδυνοι για τα δικαιώματα και τα συμφέροντα που έχουν τα υποκείμενα των δεδομένων
- τεκμηρίωση και συλλογή δεδομένων για τις τρέχουσες διοικητικές πρακτικές από όλες τις λειτουργίες, τις διεργασίες, τους ρόλους, τις αρμοδιότητες και την υλοποίησή τους τόσο στα ψηφιακά συστήματα όσο και εγγράφως
- παροχή υποστηρικτικών υπηρεσιών κατά τη λειτουργία του Διαγνωστικού στην πρακτική εφαρμογή των πολιτικών ιδιωτικότητας και της νομοθεσίας, εντός της οποίας λειτουργεί αυτό
- επίλυση πρακτικών προβλημάτων
- εκπαίδευση προσωπικού στις αλλαγές του νομοθετικού πλαισίου
- εκπροσώπηση έναντι της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και επίλυση τυχόν ερωτημάτων, καθώς και παροχή γνωστοποιήσεων σε περίπτωση καταγγελίας/ έρευνας.

ο Οι αρμοδιότητες του προσωπικού (εργαζομένων/ συνεργατών)

Όλοι όσοι ανήκουν στο προσωπικό του Διαγνωστικού και επεξεργάζονται προσωπικά δεδομένα σχετικά με τους ασθενείς, τους εργαζόμενους, τους αιτούντες θέση εργασίας ή οποιοδήποτε άλλο άτομο πρέπει να συμμορφώνονται με τις απαιτήσεις της παρούσας Πολιτικής. Το προσωπικό του Διαγνωστικού Κέντρου εξασφαλίζει ότι:

- (α) όλα τα δεδομένα προσωπικού χαρακτήρα φυλάσσονται με ασφάλεια.
- (β) καμία προσωπική πληροφορία δεν αποκαλύπτεται ούτε προφορικά ούτε γραπτώς, τυχαία ή με άλλο τρόπο, σε οποιοδήποτε τρίτο εξουσιοδοτημένο τρίτο πρόσωπο.
- (γ) τα προσωπικά δεδομένα τηρούνται σύμφωνα με το χρονοδιάγραμμα διατήρησης το Διαγνωστικού Κέντρου.
- (δ) οποιοσδήποτε ερωτήσεις σχετικά με την προστασία των δεδομένων, συμπεριλαμβανομένων των αιτήσεων πρόσβασης και των καταγγελιών, απευθύνονται αμελλητί στους αρμοδίους.
- (ε) οποιοσδήποτε παραβιάσεις προστασίας δεδομένων γνωστοποιούνται ταχέως στον Υπεύθυνο Προστασίας Δεδομένων, ο οποίος παρέχει κάθε διευκόλυνση για την επίλυση του ζητήματος.
- (στ) όταν υπάρχει αβεβαιότητα γύρω από ένα θέμα προστασίας δεδομένων, ζητείται συμβουλή από τον Υπεύθυνο Προστασίας Δεδομένων.

Το προσωπικό του Διαγνωστικού Κέντρου, όταν διατηρεί αμφιβολία για το ποιοι είναι οι εξουσιοδοτημένοι τρίτοι στους οποίους μπορεί νόμιμα να αποκαλύψει προσωπικά δεδομένα, θα πρέπει να ζητήσει συμβουλές από τον Υπεύθυνο Προστασίας Δεδομένων.

ο Τρίτοι Υπεργολάβοι ή Συνεργάτες

Όταν χρησιμοποιούνται εξωτερικές εταιρείες για την επεξεργασία δεδομένων προσωπικού χαρακτήρα για λογαριασμό του ΙΑΤΡΟΚΟΣΜΟΥ, η ευθύνη για την ασφάλεια και την κατάλληλη χρήση αυτών των δεδομένων παραμένει στον ΙΑΤΡΟΚΟΣΜΟ (ο οποίος είναι ο Υπεύθυνος Επεξεργασίας).

Όταν χρησιμοποιείται τρίτος ως εκτελών την επεξεργασία:

α) θα πρέπει να παρέχει επαρκείς εγγυήσεις όσον αφορά στα μέτρα ασφαλείας του για την προστασία της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

β) θα πρέπει να ληφθούν εύλογα μέτρα για την εφαρμογή μέτρων ασφαλείας.

