

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΥΓΕΙΑΣ
ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ Α Θ Η Ν Ω Ν
ΚΟΡΓΙΑΛΕΝΕΙΟ – ΜΠΕΝΑΚΕΙΟ Ε.Ε.Σ.
ΤΜΗΜΑ ΠΡΟΜΗΘΕΙΩΝ
ΑΘΑΝΑΣΑΚΗ 2
Τ.Κ.: 11526
ΤΗΛ.: 213 2068917-18
FAX : 213 2068259
e- mail: prom@0310.syzefxis.gov.gr

ΑΘΗΝΑ 18/02/2021

ΑΡ. ΠΡΩΤ. 4127

ΠΡΟΣΚΛΗΣΗ ΓΙΑ Α ΦΑΣΗ ΔΗΜΟΣΙΑΣ ΔΙΑΒΟΥΛΕΥΣΗΣ ΤΕΧΝΙΚΩΝ ΠΡΟΔΙΑΓΡΑΦΩΝ

Επειδή το Νοσοκομείο προτίθεται να διενεργήσει Διαγωνισμό για:

Κωδικός Αριθμός είδους CPV	Περιγραφή Είδους CPV
79417000-0	Υπηρεσίες παροχής συμβουλών σε θέματα ασφάλειας (Παροχή υπηρεσιών για τη διαδικασία συμμόρφωσης στο Γενικό Κανονισμό Προστασίας Δεδομένων στις οποίες θα περιλαμβάνεται και ο Υπεύθυνος Προστασίας Δεδομένων (DPO))

ΠΡΟΥΠΟΛΟΓΙΣΜΕΝΗΣ ΕΤΗΣΙΑΣ ΔΑΠΑΝΗΣ 20.000,00 € + ΦΠΑ

- 1.) Προβαίνει, με την παρούσα πρόσκληση (**Α Φάση**) σε Δημόσια Διαβούλευση των επισυναπτόμενων τεχνικών προδιαγραφών.
- 2.) Σημειώνεται ότι: Με την παρούσα πρόσκληση σε Δημόσια Διαβούλευση (**Α ΦΑΣΗ**), το Νοσοκομείο μας καταθέτει τις τεχνικές προδιαγραφές, όπως συντάχθηκαν από την Επιτροπή Σύνταξης Τεχνικών προδιαγραφών, με σκοπό την Δημόσια συζήτηση και την λήψη ενδεχομένων παρατηρήσεων – σχολίων επί του περιεχομένου αυτών, στο πλαίσιο της διαφάνειας των διαδικασιών και της ευρύτερης συμμετοχής υποψήφιων προμηθευτών/αναδόχων.
- 3.) Η διάρκεια της διαβούλευσης ορίζεται σε δεκαπέντε (15) ημερολογιακές ημέρες από την ημερομηνία ανάρτησης της στην ιστοσελίδα του Νοσοκομείου (<http://www.korgialenio-benakio.gr>), δηλαδή **μέχρι και τις 5/03/2021**.
- 4.) Οι ενδιαφερόμενοι παρακαλούνται, μετά την εγγραφή τους στο site του Νοσοκομείου, να υποβάλλουν τεκμηριωμένες παρατηρήσεις και να επισημάνουν τους όρους που ενδέχεται να θέσουν σε κίνδυνο τον διαγωνισμό και να δημιουργήσουν ενστάσεις ή ερωτήματα κατά τη χρονική περίοδο από τη δημοσίευση ως την αποσφράγιση των προσφορών.
- 5.) Το Νοσοκομείο δεν δεσμεύεται να υιοθετήσει τις προτάσεις και θα αποφασίσει για την οριστικοποίηση των τεχνικών προδιαγραφών με αντικειμενικά κριτήρια ώστε να επιτευχθεί η μέγιστη δυνατή συμμετοχή προμηθευτών/αναδόχων, εξασφαλίζοντας όμως ταυτόχρονα και την ποιότητα των παρεχομένων υπηρεσιών.

6.) Σε περίπτωση τροποποίησης των αρχικών τεχνικών προδιαγραφών ως αποτέλεσμα της διαβούλευσης θα αναρτηθούν οι αναδιαμορφωμένες Τεχνικές Προδιαγραφές για επιπλέον τέσσερις (4) ημερολογιακές ημέρες.

7.) Ευελπιστούμε για την συμμετοχή σας στην όλη διαδικασία, συνδράμοντας έτσι στην διαμόρφωση συνθηκών υγιούς ανταγωνισμού και βελτιστοποίησης των τεχνικών προδιαγραφών.

8.) Τυχόν Πληροφορίες για την πρόσκληση δίδονται όλες τις εργάσιμες ημέρες και ώρες από το τμήμα Προμηθειών.

ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ

Παροχή υπηρεσιών για τη διαδικασία συμμόρφωσης στο Γενικό Κανονισμό Προστασίας Δεδομένων (ΕΕ 679/2016) καθώς και στις διατάξεις του Ν 4624/29-08-2019 στις οποίες θα περιλαμβάνεται και ο Υπεύθυνος Προστασίας Δεδομένων (DPO) με τον αναπληρωτή του για χρονικό διάστημα ενός (1) έτους.

Η παρούσα τεχνική έκθεση αφορά:

- την ανάθεση σε Ανάδοχο της διαδικασίας συμμόρφωσης του **Γ.Ν.Α. «Κοργιαλένιου - Μπενάκειου» Ε.Ε.Σ.** στο «Γενικό Κανονισμό Προστασίας Δεδομένων» (ΓΚΠΔ - GDPR), Κανονισμός (ΕΕ) 2016/679 καθώς και του νόμου 4624/29-08-2019 (ΦΕΚ Α 137 /29-08-2019)
- Την παροχή Υπηρεσιών Υπεύθυνου Προστασίας Δεδομένων (Data Protection Officer, DPO) με τον αναπληρωτή του, στο **Γ.Ν.Α. «Κοργιαλένιο - Μπενάκειο» Ε.Ε.Σ.** για χρονικό διάστημα ενός (1) έτους.

