



#### Α. ΣΤΟΙΧΕΙΑ ΕΓΓΡΑΦΟΥ

Κωδικός	<b>Δ 00-1</b>
Τίτλος	<b>Πολιτική Προστασίας Δεδομένων Προσωπικού Χαρακτήρα</b>
Σκοπός	Η παρούσα διαδικασία περιγράφει την Πολιτική Προστασίας Δεδομένων Προσωπικού Χαρακτήρα που ακολουθεί η Εταιρία ως προς την Συλλογή και κάθε μορφής Επεξεργασίας των Δεδομένων.
Έκδοση	3.0
Ημνία Έγκρισης	1/5/2018
Έγκριση 1 <sup>η</sup>	Υπεύθυνος Προστασίας Προσωπικών Δεδομένων (DPO)
Έγκριση 2 <sup>η</sup>	Διευθύνων Σύμβουλος

## 1. Σκοπός

Σκοπός της παρούσας πολιτικής είναι η ενημέρωση για τους τρόπους που η Κλινική ΓΕΝΕΣΙΣ (εφεξής Εταιρία) συλλέγει, επεξεργάζεται και προστατεύει τα δεδομένα προσωπικού χαρακτήρα, για τους λόγους που συλλέγει τα δεδομένα, για το είδος των δεδομένων που συλλέγει, για το χρονικό διάστημα που αποθηκεύει τα δεδομένα και για τα κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας που υιοθετεί για την προστασία των δεδομένων.

Πιο συγκεκριμένα, η παρούσα πολιτική σχετίζεται με όλες τις απαραίτητες ενέργειες που αναπτύσσει και υλοποιεί η Εταιρία, όπως αυτές προκύπτουν από τον Γενικό Κανονισμό Προστασίας Δεδομένων Προσωπικού Χαρακτήρα 2016/679 (GDPR) και την ισχύουσα εθνική Νομοθεσία και οι οποίες αφορούν την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, τους κανόνες που αφορούν την ελεύθερη κυκλοφορία τους, καθώς και την προστασία των θεμελιωδών δικαιωμάτων και τις ελευθερίες των φυσικών προσώπων και ειδικότερα το δικαίωμα τους στην προστασία των δεδομένων προσωπικού χαρακτήρα. Η επεξεργασία μπορεί να αφορά την συλλογή, την καταχώριση, την οργάνωση, την διάρθρωση, την αποθήκευση, την προσαρμογή, την μεταβολή, την ανάκτηση, την αναζήτηση πληροφοριών χρήση, την κοινολόγηση, με διαβίβαση, την διαγραφή, την καταστροφή δεδομένων προσωπικού χαρακτήρα.

Η φύση της εργασίας στην Εταιρία είναι τέτοια ώστε καθημερινά να έρχεται σε επαφή με Δεδομένα Προσωπικού Χαρακτήρα πελατών, προσωπικού, ιατρών – συνεργατών, λοιπών συνεργατών – προμηθευτών - υπεργολάβων, επισκεπτών ηλεκτρονικής ιστοσελίδας ή/και λήπτες ηλεκτρονικών επικοινωνιών κλπ.

Η Εταιρεία διατηρεί μονομερώς το δικαίωμα να επικαιροποιεί, τροποποιεί, προσθέτει, μεταβάλλει τις υπηρεσίες της και την παρούσα Πολιτική, ανά διαστήματα, οποτεδήποτε κρίνει τούτο αναγκαίο, χωρίς προηγούμενη ειδοποίηση, πάντα εντός του εκάστοτε ισχύοντος νομικού πλαισίου και σύμφωνα με τυχόν μεταβολές στην κείμενη νομοθεσία περί προστασίας προσωπικών δεδομένων. Η Εταιρεία ενθαρρύνει κάθε ενδιαφερόμενο να ελέγχει την παρούσα Πολιτική ανά τακτά χρονικά διαστήματα ώστε να ενημερώνεται για τις αλλαγές που έχουν πραγματοποιηθεί.

## 2. Δεδομένα Προσωπικού Χαρακτήρα

Δεδομένα Προσωπικού Χαρακτήρα είναι κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο, του οποίου η ταυτότητα μπορεί να εξακριβωθεί άμεσα ή έμμεσα, μέσω της αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας όπως ονοματεπώνυμο, αριθμός ταυτότητας, ΑΦΜ, ΑΜΚΑ κλπ ή/και μέσω παραγόντων που προσδιορίζουν την σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική, κοινωνική ταυτότητα του φυσικού προσώπου. Τα γενετικά δεδομένα, τα βιομετρικά δεδομένα και τα δεδομένα που αφορούν την υγεία, αποτελούν ειδικές κατηγορίες δεδομένων (ευαίσθητα) και απαιτούν αυξημένη προστασία.