γ) θα πρέπει να έχει καταρτιστεί γραπτή σύμβαση που να καθορίζει συγκεκριμένα ποια δεδομένα προσωπικού χαρακτήρα θα αποτελέσουν αντικείμενο επεξεργασίας και για ποιο σκοπό.

δ) θα πρέπει να έχει υπογραφεί η Σύμβαση Επεξεργασίας Δεδομένων σύμφωνα με το πρότυπο του ΙΑΤΡΟΚΟΣΜΟΥ.

ο Το χρονικό διάστημα διατήρησης των προσωπικών δεδομένων

Ανάλογα με τον τύπο των δεδομένων, ο ΙΑΤΡΟΚΟΣΜΟΣ διατηρεί τα δεδομένα των εργαζομένων του για μια περίοδο από 1 ημέρα έως 10 έτη. Σε εξαιρετικές περιπτώσεις, αυτή η περίοδος διατήρησης μπορεί να είναι μεγαλύτερη όταν απαιτείται ή επιτρέπεται από την κείμενη νομοθεσία. Όσον αφορά στους ασθενείς – εξεταζόμενους, το Διαγνωστικό Κέντρο διατηρεί τα προσωπικά τους δεδομένα για χρονικό διάστημα 10 ετών, όπως ορίζεται στην εθνική νομοθεσία. Μετά την πάροδο του ανωτέρω χρονικού διαστήματος το Διαγνωστικό Κέντρο προβαίνει σε ασφαλή διαγραφή των προσωπικών δεδομένων των ασθενών - εξεταζόμενων. Κατ' εξαίρεση το Διαγνωστικό Κέντρο διατηρεί τα προσωπικά δεδομένα των τελευταίων για χρονικό διάστημα μεγαλύτερο των 10 ετών, μόνο στην περίπτωση που αυτό είναι απαραίτητο για την εξυπηρέτηση των εννόμων συμφερόντων του. Στην τελευταία αυτή περίπτωση οι ενδιαφερόμενοι θα λάβουν σχετική ενημέρωση.

ο Οι αποδέκτες των προσωπικών δεδομένων

1. Ο ΙΑΤΡΟΚΟΣΜΟΣ επιτρέπει την πρόσβαση στα προσωπικά δεδομένα **των εργαζομένων** της μόνο σε όσους είναι απολύτως αναγκαίο να έχουν τέτοια πρόσβαση προκειμένου να εκτελέσουν τα καθήκοντά τους, καθώς και σε τρίτους, εφόσον έχουν νόμιμο λόγο για να αποκτήσουν πρόσβαση σε αυτά. Κάθε φορά που το Διαγνωστικό Κέντρο επιτρέπει σε τρίτο να έχει πρόσβαση στα προσωπικά δεδομένα των εργαζομένων της, το Διαγνωστικό θα εφαρμόζει τα κατάλληλα μέτρα για να διασφαλίζει ότι αυτά τα δεδομένα χρησιμοποιούνται κατόπιν γνωστοποίησης και ότι διατηρείται η εμπιστευτικότητα και η ακεραιότητα των δεδομένων.

Το Διαγνωστικό Κέντρο μπορεί να χρειαστεί να παρέχει ορισμένα προσωπικά δεδομένα των εργαζομένων του σε τρίτους που παρέχουν υπηρεσίες σε αυτό, σε μια «βάση απόλυτης αναγκαιότητας γνώσης» και σύμφωνα με τον ισχύοντα νόμο περί προστασίας προσωπικών δεδομένων. Για παράδειγμα, ορισμένα προσωπικά στοιχεία θα είναι διαθέσιμα σε εταιρείες τρίτων που παρέχουν υπηρεσίες στον ΙΑΤΡΟΚΟΣΜΟ, όπως πχ. υποστήριξη μισθοδοσίας, ιατρικές, νομικές οικονομικές και άλλες συμβουλές, διαχείριση ταξιδιών των εργαζομένων, κλπ. Επιπρόσθετα, το Διαγνωστικό Κέντρο μπορεί να αποκαλύψει προσωπικά δεδομένα σε άλλα τρίτα μέρη για άλλους νόμιμους λόγους όπως:

(α) προς συμμόρφωση με τις νόμιμες υποχρεώσεις του Διαγνωστικού Κέντρου, συμπεριλαμβανομένης της συμμόρφωσης σε νόμο, κανονισμό ή σύμβαση ή προς συμμόρφωση με δικαστική απόφαση ή ανταπόκριση σε διοικητική ή δικαστική διαδικασία ή προς ανταπόκριση σε αιτήματα επιβολής του νόμου συμπεριλαμβανομένων δικαστικής απόφασης ή ένταλμα έρευνας.