Τα βασικά στοιχεία του Κανονισμού που έχουν εφαρμογή είναι τα εξής:

α. Δικαίωμα στη λήθη: Όταν εκλείπει ο λόγος της επεξεργασίας των δεδομένων ή το υποκείμενο αίρει τη συγκατάθεσή του (σε περίπτωση που αυτή είναι αναγκαία) ή όταν τα δεδομένα υποβλήθηκαν σε παράνομη επεξεργασία κ.τ.λ., το υποκείμενο έχει δικαίωμα να ζητήσει τη διαγραφή των δεδομένων και ο υπεύθυνος επεξεργασίας έχει υποχρέωση άμεσα να τα διαγράψει και αν τα έχει δημοσιοποιήσει να ενημερώσει και όλους όσους τα έχουν αναδημοσιεύσει ότι το υποκείμενο ζήτησε τη διαγραφή τους.

β. Σαφής συγκατάθεση: Το κάθε άτομο (ενδιαφερόμενο πρόσωπο) πρέπει να δώσει τη συγκατάθεσή του για την επεξεργασία των προσωπικών του δεδομένων.

γ. Δικαίωμα φορητότητας των δεδομένων: Το υποκείμενο (ενδιαφερόμενο πρόσωπο) έχει δικαίωμα να ζητά από τον υπεύθυνο επεξεργασίας να λαμβάνει τα δεδομένα σε κοινώς αναγνωρίσιμο μορφότυπο, καθώς και την απευθείας

διαβίβαση των δεδομένων του σε άλλον υπεύθυνο επεξεργασίας.

δ. Υποχρέωση γνωστοποίησης παραβιάσεων ασφάλειας: Όταν ο υπεύθυνος λάβει γνώση για την παραβίαση της ασφάλειας του συστήματος οφείλει να ειδοποιήσει την ανεξάρτητη Αρχή υπεύθυνη για την προστασία προσωπικών δεδομένων. Η γνωστοποίηση πρέπει να γίνεται και στο ίδιο το υποκείμενο των δεδομένων.

ε. Διασυννοριακή διαβίβαση δεδομένων: Η οδηγία περιλαμβάνει ξεκάθαρους κανόνες για τη διαβίβαση των προσωπικών δεδομένων από τις Αρχές επιβολής του νόμου σε Αρχές εκτός της ΕΕ, έτσι ώστε να μην υπονομεύεται το επίπεδο προστασίας των φυσικών προσώπων που είναι κατοχυρωμένο στην ΕΕ.

στ. Ενημέρωση για Δεδομένα Προσωπικού Χαρακτήρα: Ο υπεύθυνος επεξεργασίας πρέπει να παρέχει όλες τις εξηγήσεις για τις πολιτικές απορρήτου σε σαφή και κατανοητή γλώσσα.

ζ. Πρόστιμα από μη συμμόρφωση: Η μη συμμόρφωση με τους κανόνες προστασίας προσωπικών δεδομένων επιφέρει και πρόστιμα στις επιχειρήσεις που τον παραβιάζουν - έως 20 εκατομ. € ή 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών ("τζίρος") του προηγούμενου οικονομικού έτους (παρ. 4, 5 & 6 του άρθρου 83 του κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016).

Αρχές ως προς την ποιότητα των δεδομένων.

Ο υπεύθυνος επεξεργασίας πρέπει να επιβεβαιώνει ότι οι ακόλουθες Αρχές προστασίας δεδομένων τηρούνται:

α. Πρώτη Αρχή: Νόμιμη Επεξεργασία (Lawful Processing): Τα προσωπικά δεδομένα θα πρέπει να επεξεργάζονται με θεμιτό και νόμιμο τρόπο.

β. Δεύτερη Αρχή: Προσδιορισμός του Σκοπού (Purpose Specification): Τα προσωπικά δεδομένα θα πρέπει να λαμβάνονται μόνο για έναν ή περισσότερους συγκεκριμένους και νόμιμους σκοπούς, και δεν πρέπει να υποβάλλονται σε περαιτέρω επεξεργασία με οποιονδήποτε τρόπο ασυμβίβαστο με το σκοπό ή τους σκοπούς αυτούς.

γ. Τρίτη Αρχή: Σχετικότητα Δεδομένων (Data Relevancy): Τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι κατάλληλα, συναφή και όχι υπερβολικά σε σχέση με το σκοπό ή τους σκοπούς για τους οποίους υφίστανται επεξεργασία.

δ. Τετάρτη Αρχή: Ακρίβεια Δεδομένων (Data Accuracy): Τα προσωπικά δεδομένα πρέπει να είναι ακριβή και εφόσον χρειάζεται, να ενημερώνονται.

ε. Πέμπτη Αρχή: Περιορισμένη Διατήρηση Δεδομένων (Limited Data

Retention): Τα προσωπικά δεδομένα που έχουν επεξεργασθεί για οποιονδήποτε σκοπό ή σκοπούς δεν θα πρέπει να διατηρούνται για μεγαλύτερο χρονικό διάστημα από ό, τι είναι απαραίτητο για το σκοπό αυτό ή τους σκοπούς αυτούς.

στ. **Έκτη Αρχή:** Θεμιτή Επεξεργασία (Fair Processing): Τα προσωπικά δεδομένα θα πρέπει να υποβάλλονται σε επεξεργασία σύμφωνα με τα δικαιώματα των υποκειμένων των δεδομένων δυνάμει του παρόντος νόμου.

ζ. **Έβδομη Αρχή:** Λογοδοσία (Accountability): Θα πρέπει να ληφθούν τα κατάλληλα **διοικητικά, τεχνικά και οργανωτικά** μέτρα έναντι μη εξουσιοδοτημένης ή παράνομης επεξεργασίας δεδομένων προσωπικού χαρακτήρα και έναντι τυχαίας απώλειας ή καταστροφής ή βλάβης ή άλλης ζημίας στα προσωπικά δεδομένα που τηρούνται από την επιχείρηση.

Υπεύθυνος Προστασίας Δεδομένων: Σε κάθε δημόσιο φορέα (εκτός από τα δικαστήρια στο πλαίσιο των δικαιοδοτικών τους αρμοδιοτήτων, εάν τα κράτη επιλέξουν να τα εξαιρέσουν) και σε κάθε ιδιωτικό φορέα που λόγω της φύσης των δραστηριοτήτων τους παρακολουθούν υποκείμενα δεδομένων σε μεγάλη κλίμακα ή επεξεργάζονται ευαίσθητα δεδομένα, ορίζεται ένα πρόσωπο ως ΥΠΔ. Ο ΥΠΔ λειτουργεί ως μια **εσωτερική Αρχή Προστασίας Δεδομένων** που διασφαλίζει ότι η δημόσια υπηρεσία ή ο ιδιωτικός φορέας τηρεί τις διατάξεις του Κανονισμού και συνεργάζεται με την Εθνική Αρχή Προστασίας για την τήρηση των διατάξεων.

