

**ΠΟΛΙΤΙΚΗ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΤΟΥ
ΙΔΡΥΜΑΤΟΣ ΠΕΡΙΘΑΛΨΕΩΣ ΧΡΟΝΙΩΣ ΠΑΣΧΟΝΤΩΝ**

περιεχόμενα

1. Εισαγωγή.....	2
2. Πεδίο εφαρμογής.....	2
3. Σκοπός.....	2
4. Ορισμοί.....	2
5. Αρχές επεξεργασίας προσωπικών δεδομένων.....	4
6. Σκοποί Επεξεργασίας.....	5
7. Κατηγορίες Υποκειμένων των Δεδομένων.....	6
8. Κατηγορίες Δεδομένων.....	6
9. Ενημέρωση Υποκειμένων.....	7
10. Στοιχεία που περιλαμβάνονται στη δήλωση ενημέρωσης.....	7
11. Νόμιμες βάσεις επεξεργασίας.....	8
12. Συγκατάθεση Υποκειμένου.....	9
13. Αποδέκτες προσωπικών δεδομένων.....	10
14. Δικαιώματα των υποκειμένων.....	10
15. Χρόνος διατήρησης των δεδομένων.....	12
16. Οργανωτικά και τεχνικά μέτρα.....	12
17. Εκτίμηση Αντικτόπου.....	13
18. Αρχείο Δραστηριοτήτων.....	13
19. Συνεργάτες – Εκτελούντες την Επεξεργασία – Από κοινού Υπεύθυνοι Επεξεργασίας.....	14
20. Παραβίαση Προσωπικών Δεδομένων.....	14
21. Μητρώο Καταγραφής Περιστατικών Παραβίασης.....	15
22. Ανακοίνωση Παραβίασης Δεδομένων.....	15
23. διαβίβαση Προσωπικών Δεδομένων σε τρίτες χώρες.....	15
24. Αυτοματοποιημένη λήψη αποφάσεων – Κατάρτιση προφίλ.....	16
25. Ρόλοι και αρμοδιότητες.....	16
26. Καθήκοντα και υποχρεώσεις.....	17
27. Ενημέρωση διοικητικού συμβουλίου η/και του υπευθύνου προστασίας δεδομένων.....	17
28. Αναθεώρηση της πολιτικής.....	18

1. ΕΙΣΑΓΩΓΗ

Το Ίδρυμα Περιθάλψεως Χρονίως Πασχόντων, στο πλαίσιο ενάσκησης των δραστηριοτήτων του και της εκπλήρωσης των καταστατικών του σκοπών προβαίνει στην επεξεργασία δεδομένων προσωπικού χαρακτήρα (ενδεικτικά δεδομένα ωφελούμενων, προσωπικού και τρίτων) και ως εκ τούτου οφείλει να τηρεί τις διατάξεις της ισχύουσας Νομοθεσίας περί προστασίας προσωπικών δεδομένων και να υιοθετεί κατάλληλες διαδικασίες και πολιτικές για την προστασία των δεδομένων αυτών.

2. ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Πολιτική Προστασίας Προσωπικών Δεδομένων (εφεξής «η Πολιτική») ισχύει για όλο το προσωπικό του Ιδρύματος, καθώς και για όλους τους ωφελούμενους, συνεργάτες, συμβούλους, προμηθευτές, επισκέπτες και οποιαδήποτε τρίτα πρόσωπα συναλλάσσονται με το Ίδρυμα, οι οποίοι γνωστοποιούν με οιοδήποτε τρόπο προσωπικά δεδομένα στο Ίδρυμα ή αντίστοιχα ζητούν να λάβουν πληροφορίες που ενδεχομένως εμπεριέχουν προσωπικά δεδομένα.

Η εν λόγω Πολιτική αφορά οποιαδήποτε μορφή δεδομένων, συστημάτων, διεργασιών και διαδικασιών που αφορούν στη συλλογή, αποθήκευση, χρήση ή μεταφορά δεδομένων προσωπικού χαρακτήρα, τα οποία διαχειρίζεται το Ίδρυμα στο πλαίσιο ενάσκησης των δραστηριοτήτων του.

3. ΣΚΟΠΟΣ

Σκοπός της Πολιτικής είναι η συμμόρφωση του Ιδρύματος με τις υποχρεώσεις του και η εξασφάλιση επαρκούς επιπέδου προστασίας προσωπικών δεδομένων στο Ίδρυμα. Η Πολιτική περιλαμβάνει κανόνες προστασίας των προσωπικών δεδομένων οι οποίοι ανταποκρίνονται στις απαιτήσεις του Γενικού Κανονισμού για την Προστασία Δεδομένων της Ευρωπαϊκής Ένωσης 2016/679 και της λοιπής ισχύουσας νομοθεσίας επιτρέποντας ταυτόχρονα την αποτελεσματική προώθηση των καταστατικών σκοπών του Ιδρύματος.

Η παρούσα Πολιτική προσδιορίζει τους όρους και παρέχει οδηγίες και κατευθυντήριες γραμμές για τη σωστή εφαρμογή της. Η μη εφαρμογή της μπορεί να οδηγήσει σε παραβίαση του νόμου, με συνέπειες την οικονομική ζημία του Ιδρύματος ή/και την αρνητική επίπτωση στην φήμη του.

4. ΟΡΙΣΜΟΙ

Το Ίδρυμα έχει δεσμευθεί να σέβεται και να προστατεύει τα προσωπικά δεδομένα τα οποία συλλέγει και επεξεργάζεται στα πλαίσια των

δραστηριοτήτων του, συμμορφούμενο πλήρως με τις υποχρεώσεις που απορρέουν από το Ευρωπαϊκό και το εσωτερικό Κανονιστικό Πλαίσιο για την προστασία προσωπικών δεδομένων. Στα πλαίσια αυτά, ενημερώνει για τις κάτωθι έννοιες και όρους της νομοθεσίας:

«Δεδομένα προσωπικού χαρακτήρα»: Κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»): το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.

«Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα»: Δεδομένα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό.

«Υποκείμενο των δεδομένων»: το φυσικό πρόσωπο, στο οποίο αναφέρονται τα δεδομένα και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί.

«Επεξεργασία δεδομένων προσωπικού χαρακτήρα»: Κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.

«Κατάρτιση προφίλ»: οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση/πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις ενός φυσικού προσώπου.

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

«Υπεύθυνος επεξεργασίας προσωπικών δεδομένων»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

«Εκτελών την εργασία»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας.

«Αποδέκτης»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, στα οποία κοινολογούνται τα δεδομένα προσωπικού χαρακτήρα.

«Τρίτος»: οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέας, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα.