(β) όπου είναι απαραίτητο για την προστασία των συμφερόντων των εργαζομένων ή άλλου προσώπου (πχ. δικαστικές διαμάχες στις οποίες μετέχουν οι εργαζόμενοι) και

(γ) σε σχέση με την πώληση, ανάθεση ή άλλη μεταφορά του συνόλου ή μέρους της επιχείρησης του Διαγνωστικού Κέντρου.

2. Όσον αφορά **τους ασθενείς**, ο ΙΑΤΡΟΚΟΣΜΟΣ μπορεί να κοινολογεί τα προσωπικά τους δεδομένα σε τρεις διαφορετικές κατηγορίες αποδεκτών:

ι) Σε παρόχους ιατρικών υπηρεσιών – συνεργάτες του Διαγνωστικού:

Ο ΙΑΤΡΟΚΟΣΜΟΣ διατηρεί εξωτερικές συνεργασίες με τρίτους (μηχανικούς πληροφορικής, ιατρούς, παρόχους υπηρεσιών υγείας – εργαστήρια αναφοράς), οι οποίοι προβαίνουν σε επεξεργασία προσωπικών δεδομένων στο όνομα και για λογαριασμό του Διαγνωστικού, δυνάμει ισχυρών συμβατικών δεσμεύσεων και οι οποίοι έχουν επιλεγεί με κριτήριο την ουσιαστική εφαρμογή υψηλού επιπέδου μέτρων ασφάλειας σχετικά με την προστασία των προσωπικών δεδομένων.

ii) Σε τρίτους παρόχους υπηρεσιών υγείας.

Ο ΙΑΤΡΟΚΟΣΜΟΣ κοινοποιεί τα προσωπικά δεδομένα των ασθενών σε τρίτους αποδέκτες (με τους οποίους δεν διατηρεί συνεργασία) μόνο στις ακόλουθες περιπτώσεις:

- Σε περίπτωση που η κοινολόγηση απαιτείται στο πλαίσιο ασφαλιστικής σύμβασης που διατηρούν οι ασθενείς με συγκεκριμένη ασφαλιστική εταιρεία
- Για λόγους διαφύλαξης ζωτικών συμφερόντων των ασθενών
- Εφόσον απαιτείται από συγκεκριμένη νομοθετική διάταξη

iii) Σε τρίτους παρόχους κατόπιν αιτήματος των ασθενών

Ο ΙΑΤΡΟΚΟΣΜΟΣ κοινολογεί τα προσωπικά δεδομένα των ασθενών σε τρίτους παρόχους υπηρεσιών υγείας μόνο κατόπιν υποβολής δικού τους σχετικού γραπτού αιτήματος. Για περισσότερες πληροφορίες σχετικά με τον τρόπο διαβίβασης των προσωπικών δεδομένων των ασθενών σε τρίτους, οι τελευταίοι μπορούν να συμβουλευθούν την ιστοσελίδα ή τη γραμματεία του Διαγνωστικού Κέντρου.

Διευκρινίζεται ότι το Διαγνωστικό Κέντρο δε φέρει ουδεμία ευθύνη για τη διαχείριση των προσωπικών δεδομένων των ασθενών από τρίτους.

ο Η Καταγραφή ενεργειών ή πράξεων των εργαζομένων ή των ασθενών

1.Ο ΙΑΤΡΟΚΟΣΜΟΣ πραγματοποιεί αυτοματοποιημένη παρακολούθηση των δικτύων του, των συστημάτων πληροφορικής και επικοινωνιών και των κινητών και άλλων συσκευών μέσω αυτοματοποιημένων εργαλείων, όπως το λογισμικό προστασίας από κακόβουλο λογισμικό, το φιλτράρισμα ιστότοπων και το φιλτράρισμα ανεπιθύμητων μηνυμάτων. Παρακολουθεί επίσης τις φυσικές της εγκαταστάσεις, για παράδειγμα μέσω της χρήσης συστημάτων καμερών παρακολούθησης CCTV και ελέγχου πρόσβασης.