### 3. Σκοποί Συλλογής, Επεξεργασίας και Διάθεσης Δεδομένων Προσωπικού Χαρακτήρα

Η Εταιρία συλλέγει, επεξεργάζεται και αποθηκεύει δεδομένα προσωπικού χαρακτήρα για την εκπλήρωση των ακόλουθων σκοπών:

- Για την παροχή ιατρικών και νοσηλευτικών υπηρεσιών πρωτοβάθμιας και δευτεροβάθμιας φροντίδας προς τους ανθρώπους που την επισκέπτονται (πελάτες: εσωτερικοί ασθενείς, εξωτερικοί ασθενείς και επισκέπτες διαγνωστικού τομέα)
- Για τη διαχείριση θεμάτων διοίκησης ανθρώπινου δυναμικού, όσον αφορά το προσωπικό που απασχολεί η Εταιρία, ανεξαρτήτως σχέσης εργασίας και ειδικότητας (προσλήψεις, απολύσεις – παραιτήσεις, μισθοδοσίες, αξιολογήσεις, εταιρικές επικοινωνίες κλπ)
- Για την εύρυθμη συνεργασία της Εταιρίας με τους συνεργάτες ιατρούς της, ανεξαρτήτως σχέσης εργασίας και ιατρικής ειδικότητας
- Για τη διαχείριση θεμάτων συνεργασίας με προμηθευτές προϊόντων και υπηρεσιών, υπεργολάβων και λοιπών συνεργατών, μέσω σχετικών συμβάσεων ή πρόσθετων πράξεων
- Για την ανταπόκριση σε αιτήματα ελεγκτικών αρχών και τη διαχείριση από το νόμο προβλεπόμενων απαιτήσεων και ελέγχων
- Για την διαχείριση παραπόνων των πελατών και επισκεπτών
- Για βοηθητικές υπηρεσίες όπως η πρόσβαση και η ασφάλεια, καθώς και ο έλεγχος εισόδου σε όλους τους χώρους της Εταιρίας, συμπεριλαμβανομένου και του κλειστού κυκλώματος CCTV για λόγους ασφαλείας
- Για την προβολή και προώθηση των υπηρεσιών, συμπεριλαμβανομένων των πεδίων του Internet & Social Media Marketing, του e-mail marketing, του SMS Marketing, της διοργάνωσης ενημερωτικών δράσεων και εκδηλώσεων πολύ-θεματικού χαρακτήρα προς τους πελάτες αλλά και το ευρύ κοινό, καθώς και πάσης φύσεως λοιπές ενέργειες marketing (direct marketing, έντυπη προβολή κλπ).
- Για την προώθηση των δημοσίων σχέσεων της Εταιρίας (ενέργειες εταιρικής κοινωνικής ευθύνης, χορηγίες κλπ.)
- Για την οργάνωση και διεξαγωγή εκπαιδευτικών σεμιναρίων / προγραμμάτων προς το προσωπικό, αλλά και επιστημονικών ημερίδων / εκδηλώσεων ή/και εκπαιδεύσεων προς τους συνεργάτες ιατρούς κάθε ειδικότητας
- Για τη διεκπεραίωση νομικών ζητημάτων (μέσω της νομικής υπηρεσίας)
- Για τη διαχείριση λογιστικών και φοροτεχνικών υπηρεσιών
- Για την ασφαλή λειτουργία του χώρου απασχόλησης παιδιών που βρίσκεται εντός της Εταιρίας

#### 4. Βασικές Αρχές Συλλογής και Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα

Η Εταιρία τηρεί τις κάτωθι θεμελιώδεις αρχές:

- Τα δεδομένα συλλέγονται κατά τρόπο θεμιτό και νόμιμο, για καθορισμένους, σαφείς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο μη συμβατό προς τους σκοπούς αυτούς
- Τα δεδομένα είναι κατάλληλα και συναφή και περιορίζονται στα ελάχιστα αναγκαία σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία
- Τα δεδομένα είναι ακριβή και επικαιροποιούνται όποτε απαιτείται, ενώ λαμβάνονται όλα τα εύλογα μέτρα, ώστε δεδομένα προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία, να διαγράφονται ή να διορθώνονται χωρίς καθυστέρηση
- Τα δεδομένα διατηρούνται σε μορφή που επιτρέπει τον προσδιορισμό της ταυτότητας των προσώπων στα οποία αναφέρονται και για χρονικό διάστημα όχι μεγαλύτερο από αυτό που είναι αναγκαίο για την επίτευξη των σκοπών επεξεργασίας και βάσει της κείμενης νομοθεσίας.
- Η επεξεργασία των προσωπικών δεδομένων, συμπεριλαμβανομένης και της διαβίβασης σε τρίτους, πραγματοποιείται μόνο με ρητή και γραπτή συγκατάθεση του φυσικού προσώπου (υποκείμενου), εκτός από τις περιπτώσεις για τις οποίες προβλέπεται από το εκάστοτε ισχύον κανονιστικό πλαίσιο, σχετική εξαίρεση
- Η συλλογή και η επεξεργασία των δεδομένων πραγματοποιείται με σεβασμό στα δικαιώματα ενημέρωσης, πρόσβασης και αντίρρησης των υποκειμένων
- Η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι απόρρητη και διεξάγεται από πρόσωπα τα οποία δεσμεύονται για την τήρηση του απορρήτου
- Λαμβάνονται τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας
- Τα δεδομένα υποβάλλονται σε επεξεργασία υπό την ευθύνη της Εταιρίας (υπεύθυνος επεξεργασίας), η οποία διασφαλίζει και αποδεικνύει για κάθε πράξη επεξεργασίας τη συμμόρφωση της προς τις διατάξεις του εκάστοτε ισχύοντος κανονιστικού πλαισίου.

## 5. Είδη Δεδομένων Προσωπικού Χαρακτήρα που συλλέγονται

Ενδεικτικά, τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται στην Εταιρία και επιδέχονται επιπλέον επεξεργασία αφορούν όλα εκείνα τα απαραίτητα στοιχεία για την εισαγωγή ενός πελάτη / ασθενή ή επισκέπτη διαγνωστικού τμήματος, για την πρόσληψη ενός υπαλλήλου, για την πάσης φύσεως συνεργασία με ιατρό ασχέτου ιατρικής ειδικότητας, για την συνεργασία με προμηθευτή – υπεργολάβο – λοιπούς συνεργάτες, για την ηλεκτρονική αποστολή ενημερωτικού δελτίου / newsletter προς τρίτους κ.ο.κ.

Στην περίπτωση των πελατών, τα δεδομένα αφορούν ονοματεπώνυμο και γενικότερα στοιχεία επικοινωνίας, οικογενειακής κατάστασης κλπ., συμπεριλαμβανομένης της διεύθυνσης ηλεκτρονικού ταχυδρομείου και του αριθμού τηλεφώνου, δικών τους ή συγγενών τους. Παράλληλα, συλλέγονται δεδομένα υγείας σχετικά με τις παρεχόμενες από την Εταιρεία ιατρικές ή νοσηλευτικές υπηρεσίες ή ακόμα και δεδομένα υγείας για ιατρικές υπηρεσίες που δεν παρασχέθηκαν από την Εταιρία, αλλά αναφέρθηκαν στην Εταιρία είτε από τους ίδιους τους πελάτες, είτε από τρίτους. Επιπλέον, μπορεί να συλλέγονται πληροφορίες για την διεκπεραίωση της πληρωμής (πχ πιστωτική κάρτα).

Επιπρόσθετα, πληροφορίες προέρχονται από τη χρήση της ιστοσελίδας της Εταιρίας και πάσης φύσεως ψηφιακών πλατφορμών που χρησιμοποιεί ή μπορεί να χρησιμοποιήσει στο μέλλον η εταιρία, με σκοπό την ενημέρωσή τρίτων, σχετικά με τις υπηρεσίες που παρέχει. Ενδεικτικά, και πέρα από την χρήση / επίσκεψη στην εταιρική ιστοσελίδα, συλλογή δεδομένων πραγματοποιείται και μέσω εγγραφής στην ηλεκτρονική εφαρμογή για την λήψη ενημερωτικού δελτίου / newsletter σε τακτική βάση ή/και την λήψη ηλεκτρονικής αλληλογραφίας ή αλληλογραφίας ανακοινώσεων/ ειδήσεων και υποβολή ερωτημάτων σε σχέση με υπηρεσίες που παρέχονται.