«Από κοινού υπεύθυνοι επεξεργασίας»: Σε περίπτωση που δύο ή περισσότεροι υπεύθυνοι επεξεργασίας καθορίζουν από κοινού τους σκοπούς και τα μέσα της επεξεργασίας, καθίστανται από κοινού υπεύθυνοι επεξεργασίας. Τα καθήκοντα και οι ευθύνες καθενός εκ των από κοινού υπευθύνων επεξεργασίας ορίζονται με διαφανή τρόπο, με έγγραφη συμφωνία στο βαθμό που τα καθήκοντα και οι ευθύνες τους δεν καθορίζονται από τον νόμο. Συγκεκριμένα, η συμφωνία πρέπει να καθορίζει ποιος πρέπει να εκπληρώσει τις υποχρεώσεις πληροφόρησης και ενώπιον τίνος τα πρόσωπα στα οποία αναφέρονται τα δεδομένα προσωπικού χαρακτήρα μπορούν να ασκήσουν τα δικαιώματά τους.

«Συγκατάθεση του υποκειμένου»: κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν κατόπιν προηγούμενης σαφούς ενημέρωσης.

«Παραβίαση δεδομένων προσωπικού χαρακτήρα»: νοείται η παραβίαση της ασφάλειας που οδηγεί στην τυχαία ή κακόβουλη καταστροφή, απώλεια, αλλαγή, τη μη εξουσιοδοτημένη αποκάλυψη ή πρόσβαση στα μεταφερθέντα, αποθηκευμένα ή άλλως επεξεργασμένα δεδομένα προσωπικού χαρακτήρα.

5. ΑΡΧΕΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Το Ίδρυμα, κατά τη συλλογή των προσωπικών δεδομένων σε οποιαδήποτε μορφή (έντυπη ή ηλεκτρονική) τηρεί τις ακόλουθες αρχές, που τίθενται από τον ΓΚΠΔ:

α) Τα δεδομένα προσωπικού χαρακτήρα συλλέγονται κατά τρόπο θεμιτό, νόμιμο και διαφανή, (**«αρχή νομιμότητας, αντικειμενικότητας και διαφάνειας»**) για καθορισμένους, σαφείς και νόμιμους σκοπούς και υφίστανται νόμιμη επεξεργασία βάσει των σκοπών αυτών και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς. (**«αρχή περιορισμού του σκοπού»**)

β) Τα δεδομένα που συλλέγονται είναι κατάλληλα, συναφή, πρόσφορα και όχι περισσότερα των όσων απαιτούνται για τον εκάστοτε συγκεκριμένο σκοπό επεξεργασίας. (**« αρχή ελαχιστοποίησης των δεδομένων»**)

γ) Τα δεδομένα είναι ακριβή και, εφόσον απαιτείται, να υποβάλλονται σε ενημέρωση. (**«αρχή ακρίβειας»**)

δ) Τα δεδομένα διατηρούνται σε μορφή που επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια της περιόδου που απαιτείται για την πραγματοποίηση των σκοπών της συλλογής και της επεξεργασίας τους. (**«αρχή περιορισμού της περιόδου αποθήκευσης»**)

ε) Τα δεδομένα υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων. (**«αρχή ακεραιότητας και εμπιστευτικότητας»**)

6. ΣΚΟΠΟΙ ΕΠΕΞΕΡΓΑΣΙΑΣ

Το Ίδρυμα τηρεί αρχείο και προβαίνει σε επεξεργασία δεδομένων προσωπικού χαρακτήρα για την εξυπηρέτηση των δραστηριοτήτων του και των καταστατικών σκοπών του.

Ειδικά όσον αφορά προσωπικά δεδομένα των ωφελουμένων αυτά συλλέγονται και υπόκεινται σε επεξεργασία για το σκοπό της παροχής ιατροφαρμακευτικής και νοσηλευτικής περίθαλψης στους ωφελούμενους, για συμμόρφωση του Ιδρύματος με έννομη υποχρέωση, για κατάρτιση και εκτέλεση σύμβασης ή και για εκπλήρωση εννόμων συμφερόντων του Ιδρύματος. Επίσης, αναφορικά με τα προσωπικά δεδομένα των εργαζόμενων του Ιδρύματος αυτά συλλέγονται για το σκοπό κατάρτισης σύμβασης εργασίας και εκτέλεσης των όρων της, για συμμόρφωση του Ιδρύματος με έννομη υποχρέωση καθώς και για εκπλήρωση εννόμων συμφερόντων του Ιδρύματος. Αναφορικά με τα δεδομένα προσωπικού χαρακτήρα τρίτων υπόκεινται σε επεξεργασία για σκοπούς κατάρτισης σύμβασης, ή για εξυπηρέτηση εννόμων συμφερόντων του Ιδρύματος.

7. ΚΑΤΗΓΟΡΙΕΣ ΥΠΟΚΕΙΜΕΝΩΝ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Για την εκπλήρωση των ανωτέρω σκοπών, το Ίδρυμα τηρεί αρχείο και προβαίνει σε επεξεργασία προσωπικών δεδομένων των παρακάτω προσώπων:

- Ωφελουμένων και υποψήφιων ωφελουμένων του Ιδρύματος
- Συγγενικών προσώπων, δικαστικών συμπαραστατών, κηδεμόνων των ωφελουμένων, τρίτων επισκεπτών
- Προσωπικού εν γένει (ανεξαρτήτως της μορφής της εργασιακής τους σύμβασης), περιλαμβανομένων και των υποψήφιων προς εργασία και των τώως εργαζομένων
- Εξωτερικών συνεργατών, προμηθευτών

8. ΚΑΤΗΓΟΡΙΕΣ ΔΕΔΟΜΕΝΩΝ

Το Ίδρυμα προβαίνει στη συλλογή και επεξεργασία των απαραίτητων για την εκπλήρωση των ανωτέρω σκοπών επεξεργασίας προσωπικών δεδομένων των παραπάνω υποκειμένων, για την εκπλήρωση των έννομων και συμβατικών υποχρεώσεών του.

Το Ίδρυμα προβαίνει σε τήρηση αρχείου και επεξεργασία των προσωπικών δεδομένων των εργαζομένων που είναι απαραίτητα για την ορθή λειτουργία της εργασιακής σχέσης και την εκπλήρωση των υποχρεώσεων που πηγάζουν από στην ισχύουσα εργατική και κοινωνικοασφαλιστική νομοθεσία.

