



**ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΥΓΕΙΑΣ &
ΚΟΙΝΩΝΙΚΗΣ ΑΛΛΗΛΕΓΓΥΗΣ
2η Υ. ΠΕ. ΠΕΙΡΑΙΩΣ & ΑΙΓΑΙΟΥ
ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΧΙΟΥ
«ΣΚΥΛΙΤΣΕΙΟ»**

Γραφείο Προμηθειών
Πληροφορίες: Α. Μυλωνά
Τηλ.: 22713/50258
E-mail:promithion@xioshosp.gr

**ΠΡΟΣ
ΚΑΘΕ ΕΝΔΙΑΦΕΡΟΜΕΝΟ**

ΠΡΟΣΚΛΗΣΗ 2/2025

**ΓΙΑ ΤΗΝ ΠΡΟΜΗΘΕΙΑ «ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΟΡΙΣΜΟΥ ΥΠΕΥΘΥΝΟΥ
ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (DPO)»
CPV:48311000-1, ΚΑΕ:0419**

ΠΡΟΫΠΟΛΟΓΙΣΜΟΣ 12.000,00€ ΜΕ ΦΠΑ

Με την παρούσα Πρόσκληση το Γ.Ν. Χίου «ΣΚΥΛΙΤΣΕΙΟ» ως Αναθέτουσα Αρχή, δυνάμει των άρθρ.118 και 120 του Ν.4412/16, ΠΡΟΣΚΑΛΕΙ κάθε ενδιαφερόμενο να καταθέσει την προσφορά του για την προμήθεια **«ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΟΡΙΣΜΟΥ ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (DPO)»**.

Οι Προσφορές που θα υποβληθούν θα είναι για το σύνολο της υπηρεσίας.

Το κριτήριο κατακύρωσης είναι η πλέον συμφέρουσα από οικονομική άποψη βάσει τιμής.

Ο προϋπολογισμός της προμήθειας ανέρχεται έως του ποσού των € με ΦΠΑ σύμφωνα με τον πίνακα προγραμματισμού διαχειριστικού έτους 2024, ο οποίος εγκρίθηκε με την υπ' αριθ.07/18.01.2024 Απόφαση του Δ.Σ. του Γ.Ν. Χίου «ΣΚΥΛΙΤΣΕΙΟ».

Η διάρκεια της σύμβασης ορίζεται σε ένα (1) έτος, από την ημερομηνία καταχώρησης της, στο ΚΗΜΔΗΣ ή εάν άλλως αναφέρεται στο κείμενο αυτής

Κανονιστικό πλαίσιο που διέπει την ανάθεση και εκτέλεση της προκηρυσσόμενης σύμβασης:

- τη με αριθ.50/11.10.2024 (θέμα 3ο) (ΑΔΑ:9ΒΞ4469073-2ΚΖ) Απόφαση του Δ.Σ. του Γ.Ν. Χίου «ΣΚΥΛΙΤΣΕΙΟ» που αφορά την έγκριση σκοπιμότητας της προμήθειας **«ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΟΡΙΣΜΟΥ ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (DPO)»**, την έγκριση διενέργειας διαγωνιστικής διαδικασίας με Πρόσκληση προς κάθε ενδιαφερόμενο, δυνάμει των άρθρ.118 & 120 του Ν.4412/16 και την έγκριση των τεχνικών προδιαγραφών.
- τη με αριθ.1386/20.11.2024 (ΑΔΑ:ΨΕ80469073-ΞΑΘ) Απόφαση Ανάλυσης Πίστωσης.
- τον Ν.4412/2016 «Δημόσιες Συμβάσεις Έργων, Προμηθειών και Υπηρεσιών (προσαρμογή στις Οδηγίες 2014/24/ΕΕ και 2014/25/ΕΕ)» (Α'147)
- του πδ. 80/2016 «Ανάληψη υποχρεώσεων από τους Διατάκτες» (Α'145)

