Τεχνικές Προδιαγραφές για την ανάδειξη αναδόχου για την κάλυψη των αναγκών του Νοσοκομείου που αφορά σε «Υπηρεσίες Υπευθύνου Προστασίας Δεδομένων Data Protection Officer (DPO)» (CPV 79417000-0).

<u>Περιγραφή του Έργου</u>

Αντικείμενο του Έργου είναι οι υπηρεσίες Υπεύθυνου Προστασίας Δεδομένων (DPO) για ένα (1) έτος σχετικά με την προσαρμογή του Γενικού Νοσοκομείου Άρτας στις απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων.

Συγκεκριμένα ο DPO πρέπει να:

- Είναι διαθέσιμος για κάθε ζήτημα σχετικά με την επεξεργασία των δεδομένων. Η διαθεσιμότητα της δύναται να εξασφαλισθεί είτε με φυσική παρουσία στις ίδιες εγκαταστάσεις με τους υπαλλήλους, είτε μέσω ανοικτής τηλεφωνικής γραμμής ή άλλου ασφαλούς μέσου επικοινωνίας όλο το 24ωρο και όλο το χρόνο Προσωπικού Χαρακτήρα, αλλά και από τα υποκείμενα των δεδομένων

- Ενημερώνει και θα συμβουλεύει τους υπαλλήλους που επεξεργάζονται ή εμπλέκονται με οποιονδήποτε τρόπο στην διαχείριση δεδομένων προσωπικού χαρακτήρα αναφορικά με τις υποχρεώσεις τους που απορρέουν από την Ευρωπαϊκή και την Εθνική Νομοθεσία σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα

- Καθοδηγεί για την εφαρμογή των κατάλληλων μέτρων και για την απόδειξη της συμμόρφωσης, ιδίως όσον αφορά τον προσδιορισμό των κινδύνων που συνδέονται με την επεξεργασία, την εκτίμηση τους από άποψη προέλευσης, φύσης, πιθανότητας και σοβαρότητας και τον εντοπισμό των βέλτιστων πρακτικών για τον περιορισμό των κινδύνων

- Παρακολουθεί τη συμμόρφωση με τη νομοθεσία σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της πρότασης αναμόρφωσης των διαδικασιών, της επικαιροποίησης της χαρτογράφησης δεδομένων και ροών, της ανάθεσης αρμοδιοτήτων, της ευαισθητοποίησης και της κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας, και της διενέργειας σχετικών ελέγχων

- Παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντίκτυπου σχετικά με την προστασία των δεδομένων και θα παρακολουθεί την υλοποίηση της σύμφωνα με το άρθρο 35 του Κανονισμού

- Συμμετέχει, δεόντως και εγκαίρως, στη διαδικασία λήψης αποφάσεων για τα ζητήματα τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα.

- Έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα και σε πράξεις επεξεργασίας και εγκαταστάσεις σχετικών υποδομών, εφόσον κρίνεται απολύτως απαραίτητη, με σκοπό την ορθή ενάσκηση των καθηκόντων του.

- Εισηγείται και θα ελέγχει τις διατυπώσεις σε συμβάσεις, έντυπα ενημέρωσης και χορήγησης συγκατάθεσης.

- Υποστηρίζει στη Διαχείριση Αιτημάτων και Παραβιάσεων.

- Αναπτύσσει σχέδιο απόκρισης για την παραβίαση δεδομένων και προετοιμασία πρωτοκόλλου γνωστοποίησης παραβίασης στην εποπτεύουσα αρχή και σχετικής ανακοίνωσης στα υποκείμενα.

- Προτείνει τη διαμόρφωση οργανωτικών και τεχνικών μέτρων και ανάπτυξη και υλοποίηση πρότυπων έγγραφων διαδικασιών.

- Συνεργάζεται με τη Διοίκηση και τα αρμόδια στελέχη για την επικαιροποίηση Πολιτικών Ασφαλείας και Διαδικασιών.