Ενδεικτικά, τα δεδομένα που επεξεργάζεται το Ίδρυμα εντάσσονται στις ακόλουθες κατηγορίες:

- **Δεδομένα Ταυτοποίησης:** ονοματεπώνυμο, αριθμός δελτίου ταυτότητας, ημερομηνία γέννησης, χώρα, ΑΦΜ, ΑΜΚΑ, ΑΜΑ
- **Δεδομένα Επικοινωνίας:** σταθερό τηλέφωνο, κινητό τηλέφωνο, ηλεκτρονική διεύθυνση (email), ταχυδρομική διεύθυνση
- **Δεδομένα υγείας ωφελουμένων** όπως πιστοποιητικό νοσηλείας, ιατρικές γνωματεύσεις, εξετάσεις, φαρμακευτική αγωγή κ.ά. ή όταν η επεξεργασία είναι απαραίτητη για την εκπλήρωση των υποχρεώσεων που απορρέουν από το εργατικό δικαιο ή το δικαιο κοινωνικής ασφάλισης κ.ά.
- **Οικονομικά Δεδομένα:** μισθοί εργαζομένων, αμοιβές συνεργατών, αριθμοί τραπεζικών λογαριασμών, εκκαθαριστικά σημειώματα
- **Δεδομένα για την οικογενειακή κατάσταση** εργαζομένων και ωφελούμενων
- Δεδομένα εργασιακής κατάστασης, εργασιακής εμπειρίας και εκπαίδευσης των εργαζομένων (βιογραφικά κ.λπ.)

Το Ίδρυμα επεξεργάζεται δεδομένα που αφορούν **ποινικές διώξεις, μέτρα ασφαλείας και καταδικές**, όταν αυτό προβλέπεται από το νόμο

9. ΕΝΗΜΕΡΩΣΗ ΥΠΟΚΕΙΜΕΝΩΝ

Το Ίδρυμα διασφαλίζει ότι τα υποκείμενα στα οποία αναφέρονται τα δεδομένα έχουν στη διάθεσή τους επαρκείς πληροφορίες σχετικά με την επεξεργασία και χρήση των δεδομένων τους από το Ίδρυμα και δίδουν τη συναίνεσή τους, όταν αυτό απαιτείται.

Στην περίπτωση που τα δεδομένα λαμβάνονται από το ίδιο το υποκείμενο και όχι από τρίτους, παρέχεται σε αυτό κατά τη στιγμή της συλλογής των δεδομένων κατάλληλη δήλωση ενημέρωσης, στην οποία συμπεριλαμβάνονται εύλογες πληροφορίες σχετικά με την επεξεργασία των δεδομένων σύμφωνα με το άρθρο 13 του ΓΚΠΔ.

Σε περίπτωση που τα δεδομένα λαμβάνονται από τρίτους, το Ίδρυμα ενημερώνει τα υποκείμενα, το αργότερο εντός ενός (1) μήνα από τη συλλογή, ή, εάν τα δεδομένα πρόκειται να χρησιμοποιηθούν για επικοινωνία με το υποκείμενο των δεδομένων, το αργότερο κατά τη διάρκεια της πρώτης επικοινωνίας με αυτό, ή, εάν προβλέπεται γνωστοποίηση σε άλλο αποδέκτη, το αργότερο όταν τα δεδομένα γνωστοποιούνται για πρώτη φορά.

10. ΣΤΟΙΧΕΙΑ ΠΟΥ ΠΕΡΙΛΑΜΒΑΝΟΝΤΑΙ ΣΤΗ ΔΗΛΩΣΗ ΕΝΗΜΕΡΩΣΗΣ

Οι ακόλουθες πληροφορίες περιλαμβάνονται στη δήλωση ενημέρωσης υποκειμένου προκειμένου να διασφαλιστεί η δίκαιη και διαφανής επεξεργασία των προσωπικών του δεδομένων:

- η ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας,
- τα στοιχεία επικοινωνίας του Υπεύθυνου Προστασίας Δεδομένων,
- οι σκοποί επεξεργασίας για τους οποίους προορίζονται τα δεδομένα προσωπικού χαρακτήρα,
- οι σχετικές κατηγορίες προσωπικών δεδομένων,
- η νομική βάση για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα,
- η ύπαρξη του δικαιώματος του υποκειμένου να ανακαλέσει τη συγκατάθεσή του, εφόσον η επεξεργασία των δεδομένων του βασίζεται σε αυτή,
- οι αποδέκτες ή οι κατηγορίες αποδεκτών των προσωπικών δεδομένων, εάν υπάρχουν,
- η χρονική περίοδος για την οποία τυγχάνουν επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα, καθώς και το χρονικό διάστημα κατά το οποίο θα αποθηκευτούν,
- το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή καθώς και επαρκείς πληροφορίες για τα δικαιώματα των υποκειμένων και τον τρόπο άσκησης των δικαιωμάτων τους σύμφωνα με τις διατάξεις του ΓΚΠΔ,

- η ύπαρξη δικαιώματος υποβολής αιτήματος στον Υπεύθυνο Επεξεργασίας για πρόσβαση, διόρθωση ή διαγραφή των δεδομένων προσωπικού χαρακτήρα, περιορισμό της επεξεργασίας τους, αντίταξη στην επεξεργασία τους, καθώς και για τη φορητότητά τους, και
- πληροφορίες σχετικά με την ύπαρξη ή μη αυτοματοποιημένης λήψης αποφάσεων,
- η πηγή από την οποία αντλούνται τα δεδομένα προσωπικού χαρακτήρα στην περίπτωση που αυτά δεν συλλέγονται από το υποκείμενο των δεδομένων.

11. ΝΟΜΙΜΕΣ ΒΑΣΕΙΣ ΕΠΕΞΕΡΓΑΣΙΑΣ

Η επεξεργασία των ανωτέρω δεδομένων προσωπικού χαρακτήρα είναι απαραίτητη για την εκπλήρωση των προαναφερθέντων σκοπών. Εκτός αν ορίζεται διαφορετικά κατά τη συλλογή των δεδομένων προσωπικού χαρακτήρα, η νομική βάση για την επεξεργασία τους είναι μία από τις ακόλουθες:

- έχει δοθεί η ρητή **συγκατάθεση** του υποκειμένου για την επεξεργασία δεδομένων προσωπικού χαρακτήρα (Άρθρο 6 (1) (α), 7, 8 του ΓΚΠΔ π.χ. άνοιγμα τραπεζικού λογαριασμού και 9 (2) (α) του ΓΚΠΔ, όταν αφορά δεδομένα ειδικών κατηγοριών π.χ. λήψη φωτογραφιών κ.ά.),
- η επεξεργασία είναι απαραίτητη για την **εκτέλεση συμβατικής σχέσης** (Άρθρο 6 (1) (β) του ΓΚΠΔ),
- η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με **έννομη υποχρέωση** του υπευθύνου επεξεργασίας (Άρθρο 6 (1) (γ) του ΓΚΠΔ),
- η επεξεργασία είναι απαραίτητη για τη **διαφύλαξη ζωτικού συμφέροντος** του υποκειμένου των δεδομένων (Άρθρο 6 (1) (δ) του ΓΚΠΔ),
- η επεξεργασία είναι απαραίτητη για τους σκοπούς των **έννομων συμφερόντων** που επιδιώκει το Ίδρυμα (Άρθρο 6 (1) (στ) του ΓΚΠΔ),
- η επεξεργασία δεδομένων ειδικών κατηγοριών των εργαζομένων είναι σε ορισμένες περιπτώσεις (π.χ. αναρρωτικές άδειες) απαραίτητη για την εκτέλεση των υποχρεώσεων του Ιδρύματος στον τομέα του **εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης** (Άρθρο 9 (2) (β) του ΓΚΠΔ),
- η επεξεργασία δεδομένων ειδικών κατηγοριών των ωφελούμενων είναι απαραίτητη για την **προστασία των ζωτικών συμφερόντων** του υποκειμένου των δεδομένων, εάν το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να συγκατατεθεί (Άρθρο 9 (2) (γ) του ΓΚΠΔ) και για σκοπούς **προληπτικής ή επαγγελματικής ιατρικής, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών** (Άρθρο 9 (2) (η) του ΓΚΠΔ),