Εκτίμηση Επιπτώσεων Προστασίας Δεδομένων: Ο υπεύθυνος επεξεργασίας πρέπει να επιβεβαιώνει ότι εφαρμόζεται μία διαδικασία για τη διεξαγωγή μίας αξιολόγησης του κινδύνων προστασίας των δεδομένων (Data Protection Impact Assessment) σε όλες τις επιχειρησιακές μονάδες.

A. ΥΠΗΡΕΣΙΕΣ ΕΝΑΡΜΟΝΙΣΗΣ-ΣΥΜΜΟΡΦΩΣΗΣ ΤΟΥ ΝΟΣΟΚΟΜΕΙΟΥ ΜΕ ΤΟΝ Γ.Κ.Π.Δ. (G.D.P.R) (ΕΕ/2016/679) ΚΑΙ ΤΟΥ 4624/29-08-2019 (ΦΕΚ Α 137 /29-08-2019)

Για τη **διαδικασία συμμόρφωσης** του Γ.Ν.Α. «Κοργιαλένειου - Μπενάκειου» Ε.Ε.Σ στο «Γενικό Κανονισμό Προστασίας Δεδομένων» (ΓΚΠΔ - GDPR), Κανονισμός (ΕΕ) 2016/679 καθώς και του νόμου 4624/29-08-2019 (ΦΕΚ Α 137 /29-08-2019), απαιτούνται να γίνουν οι παρακάτω ενέργειες (**Πλάνο Υλοποίησης**):

A. Φάση 1η

Παρουσίαση του Κανονισμού στην Διοίκηση και τα ανώτερα στελέχη του Ιδρύματος. Θα πραγματοποιηθεί αρχική συνάντηση του Αναδόχου με τη Διοίκηση και τα ανώτερα στελέχη κατά την οποία θα γίνει αναλυτική παρουσίαση του Κανονισμού (άρθρα και απαιτήσεις) και των κύριων μέτρων συμμόρφωσης που θα πρέπει να ληφθούν από το Ίδρυμα. Θα παρουσιαστεί

Πλάνο Υλοποίησης του έργου, στο οποίο θα αποτυπώνεται λεπτομερώς η **ομάδα εργασίας** του Αναδόχου, η **μεθοδολογία** που θα ακολουθηθεί, οι **επιμέρους φάσεις**, το **χρονοδιάγραμμα** υλοποίησης και τα **παραδοτέα** που θα προκύψουν από κάθε φάση. Θα δοθούν οδηγίες σχετικά με τις πρώτες ενέργειες που θα πρέπει να γίνουν, τη σύνταξη δεσμευτικής δήλωσης της Διοίκησης, τη λήψη απόφασης στο Διοικητικό Συμβούλιο για την εφαρμογή της συμμόρφωσης κ.λ.π.

Παραδοτέα: **Π1. Πλάνο Υλοποίησης του έργου**

B. Φάση 2η

1. **Ανάλυση της τρέχουσας κατάστασης** όσον αφορά τα προσωπικά δεδομένα. Θα γίνει καταγραφή και κατηγοριοποίηση των προσωπικών δεδομένων (απλά, ευαίσθητα, ειδικού σκοπού κλπ) που κατέχει και επεξεργάζεται το Νοσοκομείο , ανά οργανική μονάδα (Διεύθυνση και Τμήμα) - (Personal Data Register). Η συλλογή των στοιχείων θα γίνει μέσω της διεξαγωγής συνεντεύξεων από στελέχη του Αναδόχου, σε στελέχη του Ιδρύματος και συμπλήρωσης κατάλληλων ερωτηματολογίων κ.λ.π.
2. Θα αναλυθεί η **τρέχουσα κατάσταση** ως προς την **προστασία** των προσωπικών δεδομένων, θα αξιολογηθούν οι **υφιστάμενες πρακτικές**, των γραπτών πολιτικών και διαδικασιών, των πληροφοριακών συστημάτων και δικτυακών υποδομών και κάθε στοιχείου που επηρεάζει την προστασία προσωπικών δεδομένων ανά οργανική μονάδα (Διεύθυνση και Τμήμα). Θα αξιολογηθεί η υφιστάμενη κατάσταση ως προς την **ασφάλεια** των πληροφοριών και την **επιχειρησιακή συνέχεια** που αποτελούν συστατικά της προστασίας των δεδομένων.
3. Η ανωτέρω αξιολόγηση θα περιλαμβάνει κατ' ελάχιστο τα ακόλουθα:
 - (1) Αξιολόγηση της **νομικής βάσης**, στην οποία στηρίζεται η συλλογή του συνόλου των συλλεγόμενων προσωπικών δεδομένων, της παρεχόμενης συναίνεσης από τον εκάστοτε συμβαλλόμενο, των παρεχόμενων πληροφοριών κ.λπ.
 - (2) Αξιολόγηση δυνατότητας ικανοποίησης των δικαιωμάτων των φυσικών προσώπων.
 - (3) Αξιολόγηση του επιπέδου ασφαλείας και επιχειρησιακής συνέχειας
 - (4) Αξιολόγηση της οργανωτικής δομής.
 - (5) Αξιολόγηση της κουλτούρας και ευαισθητοποίησης στα θέματα προστασίας προσωπικών δεδομένων.
 - (6) Αξιολόγηση πληροφορικών συστημάτων και πολιτικών που επιβάλλονται από την πληροφορική.
 - (7) Αξιολόγηση μηχανισμών ελέγχου και διασφάλισης της συμμόρφωσης

(8) Αξιολόγηση σχετικών γραπτών πολιτικών και διαδικασιών

Παραδοτέα: **Π2**. Κατάλογος **κατηγοριοποιημένων προσωπικών δεδομένων** που κατέχει και επεξεργάζεται το Ίδρυμα, ανά οργανική μονάδα (Διεύθυνση και Τμήμα) (Personal Data Register)