- του άρθρου 11 του ν. 4013/2011 (Α' 204) «Σύσταση ενιαίας Ανεξάρτητης Αρχής Δημοσίων Συμβάσεων και Κεντρικού Ηλεκτρονικού Μητρώου Δημοσίων Συμβάσεων...»,
- της υπ' αριθμ. 76928/13.07.2021 Απόφασης των Υπουργών Ανάπτυξης και Επενδύσεων και Επικρατείας: "Ρύθμιση ειδικότερων θεμάτων λειτουργίας και διαχείρισης του Κεντρικού Ηλεκτρονικού Μητρώου Δημοσίων Συμβάσεων (ΚΗΜΔΗΣ)" (Β' 3075)
- τον Ν. 4601/2019 (Τμήμα Δεύτερο «εναρμόνιση του νομοθετικού πλαισίου με τις διατάξεις της οδηγίας 2014/55/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του συμβουλίου της 16ης Απριλίου 2014 για την έκδοση ηλεκτρονικών τιμολογίων στο πλαίσιο δημοσίων συμβάσεων (ΕΕ L 133) (Α'44) όπως τροποποιήθηκε και ισχύει.
- της υπ' αριθμ.Κ.Υ.Α.52445 ΕΞ 2023 (ΦΕΚ Β'2385/12.04.2023) «Υποχρέωση υποβολής ηλεκτρονικών τιμολογίων από τους οικονομικούς φορείς»
- της παρ. Ζ του Ν.4152/2013 «Προσαρμογή της ελληνικής νομοθεσίας στην Οδηγία 2011/7 της 16.02.2011 για την καταπολέμηση των καθυστερήσεων πληρωμών στις εμπορικές συναλλαγές» (Α'107)
- του Ν.5135/2024 «Ψηφιακό τέλος συναλλαγής και άλλες διατάξεις»

Η πρόσκληση απευθύνεται προς **κάθε ενδιαφερόμενο**, προκειμένου να υποβάλλει οικονομική προσφορά προσκομίζοντας όλα τα έγγραφα και δικαιολογητικά που απαιτούνται από την παρούσα πρόσκληση σε ηλεκτρονική μορφή, μέσω ηλεκτρονικού μηνύματος στην ηλεκτρονική διεύθυνση promithion@xioshosp.gr (Γραφείο Προμηθειών) του Γ.Ν. Χίου «ΣΚΥΛΙΤΣΕΙΟ» **μέχρι την Πέμπτη 16.01.2025 και ώρα 14:30 μμ.**, σύμφωνα με τους όρους και τις τεχνικές προδιαγραφές της παρούσας πρόσκλησης

Αναθέτουσα Αρχή	Γ. Ν. ΧΙΟΥ «ΣΚΥΛΙΤΣΕΙΟ»
Τίτλος προμήθειας/ CPV	«ΠΑΡΟΧΗ ΥΠΗΡΕΣΙΩΝ ΟΡΙΣΜΟΥ ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (DPO)» CPV: 48311000-1
Χρηματοδότηση	<ul style="list-style-type: none"> • ΚΑΕ 0419 • Ανάληψη Υποχρέωσης:1386/20.11.2024 (ΑΔΑ:ΨΕ80469073-ΞΑΘ)
Τρόπος Υποβολής Προσφορών	Σε ηλεκτρονική μορφή, μέσω ηλεκτρονικού μηνύματος στην ηλεκτρονική διεύθυνση promithion@xioshosp.gr του Γ.Ν. Χίου «ΣΚΥΛΙΤΣΕΙΟ» με την ένδειξη « ΣΥΜΜΕΤΟΧΗ ΣΕ ΔΙΑΓΩΝΙΣΤΙΚΗ ΔΙΑΔΙΚΑΣΙΑ ΓΙΑ ΤΗΝ ΠΡΟΜΗΘΕΙΑ «ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΟΡΙΣΜΟΥ ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (DPO)», ΣΧΕΤΙΚΗ ΠΡΟΣΚΛΗΣΗ 2/2025 »
Καταληκτική Ημερομηνία Υποβολής Προσφορών	Πέμπτη 16.01.2025 και ώρα 14:30 μμ.
Ημερομηνία/Τόπος Αξιολόγηση προσφοράς	Γ.Ν. ΧΙΟΥ «ΣΚΥΛΙΤΣΕΙΟ» (Γραφείο Προμηθειών) Παρασκευή 17.01.2024 και ώρα 11:30 πμ.
Δημοσιότητα	<ul style="list-style-type: none"> • ΚΗΜΔΗΣ • www.xioshosp.gr
Διάρκεια σύμβασης	ΕΝΑ (1) ΕΤΟΣ