- η επεξεργασία δεδομένων ειδικών κατηγοριών είναι απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη **νομικών αξιώσεων** του υπευθύνου επεξεργασίας (Άρθρο 9 (2) (η) του ΓΚΠΔ)

12. ΣΥΓΚΑΤΑΘΕΣΗ ΥΠΟΚΕΙΜΕΝΟΥ

Στην περίπτωση που απαιτείται συγκατάθεση του υποκειμένου, το Ίδρυμα μεριμνά προκειμένου να λαμβάνει τη συναίνεσή του κατά τη στιγμή της συλλογής των δεδομένων και πριν από οποιαδήποτε επεξεργασία τους. Σε περίπτωση που προκύψει νέος σκοπός επεξεργασίας για τα εν λόγω δεδομένα, το Ίδρυμα οφείλει να λαμβάνει εκ νέου συγκατάθεση από το υποκείμενο των δεδομένων.

Το Ίδρυμα διασφαλίζει ότι:

- η συγκατάθεση ζητείται με τρόπο εύκολα προσβάσιμο και κατανοητό, διατυπωμένη σε σαφή και απλή γλώσσα,
- η συγκατάθεση υποβάλλεται κατά τρόπο σαφώς διακριτό από άλλα θέματα στα οποία το υποκείμενο επίσης ενδεχομένως συναινεί,
- η συγκατάθεση παρέχεται ελεύθερα, ρητά και με καταφατικό τρόπο από το υποκείμενο των δεδομένων,
- ο τύπος δια του οποίου ζητείται η συγκατάθεση δεν είναι προεπιλεγμένος / προσυμπληρωμένος,
- η συγκατάθεση παρέχεται για συγκεκριμένους σκοπούς συλλογής και επεξεργασίας δεδομένων προσωπικού χαρακτήρα,
- όπου η συγκατάθεση παρέχεται από το υποκείμενο με ηλεκτρονικά ή άλλως αυτοματοποιημένα μέσα, αποθηκεύεται αυτόματα σε ασφαλές περιβάλλον,
- η λήψη ή η ανάκληση συγκατάθεσης αποθηκεύεται και συνοδεύεται από τις παρακάτω πληροφορίες: όνομα υποκειμένου, ημερομηνία και τρόπος δήλωσης/ανάκλησης συγκατάθεσης, η δήλωση συγκατάθεσης που κοινολογήθηκε στο υποκείμενο,
- τα υποκείμενα ενημερώνονται ότι μπορούν να τροποποιήσουν ή να αποσύρουν τη συναίνεσή τους ανά πάσα στιγμή, χωρίς, ωστόσο, να θίγεται η επεξεργασία που έχει γίνει πριν την ανάκληση της συγκατάθεσης,
- η ανάκληση της συγκατάθεσης είναι στην πράξη εξίσου εύκολη με την παροχή της,
- τα κατάλληλα οργανωτικά και τεχνικά μέτρα έχουν υλοποιηθεί ώστε να επιτρέπεται η παύση της επεξεργασίας των προσωπικών δεδομένων σε περίπτωση ανάκλησης της συγκατάθεσης, και
- τα αποδεικτικά δήλωσης/ανάκλησης συγκατάθεσης είναι εύκολα προσβάσιμα.

13. ΑΠΟΔΕΚΤΕΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Αποδέκτες των προσωπικών δεδομένων που επεξεργάζεται το Ίδρυμα ενδέχεται να είναι κατά περίπτωση:

- Δημόσιες αρχές.
- Δικαστικές και Εισαγγελικές Αρχές, εφόσον απαιτηθεί για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων και στο πλαίσιο που το ορίζει η νομοθεσία ή δικαστική απόφαση.
- Συνεργάτες του Ιδρύματος, οι οποίοι έχουν δεσμευτεί με τήρηση εμπιστευτικότητας και έχουν υπογράψει σχετικές συμβάσεις επεξεργασίας προσωπικών δεδομένων σύμφωνα με τις προϋποθέσεις που τίθενται από τον Γενικό Κανονισμό για την Προστασία Δεδομένων.
- Τράπεζες ή άλλα πιστωτικά ιδρύματα.

Εντός του Ιδρύματος τα δεδομένα τυγχάνουν επεξεργασίας από τους αρμόδιους και ειδικά εξουσιοδοτημένους υπαλλήλους του Ιδρύματος αποκλειστικά στο πλαίσιο των καθηκόντων και αρμοδιοτήτων τους, άλλως από αρμοδιους και ειδικά εξουσιοδοτημένους υπαλλήλους του Ασύλου Ανιάτων, το οποίο υποστηρίζει διοικητικά το Ίδρυμα Περιθάλψεως Χρονίως Πασχόντων βάσει του ισχυόντων καταστατικών τους.

14. ΔΙΚΑΙΩΜΑΤΑ ΤΩΝ ΥΠΟΚΕΙΜΕΝΩΝ

Τα δικαιώματα των υποκειμένων των δεδομένων ισχύουν και ασκούνται σύμφωνα με τις προϋποθέσεις, τους περιορισμούς και τις εξαιρέσεις που τίθενται στα άρθρα 12 - 22 του ΓΚΠΔ και των διατάξεων του ν. 4624/2019, ενδεικτικά άρθρα 29 - 35.

Τα υποκείμενα των δεδομένων έχουν τα εξής δικαιώματα αναφορικά με τα προσωπικά δεδομένα τους:

- **δικαίωμα ενημέρωσης:** Το Ίδρυμα ενημερώνει το υποκείμενο των δεδομένων για την ταυτότητα και τα στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας, τους σκοπούς της επεξεργασίας, τις νομικές βάσεις, τους αποδέκτες και παρέχει λοιπές πληροφορίες για την επεξεργασία και σύμφωνα με οριζόμενα στα άρθρα 13 και 14 του Γενικού Κανονισμού για την Προστασία Δεδομένων.
- **δικαίωμα πρόσβασης:** Το Ίδρυμα ενημερώνει το φυσικό πρόσωπο για το κατά πόσον ή όχι επεξεργάζεται προσωπικά δεδομένα που του ανήκουν (άρθρο 15 ΓΚΠΔ).
- **δικαίωμα διόρθωσης:** Το Ίδρυμα ικανοποιεί το δικαίωμα διόρθωσης των προσωπικών δεδομένων, κατόπιν αιτήματος του φυσικού προσώπου, προκειμένου να τηρείται επικαιροποιημένο το φυσικό και ηλεκτρονικό αρχείο του (άρθρο 16 ΓΚΠΔ).
- **δικαίωμα διαγραφής:** Το Ίδρυμα ικανοποιεί το δικαίωμα των φυσικών προσώπων για διαγραφή των προσωπικών τους δεδομένων, εφόσον πληρούνται οι προϋποθέσεις του άρθρου 17 του ΓΚΠΔ.