Γ. Φάση 3η

1. Δημιουργία **Λεπτομερών Χαρτογραφημένων Αρχείων** (Data Flow Maps). Σε συνέχεια του παραδοτέου Π2, θα δημιουργηθούν Λεπτομερή Χαρτογραφημένα Αρχεία (Data Flow Maps), ανά οργανική μονάδα (Διεύθυνση και Τμήμα), ανά κατηγορία προσωπικών δεδομένων, όπου θα απεικονίζονται όλες οι πληροφορίες σχετικά με τη διαχείριση των προσωπικών δεδομένων του Νοσοκομείου. Τα λεπτομερή αρχεία θα καλύπτουν την απαίτηση του Κανονισμού για το **Αρχείο Δραστηριοτήτων Επεξεργασίας** Δεδομένων και θα περιέχουν όλες τις επιπλέον απαραίτητες πληροφορίες, ώστε να απεικονίζεται πλήρως η τρέχουσα κατάσταση ως προς τη διαχείριση προσωπικών δεδομένων και να εντοπίζονται **κενά** ως προς τις απαιτήσεις του θεσμικού πλαισίου.
2. Εύρεση **κενών** (Gap Analysis) ως προς την ικανοποίηση των απαιτήσεων του Κανονισμού. Θα γίνει ανάλυση των κενών (**Gap Analysis**) ως προς την ικανοποίηση των απαιτήσεων του Κανονισμού, κατηγοριοποιημένα ανά θεματική περιοχή και κρισιμότητα.
3. Δημιουργία **Σχεδίου Συμμόρφωσης** (Compliance Plan). Για κάθε κενό που εντοπίζεται, θα καθορίζονται οι απαραίτητες ενέργειες αντιμετώπισης και θα δημιουργηθεί ένα λεπτομερές, ιεραρχημένο και ολοκληρωμένο Σχέδιο Συμμόρφωσης (Compliance Plan and Road Map).
4. Θα πραγματοποιηθεί **έλεγχος** σε όλες τις εμπλεκόμενες εφαρμογές λογισμικού, σε όλα τα αποθηκευτικά μέσα (ψηφιακά, έντυπα, ηχητικά κλπ), τις ιστοσελίδες του Νοσοκομείου κλπ και θα προταθούν με σαφήνεια οι **απαιτούμενες αλλαγές και τροποποιήσεις** βάσει του νέου Κανονισμού. Η αξιολόγηση θα περιλαμβάνει το σύνολο των συλλεγόμενων προσωπικών δεδομένων, της νομικής βάσης πάνω στην οποία στηρίζεται η συλλογή, της παρεχόμενης συναίνεσης από τον εκάστοτε συμβαλλόμενο, των παρεχόμενων πληροφοριών κ.λπ. Θα πραγματοποιηθεί αξιολόγηση όλων των πρακτικών που σχετίζονται με την επεξεργασία των προσωπικών δεδομένων και θα δοθούν συγκεκριμένες και λεπτομερείς προτάσεις για δράσεις συμμόρφωσης με τον νέο Κανονισμό. Όλες οι προτεινόμενες ενέργειες συμμόρφωσης θα καλύπτουν ολόκληρο τον κύκλο ζωής των προσωπικών δεδομένων (δηλ. συλλογή, καταγραφή, τροποποίηση/ενημέρωση, αποθήκευση, μεταφορά, διαγραφή/καταστροφή κ.λπ.) και θα έχουν συμφωνηθεί με την διοίκηση πριν την παράδοση του πλάνου συμμόρφωσης.

5. Παραδοτέα:

- (1) **Π3.** Λεπτομερή Χαρτογραφημένα Αρχεία (Data Flow Maps).
- (2) **Π4.** Αρχείο Δραστηριοτήτων Επεξεργασίας Δεδομένων.
- (3) **Π5.** Λίστα κενών ως προς την ικανοποίηση των απαιτήσεων του Κανονισμού.
- (4) **Π6.** Σχέδιο Συμμόρφωσης (Compliance Plan and Road Map).

Δ. Φάση 4η

1. Εκτίμηση **Αντίκτυπου Προστασίας Δεδομένων** (Data Protection Impact Assessment).
2. Ανάλυση **Επικινδυνότητας Ασφάλειας Πληροφοριών** (Information Security Risk Assessment). Θα συνταχθεί Μελέτη Ανάλυσης Επικινδυνότητας Ασφάλειας Πληροφοριών (Information Security Risk Assessment). Οι ανωτέρω αναλύσεις επικινδυνότητας και εκτίμησης επιπτώσεων θα είναι συμβατές μεταξύ τους και δεν θα περιέχουν αλληλεπικαλύψεις, κενά ή αλληλοσυγκρουόμενες πληροφορίες.
3. Δημιουργία **Εγχειριδίου Προστασίας Προσωπικών Δεδομένων**, το οποίο θα περιλαμβάνει όλες τις απαραίτητες Πολιτικές και Διαδικασίες Προστασίας Προσωπικών Δεδομένων, Ασφάλειας Πληροφοριών και Επιχειρησιακής Συνέχειας, έντυπα και ότι άλλο είναι απαραίτητο. Το Εγχειρίδιο Προστασίας Προσωπικών Δεδομένων θα καλύπτει το σύνολο των απαιτήσεων του Κανονισμού και θα λαμβάνει υπόψη τα προτεινόμενα μέτρα του πλάνου συμμόρφωσης.
4. Συγγραφή **πολιτικής ασφαλείας**. Η πολιτική Ασφαλείας (Security policy) που θα συνταχθεί θα αποτελεί έγγραφο του υπεύθυνου επεξεργασίας στο οποίο θα περιγράφονται οι στόχοι της ασφαλείας και οι αντίστοιχες διαδικασίες που πρέπει να ακολουθούνται.
5. Έλεγχος και εφαρμογή **μηχανισμού παραβιάσεων**. Θα γίνει έλεγχος υφιστάμενου ή εφαρμογή νέου μηχανισμού εντοπισμού παραβιάσεων (security Breaches) ή απλών περιστατικών ασφαλείας (security incident) με αυτόματη καταγραφή (Security log).
6. Έλεγχος των **υπαρχουσών συμβάσεων** του οργανισμού εσωτερικά και με τρίτους. Γίνεται ο έλεγχος των υπαρχουσών συμβάσεων του Νοσοκομείου, τόσο με το προσωπικό όσο και τους εξωτερικούς συνεργάτες, οι οποίοι έχουν ρόλο εκτελούντος την επεξεργασία, όσο και με τρίτους στους οποίους διαβιβάζονται δεδομένα προσωπικού χαρακτήρα. Όπου χρειάζεται, γίνεται αναμόρφωσή τους, με βάση τις

απαιτήσεις του Κανονισμού.