<p>Χρόνος ισχύος προσφορών</p>	<p>Εκατόν ογδόντα (180) μέρες (άρθ.97 του 4412/16), προθεσμία που αρχίζει από την επομένη της διενέργειας του διαγωνισμού.</p> <p>Η ισχύς της προσφοράς δύναται να παραταθεί, εφόσον ζητηθεί από την αναθέτουσα αρχή πριν από την λήξη της (άρθ.97, Ν.4412/16).</p>
<p>Τεχνική και οικονομική προσφορά</p>	<p style="text-align: center;">ΤΕΧΝΙΚΗ ΠΡΟΣΦΟΡΑ</p> <p>Περιέχει ιδίως τα έγγραφα και τα δικαιολογητικά που τεκμηριώνουν την τεχνική επάρκεια, χρησιμοποιούνται για την αξιολόγηση των προσφορών, σύμφωνα με τις τεχνικές προδιαγραφές της παρούσης.</p> <p style="text-align: center;">ΟΙΚΟΝΟΜΙΚΗ ΠΡΟΣΦΟΡΑ</p> <p>Περιλαμβάνει εγγράφως τα οικονομικά στοιχεία της προσφοράς (ποσότητες, τιμή μονάδος, σύνολο καθαρής αξίας, ποσοστό ΦΠΑ, σύνολο τελικής αξίας). <u>Σημειώνεται πως η μορφοποίηση της τιμή μονάδος του κάθε είδους θα πρέπει να είναι με δύο δεκαδικά ψηφία.</u></p>
<p>Αξιολόγηση προσφορών</p>	<p>Η κατακύρωση γίνεται στον Ανάδοχο βάσει της τιμής, εφόσον η προσφορά του δεν υπερβαίνει τον προϋπολογισμό και έχει κριθεί αποδεκτή με βάση τις τεχνικές προδιαγραφές και τους όρους της παρούσης.</p>
<p>Δικαιολογητικά κατακύρωσης/ Αποδεικτικά μέσα</p>	<p>Ο «Ανάδοχος» μαζί με την οικονομοτεχνική προσφορά του, υποβάλλει και τα παρακάτω αποδεικτικά έγγραφα νομιμοποίησης, ως αποδεικτικά στοιχεία για την μη συνδρομή των λόγων αποκλεισμού, τα οποία να είναι σε ισχύ κατά τον χρόνο υποβολής τους, άλλως στην περίπτωση που δεν αναφέρεται χρόνος ισχύος, να έχουν εκδοθεί τρεις (3) μήνες πριν την υποβολής τους έκτος από: i) το πιστοποιητικό που αφορά την καταλληλότητα άσκησης επαγγελματικής δραστηριότητας από το οποίο να αποδεικνύεται η εγγραφή των οικονομικών φορέων σε ένα από τα οικεία επαγγελματικά ή εμπορικά μητρώα και ii) το πιστοποιητικό ισχύουσας εκπροσώπησης ΓΕΜΗ (για τις ΑΕ, ΕΠΕ, ΙΚΕ), για τα οποία η έκδοσή τους πρέπει να είναι (30) εργάσιμες ημέρες πριν από την υποβολή τους, προκειμένου να υπογραφεί σύμβαση.</p> <ul style="list-style-type: none"> - Αντίγραφο Ποινικού Μητρώου για Γενική Χρήση <ul style="list-style-type: none"> • στις περιπτώσεις των Α.Ε. αφορά τον Δ/ντα Σύμβουλο, καθώς και τα μέλη του Δ.Σ. της εταιρίας ή μέλους διοικητικού, διευθυντικού ή εποπτικού οργάνου που έχει εξουσία εκπροσώπησης, λήψης αποφάσεων ή ελέγχου αυτών • στις περιπτώσεις των ΕΠΕ, ΙΚΕ, ΟΕ & ΕΕ αφορά τους διαχειριστές • στις περιπτώσεις των συνεταιρισμών αφορά τα μέλη του Δ.Σ. - Βεβαίωση Φορολογικής ενημερότητας για συμμετοχή σε διαγωνισμό - Βεβαίωση ασφαλιστικής ενημερότητας για συμμετοχή σε διαγωνισμό - Πιστοποιητικό εγγραφής στο οικείο εμπορικό / επαγγελματικό μητρώο, το οποίο να έχει εκδοθεί έως τριάντα (30) εργάσιμες ημέρες πριν από την υποβολή του, εκτός αν, σύμφωνα με τις ειδικότερες διατάξεις αυτών, φέρει συγκεκριμένο χρόνο ισχύος. Για τους οικονομικούς φορείς που είναι εγκατεστημένοι στην Ελλάδα γίνεται αποδεκτό και πιστοποιητικό που εκδίδεται από την οικεία υπηρεσία του Γ.Ε.Μ.Η. των Επιμελητηρίων (Εμπορικό, Βιομηχανικό ή Βιοτεχνικό Επιμελητήριο) - Πιστοποιητικό ισχύουσας εκπροσώπησης ΓΕΜΗ, για την απόδειξη της νόμιμης

