ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ ΥΠΗΡΕΣΙΩΝ ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (DPO)

Α. ΚΑΘΗΚΟΝΤΑ ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

1. Θα ενημερώνει και θα συμβουλεύει γραπτώς το Γ.Ν.Θ. "Γ.ΓΕΝΝΗΜΑΤΑΣ- Ο ΑΓΙΟΣ ΔΗΜΗΤΡΙΟΣ" 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 την εφαρμογή των Πολιτικών/Διαδικασιών Προστασίας Προσωπικών Δεδομένων που έχουν αναπτυχθεί για την συμμόρφωση του Φορέα με τον Κανονισμό, με φυσική παρουσία στις εγκαταστάσεις της Αναθέτουσας Αρχής όποτε αυτό κρίνεται απαραίτητο τόσο από τον ΑΝΑΔΟΧΟ, όσο και από την ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ.
3. Θα πραγματοποιήσει αξιολόγηση όλων των διαφορετικών τύπων συμβάσεων του νοσοκομείου με τρίτους, να εντοπίσει κενά και να προτείνει ενέργειες με σκοπό την προσαρμογή τους στον νέο κανονισμό
4. Θα προτείνει και θα εισηγείται προς τη Διοίκηση έγκριση για αναθεώρηση και βελτίωση στις πολιτικές / διαδικασίες / οδηγίες του συστήματος συμμόρφωσης όπου κρίνει απαραίτητο.
5. Θα προβαίνει σε εύρεση κενών ως προς την ικανοποίηση των απαιτήσεων του κανονισμού. Για κάθε κενό που εντοπίζεται, καθορισμός των απαραίτητων ενεργειών πρόληψης, αντιμετώπισης και δημιουργία ενός λεπτομερούς, προτεραιοποιημένου και ολοκληρωμένου πλάνου συμμόρφωσης
6. Θα επικαιροποιεί τις εκτιμήσεις αντικτύπου (DPIA), θα δημιουργεί καινούργιες για επεξεργασίες υψηλού ρίσκου σε μηνιαία βάση από την υπογραφή της σύμβασης και θα παρακολουθεί την υλοποίησή τους, σύμφωνα με το άρθρο 35 του Γ.Κ.Π.Δ.
7. Θα αναλαμβάνει την ενημέρωση του προσωπικού, καθώς και τις εσωτερικές επιθεωρήσεις, με σκοπό την επίτευξη του βέλτιστου επιπέδου συμμόρφωσης.
8. 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.
9. Θα είναι το πρώτο σημείο επαφής για τις εποπτικές αρχές και τα υποκείμενα των δεδομένων(ασθενείς, εργαζόμενοι κτλ)
10. 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

11. 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.
12. Θα προβαίνει ανά τακτά χρονικά διαστήματα σε ενημερώσεις στο προσωπικό των τμημάτων του νοσοκομείου, θα στέλνει ενημερωτικές επιστολές και γενικότερα θα διαδραματίζει καίριο ρόλο στην ανάπτυξη νοοτροπίας προστασίας των δεδομένων στο ανθρώπινο δυναμικό του Νοσοκομείου και θα συμβάλλει στην εφαρμογή ουσιωδών 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
13. Θα παρέχει άμεσα τη γνώμη του (εγγράφως)- εντός 24 ωρών σε περίπτωση παραβίασης προσωπικών δεδομένων ή άλλου σχετικού συμβάντος
14. Να δημιουργήσει λεπτομερές πλάνο ενεργειών αντιμετώπισης και διαχείρισης των ευρημάτων, έτσι ώστε οι επικεφαλής όλων των επιμέρους δραστηριοτήτων να είναι σε θέση να εφαρμόσουν τις απαραίτητές ενέργειες.
15. 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.
16. Θα λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο του Γ.Ν.Θ. "Γ.ΓΕΝΝΗΜΑΤΑΣ- Ο ΑΓΙΟΣ ΔΗΜΗΤΡΙΟΣ" (Διοικητικό Συμβούλιο Νοσοκομείου) 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.
17. 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 .
18. Θα έχει ελεύθερη πρόσβαση σε δεδομένα και πράξεις επεξεργασίας.
19. Για την παροχή των υπηρεσιών του ΥΠΔ το Νοσοκομείο θα παρέχει διακριτό χώρο που θα διατεθεί για το σκοπό αυτό.
20. 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.
21. Ο ρόλος του θα είναι συμβουλευτικός και όχι αποφασιστικός. Δε φέρει προσωπική ευθύνη για τη μη συμμόρφωση του Οργανισμού 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.
22. 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. Το 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. Δημιουργία λεπτομερών data flow maps ανά επιχειρησιακή μονάδα, τμήμα ή μείζονα κατηγορία προσωπικών δεδομένων, με σκοπό την επαρκή συμβατότητα με τις απαιτήσεις του GDPR, όπου θα απεικονίζονται όλες οι πληροφορίες σχετικά με τη διαχείριση των προσωπικών δεδομένων στο νοσοκομείο. Τα data flow maps θα καλύπτουν την απαίτηση του GDPR 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.