7. Κατάρτιση σχεδίου **διαχείρισης συμβάντων**. Το σχέδιο διαχείρισης συμβάντων είναι το έγγραφο που αναφέρεται στις διαδικασίες που θα ακολουθηθούν σε περίπτωση παραβίασης ασφαλείας.
8. Κατάρτιση Σχεδίου **Αναγγελίας Διαρροής** στην Αρχή Προστασίας Προσωπικών Δεδομένων, ώστε να είναι δυνατή η αναγγελία της διαρροής εντός 72 ωρών, όπως προβλέπεται από τον κανονισμό.
9. Παραδοτέα:
 - (1) **Π7.** Μελέτη Ανάλυσης Επικινδυνότητας Ασφάλειας Πληροφοριών (Information Security Risk Assessment).
 - (2) **Π8.** Εγχειρίδιο Προστασίας Προσωπικών Δεδομένων (Personal Data Protection Policies and Procedures).
 - (3) **Π9.** Κείμενο πολιτικής ασφάλειας.
 - (4) **Π10.** Αναφορά ελέγχου εντοπισμού παραβιάσεων ή απλών περιστατικών ασφαλείας
 - (5) **Π11.** Πλήρες κείμενο διαχείρισης συμβάντων.
 - (6) **Π12.** Σχέδιο Αναγγελίας Διαρροής.

Ε . Φάση 5η

1. **Εκπαίδευση** εργαζομένων, σε θέματα που αφορούν την τήρηση των προϋποθέσεων του κανονισμού. Δημιουργία κουλτούρας προστασίας προσωπικών δεδομένων.
2. **Επαναξιολόγηση** (Compliance Audit). Με την ολοκλήρωση του συνόλου των ενεργειών γίνεται επαναξιολόγηση του επιπέδου συμμόρφωσης του οργανισμού.
3. **Παρουσίαση** του έργου στην Διοίκηση και τα ανώτερα στελέχη του Νοσοκομείου. Θα γίνει εκπαίδευση των εργαζομένων και θα πραγματοποιηθεί **τελική συνάντηση** του Αναδόχου με τη Διοίκηση και τα ανώτερα στελέχη του Νοσοκομείου κατά την οποία θα γίνει αναλυτική παρουσίαση των εργασιών που έγιναν. Θα παρουσιαστούν τα παραδοτέα και θα δοθούν τελικές οδηγίες.
4. Παραδοτέα:

Π13. **Πρόγραμμα εκπαίδευσης** ανά οργανωτική μονάδα με ορισμένο εκπαιδευτικό πρόγραμμα υλικό και παρουσιολόγιο. Αποτελεί τμήμα της απαραίτητης για την συμμόρφωση τεκμηρίωσης.

Σύνολο Παραδοτέων

1. **Π1.** Πλάνο Υλοποίησης του έργου.
2. **Π2.** Κατάλογος κατηγοριοποιημένων προσωπικών δεδομένων που κατέχει και επεξεργάζεται το Νοσοκομείο, ανά οργανική μονάδα (Διεύθυνση και Τμήμα) (Personal Data Register).
3. **Π3.** Λεπτομερή Χαρτογραφημένα Αρχεία (Data Flow Maps).
4. **Π4.** Αρχείο Δραστηριοτήτων Επεξεργασίας Δεδομένων.
5. **Π5.** Λίστα κενών ως προς την ικανοποίηση των απαιτήσεων του Κανονισμού.
6. **Π6.** Σχέδιο Συμμόρφωσης (Compliance Plan and Road Map).
7. **Π7.** Μελέτη Ανάλυσης Επικινδυνότητας Ασφάλειας Πληροφοριών (Information Security Risk Assessment).
8. **Π8.** Εγχειρίδιο Προστασίας Προσωπικών Δεδομένων (Personal Data Protection Policies and Procedures).
9. **Π9.** Κείμενο πολιτικής ασφάλειας.
10. **Π10.** Αναφορά ελέγχου εντοπισμού παραβιάσεων ή απλών περιστατικών ασφαλείας.
11. **Π11.** Πλήρες κείμενο διαχείρισης συμβάντων.
12. **Π12.** Σχέδιο Αναγγελίας Διαρροής.
13. **Π13.** Πρόγραμμα εκπαίδευσης ανά οργανωτική μονάδα με ορισμένο εκπαιδευτικό πρόγραμμα υλικό και παρουσιολόγιο. Αποτελεί τμήμα της απαραίτητης για την συμμόρφωση τεκμηρίωσης.

Ενδεικτικό Χρονοδιάγραμμα Υλοποίησης (συνολικά 52 εβδομάδες από την υπογραφή της σύμβασης).

ΦΑΣΕΙΣ	ΕΝΕΡΓΕΙΕΣ	ΧΡΟΝΟΔΙΑΓΡΑΜΑ
1 ^η	Παρουσίαση του Κανονισμού στη Διοίκηση και τα ανώτερα στελέχη του Νοσοκομείου	2 εβδομάδες από την υπογραφή της σύμβασης

2 ^η	Ανάλυση της τρέχουσας κατάστασης όσον αφορά στα προσωπικά δεδομένα.	12 εβδομάδες από την υπογραφή της σύμβασης
3 ^η	Δημιουργία Λεπτομερών Χαρτογραφημένων Αρχείων (Data Flow Maps)	16 εβδομάδες από την υπογραφή της σύμβασης
	Εύρεση κενών (Gap Analysis)	16 εβδομάδες από την υπογραφή της σύμβασης
	Δημιουργία Σχεδίου Συμμόρφωσης (Compliance Plan)	16 εβδομάδες από την υπογραφή της σύμβασης
4 ^η	Ανάλυση Επικινδυνότητας ασφάλειας πληροφοριών (Information Security RiskAssessment)	24 εβδομάδες από την υπογραφή της σύμβασης
	Δημιουργία εγχειριδίου Προστασίας Προσωπικών Δεδομένων	24 εβδομάδες από την υπογραφή της σύμβασης
	Συγγραφή πολιτικής ασφαλείας	24 εβδομάδες από την υπογραφή της σύμβασης
	Έλεγχος και εφαρμογή μηχανισμού παραβιάσεων	24 εβδομάδες από την υπογραφή της σύμβασης
	Κατάρτιση σχεδίου διαχείρισης συμβάντων	24 εβδομάδες από την υπογραφή της σύμβασης
	Κατάρτιση Σχεδίου Αναγγελίας Διαρροής στην Αρχή Προστασίας Προσωπικών Δεδομένων	24 εβδομάδες από την υπογραφή της σύμβασης
5 ^η	Εκπαίδευση εργαζομένων, σε θέματα που αφορούν την τήρηση των προϋποθέσεων του κανονισμού. Δημιουργία κουλτούρας προστασίας προσωπικών δεδομένων.	52 εβδομάδες από την υπογραφή της σύμβασης
	Επιθεώρηση (Compliance Audit). Με την ολοκλήρωση του συνόλου των ενεργειών γίνεται επαναξιολόγηση του επιπέδου συμμόρφωσης του οργανισμού.	52 εβδομάδες από την υπογραφή της σύμβασης
	Παρουσίαση του έργου στην Διοίκηση και τα ανώτερα στελέχη του Νοσοκομείου	52 εβδομάδες από την υπογραφή της σύμβασης