- **δικαίωμα περιορισμού της επεξεργασίας:** Το Ίδρυμα ικανοποιεί το δικαίωμα περιορισμού της επεξεργασίας, εφόσον πληρούνται οι προϋποθέσεις του άρθρου 18 του ΓΚΠΔ.
- **δικαίωμα στη φορητότητα των δεδομένων:** Το Ίδρυμα ικανοποιεί το δικαίωμα στη φορητότητα των προσωπικών δεδομένων του υποκειμένου των δεδομένων και εξυπηρετεί το αίτημα του υποκειμένου των δεδομένων για απευθείας διαβίβαση των δεδομένων προσωπικού χαρακτήρα από το Ίδρυμα σε άλλον υπεύθυνο επεξεργασίας, σε περίπτωση που αυτό είναι τεχνικά εφικτό. Το Ίδρυμα αξιολογεί τους κινδύνους που συνεπάγεται η φορητότητα και λαμβάνει μέτρα για τον μετριασμό αυτών (άρθρο 20 ΓΚΠΔ).
- **δικαίωμα εναντίωσης στην επεξεργασία των προσωπικών τους δεδομένων, περιλαμβανομένης της εναντίωσης στην αυτοματοποιημένη λήψη αποφάσεων και στην κατάρτιση προφίλ:** Το Ίδρυμα ικανοποιεί το δικαίωμα εναντίωσης του φυσικού προσώπου προς την επεξεργασία, ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάσταση του φυσικού προσώπου. Εφόσον έχει ασκηθεί το εν λόγω δικαίωμα, το Ίδρυμα δεν υποβάλλει πλέον τα εν λόγω δεδομένα σε επεξεργασία, εκτός εάν αποδείξει ότι συντρέχουν επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία, οι οποίοι υπερισχύουν των συμφερόντων και των δικαιωμάτων του φυσικού προσώπου (άρθρο 21 ΓΚΠΔ).
- **δικαίωμα άρσης της συγκατάθεσης:** όταν η επεξεργασία βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων (άρθρο 6 παρ. 1 στοιχ. α' ΓΚΠΔ ή άρθρο 9 παρ. 2 στοιχ. α' ΓΚΠΔ), το υποκείμενο έχει το δικαίωμα να ανακαλέσει τη συγκατάθεσή του. Το Ίδρυμα παρέχει στο υποκείμενο των δεδομένων το δικαίωμα να ανακαλέσει τη συγκατάθεσή του οποτεδήποτε με τρόπο το ίδιο εύκολο με την παροχή της. Η ανάκληση της συγκατάθεσης δεν θίγει τη νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση προ της ανάκλησής της.
- **δικαίωμα υποβολής καταγγελίας** στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (www.dpa.gr).

Σε περίπτωση που το υποκείμενο των δεδομένων επιθυμεί να ασκήσει οποιοδήποτε από τα ως άνω δικαιώματά του, οφείλει να υποβάλλει σχετικό έγγραφο αίτημα στον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων του Ιδρύματος στη διεύθυνση dpo@irxp.gr, στο οποίο το Ίδρυμα θα ανταποκριθεί όπως ορίζει ο νόμος.

Το Ίδρυμα θα καταβάλει κάθε δυνατή προσπάθεια να ανταποκριθεί σε κάθε σχετικό αίτημα εντός τριάντα (30) ημερών από την παραλαβή του. Ωστόσο, σε περίπτωση που λόγω πολυπλοκότητας του αιτήματος ή λόγω του όγκου των πληροφοριών δεν είναι δυνατή η ικανοποίηση του αιτήματος εντός τριάντα (30) ημερών, το Ίδρυμα θα ενημερώσει το υποκείμενο των δεδομένων μέσα στην παραπάνω προθεσμία εγγράφως για τους λόγους της καθυστέρησης και θα καταβάλει κάθε δυνατή προσπάθεια για την ικανοποίηση του αιτήματος το συντομότερο δυνατόν και σε κάθε περίπτωση εντός δύο (2) επιπλέον μηνών.

Το Ίδρυμα διατηρεί το δικαίωμα να μην ικανοποιήσει το αίτημα, στην περίπτωση που αυτό κριθεί προδήλως αβάσιμο ή υπερβολικό, ενημερώνοντάς σχετικά με τους λόγους της μη ικανοποίησης αυτού.

15. ΧΡΟΝΟΣ ΔΙΑΤΗΡΗΣΗΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Το Ίδρυμα τηρεί τα προσωπικά δεδομένα για το απολύτως απαραίτητο χρονικό διάστημα για την εκπλήρωση των ανωτέρω σκοπών επεξεργασίας ή την τήρηση των ισχυόντων νόμων ή των όρων της παρούσας Πολιτικής.

Εφόσον ανακληθεί η συγκατάθεση του υποκειμένου στη συλλογή και επεξεργασία των προσωπικών του δεδομένων, ή ζητηθεί ο περιορισμός ή διαγραφή των δεδομένων του υποκειμένου, το Ίδρυμα διαγράφει τα δεδομένα από τα ηλεκτρονικά και φυσικά του αρχεία, εκτός εάν η τήρηση αυτών καθίσταται απαραίτητη σε συμμόρφωση με νόμιμη υποχρέωσή του ή για την άσκηση, θεμελίωση ή υπεράσπιση δικαιωμάτων ή έννομων συμφερόντων του ενώπιον δικαστικών αρχών.

Όταν η επεξεργασία επιβάλλεται ως υποχρέωση από διατάξεις του ισχύοντος νομικού πλαισίου, τα προσωπικά δεδομένα αποθηκεύονται για όσο χρονικό διάστημα επιβάλλουν οι σχετικές διατάξεις.

Όταν η επεξεργασία εκτελείται με βάση τη σύμβαση, τα προσωπικά δεδομένα αποθηκεύονται για όσο χρονικό διάστημα είναι απαραίτητο για την εκτέλεση της σύμβασης και για τη θεμελίωση, άσκηση, ή/και υποστήριξη νομικών αξιώσεων με βάση τη σύμβαση.

Όταν η επεξεργασία εκτελείται για την εξυπηρέτηση κάποιου αιτήματος, το Ίδρυμα επεξεργάζεται τα δεδομένα για όσο χρονικό διάστημα χρειάζεται για να ικανοποιήσει το εκάστοτε αίτημα.