- Παρέχει συμβουλευτικές υπηρεσίες από την έναρξη της σύμβασης όταν απαιτηθεί από το Φορέα

Δραστηριότητες του DPO

Σύμφωνα με το άρθρο 39 παράγραφος 1, τα κύρια καθήκοντα και οι δραστηριότητες που πρέπει να εκτελεστούν από τον ΥΠΔ είναι:

- ενημερώνει και να συμβουλεύει τον υπεύθυνο επεξεργασίας και τους εργαζόμενους που διεκπεραιώνουν τις υποχρεώσεις τους βάσει του GDPR και άλλων εφαρμοστέων νόμων και κανονισμών της ΕΕ,

- να παρακολουθεί τη συμμόρφωση με το GDPR κλπ., καθώς και με τις πολιτικές του υπεύθυνου επεξεργασίας όσον αφορά στην προστασία των προσωπικών δεδομένων, συμπεριλαμβανομένης της ανάθεσης ευθυνών, της ευαισθητοποίησης και της κατάρτισης του προσωπικού που εμπλέκεται στις εργασίες επεξεργασίας, καθώς και των συναφών ελέγχων

- να παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση των επιπτώσεων στην προστασία δεδομένων και να παρακολουθεί την απόδοσή της σύμφωνα με το άρθρο 35,

- να συνεργάζεται με την εποπτική αρχή και

- να ενεργεί ως σημείο επαφής της εποπτικής αρχής σε θέματα που αφορούν την επεξεργασία κ.λπ.

Κατά την εκτέλεση των καθηκόντων του, ο ΥΠΔ πρέπει «να λαμβάνει δεόντως υπόψη τον κίνδυνο που συνδέεται με τις εργασίες επεξεργασίας, λαμβανομένης υπόψη της φύσης, του πεδίου εφαρμογής, του πλαισίου και των σκοπών της επεξεργασίας» (βλ. Άρθρο 39 παράγραφος 2).

Ο ρόλος του ΥΠΔ δεν είναι επιχειρησιακός, αλλά ο έλεγχος συμμόρφωσης και η παροχή συμβουλών στον οργανισμό. Ο ρόλος πρέπει να διεξάγεται με αυτόνομο και ανεξάρτητο τρόπο. Με άλλα λόγια, ο οργανισμός δεν πρέπει να δίνει εντολή στον ΥΠΔ σχετικά με τον τρόπο εκτέλεσης του ρόλου του. Ο ΥΠΔ πρέπει να επιτρέπεται να λειτουργεί πάνω από κάθε σύγκρουση συμφερόντων που συμβαίνει στον οργανισμό, με εσωτερικούς κανόνες και διασφαλίσεις για να διευκολυνθεί αυτό. Για το λόγο αυτό, η σχετική οδηγία απαγορεύει να ορισθεί άτομο μέσα σε έναν οργανισμό που έχει ανώτερους ρόλους διαχείρισης ή που έχει λειτουργικούς ρόλους που το αναγκάζουν να καθορίσει τους σκοπούς και τα μέσα επεξεργασίας.

<u>Γενικές Προδιαγραφές</u>

Αντικείμενο εργασίας

Η παρούσα μελέτη αφορά την ανάθεση σε Ανάδοχο της υλοποίηση Έργου Συμμόρφωσης διάρκειας ενός (1) έτους σύμφωνα με τον Κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για το Γενικό Νοσοκομείο Άρτας.

Ισχύουσες διατάξεις

Η υλοποίηση της υπηρεσίας διέπεται από:

- το Ν.4412/2016 (ΦΕΚ 147/8-8-2016 τ.Α') «Δημόσιες Συμβάσεις Έργων, Προμηθειών και Υπηρεσιών (προσαρμογή στις οδηγίες 2014/24/ΕΕ και 2014/25/ΕΕ)»

- το Ν.4152/2013, υποπαρ.Ζ5 περί συναλλαγών μεταξύ επιχειρήσεων και δημοσίων Αρχών

- τις Διατάξεις του Ν.3918/2011, άρ.13 « Διαρθρωτικές αλλαγές στο σύστημα υγείας και άλλες διατάξεις»

- τις Διατάξεις του Ν.3580/2007, άρ.10 « Προμήθειες Φορέων Εποπτευόμενων από το Υπουργείο Υγείας και Κοινωνικής Αλληλεγγύης και λοιπές διατάξεις

- τις διατάξεις του Ν.3329/2005 (ΦΕΚ 81 Α'/4-4-05) «Εθνικό Σύστημα Υγείας και Αλληλεγγύης και λοιπές διατάξεις»

- Τις διατάξεις του Ν. 4013/2011 «Σύσταση Ενιαίας Ανεξάρτητης Αρχής Δημοσίων Συμβάσεων και Κεντρικού Ηλεκτρονικού Μητρώου Δημοσίων Συμβάσεων» όπως τροποποιήθηκε και ισχύει.