Το χρονοδιάγραμμα δύναται να αναπροσαρμοστεί μετά από υπόδειξη του αναδόχου, σε καμία περίπτωση όμως η λήξη της Φάσης 4 δεν θα πρέπει να ξεπερνά τους 6 μήνες. Η συνολική διάρκεια υλοποίησης του έργου ορίζεται σε δώδεκα (12) μήνες από την ημερομηνία υπογραφής της σχετικής σύμβασης. Η

παραλαβή των υπηρεσιών θα γίνεται ανά Φάση από την **Επιτροπή παρακολούθησης, συμμόρφωσης και παραλαβής** του έργου που θα ορίσει το Νοσοκομείο. Με την παράδοση από τον Ανάδοχο του μέρους του έργου που αντιστοιχεί στη συγκεκριμένη Φάση, η Επιτροπή συντάσσει πρακτικό οριστικής παραλαβής, το οποίο επιβεβαιώνει ότι τα παραδοτέα της Φάσης αυτής πληρούν τις προδιαγραφές της σχετικής σύμβασης. Μετά την επιτυχή ολοκλήρωση του συνόλου των Φάσεων του Έργου, συντάσσεται από την Επιτροπή Παρακολούθησης το Πρακτικό Ολοκλήρωσης, το οποίο επιβεβαιώνει την οριστική παραλαβή του συνόλου του έργου.

Απαραίτητη προϋπόθεση, **επί ποινή αποκλεισμού**, για τους συμμετέχοντες είναι:

α. Η εμπειρία στην παροχή συμβουλευτικών **υπηρεσιών οργάνωσης** και ιδιαίτερα στον τομέα της ασφάλειας πληροφοριών, της επιχειρησιακής συνέχειας, της ποιότητας και της βελτιστοποίησης επιχειρησιακών διαδικασιών. Για την απόδειξη του εν λόγω κριτηρίου απαιτείται η υλοποίηση πέντε συμβάσεων σε δημόσιο ή ιδιωτικό φορέα και η **επιτυχή** ολοκλήρωσή τους.

β. Να διαθέτει αποδεδειγμένη γνώση των νομικών και τεχνικών θεμάτων των **προσωπικών δεδομένων** και σχετική προϋπηρεσία περιλαμβανομένης έργων συμμόρφωσης του κανονισμού 679/2016/ΕΕ και ιδιαίτερα στον κλάδο υπηρεσιών. Για την απόδειξη του εν λόγω κριτηρίου απαιτείται η υλοποίηση πέντε συμβάσεων σε δημόσιο ή ιδιωτικό φορέα και η **επιτυχή** ολοκλήρωσή τους.

γ. Να είναι **πιστοποιημένος** κατά ISO 27001:2013 & κατά ISO 9001:2015 ή ισοδύναμο.

δ. Να έχει υλοποιήσει **έργο GDPR** σε φορέα του Δημοσίου με πάνω από 600 άτομα προσωπικό.

ε. Η **ομάδα έργου** πρέπει να απαρτίζεται από τουλάχιστον τρία (3) άτομα με τα κάτωθι χαρακτηριστικά (αθροιστικά ως ομάδα):

(1) Ένα νομικό σύμβουλο με αποδεδειγμένη νομική εμπειρία σε θέματα **προστασίας προσωπικών δεδομένων** (με σχετική πιστοποίηση ΕΣΥΔ) και με συμμετοχή σε τρία (3) τουλάχιστον έργα GDPR σε Ν.Π.Δ.Δ. (τουλάχιστον ένα μέλος της ομάδας θα πληροί το κριτήριο).

(2) **Αποδεδειγμένη** εμπειρία (να αποδεικνύεται με σχετικές βεβαιώσεις φορέων/εργοδότη) σε θέματα **ασφάλειας πληροφοριακών συστημάτων** και πληροφοριών πέντε (5) ετών (τουλάχιστον ένα μέλος της ομάδας θα πληροί το κριτήριο).

(3) Συμμετοχή σε τουλάχιστον τρία (3) έργα GDPR σε φορείς με άνω των 200 ατόμων προσωπικό.

(4) Ο **Υπεύθυνος Έργου** (ΥΕ) πρέπει να έχει συμμετάσχει σε αντίστοιχο ρόλο σε τουλάχιστον ένα (1) έργο για την **εφαρμογή του κανονισμού 679/2016/ΕΕ** για την προστασία προσωπικών δεδομένων, και να έχει συμμετάσχει σε αντίστοιχο ρόλο σε τρία (3) τουλάχιστον έργα **υλοποίησης πολιτικών ασφάλειας** δεδομένων και επιχειρησιακής συνέχειας. Ο ΥΕ θα πρέπει να διαθέτει τουλάχιστο μεταπτυχιακό τίτλο στο αντικείμενο της ασφαλούς διακίνησης πληροφοριών, με εμπειρία στην ανάπτυξη πολιτικών ασφαλείας.

(5) Ένα ή περισσότερα άτομα από την Ομάδα έργου θα πρέπει να είναι πιστοποιημένο-α ως ISO 27001 Auditor.

(6) Ένα μέλος της Ομάδας Έργου με αποδεδειγμένη γνώση στην προστασία προσωπικών δεδομένων, να διαθέτει πιστοποιητικό DPO από αναγνωρισμένο φορέα του ΕΣΥΔ.

(7) Ένα έμπειρο στέλεχος πληροφορικής με αποδεδειγμένη γνώση στην ασφάλεια των πληροφοριών και των πληροφοριακών συστημάτων. Προς απόδειξη να διαθέτει και να καταθέσει πιστοποιητικό CCNA ή αντίστοιχο.