Πέραν των ανωτέρω δεδομένων που παρέχονται στην Εταιρία, ενδέχεται να συλλέγονται τεχνικές πληροφορίες που αποτελούν προσωπικά δεδομένα, όπως για παράδειγμα η διεύθυνση πρωτοκόλλου διαδικτύου (Internet Protocol address) της συσκευής του επισκέπτη (πχ ηλεκτρονικός υπολογιστής, laptop, tablet, smartphone), μοτίβα περιήγησης στις ιστοσελίδες (browsing patterns), πληροφορίες σχετικά με τη χρήση μιας ιστοσελίδας, ιστορικό του προγράμματος περιήγησης (browser history), δεδομένα γεωγραφικού προσδιορισμού (geolocation), στοιχεία του πρωτοκόλλου HTTP κλπ. Οι τεχνικές αυτές πληροφορίες χρησιμοποιούνται για την ομαλή λειτουργία και απόδοση της ιστοσελίδας και των ηλεκτρονικών υπηρεσιών, και δεν αποθηκεύονται μόνιμα στις υποδομές της Εταιρία, ενώ τα δεδομένα τηρούνται σε συγκεντρωτική μορφή ώστε να μην είναι εφικτή κατά το δυνατό η ταυτοποίηση των χρηστών.

## 6. Συλλογή Δεδομένων Προσωπικού Χαρακτήρα και Διαβίβαση

Τα δεδομένα προσωπικού χαρακτήρα συλλέγονται από εξουσιοδοτημένους ανά υπηρεσία υπαλλήλους της Εταιρίας, για τους σκοπούς και μόνο της παροχής της εκάστοτε υπηρεσίας. Ενδεικτικά, το Γραφείο Κίνησης, η γραμματεία εξωτερικών ιατρείων, η γραμματεία διαγνωστικού τομέα, η υποδοχή επιτόκων και η κεντρική υποδοχή συλλέγουν δεδομένα πελατών (εσωτερικών – εξωτερικών ασθενών και επισκεπτών για διαγνωστικές εξετάσεις), το τμήμα ανθρωπίνου δυναμικού συλλέγει δεδομένα του προσωπικού και των συνεργατών ιατρών, το λογιστήριο συλλέγει δεδομένα προμηθευτών – υπεργολάβων – λοιπών συνεργατών, το τμήμα Μάρκετινγκ συλλέγει δεδομένα

ατόμων, μεταξύ των άλλων, για αποστολή newsletter και λοιπών εταιρικών ενημερώσεων / δράσεων Κ.Ο.Κ.

Ως προς την πηγή προέλευσης των δεδομένων, ειδικά για την περίπτωση των πελατών (εσωτερικοί, ασθενείς, εξωτερικοί ασθενείς, επισκέπτες διαγνωστικού τομέα), τα δεδομένα μπορεί να δίδονται από τα ίδια τα υποκείμενα των δεδομένων ή από άτομο/άτομα που τα συνοδεύουν.

Σχετικά με την διαβίβαση, τα συλλεχθέντα δεδομένα προσωπικού χαρακτήρα διαβιβάζονται αποκλειστικά σε εξουσιοδοτημένα τρίτα μέρη που δεσμεύονται στην τήρηση εμπιστευτικότητας, όταν αυτά απαιτείται να έχουν πρόσβαση στο πλαίσιο παροχής των πάσης φύσεως παρεχόμενων υπηρεσιών υπηρεσιών (π.χ. ιατροί για σκοπούς διάγνωσης). Μετά από εντολή των υποκειμένων των δεδομένων, τα προσωπικά μπορούν να διαβιβαστούν σε τρίτους (π.χ. άλλο ιατρό) / συνεργαζόμενες με την Εταιρεία επιχειρήσεις (π.χ. ασφαλιστικές εταιρίες στις οποίες έχει συμβληθεί το υποκείμενο). Η Εταιρεία δεσμεύεται ότι δεν θα εμπορευθεί τα προσωπικά δεδομένα διαθέτοντάς τα προς πώληση/ενοικίαση δίνοντάς τα/ μεταφέροντας /δημοσιοποιώντας ή κοινοποιώντας τα σε τρίτους ή να τα χρησιμοποιήσει με άλλον τρόπο και για άλλους σκοπούς που δύναται να διακινδυνεύσουν την ιδιωτικότητα, τα δικαιώματα ή τις ελευθερίες του υποκειμένου των δεδομένων, εκτός αν επιβάλλεται από το νόμο, δικαστική απόφαση/εντολή, διοικητική πράξη ή αν αποτελεί συμβατική υποχρέωση απαραίτητη για την εύρυθμη λειτουργία της Ιστοσελίδας της Εταιρείας και την πραγματοποίηση των λειτουργιών της.