Οι χρόνοι τήρησης αναγράφονται στο Αρχείο Δραστηριοτήτων που τηρεί το Ίδρυμα και δύνανται να τροποποιούνται ανάλογα με γνώμονα την τήρηση κάποιας νομοθεσίας, ή την εκπλήρωση των εννόμων συμφερόντων του Ιδρύματος.

Όταν λήξει ο σκοπός επεξεργασίας των προσωπικών δεδομένων και εφόσον δεν υφίσταται εκ του νόμου υποχρέωση διατήρησής τους για συγκεκριμένο χρονικό διάστημα, τα αρχεία που περιέχουν προσωπικά δεδομένα (φυσικά και ηλεκτρονικά) καταστρέφονται, σύμφωνα με την Πολιτική Διατήρησης και Διαγραφής Προσωπικών Δεδομένων του Ιδρύματος.

16. ΟΡΓΑΝΩΤΙΚΑ ΚΑΙ ΤΕΧΝΙΚΑ ΜΕΤΡΑ

16.1 Το Ίδρυμα λαμβάνει όλα τα απαραίτητα τεχνολογικά κι οργανωτικά μέτρα προκειμένου να εξασφαλιστεί η προστασία των προσωπικών δεδομένων των υποκειμένων.

Το Ίδρυμα έχει λάβει τα απαραίτητα και κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια και την προστασία των προσωπικών δεδομένων των εργαζομένων του αλλά και όσων συναλλάσσονται με αυτό στο πλαίσιο παροχής υπηρεσιών οιασδήποτε φύσης, από κάθε μορφής τυχαίας ή αθέμιτης

επεξεργασίας τόσο σε φυσικό επίπεδο όσο και σε επίπεδο λογικής ασφάλειας (ενδεικτικά διαδικασίες φυσικής ασφάλειας, διαβαθμισμένης πρόσβασης, προστασία υπολογιστικών συστημάτων λογισμικού και εξοπλισμού δικτύου) στο πλαίσιο της τηρούμενης Πολιτικής Ασφάλειας του Ιδρύματος.

Ειδικά μέτρα αυξημένης προστασίας λαμβάνονται από το Ίδρυμα για την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα (πρόσβαση ειδικά εξουσιοδοτημένων υπαλλήλων κ.λπ.)

Τα εν λόγω μέτρα επανεξετάζονται και τροποποιούνται όταν κρίνεται απαραίτητο από την ίδια το Ίδρυμα ή σε συμμόρφωση με νεότερο νομικό και κανονιστικό πλαίσιο.

16.2 Η προστασία των προσωπικών δεδομένων καλύπτει και την παροχή πληροφοριών μέσω (ηλεκτρονικής και μη) αλληλογραφίας και/ή τηλεφωνικών κλήσεων. Οι εργαζόμενοι του Ιδρύματος προτού ανταποκριθούν σε αιτήματα παροχής πληροφοριών που αφορούν και/ή εμπεριέχουν προσωπικά δεδομένα, οφείλουν να λάβουν επαρκή στοιχεία για την ταυτότητα του αιτούντος την πληροφορία και τον σκοπό για τον οποίο αιτείται η γνωστοποίηση τους. Η παροχή της πληροφορίας προϋποθέτει νομιμοποίηση του αιτούντος και συγκατάθεση του υποκειμένου των δεδομένων (δηλαδή του προσώπου για το οποίο ζητείται η πληροφορία), σε περίπτωση πληρεξουσιότητας.

Οι εργαζόμενοι οφείλουν προτού προβούν στην επεξεργασία προσωπικών αυτών δεδομένων και δη διαβίβαση αυτών σε τρίτους, ή επεξεργασία για νέο σκοπό να ενημερώνουν τον καθ' ύλην αρμόδιο Υπεύθυνο και να λαμβάνεται η γνώμη του Νομικού Συμβούλου ή του Υπεύθυνου Προστασίας Δεδομένων.

17. ΕΚΤΙΜΗΣΗ ΑΝΤΙΚΤΥΠΟΥ

Το Ίδρυμα διενεργεί εκτίμηση αντικτύπου βάσει συγκεκριμένων κριτηρίων κάθε φορά που ένα είδος επεξεργασίας ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, εκτός εάν ορίζεται διαφορετικά, τηρώντας τις προϋποθέσεις και τα κριτήρια που τίθενται στο άρθρο 35 του Γενικού Κανονισμού για την Προστασία Δεδομένων και την λοιπή ισχύουσα νομοθεσία.

18. ΑΡΧΕΙΟ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ

Το Ίδρυμα τηρεί σύμφωνα με το άρθρο 30 ΓΚΠΔ, ως υπεύθυνος επεξεργασίας σε ηλεκτρονική μορφή, αρχείο δραστηριοτήτων, για τις οποίες είναι υπεύθυνο. Το αρχείο αυτό περιλαμβάνει κατ' ελάχιστον τις ακόλουθες πληροφορίες, στις περιπτώσεις που το Ίδρυμα λειτουργεί ως υπεύθυνος επεξεργασίας: α) το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά περίπτωση, του από κοινού υπευθύνου επεξεργασίας, του εκπροσώπου του

υπευθύνου επεξεργασίας και του Υπευθύνου Προστασίας Δεδομένων και τους σκοπούς της επεξεργασίας, β) περιγραφή των κατηγοριών υποκειμένων των δεδομένων και των κατηγοριών δεδομένων προσωπικού χαρακτήρα, γ) τις κατηγορίες αποδεκτών στους οποίους πρόκειται να γνωστοποιηθούν ή γνωστοποιήθηκαν τα δεδομένα προσωπικού χαρακτήρα, δ) το χρονικό διάστημα διατήρησης των διάφορων κατηγοριών δεδομένων, όπου είναι δυνατό, και ε) γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφάλειας, όπου είναι δυνατό.

19. ΣΥΝΕΡΓΑΤΕΣ - ΕΚΤΕΛΟΥΝΤΕΣ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ - ΑΠΟ ΚΟΙΝΟΥ ΥΠΕΥΘΥΝΟΙ ΕΠΕΞΕΡΓΑΣΙΑΣ

Η με οποιοδήποτε τρόπο επεξεργασία των προσωπικών δεδομένων επιτρέπεται μόνο σε εξουσιοδοτημένα από το Ίδρυμα πρόσωπα, εργαζόμενους και συνεργάτες αποκλειστικά για τους ως άνω αναφερόμενους σκοπούς, με τους οποίους υφίσταται έγγραφη συμβατική σχέση και οι οποίοι έχουν δεσμευτεί ρητά και εγγράφως να τηρούν καθήκον εχεμύθειας και να προστατεύουν τα προσωπικά δεδομένα.