Το Διαγνωστικό Κέντρο μπορεί ωστόσο να διεξάγει ορισμένες μη αυτοματοποιημένες δραστηριότητες παρακολούθησης ή μερικής αυτόματης παρακολούθησης, όπως για παράδειγμα επισκοπήσεις ηλεκτρονικού ταχυδρομείου και άλλων επικοινωνιών. Αυτά τα δεδομένα θα διατηρηθούν σύμφωνα με το χρονοδιάγραμμα διατήρησης.

Λόγω αυτού του ελέγχου παρακολούθησης, όλοι οι υπάλληλοι και εργαζόμενοι του Διαγνωστικού Κέντρου θα πρέπει να δίνουν ιδιαίτερη προσοχή κάθε φορά που κάνουν χρήση των περιουσιακών στοιχείων του Διαγνωστικού για προσωπικούς λόγους, ιδιαίτερα αναφορικά με τα συστήματα ηλεκτρονικού ταχυδρομείου.

Ο πρωταρχικός σκοπός αυτής της καταγραφής είναι η προστασία του Διαγνωστικού Κέντρου, των υπαλλήλων και λοιπών συνεργατών της, όπως για παράδειγμα η γενική λειτουργία και ασφάλεια του δικτύου, η αξιολόγηση και παρακολούθηση των επιδόσεων των υπαλλήλων, συνεργατών και λοιπών απασχολούμενων, η φυσική ασφάλεια των χώρων, οχημάτων και περιουσιακών στοιχείων του Διαγνωστικού Κέντρου κλπ. Οι δραστηριότητες παρακολούθησης είναι πιθανόν να είναι συνεχείς και σε εξέλιξη. Ωστόσο, ο ΙΑΤΡΟΚΟΣΜΟΣ δεσμεύεται να διασφαλίσει ότι σέβεται σε κάθε περίπτωση την αρχή της αναλογικότητας.

Οι εργαζόμενοι στον ΙΑΤΡΟΚΟΣΜΟ πρέπει να γνωρίζουν ότι οποιοδήποτε μήνυμα ηλεκτρονικού ταχυδρομείου, αρχείο, δεδομένο, έγγραφο, τηλεομοιοτυπία, τηλεφωνική συνομιλία, κλπ. που μεταδίδεται προς ή από αυτό, λαμβάνεται ή εκτυπώνεται από ή καταγράφεται στα συστήματα πληροφορικής ή στις συσκευές του, θεωρείται ότι σχετίζεται με τη λειτουργία του και μπορεί να παρακολουθείται από το Διαγνωστικό Κέντρο, σύμφωνα με την ισχύουσα νομοθεσία.

2.Ο ΙΑΤΡΟΚΟΣΜΟΣ είναι δυνατόν να καταγράφει και να τηρεί τις συνομιλίες που έχει ο ασθενής με το Διαγνωστικό Κέντρο του - συμπεριλαμβανομένων επιστολών, μηνυμάτων ηλεκτρονικού ταχυδρομείου, ζωντανών συζητήσεων μέσω μηνυμάτων (live chats) ή και οποιωνδήποτε άλλων μορφών επικοινωνίας. Οι καταγραφές αυτές αξιοποιούνται από το Διαγνωστικό Κέντρο για να αξιολογήσει, αναλύσει και βελτιώσει τις υπηρεσίες του, να εκπαιδεύσει το προσωπικό του, να διαχειριστεί ή να προλάβει ενδεχόμενους κινδύνους και να εντοπίσει απάτη και άλλες εγκληματικές πράξεις. Ενδέχεται να συλλέξει επιπρόσθετες πληροφορίες σχετικά με αυτές τις επικοινωνίες, π.χ. τηλεφωνικούς αριθμούς από τους οποίους οι ασθενείς

καλούν και πληροφορίες για τις συσκευές ή το λογισμικό που χρησιμοποιούν οι τελευταίοι, μόνο εφόσον αυτό κρίνεται αναγκαίο για τους παραπάνω σκοπούς.

ο **Η προστασία των ανήλικων**

Ο ΙΑΤΡΟΚΟΣΜΟΣ λαμβάνει ιδιαίτερα μέτρα για την προστασία των ανηλίκων και την ιδιωτικότητα των προσωπικών τους δεδομένων υγείας. Ειδικότερα, η παρουσία των γονέων/κηδεμόνων κατά τη διάρκεια ιατρικής εξέτασης ή διενέργειας απλών ιατρικών πράξεων (λ.χ. αιμοληψίας) στα ανήλικα παιδιά τους επιτρέπεται και ενθαρρύνεται από τους επαγγελματίες υγείας του Διαγνωστικού Κέντρου. Ζητείται η συγκατάθεση του κηδεμόνα για κάθε ιατρική πράξη, καθώς και για την κοινοποίηση των αποτελεσμάτων των εξετάσεων, η οποία αποδεικνύεται μόνο εγγράφως.