Ενδέχεται τα προσωπικά δεδομένα να διαβιβαστούν σε συνεργάτες, ή σε τρίτους, συμμορφούμενους με τους όρους της παρούσας Πολιτικής και δεσμευόμενους στην τήρηση εμπιστευτικότητας, οι οποίοι ενεργούν εκ μέρους της Εταιρείας για περαιτέρω επεξεργασία με σκοπό την παροχή υπηρεσιών, την αξιολόγηση και την βελτίωση της λειτουργικότητας της ιστοσελίδας, σκοπούς μάρκετινγκ, διαχείρισης δεδομένων και τεχνικής υποστήριξης, μόνο, αφότου ενημερωθεί ο χρήστης εκ των προτέρων και ληφθεί η συγκατάθεσή του. Οι εν λόγω τρίτοι έχουν δεσμευτεί συμβατικά με την Εταιρεία, ότι θα χρησιμοποιήσουν τα προσωπικά δεδομένα μόνο για τους παραπάνω λόγους, και δεν θα διαβιβάσουν τις προσωπικές πληροφορίες σε τρίτα μέρη, καθώς και δεν θα τις κοινοποιήσουν σε τρίτους εκτός αν το επιβάλλει ο νόμος.

## **7. Διάρκεια Τήρησης Δεδομένων**

Τα δεδομένα προσωπικού χαρακτήρα τηρούνται για όσο χρόνο απαιτείται από τη φύση της παρεχόμενης από την Εταιρεία υπηρεσίας (ανάλογα με την εκάστοτε υπηρεσία) και επιπρόσθετα, για όσο χρόνο καθορίζει η σχετική νομοθεσία.

## **8. Θεμελιώδη δικαιώματα υποκειμένων (φυσικών προσώπων / κατόχων των δεδομένων)**

Τα υποκείμενα έχουν τα ακόλουθα δικαιώματα έναντι των δεδομένων προσωπικού χαρακτήρα:

- Το δικαίωμα ενημέρωσης τους

Ενδεικτικά, κατά το στάδιο συλλογής δεδομένων προσωπικού χαρακτήρα, η Εταιρία έχει την υποχρέωση να ενημερώσει το υποκείμενο των δεδομένων προσωπικού χαρακτήρα με τρόπο κατανοητό για:

- Την ταυτότητα και τα στοιχεία επικοινωνίας της Εταιρίας
- Τον σκοπό της επεξεργασίας των δεδομένων τους
- Για τους αποδέκτες ή κατηγορίες αποδεκτών των προσωπικών δεδομένων
- Για το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα
- Για τα δικαιώματα πρόσβασης, διόρθωσης, διαγραφής και αντίταξης στην επεξεργασία των προσωπικών δεδομένων
- Για τον υποχρεωτικό χαρακτήρα ή μη της χορήγησης των δεδομένων, καθώς και για τις ενδεχόμενες συνέπειες σε περίπτωση μη χορήγησης τους
- Για το δικαίωμα υποβολής καταγγελίας στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, παρέχοντας του τα στοιχεία επικοινωνίας της Αρχής
- Σε περίπτωση που τα δεδομένα δεν χορηγούνται από το πρόσωπο στο οποίο αναφέρονται, η Εταιρία οφείλει να ενημερώσει το πρόσωπο στο οποίο αναφέρονται τα δεδομένα, για την πηγή προέλευσης των δεδομένων τους
- Σε περίπτωση που η Εταιρία προτίθεται να διαβιβάσει τα δεδομένα σε τρίτη χώρα ή διεθνή οργανισμό, το υποκείμενο ενημερώνεται για το επίπεδο προστασίας που παρέχει η εν λόγω τρίτη χώρα ή ο διεθνής οργανισμός

Η Εταιρία έχει την υποχρέωση να προβαίνει στις απαραίτητες τροποποιήσεις στα έντυπα που χρησιμοποιούνται για την προ-συμβατική και συμβατική ενημέρωση του υποκειμένου