Σε περίπτωση που το Ίδρυμα αναθέτει δυνάμει συμβάσεως παροχής υπηρεσιών την επεξεργασία δεδομένων **σε εκτελούντα την επεξεργασία**, η σχετική ανάθεση γίνεται υποχρεωτικά εγγράφως και προβλέπει ειδικά ότι ο εκτελών την επεξεργασία διεξάγει αυτήν μόνο κατ' εντολή του Ιδρύματος και περιέχει κατ' ελάχιστο τα όσα ορίζονται στο άρθρο 28 του Γενικού Κανονισμού για την Προστασία Δεδομένων (ΕΕ) 2016/679, όπως αυτό ισχύει στην ελληνική έννομη τάξη. Δικαίωμα πρόσβασης στα συστήματα του Ιδρύματος σε μέλη του προσωπικού του εκτελούντος την επεξεργασία εκχωρείται μόνο όταν αυτό είναι απαραίτητο για την υλοποίηση των συμβατικών υποχρεώσεων. Ο εκτελών την επεξεργασία δεν επιτρέπεται να προσλαμβάνει άλλον εκτελούντα την επεξεργασία χωρίς προηγούμενη γραπτή άδεια του Ιδρύματος, αλλά ούτε και να αναθέτει σε τρίτον την επεξεργασία.

Ο Προϊστάμενος κάθε τμήματος του Ιδρύματος οφείλει να τηρεί αρχείο όλων των εκτελούντων την επεξεργασία που χειρίζονται προσωπικά δεδομένα για λογαριασμό της μονάδας του εντός ή εκτός των εγκαταστάσεων του Ιδρύματος, καθώς και αρχείο όλων των συμβάσεων ανάθεσης τέτοιων επεξεργασιών.

Σε περίπτωση που το Ίδρυμα καθορίζει από κοινού τους σκοπούς και τα μέσα επεξεργασίας με άλλον Υπεύθυνο Επεξεργασίας, στο πλαίσιο της συνεργασίας του, υπογράφεται συμφωνία όπου καθορίζονται οι ευθύνες και ο ρόλος κάθε Υπεύθυνου Επεξεργασίας.

20. ΠΑΡΑΒΙΑΣΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Παραβίαση δεδομένων προσωπικού χαρακτήρα συνιστά ένα περιστατικό το οποίο σχετίζεται με την ακούσια ή παράνομη καταστροφή, απώλεια,

παραμετροποίηση, μη εξουσιοδοτημένη κοινολόγηση ή πρόσβαση σε δεδομένα προσωπικού χαρακτήρα που μεταφέρονται, αποθηκεύονται ή τυγχάνουν επεξεργασίας με κάποιο άλλο τρόπο από το Ίδρυμα. Το Ίδρυμα διαθέτει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την έγκαιρη αναγνώριση καθώς και την αποτελεσματική διαχείριση τέτοιων περιστατικών. Κατά την αξιολόγηση του κινδύνου, λαμβάνονται υπόψη τα ακόλουθα κριτήρια:

- το είδος της παραβίασης,
- η φύση, ευαισθησία και ο όγκος των δεδομένων προσωπικού χαρακτήρα που επηρεάζονται,
- η ευκολία αναγνώρισης του υποκειμένου των δεδομένων,
- η σοβαρότητα των συνεπειών για το υποκείμενο των δεδομένων,
- τα ειδικά χαρακτηριστικά του υποκειμένου των δεδομένων, και
- ο αριθμός των υποκειμένων που αφορούν τα δεδομένα.

21. ΜΗΤΡΩΟ ΚΑΤΑΓΡΑΦΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ ΠΑΡΑΒΙΑΣΗΣ

Όλα τα περιστατικά παραβίασης δεδομένων προσωπικού χαρακτήρα τηρούνται σε κατάλληλο αρχείο καταγραφής των περιστατικών παραβίασης. Στο αρχείο αυτό καταγράφονται όλες οι λεπτομέρειες σχετικά με το περιστατικό (ημερομηνία, ενέργειες, εμπλεκόμενα μέρη, σχέδιο δράσης κ.ά.), καθώς και λεπτομέρειες σχετικά με την αξιολόγησή του και την ενημέρωση των υποκειμένων ή/και των εποπτικών αρχών.

22. ΑΝΑΚΟΙΝΩΣΗ ΠΑΡΑΒΙΑΣΗΣ ΔΕΔΟΜΕΝΩΝ

Σε περίπτωση περιστατικού που δύναται να οδηγήσει σε απώλεια προσωπικών δεδομένων, τότε το Ίδρυμα ενημερώνει την Υπεύθυνο Προστασίας Προσωπικών Δεδομένων του Ιδρύματος, προκειμένου να γνωστοποιήσει την παραβίαση στην Αρχή Προστασίας Προσωπικών Δεδομένων εντός 72 ωρών καθώς και στο Υποκείμενο των δεδομένων, εκτός εάν η παραβίαση δεν επιφέρει κίνδυνο για τα δικαιώματα και τις ελευθερίες των Υποκειμένων. Ακολουθούνται δε οι διαδικασίες που περιγράφονται στην Πολιτική Ενημέρωσης Παραβίασης Δεδομένων.

23. ΔΙΑΒΙΒΑΣΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΕ ΤΡΙΤΕΣ ΧΩΡΕΣ

Τα Προσωπικά Δεδομένα που επεξεργάζεται το Ίδρυμα αποτελούν αντικείμενο αποθήκευσης και επεξεργασίας μόνο εντός της Ευρωπαϊκής Ένωσης.

24. ΑΥΤΟΜΑΤΟΠΟΙΗΜΕΝΗ ΛΗΨΗ ΑΠΟΦΑΣΕΩΝ – ΚΑΤΑΡΤΙΣΗ ΠΡΟΦΙΛ

Το Ίδρυμα δεν προβαίνει σε χρήση αυτοματοποιημένης λήψης αποφάσεων, ούτε προβαίνει σε κατάρτιση προφίλ, βάσει αυτοματοποιημένης επεξεργασίας δεδομένων.

25. ΡΟΛΟΙ ΚΑΙ ΑΡΜΟΔΙΟΤΗΤΕΣ

Όλοι οι εργαζόμενοι στο Ίδρυμα οφείλουν να σέβονται και να συμμορφώνονται με την Πολιτική και να εξασφαλίζουν την τήρηση των αρχών για την επεξεργασία και την προστασία των προσωπικών δεδομένων σύμφωνα με το νόμο.

α) Η διοίκηση του Ιδρύματος είναι υπεύθυνη για την συμμόρφωση του Ιδρύματος με τον Γενικό Κανονισμό για την Προστασία Δεδομένων, όπως αυτός ισχύει στην Ελλάδα. Επίσης δεσμεύεται να ενημερώνει συνεχώς και να εκπαιδεύει τους εργαζομένους αναφορικά με το νέο πνεύμα και την νοοτροπία που υιοθετεί ο Κανονισμός και να δημιουργεί τις κατάλληλες δομές, προκειμένου να διασφαλίζεται η συμμόρφωση του Ιδρύματος ως προς την προστασία των προσωπικών δεδομένων. Τέλος οφείλει να παρέχει τις αναγκαίες υποδομές, τεχνολογικές και μη, και να υιοθετεί τις κατάλληλες εσωτερικές διαδικασίες συμμόρφωσης, σύμφωνα με το άρθρο 5 της παρούσας Πολιτικής.