	<p>εκπροσώπησης στις περιπτώσεις που ο οικονομικός φορέας είναι νομικό πρόσωπο (ισχύς 30 εργάσιμες ημέρες) εκτός από ΟΕ και ΕΕ σύμφωνα με το έγγραφο του Επιμελητηρίου.</p> <ul style="list-style-type: none"> - Αναλυτικό Πιστοποιητικό Εκπροσώπησης στο οποίο να αναφέρεται αναλυτικά η εκπροσώπηση της εταιρίας και η άσκηση των δικαιωμάτων και εξουσιών. (για τις ΟΕ και ΕΕ να έχει εκδοθεί δύο (2) μήνες πριν την υποβολής του). - Γενικό Πιστοποιητικό ΓΕΜΗ από το οποίο προκύπτει ότι το νομικό πρόσωπο δεν έχει λυθεί και τεθεί υπό εκκαθάριση με απόφαση των εταίρων. - Πιστοποιητικό / βεβαίωση που να αναφέρονται οι ΚΑΔ - Για τις ΙΚΕ προσκομίζεται επιπλέον και πιστοποιητικό του ΓΕΜΗ περί μη έκδοσης απόφασης λύσης ή κατάθεση αίτησης λύσης του νομικού προσώπου - Για τις ΕΠΕ προσκομίζεται επιπλέον πιστοποιητικό μεταβολών. - Υπεύθυνη Δήλωση ότι δεν βρίσκεται σε μια από τις καταστάσεις των άρθ.73 & 74 του Ν.4412/16 όπως ισχύει, ως απόδειξη της μη ύπαρξης λόγων αποκλεισμού, η οποία θα πρέπει να έχει μεταγενέστερη ημερομηνία της πρόσκλησης.
<p>Υπογραφή σύμβασης</p>	<p>Ο ανάδοχος υποχρεούται να προσέλθει εντός δεκαπέντε (15) ημερών (αρθ.105, παρ.2 του Ν.4412/16) από την ημερομηνία κοινοποίησης της πρόσκλησης για την υπογραφή της σύμβασης.</p> <p>Με την υπογραφή της σύμβασης κατατίθεται εγγυητική καλής εκτέλεσης ποσοστού 4% επί της καθαρής αξίας του προϋπολογισμού της διακήρυξης ανά κατηγορία συμμετοχής του οικονομικού φορέα στην διαγωνιστική διαδικασία.</p> <p>Η ημερομηνία λήξης της εγγυητικής καλής εκτέλεσης πρέπει να είναι ανώτερη των δεκαπέντε (15) μηνών από την υπογραφή της σύμβασης.</p> <p>Η εγγύηση καλής εκτέλεσης της σύμβασης καλύπτει συνολικά και χωρίς διακρίσεις την εφαρμογή όλων των όρων της σύμβασης και κάθε απαίτηση της αναθέτουσας αρχής έναντι του αναδόχου.</p>