Για την δειγματοληψία για ανίχνευση ουσιών απαιτείται η συγκατάθεση του ανηλίκου, εκτός αν πρόκειται για κρίσιμη περίπτωση, όπου η υγεία του βρίσκεται σε άμεσο κίνδυνο, οπότε η εξέταση εκτελείται και χωρίς αυτήν. Οι γονείς νομιμοποιούνται βάσει των διατάξεων του ΑΚ να παραλάβουν τα αποτελέσματα των εξετάσεων των ανήλικων τέκνων τους.

ο **Η Ασφάλεια των προσωπικών δεδομένων**

Προτεραιότητα του ΙΑΤΡΟΚΟΣΜΟΥ είναι η διατήρηση των προσωπικών δεδομένων ασφαλών. Το Διαγνωστικό Κέντρο έχει λάβει και εφαρμόζει μία σειρά μέτρων για να τηρεί τα προσωπικά δεδομένα των εργαζομένων και των ασθενών ασφαλή και προστατευμένα. Τα μέτρα αυτά ανά περίπτωση περιλαμβάνουν έλεγχο προσβασιμότητας στα δεδομένα (role based access control), καθώς και ψευδωνυμοποίηση, κρυπτογράφηση ή άλλα τεχνικά και οργανωτικά μέτρα, όπως η ασφαλής φύλαξη του φυσικού αρχείου. Τα μέτρα ασφαλείας περιγράφονται αναλυτικά στην Πολιτική Προστασίας Προσωπικών Δεδομένων του Διαγνωστικού και επικαιροποιούνται διαρκώς, ανάλογα με τις τεχνολογικές εξελίξεις και τις οργανωτικές ανάγκες.

ο **Η αναφορά συμβάντος παραβίασης προσωπικών δεδομένων**

Ο GDPR απαιτεί να αναφέρει το Διαγνωστικό Κέντρο στην ΑΠΔΠΧ οποιαδήποτε παραβίαση των προσωπικών δεδομένων όταν υπάρχει κίνδυνος για τα δικαιώματα και τις ελευθερίες οποιουδήποτε υποκειμένου των δεδομένων. Όταν η παραβίαση προσωπικών δεδομένων υπέχει υψηλό κίνδυνο για το υποκείμενο των δεδομένων, πρέπει αυτό να ειδοποιηθεί, εκτός εάν έχουν ληφθεί μεταγενέστερα μέτρα για να εξασφαλιστεί ότι ο κίνδυνος δεν είναι πιθανόν να υλοποιηθεί ή εφαρμόστηκαν μέτρα ασφαλείας για την αποσαφήνιση των προσωπικών δεδομένων (π.χ. κρυπτογράφηση) ή υπάρχει δυσανάλογη προσπάθεια άμεσης ενημέρωσης του υποκειμένου των δεδομένων. Στις τελευταίες αυτές περιπτώσεις, πρέπει να γίνει δημόσια ανακοίνωση ή να θεσπιστεί ένα εξίσου αποτελεσματικό εναλλακτικό μέτρο για την ενημέρωση των υποκειμένων των δεδομένων, ούτως ώστε οι ίδιοι να λάβουν οποιαδήποτε διορθωτική ενέργεια.

Ο ΙΑΤΡΟΚΟΣΜΟΣ έχει υιοθετήσει συγκεκριμένη διαδικασία για την αντιμετώπιση τυχόν παραβιάσεων προσωπικών δεδομένων.

Εργαζόμενοι του Διαγνωστικού ή ασθενείς – εξεταζόμενοι που γνωρίζουν ή υποψιάζονται ότι έχει σημειωθεί παραβίαση προσωπικών δεδομένων, πρέπει να επικοινωνήσουν αμέσως με τον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων και να ακολουθήσουν τις οδηγίες που ορίζονται στην σχετική διαδικασία, συμπληρώνοντας τη σχετική φόρμα αναφοράς. Πρέπει, εξάλλου, να διατηρούν τα ανωτέρω υποκείμενα όλα τα αποδεικτικά στοιχεία που αφορούν παραβιάσεις προσωπικών δεδομένων, ιδίως προκειμένου να επιτρέψουν στο Διαγνωστικό Κέντρο να τηρεί αρχείο των παραβιάσεων αυτών, όπως απαιτείται από τον GDPR.