23. Υποχρεούται να πραγματοποιεί τουλάχιστον 1 επίσκεψη κάθε 15 ημέρες , διάρκειας έξι (6) πλήρων ωρών σε πρωινή και εργάσιμη ημέρα (2 μηνιαίες επισκέψεις στο νοσοκομείο έδρας "Γ.ΓΕΝΝΗΜΑΤΑΣ" και 2 μηνιαίες επισκέψεις στην οργανική μονάδα "Ο ΑΓΙΟΣ ΔΗΜΗΤΡΙΟΣ") και χρονικό διάστημα 6 μηνών . Μετά τη συμπλήρωση του 6μηνου και έως τη λήξη της σύμβασης ο ΥΠΔ υποχρεούται να παρίσταται σε συναντήσεις στο νοσοκομείο όποτε κρίνεται αναγκαίο από τη Διοίκηση του Νοσοκομείου.
24. Υποχρεούται να ορίσει συγκεκριμένο αριθμό σταθερού και κινητού τηλεφώνου ο οποίος λειτουργεί σε εργάσιμες ώρες και τουλάχιστον μεταξύ 8:00 με 17:00 προκειμένου να απευθύνεται ο εργαζόμενος που έχει οριστεί κάθε φορά με σχετική απόφαση του Οργανισμού για γνωμοδοτήσεις ή συμβουλές και διευκρινίσεις σχετικά με το αντικείμενο της Υπηρεσίας του

Β. ΠΡΟΣΟΝΤΑ ΥΠΟΨΗΦΙΟΥ

1. Στον διαγωνισμό μπορούν να συμμετέχουν φυσικά ή νομικά πρόσωπα. Εφόσον πρόκειται για νομικό πρόσωπο, αυτό θα ορίσει με την πρότασή του το φυσικό πρόσωπο εκείνου που θα αναλάβει το ρόλο του ΥΠΔ (DPO). Ο υποψήφιος μπορεί να δηλώσει ότι πλαισιώνεται από συνεργάτες φυσικά πρόσωπα.
2. Η προσφορά θα περιλαμβάνει περιγραφή της μεθοδολογίας υλοποίησης, καθώς και αναφορά στις τεχνικές και τα πρότυπα που θα χρησιμοποιηθούν για την παροχή των σχετικών υπηρεσιών.
3. Ο Ανάδοχος θα προσαρμόσει την μεθοδολογία του στις ανάγκες του Οργανισμού, διασφαλίζοντας την ελάχιστη χρονική επιβάρυνση των εργαζομένων και την απρόσκοπτη λειτουργία του Νοσοκομείου.
4. Οι ενδιαφερόμενοι υποψήφιοι (φυσικά πρόσωπα ή ο εκπρόσωπος των νομικών προσώπων άλλως/ή και το υποδεικνυόμενο από το νομικό άτομο ως DPO), θα πρέπει να συγκεντρώνουν τα παρακάτω αναφερόμενα προσόντα:

α) Επαγγελματικά προσόντα, ιδίως βάσει της εμπειρογνωσίας στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, καθώς και βάσει της ικανότητας εκπλήρωσης των καθηκόντων που αναφέρονται στο άρθρο 39 του ΓΚΠΔ.
β) Πτυχίο ΑΕΙ Νομικής Σχολής ή Σχολής Πληροφορικής ή Πτυχίο Οικονομικών Σπουδών και Διοίκησης Επιχειρήσεων ή Σχολής Μηχανικών Πληροφορικής ή αντίστοιχο τίτλο σπουδών της Αλλοδαπής αναγνωρισμένο από τον Διεπιστημονικό Οργανισμό Αναγνώρισης Τίτλων Ακαδημαϊκών και Πληροφόρησης.
γ) Άδεια Ασκήσεως Επαγγέλματος εφόσον αυτή προβλέπεται ανάλογα με την ιδιότητα του προσώπου.
δ) Πολύ καλή γνώση της Αγγλικής γλώσσας (αναγνωρισμένος τίτλος ΑΣΕΠ)
ε) Ανεπτυγμένες γνώσεις Η/Υ (αποδεικνυόμενες με: α) αναγνωρισμένο πιστοποιητικό χρήσης Η/Υ (π.χ. ECDL ή ACTA ή ισοδύναμο) β) με τίτλους σπουδών, βασικούς ή/και μεταπτυχιακούς, Πανεπιστημιακής ή/και Τεχνολογικής εκπαίδευσης, από την αναλυτική βαθμολογία των οποίων προκύπτει ότι οι υποψήφιοι έχουν παρακολουθήσει επιτυχώς τέσσερα τουλάχιστον μαθήματα, υποχρεωτικά ή κατ' επιλογή, Πληροφορικής ή γνώσης χειρισμού Η/Υ).
στ) Εμπειρία στον τομέα του Δικαίου και των πρακτικών περί προστασίας δεδομένων και
άριστη γνώση του ΓΚΠΔ
ζ) Γνώση του τομέα ηλεκτρονικής διακυβέρνησης, των τεχνολογιών πληροφορίας, των συστημάτων πληροφορικής σε θέματα υγείας και ασφάλειας των δεδομένων
η) Καλή γνώση του τομέα δραστηριότητας του Οργανισμού, των διοικητικών κανόνων και διαδικασιών απόδοσης του οργανισμού
θ) Καλή γνώση των πράξεων επεξεργασίας που διενεργούνται και των αναγκών του υπεύθυνου επεξεργασίας