- Η Αναθέτουσα Αρχή ματαιώνει ή δύναται να ματαιώσει εν όλω ή εν μέρει, αιτιολογημένα, τη διαδικασία ανάθεσης, για τους λόγους και υπό τους όρους του άρθ.106 του Ν.4412/16, καθώς και σε περίπτωση συμφωνίας – πλαίσιο σύμφωνα με τα οριζόμενα στο ΦΕΚ Β'3103/20.06.2022.

- Η σύμβαση μπορεί να τροποποιηθεί κατά την διάρκειά της, χωρίς να απαιτείται νέα διαδικασία σύναψη σύμβασης, μόνο σύμφωνα με τους όρους και τις προϋποθέσεις του άρθ.132 του Ν.4412/16.

- Για την αναπροσαρμογή των τιμών της παρούσας σύμβασης, τίθεται η προβλεπόμενη στο άρθρ. 53, παρ.10α του Ν.4412/16 και υπό τους περιορισμούς του άρθ.132 του Ν.4412/16 ρήτρα αναπροσαρμογής του τιμήματος εφαρμόζοντας τον ακόλουθο τύπο: $T = T_{\text{προσφοράς}} \times (1 + \alpha)$. (όπου απαιτείται)

- Η αναθέτουσα αρχή, αιτιολογημένα και κατόπιν γνώμης της αρμόδιας επιτροπής του διαγωνισμού, μπορεί να κατακυρώσει τη σύμβαση για ολόκληρη ή μεγαλύτερη ή μικρότερη ποσότητα αγαθών ή παρεχόμενων υπηρεσιών, από αυτή που καθορίζεται στην παρούσα πρόσκληση σύμφωνα με το άρθ.105 του Ν.4412/16 όπως ισχύει.

- Εναλλακτικές προσφορές δεν γίνονται δεκτές.

- Η πληρωμή του συμβατικού τιμήματος θα γίνεται σε € με την προσκόμιση των νομίμων παραστατικών και δικαιολογητικών που προβλέπονται από τις διατάξεις του άρθρου 200 παρ. 4 του ν. 4412/2016, καθώς και κάθε άλλου δικαιολογητικού που τυχόν ήθελε ζητηθεί από τις αρμόδιες υπηρεσίες που διενεργούν τον έλεγχο και την πληρωμή.

- Στις εμπορικές συναλλαγές στις οποίες ο οφειλέτης είναι δημόσια αρχή, η προθεσμία πληρωμής ορίζεται σύμφωνα με τον Ν.4152/2013(Α'107) υποπαράγραφος Ζ.5 «συναλλαγές μεταξύ επιχειρήσεων και δημόσιων αρχών».

- Η πληρωμή υποχρεώσεων μπορεί να γίνεται και τμηματικά, με την έκδοση περισσότερων του ενός χρηματικών ενταλμάτων σύμφωνα με το ΠΔ 80/16 (άρθ.6).