- Δικαίωμα Πρόσβασης, ότι η Εταιρία ως υπεύθυνος επεξεργασίας θα επεξεργαστεί τα δεδομένα προσωπικού χαρακτήρα
- Το δικαίωμα του υποκειμένου των δεδομένων στη διόρθωση των δεδομένων τους, με έγγραφη αίτηση προς τον υπεύθυνο επεξεργασίας, ο οποίος οφείλει να ικανοποιήσει το αίτημα χωρίς καθυστέρηση και εντός ενός μηνός εκτός αν συντρέχουν άλλοι λόγοι για μεγαλύτερο διάστημα
- Το δικαίωμα στη λήθη (διαγραφή) των υποκειμένων των δεδομένων
- Το δικαίωμα των υποκειμένων των δεδομένων στον περιορισμό της επεξεργασίας
- Το δικαίωμα των υποκειμένων των δεδομένων στη φορητότητα των δεδομένων τους
- Το δικαίωμα αντίρρησης
- Το δικαίωμα αντίρρησης στις περιπτώσεις profiling
- Οι περιορισμοί των δικαιωμάτων των υποκειμένων των δεδομένων

Ειδικότερα, αναφορικά με την υπηρεσία λήψης ενημερωτικού δελτίου ("newsletter"), υπάρχει η δυνατότητα απεγγραφής ("unsubscribe") ακολουθώντας τις οδηγίες που περιλαμβάνονται σε κάθε ενημερωτικό δελτίο ("newsletter"), ώστε να σταματήσει η επεξεργασία των προσωπικών δεδομένων που σχετίζονται με την υπηρεσία αυτή.

Τα παραπάνω δικαιώματά μπορούν να υποβληθούν εγγράφως από τα υποκείμενα των δεδομένων με σχετική αίτηση στην ηλεκτρονική διεύθυνση [dpo@genesishospital.gr](mailto:dpo@genesishospital.gr), ενώ για οποιοδήποτε θέμα σχετικά με τα προσωπικά δεδομένα ή/ και για διευκρινήσεις, υπάρχει η δυνατότητα επικοινωνίας με τον Υπεύθυνο Προστασίας Δεδομένων ("Data Protection Officer") της Εταιρείας κ. Δημοσθένη Κωστούλα, είτε τηλεφωνικώς στο 2310-984000, είτε μέσω e-mail στην παραπάνω ηλεκτρονική διεύθυνση, είτε μέσω τηλεμοιτυπίας (φαξ) στο 2310-984460. Σε κάθε περίπτωση, τα υποκείμενα των δεδομένων έχουν το δικαίωμα να απευθύνονται στην αρμόδια Αρχή για την Προστασία των Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ, [www.dpa.gr](http://www.dpa.gr)) ή/και να ασκούν δικαστική προσφυγή. Κάθε αίτημα που υποβάλλεται θα πρέπει να συνοδεύεται από τα κατάλληλα αποδεικτικά στοιχεία ταυτοποίησης και να παρέχονται οι απαιτούμενες πληροφορίες (π.χ. τα δεδομένα που χρειάζονται διόρθωση), όπως περιγράφονται στους όρους χρήσης της εκάστοτε υπηρεσίας. Η Εταιρεία μπορεί να ζητήσει την παροχή πρόσθετων πληροφοριών αναγκαίων για την επιβεβαίωση της ταυτότητάς του υποκειμένου των δεδομένων.

Η Εταιρεία καταβάλλει κάθε δυνατή προσπάθεια ώστε τα αιτήματά να απαντούνται χωρίς καθυστέρηση και σε κάθε περίπτωση εντός μηνός από την παραλαβή τους. Η εν λόγω προθεσμία μπορεί να παραταθεί κατά δύο (2) ακόμη μήνες, εφόσον απαιτείται, λαμβανομένων υπόψη της πολυπλοκότητας του αιτήματος και του αριθμού των αιτημάτων. Για την εν λόγω παράταση καθώς και για τους λόγους της καθυστέρησης υποκείμενα των δεδομένων θα ενημερώνονται εντός μηνός από την παραλαβή του αιτήματος από την Εταιρεία. Εάν το υποβληθεί με ηλεκτρονικά μέσα, η απάντηση θα παρέχεται, εάν είναι δυνατόν, με ηλεκτρονικά μέσα, εκτός αν ζητηθεί κάτι διαφορετικό (πχ έγγραφη επιστολή).

Σε κάθε περίπτωση, τα υποκείμενα μπορούν να απευθύνονται στον Υπεύθυνο Προστασίας Δεδομένων, στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) ή/ και να ασκούν δικαστική προσφυγή, εφόσον θεωρήσουν ότι τα ανωτέρω δικαιώματά σας παραβιάστηκαν.