β) Ο Υπεύθυνος Προστασίας Δεδομένων προάγει την νέα κουλτούρα της προστασίας προσωπικών δεδομένων εντός του Ιδρύματος, ενημερώνει και συμβουλεύει το Ίδρυμα (Διοίκηση και εργαζομένους) σχετικά με τις υποχρεώσεις τους που απορρέουν από τον Κανονισμό και άλλες διατάξεις περί προστασίας δεδομένων, και ασφάλειας πληροφοριών και παρακολουθεί την υλοποίηση της συμμόρφωσης του Ιδρύματος με τον Κανονισμό και άλλες διατάξεις περί προστασίας δεδομένων, παρέχει συμβουλές για την εκτίμηση αντικτύπου, παρακολουθεί την υλοποίησή της και ανταποκρίνεται σε οιαδήποτε αιτήματα εργαζομένων και λοιπών υποκειμένων των δεδομένων ως προς τα δικαιώματά τους. Ο Υπεύθυνος Προστασίας Δεδομένων είναι το σημείο επαφής του Ιδρύματος απέναντι στις εποπτικές αρχές και τα υποκείμενα των δεδομένων.

Στοιχεία Υπευθύνου Επεξεργασίας Δεδομένων: Υπεύθυνος Επεξεργασίας Δεδομένων είναι το Ίδρυμα Περιθάλψεως Χρονίως Πασχόντων, Αγ. Ζώνης 39 Αθήνα, Τ.Κ.: 112 56, τηλέφωνο: 210-8670488, email: info@ipxp.gr

Στοιχεία Υπευθύνου Προστασίας Δεδομένων: Υπεύθυνος Προστασίας Δεδομένων είναι η κα Καλλιόπη Κρητικού, δικηγόρος, Πλατεία Ελευθερίας 5, Αθήνα, Τ.Κ.: 105 53 τηλέφωνο: 210-3245888, email: dpo@ipxp.gr

26. ΚΑΘΗΚΟΝΤΑ ΚΑΙ ΥΠΟΧΡΕΩΣΕΙΣ

7.1 Το Ίδρυμα μέσα στο πλαίσιο εφαρμογής της Πολιτικής οφείλει:

(1) να τηρεί τη διαδικασία που έχει θεσπιστεί για την αναγνώριση, αναφορά και αντιμετώπιση των περιστατικών παραβίασης της ασφάλειας των προσωπικών δεδομένων, σύμφωνα με την Πολιτική Αναφοράς και Γνωστοποίησης Περιστατικών Ασφαλείας του Ιδρύματος.

(2) να ενημερώνεται και να εφαρμόζει 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.

(3) να ενημερώνει άμεσα τον Υπεύθυνο Προστασίας Δεδομένων σχετικά με κάθε ουσιαστική μεταβολή στα στοιχεία των αρχείων του (μεταβολή που αφορά τη διεύθυνση που είναι εγκατεστημένο το αρχείο, τον κύριο εξοπλισμό που υποστηρίζει την επεξεργασία, την περιγραφή του σκοπού της επεξεργασίας των δεδομένων που περιέχονται στο αρχείο, το είδος των δεδομένων, το χρονικό διάστημα τήρησης του αρχείου, τους αποδέκτες ή κατηγορίες αποδεκτών, τις ενδεχόμενες διαβιβάσεις εκτός Ελλάδος ή εκτός Ευρωπαϊκής Ένωσης, τα βασικά χαρακτηριστικά του συστήματος και των μέτρων ασφαλείας), προκειμένου αυτή να καταχωρείται χωρίς καθυστέρηση από το Ίδρυμα στο υποχρεωτικά τηρούμενο αρχείο δραστηριοτήτων επεξεργασίας του Ιδρύματος.

7.2 Όλοι οι εργαζόμενοι του Ιδρύματος υποχρεούνται να συμμορφώνονται με τις εσωτερικές διαδικασίες και τις οδηγίες που διασφαλίζουν την προστασία των προσωπικών δεδομένων και το απόρρητο αυτών.

7.3 Η Διοίκηση του Ιδρύματος δύναται, σύμφωνα με το Καταστατικό του Ιδρύματος, να θεσπίζει διαδικασίες και να λαμβάνει μέτρα για την προστασία προσωπικών δεδομένων όλων των υποκειμένων των δεδομένων.

27. ΕΝΗΜΕΡΩΣΗ ΔΙΟΙΚΗΤΙΚΟΥ ΣΥΜΒΟΥΛΙΟΥ Η/ΚΑΙ ΤΟΥ ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Όλοι οι εργαζόμενοι υποχρεούνται να ενημερώνουν άμεσα το Διοικητικό Συμβούλιο για τυχόν περιστατικά που άπτονται θεμάτων προστασίας προσωπικών δεδομένων και δύνανται να επιφέρουν κυρώσεις ή/και αρνητικές επιπτώσεις ως προς το όνομα και τη φήμη του Ιδρύματος. Σε περίπτωση αμφιβολίας ως προς την τήρηση των διατάξεων της προστασίας προσωπικών δεδομένων, οι εργαζόμενοι οφείλουν να απευθυνθούν στον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων.

28. ΑΝΑΘΕΩΡΗΣΗ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

Η Πολιτική Προστασίας Προσωπικών Δεδομένων τέθηκε σε ισχύ μετά την έγκρισή της από το Διοικητικό Συμβούλιο του Ιδρύματος.

Η Πολιτική αναθεωρείται κάθε 5 έτη, εκτός εάν σημαντικές αλλαγές στο νομικό ή κανονιστικό πλαίσιο ή στη λειτουργία του Ιδρύματος καταστήσουν αναγκαία την αναθεώρησή της νωρίτερα.

Το Διοικητικό Συμβούλιο του Ιδρύματος είναι αρμόδιο για την αναθεώρηση της Πολιτικής και εντοπίζει τυχόν αλλαγές που οφείλουν να γίνουν λαμβάνοντας πάντα υπόψη τις εκάστοτε βέλτιστες πρακτικές και τυχόν μεταβολές του σχετικού νομικού ή κανονιστικού πλαισίου.

Κάθε σημαντική μεταβολή κοινοποιείται εγγράφως σε όλους τους εργαζομένους του Ιδρύματος.

Οι εκδόσεις της παρούσας καταγράφονται στον κατωτέρω πίνακα:

Αρ. Έκδοσης	Αρ. Αναθ.	Περιγραφή Αναθεώρησης - Αλλαγών	Ισχύει από
01	-	Αρχική έκδοση	1.12.2020
02		1η Αναθεώρηση (ΔΕ 425/2024)	26.4.2024