- Τις διατάξεις του Ν. 4250/2014 «Διοικητικές Απλουστεύσεις – Καταργήσεις, Συγχωνεύσεις Νομικών Προσώπων και Υπηρεσιών του Δημοσίου Τομέα – Τροποποίηση Διατάξεων του Π.Δ. 318/1992 (ΦΕΚ Α΄161) και λοιπές ρυθμίσεις».

- Τις διατάξεις του Π.Δ. 80/2016 «Ανάληψη υποχρεώσεων από τους Διατάκτες» (ΦΕΚ 145/Α΄/5-8-2016).

- Τις διατάξεις του Ν. 4412/2016 (ΦΕΚ 147/Α/8-8-2016) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών.

- Τις διατάξεις του Ν. 4624/2019 αναφορικά με τα καθήκοντα, τις θέσεις και τον ορισμό του Υπεύθυνου Προστασίας Δεδομένων σε Οργανισμού.

- Τις διατάξεις των άρθρων του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) 2016/679

Χρόνος εκτέλεσης υπηρεσίας

Η συνολική διάρκεια της υπηρεσίας ορίζεται για ένα (1) έτος.

Το Νοσοκομείο διατηρεί το Δικαίωμα να παρατείνει την διάρκεια της σύμβασης για ένα (1) επιπλέον έτος.

Δικαιούχοι συμμετοχής

Οι συμμετέχοντες θα πρέπει να πληρούν τις απαιτήσεις του άρθρου 37 του 2016/679 Κανονισμού **δηλώνοντας παράλληλα την ομάδα έργου** που θα παρέχει τις υπηρεσίες στο πλαίσιο συμμόρφωσης με τον νέο Κανονισμό.

Δικαιολογητικά συμμετοχής (επιπλέον)

Κατάλογο των μελών της ομάδας έργου των υποψηφίων με τις προϋποθέσεις επαγγελματικής και τεχνικής ικανότητας και εμπειρογνωσίας όπως αυτές προβλέπονται πιο κάτω.

<u>Προϋποθέσεις επαγγελματικής και τεχνικής ικανότητας και εμπειρογνωσίας</u>

Ο υποψήφιος ανάδοχος θα πρέπει:

- Να είναι πιστοποιημένος με ISO 27001:2022, ISO 90001, ISO 20000-1, ISO 37001, ISO 22301, ISO 27701
- Να έχει υλοποιήσει τουλάχιστον δύο (2) Έργα Συμμόρφωσης με το GDPR
- Να διαθέτει κατάλληλη ομάδα έργου που να καλύπτει τις προϋποθέσεις για την υλοποίηση του έργου

Συγκεκριμένα θα πρέπει να διαθέτει ομάδα με τουλάχιστον έξι (6) μέλη για την ολοκλήρωση του Έργου. Η ομάδα θα πρέπει να διαθέτει τουλάχιστον μέλη με τους εξής ρόλους και προσόντα:

Υπεύθυνος Έργου / Project Manager:

- Πανεπιστημιακό δίπλωμα ή πτυχίο σπουδών (ΑΕΙ) της ημεδαπής ή αντίστοιχου ιδρύματος της αλλοδαπής
- Εικοσαετή (20 έτη) επαγγελματική εμπειρία στην υλοποίηση ή/και διοίκηση έργων πληροφορικής.

Υπεύθυνος Νομικός Σύμβουλος: Θα πρέπει να διαθέτει τουλάχιστον τα προσόντα και την εμπειρία που αναφέρονται παρακάτω και να αποδεικνύεται επαρκώς:

- Μεταπτυχιακό Τίτλο σπουδών από την ημεδαπή ή αντίστοιχου ιδρύματος της αλλοδαπής σε αντικείμενο σχετικό με το Δίκαιο της Πληροφορικής.
- Πανεπιστημιακό Δίπλωμα (ΑΕΙ) από την ημεδαπή ή αντίστοιχο πανεπιστήμιο της αλλοδαπής
- Πιστοποίηση ISO/IEC 17024 για Υπεύθυνους Προστασίας Δεδομένων (DPO Executives)
- Πιστοποίηση Certified Information Privacy Manager (CIPM)

Υπεύθυνος Ασφάλειας Πληροφοριακών Συστημάτων. Για την επιτυχή ολοκλήρωση του Έργου είναι απαραίτητο να υπάρχει άτομο το οποίο να έχει εμπειρία από ασφάλεια των πληροφοριακών συστημάτων και ειδικότερα των δεδομένων που κυκλοφορούν στα συστήματα αυτά. Το άτομο που θα αναλάβει το ρόλο αυτό θα πρέπει να διαθέτει τουλάχιστον τα εξής προσόντα:

- Πανεπιστημιακό Δίπλωμα (ΑΕΙ) από την ημεδαπή ή αντίστοιχο πανεπιστήμιο της αλλοδαπής
- Μεταπτυχιακό Δίπλωμα (ΑΕΙ) ή/και διδακτορικό δίπλωμα από την ημεδαπή ή αντίστοιχο πανεπιστήμιο της αλλοδαπής σε αντικείμενο σχετικό με την προστασία δεδομένων σε ψηφιακά περιβάλλοντα.

Εμπιστευτικότητα – Εχεμύθεια

Με την έναρξη της υπηρεσίας ο Ανάδοχος υποχρεούται να υπογράψει Συμφωνητικό Εχεμύθειας – Εμπιστευτικότητας, σύμφωνα με το οποίο θα εγγυάται την εχεμύθεια των αποτελεσμάτων και όσων δεδομένων συλλεχθούν κατά την υλοποίηση της εργασίας. Το Συμφωνητικό θα καλύπτει όλα τα αποτελέσματα, καθώς και όλες τις πληροφορίες που θα πρέπει να ανακτηθούν κατά τη διάρκεια του έργου. Σύμφωνα με αυτό ο Ανάδοχος θα αναλαμβάνει την ευθύνη για τη διασφάλιση της εμπιστευτικότητας των εμπλεκόμενων συμβούλων, μηχανικών και τεχνικών, όσον αφορά τη μη διαρροή πληροφοριών του είδους, του βαθμού διεκπεραίωσης του έργου καθώς και τις λεπτομέρειες αυτού.

Όλες οι εκθέσεις και τα συναφή στοιχεία, όπως διαγράμματα, σχέδια, πλάνα, στατιστικά στοιχεία και κάθε άλλο σχετικό έγγραφο ή στοιχείο που αποκτάται, συγκεντρώνεται ή καταρτίζεται από τον

συμβαλλόμενο, κατά την εκτέλεση του έργου, είναι εμπιστευτικά και ανήκουν στην απόλυτη κυριότητα του Φορέα

Ο συμβαλλόμενος, χωρίς την προηγούμενη γραπτή συναίνεση του Φορέα, δεν αποκαλύπτει καμία πληροφορία που του δόθηκε, ούτε κοινοποιεί στοιχεία ή έγγραφα των οποίων έλαβε γνώση κατά την εκτέλεση των καθηκόντων του.

Σε περίπτωση αθέτησης από τον συμβαλλόμενο της ως άνω υποχρέωσης του, ο Φορέας δικαιούται να απαιτήσει: α) την αποκατάσταση κάθε ζημίας, που ενδεχομένως προκύψει, συνεπεία της κοινοποιήσεως εγγράφων - στοιχείων, πληροφοριών, σε τρίτους και β) την άμεση και στο διηνεκές παύση κοινοποίησης εγγράφων - στοιχείων, σε τρίτους, στο μέλλον.

Ο συμβαλλόμενος με κανένα τρόπο, δεν προβαίνει σε δημόσιες δηλώσεις, σχετιζόμενες με την εν γένει κατάσταση του Φορέα, χωρίς την προηγούμενη γραπτή άδεια του Φορέα.

Ο συμβαλλόμενος δεσμεύεται από την τήρηση του απόρρητου και εμπιστευτικότητας σχετικά με την άσκηση των καθηκόντων του, ευθυνόμενος και για τυχόν συναφείς παραβάσεις των μελών της ομάδας που τον συνεπικουρεί, υπογράφοντας υπεύθυνη δήλωση απορρήτου αμέσως μετά την υπογραφή της Σύμβασης.

Ενδεικτικός Προϋπολογισμός

Α/Α	**CPV**	**ΕΙΔΟΣ**	**ΠΟΣΟΤΗΤΑ**	**ΤΙΜΗ** (χωρίς ΦΠΑ)	**ΦΠΑ**	**ΣΥΝΟΛΟ**
1.	CPV 79417000-0	Υπηρεσίες Υπεύθυνου Προστασίας Δεδομένων (DPO) για το Γενικό Νοσοκομείο Άρτας	**1** (για ένα έτος)	3.000,00 €	24%	3.720,00 €