## 9. Υποχρεώσεις Εταιρείας / Υπεύθυνου Επεξεργασίας

Η Εταιρεία ως υπεύθυνος επεξεργασίας έχει τις ακόλουθες υποχρεώσεις:

- Υποχρέωση γνωστοποίησης όσον αφορά τη διόρθωση ή τη διαγραφή δεδομένων προσωπικού χαρακτήρα ή τον περιορισμό της επεξεργασίας
- Υποχρέωση πρόβλεψης προστασίας των δεδομένων προσωπικού χαρακτήρα ήδη από το σχεδιασμό της επεξεργασίας (privacy by design) και εξ' ορισμού (privacy by default)
- Υποχρέωση του υπευθύνου επεξεργασίας για τήρηση αρχείων σχετικά με τις δραστηριότητες επεξεργασίας και καταχωρήσεων
- Υποχρέωση του υπευθύνου επεξεργασίας για τη συνεργασία με την εποπτική αρχή



- Υποχρέωση του υπευθύνου επεξεργασίας για τη διασφάλιση του απορρήτου και της ασφάλειας της επεξεργασίας
- Υποχρεώσεις του υπευθύνου επεξεργασίας σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα (data breaches):
  - Ενημέρωση της εποπτικής αρχής εντός 72 ωρών
  - Ενημέρωση του υποκείμενου των δεδομένων, εφόσον ο κίνδυνος είναι μεγάλος
- Υποχρεώσεις του υπευθύνου επεξεργασίας για εκτίμηση αντικτύπου (Privacy Impact Assessment) σχετικά με την προστασία δεδομένων
- Υποχρέωση του υπευθύνου επεξεργασίας για τον ορισμό Υπευθύνου Προστασίας Δεδομένων (Data Protection Officer - DPO)

## 10. Ασφάλεια Δεδομένων Προσωπικού Χαρακτήρα

Η Εταιρεία θεωρεί άκρως σημαντική την ιδιωτικότητα των προσώπων των οποίων επεξεργάζεται τα προσωπικά τους δεδομένα, είτε πελατών της, είτε εργαζομένων, είτε τρίτων και καταβάλλει κάθε δυνατή προσπάθεια για την προστασία τους, τόσο ως προς την εμπιστευτικότητα/ εχεμύθεια των πληροφοριών, όσο και ως προς την ακεραιότητά τους (να μην αλλοιωθούν, να μην καταστραφούν κατά λάθος κ.λπ.).

Γενικά, η Εταιρία, ως υπεύθυνος επεξεργασίας δεδομένων προσωπικού χαρακτήρα, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία και το κόστος εφαρμογής, τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και την σοβαρότητα και πιθανότητα επέλευσης των κινδύνων που θέτει η επεξεργασία για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, εφαρμόζει με αποτελεσματικό τρόπο, τόσο κατά τον καθορισμό των μέσων επεξεργασίας, όσο και κατά την ίδια την επεξεργασία, κατάλληλα τεχνικά και οργανωτικά μέτρα, ώστε να ενσωματώσει κατά την επεξεργασία τις αρχές προστασίας και τις αναγκαίες διασφαλίσεις για τα δεδομένα προσωπικού χαρακτήρα. Τα κατάλληλα τεχνικά και οργανωτικά μέτρα εφαρμόζονται για να διασφαλίζεται ότι, εξ ορισμού, υποβάλλονται σε επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας.

Επιπλέον η Εταιρία διατηρεί αρχείο όλων των κατηγοριών δραστηριοτήτων επεξεργασίας για τις οποίες είναι υπεύθυνο. Ενδεικτικά: βασικά στοιχεία υπευθύνων, σκοπός επεξεργασίας, κατηγορίες αποδεκτών, περιγραφή υποκειμένων, τυχών διαβίβαση σε τρίτες χώρες, την νόμιμη βάση επεξεργασίας, προθεσμίες για διαγραφή των διαφόρων κατηγοριών δεδομένων προσωπικού χαρακτήρα, περιγραφή κατάλληλα τεχνικά και οργανωτικά μέτρα. Παράλληλα, η Εταιρία τηρεί καταχωρήσεις για τις ακόλουθες πράξεις επεξεργασίας στα συστήματα αυτοματοποιημένης επεξεργασίας: συλλογή, μεταβολή, αναζήτηση πληροφοριών, κοινολόγηση περιλαμβανομένων των διαβιβάσεων, συνδυασμό και διαγραφή.