- Για τα τιμολόγια που εκδίδονται κατά την εκτέλεση των δημοσίων συμβάσεων, ανεξαρτήτως αξίας αυτών, οι αναθέτουσες αρχές υποχρεούνται να παραλαμβάνουν και να επεξεργάζονται ηλεκτρονικά τιμολόγια που είναι σύμφωνα με το ευρωπαϊκό πρότυπο έκδοσης ηλεκτρονικών τιμολογίων, σύμφωνα με τις διατάξεις των άρθρων 148 έως και 153 του Ν.4601/2019 (Α'44) και των, κατ' εξουσιοδότηση του άρθ.154 του νόμου αυτού, (όπως τροποποιήθηκε και ισχύει), κανονιστικών αποφάσεων.

- Τον Ανάδοχο βαρύνουν οι υπέρ τρίτων κρατήσεις, ως και κάθε άλλη επιβάρυνση, σύμφωνα με την κείμενη νομοθεσία, μη συμπεριλαμβανομένου Φ.Π.Α., για την παράδοση του υλικού στον τόπο και με τον τρόπο που προβλέπεται στα έγγραφα της σύμβασης. Ιδίως βαρύνεται με τις ακόλουθες κρατήσεις:

- α) Για τις συμβάσεις αξίας άνω των χιλίων (1.000) €, μη συμπεριλαμβανομένου ΦΠΑ, κράτηση 0,1% η οποία υπολογίζεται επί της αξίας κάθε πληρωμής προ φόρων και κρατήσεων της αρχικής, καθώς και κάθε συμπληρωματικής υπέρ της Ενιαίας Αρχής Δημοσίων Συμβάσεων (Ε.Α.ΔΗ.ΣΥ) σύμφωνα με τα οριζόμενα στο άρθ.350, παρ.3 του Ν.4412/16 και σε συνάρτηση με τα άρθ.3 & 7 του Ν.4912/2022 (ΦΕΚ Α'59/17.03.2022)
- β) Κράτηση 2% υπέρ των Οργανισμών Ψυχικής Υγείας (άρθ. 3 του Ν.3580/2007)

Οι υπέρ τρίτων κρατήσεις υπόκεινται στο εκάστοτε ισχύον αναλογικό τέλος χαρτοσήμου 3% και στην επ' αυτού εισφορά υπέρ ΟΓΑ 20%

Η κράτηση υπέρ ΕΑΔΗΣΥ δεν επιβαρύνεται με τέλος χαρτοσήμου.

Με κάθε πληρωμή θα γίνεται η προβλεπόμενη από την κείμενη νομοθεσία παρακράτηση φόρου εισοδήματος αξίας 8% επί του καθαρού ποσού.

**Η Διοικήτρια
του Γ.Ν. Χίου «ΣΚΥΛΙΤΣΕΙΟ»
α/α**

Σμυρνιούδης Νικόλαος

Διευθυντής Ιατρικής Υπηρεσίας

ΠΑΡΑΡΤΗΜΑ ΤΕΧΝΙΚΩΝ ΠΡΟΔΙΑΓΡΑΦΩΝ

Το Γενικό Νοσοκομείο Χίου «Σκυλίτσειο» επεξεργάζεται πληθώρα δεδομένων προσωπικού χαρακτήρα, καθώς και πληροφορίες (σε ηλεκτρονικά ή/και φυσικά αρχεία) που μπορούν να ταυτοποιήσουν φυσικά πρόσωπα (ασθενείς, εργαζομένους, συνεργάτες, προμηθευτές κ.ά.). Αντικείμενο του παρόντος Έργου είναι η εναρμόνιση του Νοσοκομείου με τις απαιτήσεις Ευρωπαϊκού Κανονισμού Προστασίας Προσωπικών Δεδομένων ΕΕ 679/2016 (GDPR) και η παροχή υπηρεσιών Data Protection Officer (DPO).