<u>Οι υποψήφιοι καλούνται να προσκομίσουν:</u>

1. Πλήρες βιογραφικό σημείωμα (του υποψηφίου και όλων των τυχόν φυσικών προσώπων που απαρτίζουν την ομάδα του).
2. Ευκρινές φωτοαντίγραφο του Πτυχίου Τίτλου Σπουδών (προσόν β).
3. Ευκρινές φωτοαντίγραφο του Πτυχίου Αγγλικής Γλώσσας (προσόν δ).
4. Ευκρινές φωτοαντίγραφο της Άδειας Ασκήσεως Επαγγέλματος εφόσον αυτή προβλέπεται ανάλογα με την ιδιότητα του προσώπου (προσόν γ).
5. Ευκρινές φωτοαντίγραφο του Πιστοποιητικού Γνώσης Η/Υ (προσόν ε).
6. Στοιχεία (βεβαιώσεις, πιστοποιητικά), τα οποία θα αποδεικνύουν:

- ✓ Την εξειδικευμένη επιστημονική γνώση και εμπειρογνωσία των πρακτικών περί προστασίας και διαχείρισης δεδομένων και της ικανότητας εκπλήρωσης των καθηκόντων που προβλέπονται στον ΓΚΠΔ στο πλαίσιο συμμόρφωσης και υλοποίησης αυτού, ειδικά σε συνάρτηση με τον τομέα της παροχής υπηρεσιών υγείας.
- ✓ Τη γνώση του τομέα της Υγείας και ειδικότερα των διοικητικών κανόνων που τον διέπουν
- ✓ Τη γνώση για τα πληροφοριακά συστήματα και ειδικότερα την διαχείριση δεδομένων μέσω αυτών και την ασφάλειά τους

Εφόσον ο υποψήφιος δηλώσει ότι πλαισιώνεται από συνεργάτες φυσικά πρόσωπα θα πρέπει να αναφέρεται στην προσφορά του σαφής καταμερισμός των καθηκόντων

στους κόλπους της ομάδας του αναδόχου και να ορίζεται ένα μόνο άτομο ως επικεφαλής επικοινωνίας για κάθε οργανική μονάδα (νοσοκομείο έδρας "Γ.ΓΕΝΝΗΜΑΤΑΣ" και οργανική μονάδα "Ο ΑΓΙΟΣ ΔΗΜΗΤΡΙΟΣ").Ο υπεύθυνος προστασίας δεδομένων (DPO) που θα οριστεί θα είναι κοινός και για τις δύο οργανικές μονάδες.

Επειδή οι υπεύθυνοι προστασίας δεδομένων επιτρέπεται να επιτελούν και άλλα καθήκοντα, η ανάθεση σ΄ αυτούς άλλων καθηκόντων και υποχρεώσεων είναι δυνατή μόνο υπό την προϋπόθεση ότι δεν προκύπτουν συγκρούσεις συμφερόντων. Ο DPO δεν μπορεί να κατέχει στους κόλπους του Οργανισμού θέση από την οποία μπορεί να καθορίζει τους σκοπούς και τα μέσα επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.

Θα απορρίπτονται προσφορές που υποβάλλονται από φυσικό πρόσωπο ή νομικό πρόσωπο που θα υποδεικνύει φυσικό πρόσωπο ως DPO, το οποίο διατηρεί σχέση εργασίας με το Νοσοκομείο και μπορεί να προκύψει σύγκρουση συμφερόντων.

Προσφορές που δε συνοδεύονται από επαρκή τεκμηρίωση των προσόντων ή που καθορίζουν αμοιβή εκτός του προϋπολογισμού θα απορρίπτονται.

Σε περίπτωση που προκύψει ισοτιμία ανάμεσα σε δύο ή περισσότερους υποψηφίους θα επιλεγεί με σειρά προτεραιότητας:

- Αυτός με την μεγαλύτερη εμπειρογνωσία και την ικανότητα άσκησης καθηκόντων του άρθρου 39 του ΓΚΠΔ όπως προκύπτει από τα δικαιολογητικά που κατατέθηκαν
- Αυτός με το υψηλότερο βαθμό πτυχίου σε ΑΕΙ
- Αυτός με το υψηλότερο επίπεδο στις ξένες γλώσσες

Απαραίτητα για τις Υπηρεσίες Υπεύθυνου Προστασίας Δεδομένων, 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 (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.