B. ΥΠΗΡΕΣΙΕΣ ΥΠΕΥΘΥΝΟΥ (ΜΕ ΤΟΝ ΑΝΑΠΛΗΡΩΤΗ ΤΟΥ) ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (12 ΜΗΝΕΣ)

Ο ανάδοχος θα παρέχει στο Νοσοκομείο σε όλη τη διάρκεια της διαδικασίας συμμόρφωσης του Νοσοκομείου με τον Κανονισμό, κατάλληλα καταρτισμένο (σύμφωνα με όσα προβλέπονται στον κανονισμό GDPR για τον ΥΠΔ) και πιστοποιημένο από **αναγνωρισμένο φορέα φυσικό πρόσωπο (με το αναπληρωματικό του) ως DPO**. Ο DPO θα πρέπει ως επαγγελματικά προσόντα να διαθέτει τα ακόλουθα: (α) Δίπλωμα ή πτυχίο Πανεπιστημιακής Σχολής του κλάδου της Πληροφορικής ή Πτυχίο Νομικής κατ' ελάχιστο (β) πολύ καλή γνώση της Αγγλικής Γλώσσας και (γ) εμπειρία στον τομέα των πρακτικών και των πολιτικών περί προστασίας δεδομένων με συμμετοχή σε τουλάχιστον δύο (2) παρόμοια έργα.

Ο **υπεύθυνος προστασίας δεδομένων** θα έχει τα εξής καθήκοντα:

1. Θα ενημερώνει και θα συμβουλεύει γραπτώς τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους υπαλλήλους του, σχετικά με τις υποχρεώσεις που απορρέουν από τον Γ.Κ.Π.Δ. και άλλες διατάξεις περί προστασίας δεδομένων.
2. Θα παρακολουθεί τη συμμόρφωση του Νοσοκομείου με τον Γ.Κ.Π.Δ. και με άλλες διατάξεις περί προστασίας δεδομένων και με τις πολιτικές του υπεύθυνου επεξεργασίας ή του εκτελούντα την επεξεργασία σε σχέση με την προστασία δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της πρότασης αναμόρφωσης διαδικασιών, επικαιροποίησης της χαρτογράφησης δεδομένων και ροών και της ανάθεσης αρμοδιοτήτων, της ευαισθητοποίησης και κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας και της διενέργειας των σχετικών ελέγχων.

3. Θα ενημερώνει εγγράφως, σχετικά με τη συμμόρφωση του Νοσοκομείου με τον Γ.Κ.Π.Δ., την Επιτροπή παρακολούθησης, συμμόρφωσης και παραλαβής του έργου.
4. Θα παρέχει συμβουλές για την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και θα παρακολουθεί την υλοποίησή της, σύμφωνα με το άρθρο 35 του Γ.Κ.Π.Δ.
5. Θα είναι το πρώτο σημείο επαφής για τις εποπτικές αρχές και τα υποκείμενα των δεδομένων (ασθενείς, εργαζόμενοι κτλ).
6. Θα συνεργάζεται με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.) και θα ενεργεί ως πρόσωπο επικοινωνίας με την Α.Π.Δ.Π.Χ. για τα ζητήματα που σχετίζονται με την επεξεργασία, περιλαμβανομένης της προηγούμενης διαβούλευσης που αναφέρεται στο άρθρο 36 του Γ.Κ.Π.Δ. και θα πραγματοποιεί διαβουλεύσεις, ανάλογα με την περίπτωση, για οποιοδήποτε άλλο θέμα συνδέεται με τις πράξεις επεξεργασίας, συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς επεξεργασίας.
7. Θα συνεργάζεται με τον Υπεύθυνο Προστασίας του Υπουργείου Υγείας για την ενίσχυση των δράσεων προστασίας προσωπικών δεδομένων του Υπουργείου και την εφαρμογή τους στο σύνολο των εποπτευόμενων φορέων με ομοιογενή και εύρυθμο τρόπο.
8. Θα διαδραματίζει καίριο ρόλο στην ανάπτυξη νοοτροπίας προστασίας των δεδομένων στο ανθρώπινο δυναμικό του Νοσοκομείου και θα συμβάλλει στην εφαρμογή ουσιαστών στοιχείων του ΓΚΠΔ, όπως οι αρχές της επεξεργασίας δεδομένων, τα δικαιώματα των υποκειμένων των δεδομένων, η προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού, τα αρχεία των δραστηριοτήτων επεξεργασίας, η ασφάλεια των δεδομένων προσωπικού χαρακτήρα και η γνωστοποίηση και ανακοίνωση παραβίασης δεδομένων.
9. Θα παρέχει άμεσα (εντός 24 ωρών) τη γνώμη του εγγράφως σε περίπτωση παραβίασης προσωπικών δεδομένων ή άλλου σχετικού συμβάντος.
10. Θα απαντά σε ερωτήματα του υπεύθυνου επεξεργασίας ή του εκτελούντα την επεξεργασία, του υποκειμένου των δεδομένων ή υπαλλήλων καθώς και σε καταγγελίες που αφορούν επεξεργασία προσωπικών δεδομένων εντός 5 εργάσιμων ημερών από την κοινοποίησή τους σε αυτόν.
11. Θα λογοδοτεί απευθείας στη Διοίκηση του **Γ.Ν.Α. «Κοργιαλένιο - Μπενάκειο» Ε.Ε.Σ.** και θα συμμετέχει σε συσκέψεις και κατά τη λήψη αποφάσεων ανώτερων και μεσαίων στελεχών της διοίκησης για ζητήματα που αφορούν την προστασία προσωπικών δεδομένων, καθ' όλη τη διάρκεια της σύμβασης.