ο **Η τήρηση αρχείων**

Ο GDPR απαιτεί τη διατήρηση πλήρων και ακριβών αρχείων για όλες τις δραστηριότητες επεξεργασίας προσωπικών δεδομένων. Τα υποκείμενα πρέπει να διατηρούν ακριβή εταιρικά αρχεία που αντικατοπτρίζουν την επεξεργασία του Διαγνωστικού, συμπεριλαμβανομένων των αρχείων που περιέχουν την συγκατάθεση των υποκειμένων των δεδομένων και των διαδικασιών για την απόκτηση συγκατάθεσης, στις περιπτώσεις για τις οποίες η συγκατάθεση είναι η νομική βάση της επεξεργασίας.

Αυτά τα αρχεία πρέπει να περιλαμβάνουν τουλάχιστον το όνομα και τα στοιχεία επικοινωνίας του ΙΑΤΡΟΚΟΣΜΟΥ ως Υπευθύνου Επεξεργασίας και το όνομα του ΥΠΔ, σαφείς περιγραφές των τύπων προσωπικών δεδομένων, τύποι των δεδομένων, δραστηριότητες επεξεργασίας, σκοπούς επεξεργασίας,

αποδέκτες των δεδομένων προσωπικού χαρακτήρα τρίτων, τοποθεσίες αποθήκευσης προσωπικών δεδομένων, μεταφορά δεδομένων προσωπικού χαρακτήρα, περίοδος διατήρησης των προσωπικών δεδομένων και περιγραφή των μέτρων ασφαλείας που ισχύουν.

Πρέπει επίσης να τηρούνται αρχεία παραβιάσεων προσωπικών δεδομένων, τα οποία ορίζουν:

1. τα γεγονότα
2. τα αποτελέσματα αυτών
3. τα διορθωτικά μέτρα που ελήφθησαν

ο Η Εκπαίδευση και ο έλεγχος

Ο ΙΑΤΡΟΚΟΣΜΟΣ οφείλει να διασφαλίσει ότι όλο το προσωπικό του θα εκπαιδευτεί κατάλληλα για να μπορέσει να συμμορφωθεί με τη νομοθεσία περί προστασίας προσωπικών δεδομένων. Πρέπει επίσης το Διαγνωστικό Κέντρο να δοκιμάζει τακτικά τα συστήματα και τις διαδικασίες του για την αξιολόγηση της συμμόρφωσης. Ο ΥΠΔ καταρτίζει σε τακτικά διαστήματα πρόγραμμα εξειδικευμένης εκπαίδευσης, αποστέλλει πληροφορίες μέσω e-mail και διενεργεί ενημερωτικές παρουσιάσεις.

ο Οι Υπεύθυνοι

Ο ΙΑΤΡΟΚΟΣΜΟΣ ενημερώνει τα υποκείμενα των δεδομένων ότι μπορούν να επικοινωνούν για οποιοδήποτε ζήτημα τους απασχολεί σχετικά με την ασφάλεια των δεδομένων τους με το Διαγνωστικό μας Κέντρο στο ακόλουθο τηλέφωνο 210-6400200, καθώς και στο email: info@iatrocosmos.gr.

Η Υπεύθυνη Προστασίας των Δεδομένων σας στο Διαγνωστικό μας Κέντρο έχει ορισθεί η **Δανάη Στεργίου**, στην οποία μπορείτε να απευθυνθείτε στο email: dpo@iatrocosmos.gr και τον αριθμό τηλεφώνου: 210-8211660.

Εάν δεν είναι ικανοποιημένα τα υποκείμενα των δεδομένων, με τον τρόπο επεξεργασίας των δεδομένων τους από το Διαγνωστικό Κέντρο ΙΑΤΡΟΚΟΣΜΟΣ, μπορούν να υποβάλουν σχετική καταγγελία στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Ωστόσο, χαρά θα ήταν για το Διαγνωστικό μας Κέντρο να του δοθεί η ευκαιρία να επιλύσει οποιοδήποτε παράπονο των υποκειμένων εσωτερικά, το συντομότερο δυνατό, προτού αυτά προβούν σε καταγγελία ενώπιον της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.