Η πρόσβαση στα στοιχεία επικοινωνίας των επισκεπτών/χρηστών των Ιστοσελίδων της Εταιρείας περιορίζεται στα εξουσιοδοτημένα πρόσωπα που δεσμεύονται στην τήρηση εμπιστευτικότητας (εργαζομένους, παρόχους υπηρεσιών) και θεωρείται εύλογα ότι χρειάζεται να γνωρίζουν αυτά τα στοιχεία για την παροχή προϊόντων ή υπηρεσιών προς τους επισκέπτες/ χρήστες των Ιστοσελίδων ή για την εκτέλεση της εργασίας τους. Επίσης, η Εταιρεία ρητά απογορεύει εντός των χώρων εργασίας της εταιρείας τη χρήση από το προσωπικό και τους συνεργάτες, φωτογραφικών μηχανών, καμερών

βιντεοσκόπησης καθώς επίσης και τη χρήση των λειτουργιών φωτογράφισης και βιντεοσκόπησης των κινητών τηλεφώνων

### **11. Ενέργειες και Απαιτήσεις Ασφαλείας για την Προστασία των Δεδομένων Προσωπικού Χαρακτήρα (αφορά το προσωπικό της Εταιρίας)**

Στο πλαίσιο άσκησης των καθηκόντων του, το προσωπικό μαθαίνει δεδομένα προσωπικού χαρακτήρα (είτε προφορικά, είτε γραπτά, είτε ηλεκτρονικά) και είναι υποχρέωση του να τα διαφυλάσσει και να τηρεί απόλυτη εχεμύθεια για οποιοδήποτε στοιχείο υποπίπτει στην αντίληψή του ή του αποκαλύπτει ο ασθενής ή τρίτοι (συγγενείς, συνοδοί, επισκέπτες, ιατροί, λοιποί συνεργάτες κλπ).

Ευαίσθητα Προσωπικά Δεδομένα δίδονται (εκδίδονται) μετά από προηγούμενη γραπτή αίτηση του προσώπου στο οποίο αφορούν ή σε τρίτο πρόσωπο που έχει εξουσιοδοτηθεί ειδικά από τον αιτούντα. Ειδικότερα, το προσωπικό προσέχει:

- i. Να μην δίνει πληροφορίες με Ευαίσθητα Προσωπικά Δεδομένα τηλεφωνικώς. Σε περίπτωση επείγουσας και έκτακτης ανάγκης για αποκάλυψη τέτοιων δεδομένων, τότε είναι ευθύνη των προϊσταμένων να έχουν επιβεβαιώσει την ταυτότητα ή την εξουσιοδότηση του αιτούντος.
- ii. Να μην συζητάει με τρίτους (εντός και εκτός) Εταιρίας τα θέματα και στοιχεία πελατών / ασθενών.
- iii. Να τηρεί τα αρχεία που περιέχουν Ευαίσθητα Προσωπικά Δεδομένα σε φυλασσόμενο χώρο, ώστε να αποτρέπεται η χρήση ή η απόκτηση πληροφοριών από μη εξουσιοδοτημένα άτομα.
- iv. Να μην αποκαλύπτει και να διαφυλάσσει τους κωδικούς πρόσβασης (user names & passwords) στα ηλεκτρονικά συστήματα και αρχεία της Εταιρίας.
- v. Να μην αφήνει εκτεθειμένα στα γραφεία και στους χώρους εργασίας πληροφορίες και αρχεία που περιέχουν Ευαίσθητα Προσωπικά Δεδομένα και, ιδιαίτερα, μετά το πέρας της εργασίας.
- vi. Να μην επιτρέπει την χρήση των ηλεκτρονικών συστημάτων της Εταιρίας από μη εξουσιοδοτημένα πρόσωπα.
- vii. Να ενημερώνει άμεσα τους προϊστάμενους και τον Data Protection Officer σε περίπτωση που γίνει αντιληπτή απώλεια ή απόκτηση Ευαίσθητων Προσωπικών Δεδομένων από μη εξουσιοδοτημένα άτομα (ακόμα και αν υπάρχει η υποψία).
- viii. Να συμπληρώνει συστηματικά και πλήρως όλα τα αρχεία που εμπεριέχουν Ευαίσθητα Προσωπικά Δεδομένα.

Πρέπει να γίνει αντιληπτό ότι, η υποχρέωση τήρησης και διαφύλαξης του Ιατρικού Απορρήτου αφορά το σύνολο του προσωπικού, ασχέτου θέσης, ειδικότητας και ιεραρχικής βαθμίδας.