12. Κατά την εκτέλεση των καθηκόντων του, δεσμεύεται από την τήρηση του απορρήτου ή της εμπιστευτικότητας σχετικά με την εκτέλεση των καθηκόντων του, σύμφωνα με το δίκαιο της Ένωσης ή της χώρας μας.
13. Θα έχει ελεύθερη πρόσβαση σε δεδομένα και πράξεις επεξεργασίας.
14. Για την παροχή των υπηρεσιών του ΥΠΔ το Νοσοκομείο θα παρέχει χώρο που θα διατεθεί για το σκοπό αυτό.
15. Θα εκπληρώνει τα καθήκοντά του με ανεξάρτητο τρόπο (δεν λαμβάνει εντολές για την άσκηση του καθηκόντων του) και δεν υφίσταται κυρώσεις επειδή επιτέλεσε τα καθήκοντά του.
16. Ο ρόλος του θα είναι συμβουλευτικός και όχι αποφασιστικός. Δε φέρει προσωπική ευθύνη για τη μη συμμόρφωση του Νοσοκομείου προς τον Γ.Κ.Π.Δ., φέρει όμως την ευθύνη καθοδήγησης του νοσοκομείου προς την απαιτούμενη συμμόρφωση προς τον Γ.Κ.Π.Δ. και για τον λόγο αυτό υπόκειται σε ευθύνη αποζημίωσης προς τον οργανισμό για πρόστιμα τα οποία ενδεχομένως δεχθεί από δικές του παραλείψεις ή αμέλεια.
17. Θα δημιουργήσει καταλόγους και θα τηρεί μητρώο των πράξεων επεξεργασίας (βασικό αρχείο δραστηριοτήτων) με βάση τις πληροφορίες που λαμβάνουν από τα διάφορα τμήματα του Νοσοκομείου που είναι υπεύθυνα για την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Τα εν λόγω αρχεία θα πρέπει να θεωρούνται ως ένα από τα εργαλεία που επιτρέπουν στον υπεύθυνο προστασίας δεδομένων να επιτελεί δύο από τα καθήκοντά του, ήτοι την παρακολούθηση της συμμόρφωσης, και την ενημέρωση και παροχή συμβουλών στον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία. Σε κάθε περίπτωση, τα αρχεία που επιβάλλεται να τηρούνται δυνάμει του άρθρου 30 θα πρέπει να αντιμετωπίζονται ως εργαλείο που επιτρέπει στον υπεύθυνο επεξεργασίας και την εποπτική αρχή, κατόπιν αιτήματος, να έχουν μια επισκόπηση όλων των δραστηριοτήτων επεξεργασίας δεδομένων προσωπικού χαρακτήρα που επιτελεί ένας οργανισμός. Αποτελεί επομένως προϋπόθεση συμμόρφωσης και κατά συνέπεια, αποτελεσματικό μέτρο λογοδοσίας.
18. Θα αναλάβει την ευθύνη αποκατάστασης κάθε ζημιάς, απώλειας, κόστους και δαπάνης που μπορεί να υποστεί το Νοσοκομείο σε περίπτωση που υπάρξει αποτυχία στην επισήμανση κινδύνου και στις πρακτικές οι οποίες μπορεί να οδηγήσουν σε παραβίαση των διατάξεων του Γ.Κ.Π.Δ.
19. Υποχρεούται να πραγματοποιεί 8 επισκέψεις μηνιαίως, διάρκειας έξι (6) πλήρων ωρών σε πρωινή και εργάσιμη ημέρα και χρονικό διάστημα 12 μηνών. Υποχρεούται να παρίσταται σε συναντήσεις στο νοσοκομείο όποτε κρίνεται αναγκαίο από τη Διοίκηση του Νοσοκομείου.
20. Υποχρεούται να ορίσει συγκεκριμένο αριθμό σταθερού και κινητού

τηλεφώνου καθώς και διεύθυνση ηλεκτρονικού ταχυδρομείου (email) τα οποία θα λειτουργούν απρόσκοπτα προκειμένου να απευθύνεται τα στελέχη του νοσοκομείου. Η ανταπόκριση στα ανωτέρω αιτήματα θα πρέπει να γίνεται το αργότερο εντός 24 ωρών.

21. Υποχρεούται να ενημερώνεται διαρκώς για τις εξελίξεις στη νομοθεσία που αφορούν στο αντικείμενο απασχόλησής του.

Απαραίτητα τόσο για τις υπηρεσίες Εναρμόνισης-Συμμόρφωσης του Νοσοκομείου με τον Γ.Κ.Π.Δ (G.D.P.R) (ΕΕ/2016/679) όσο και για τις Υπηρεσίες Υπεύθυνου Προστασίας Δεδομένων με τον Αναπληρωτή του, όλες οι προτάσεις του αναδόχου θα βασίζονται και θα λαμβάνουν υπόψη εκτός από τον Κανονισμό Γενικής Προστασίας Προσωπικών Δεδομένων (GDPR), το υφιστάμενο Ελληνικό Νομοθετικό Πλαίσιο Ν 4624/29-08-2019 (ΦΕΚ Α 137 /29-08-2019) (συμπεριλαμβανομένης της νομολογίας), τις κατευθυντήριες γραμμές για το GDPR που δημοσιεύονται από την Ομάδα Εργασίας για την Προστασία Δεδομένων του Άρθρου 29 (WP 29), τις κατευθυντήριες οδηγίες, γνωμοδοτήσεις και αποφάσεις της Ελληνικής Αρχής Προστασίας Προσωπικών Δεδομένων (καθώς και τις κατά περίπτωση κατευθυντήριες γραμμές ή αποφάσεις άλλων Ευρωπαϊκών Αρχών Προστασίας Προσωπικών Δεδομένων) και τις βέλτιστες πρακτικές σύμφωνα με τα διεθνή πρότυπα.

Η ΔΙΟΙΚΗΤΡΙΑ ΤΟΥ ΝΟΣΟΚΟΜΕΙΟΥ

ΕΛΠΙΝΙΚΗ Α. ΤΑΒΙΑΝΑΤΟΥ

ΚΟΙΝΟΠΟΙΗΣΗ

ΓΡΑΦΕΙΟ ΠΡΟΕΔΡΟΥ Δ.Σ.
ΓΡΑΦΕΙΟ ΔΙΟΙΚΗΤΡΙΑΣ
ΓΡΑΦΕΙΟ ΑΝ. ΔΙΟΙΚΗΤΗ
Δ/ΝΤΡΙΑ ΔΙΟΙΚΗΤΙΚΟΥ
ΥΠ/ΝΣΗ ΟΙΚΟΝΟΜΙΚΟΥ
ΤΜΗΜΑ ΟΙΚΟΝΟΜΙΚΟΥ
ΤΜΗΜΑ ΠΡΟΜΗΘΕΙΩΝ
Δ/ΝΤΡΙΑ ΝΟΣΗΛΕΥΤΙΚΗΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΑΧ ΚΛΙΝΙΚΗ