Σκοπός είναι η αναγνώριση των τεχνολογικών και οργανωτικών αναγκών του Νοσοκομείου και η κάλυψή τους με την υλοποίηση των αντίστοιχων μέτρων για την διαμόρφωση συνεχούς συμμόρφωσής της στις απαιτήσεις του GDPR.

Το έργο θα αφορά σε όλες τις λειτουργικές Μονάδες του Νοσοκομείου, οι οποίες διαχειρίζονται προσωπικά δεδομένα:

- Τμήματα πρωτοβάθμιας φροντίδας, όπως Τμήμα Επειγόντων Περιστατικών, Τακτικά Εξωτερικά Ιατρεία
- Τμήματα δευτεροβάθμιας φροντίδας, όπως Κλινικές Παθολογικού και Χειρουργικού τομέα, Χειρουργεία, ειδικές Μονάδες (Μονάδα Εντατικής Θεραπείας, Μονάδα Εμφραγμάτων, Μονάδα Τεχνητού Νεφρού) , Διατομεακά Τμήματα κλπ.
- Εργαστήρια του Εργαστηριακού Τομέα
- Διοικητικές Υπηρεσίες, όπως Γραφείο Κίνησης, Λογιστήριο Ασθενών, Τμήμα Προσωπικού, Γραμματείες κλπ.
- Τμήμα Πληροφορικής

ΑΝΤΙΚΕΙΜΕΝΟ ΕΡΓΑΣΙΩΝ

1. Ο Υπεύθυνος Προστασίας Δεδομένων (DPO) ενημερώνει και συμβουλεύει τον Υπεύθυνο Επεξεργασίας ή τον εκτελούντα την επεξεργασία και του εργαζόμενους που επεξεργάζονται προσωπικά δεδομένα, για τις υποχρεώσεις τους που απορρέουν από τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) σχετικά με την προστασία προσωπικών δεδομένων.
2. Παρακολουθεί τη συμμόρφωση με τον παρόντα Κανονισμό σχετικά με την προστασία δεδομένων και με τις πολιτικές του Υπεύθυνου Επεξεργασίας ή του Εκτελούντος την Επεξεργασία σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της ανάθεσης αρμοδιοτήτων, της ευαισθητοποίησης, και της κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας και των σχετικών ελέγχων.
3. Παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων – εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα και παρακολουθεί την υλοποίηση της σύμφωνα με το άρθρο 35.
4. Συνεργάζεται με την εποπτική αρχή (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα).
5. Ο Υπεύθυνος Προστασίας Δεδομένων (DPO) ενεργεί ως σημείο επικοινωνίας για την εποπτική αρχή για ζητήματα που σχετίζονται με την επεξεργασία, περιλαμβανομένης της προηγούμενης διαβούλευσης που αναφέρεται στο άρθρο 36 και πραγματοποιεί διαβουλεύσεις, ανάλογα με την περίπτωση, για οποιοδήποτε άλλο θέμα.
6. Συνεργάζεται με την εποπτική αρχή και έχει δικαίωμα στον έλεγχο των προσωπικών δεδομένων των υπηρεσιών μας για την διερεύνηση περιπτώσεων που άπτονται της προστασίας δεδομένων.
7. Κατά την εκτέλεση των καθηκόντων του ο Υπεύθυνος Προστασίας Δεδομένων (DPO) λαμβάνει δεόντως υπόψη τον κίνδυνο που συνδέεται με τις πράξεις επεξεργασίας, συνεκτιμώντας της φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς επεξεργασίας.

8. Επιθεωρεί την τήρηση των συμφωνηθέντων διαδικασιών, προκειμένου να εκπληρώνεται η συμμόρφωση του Νοσοκομείου, στο Νομικό και λειτουργικό πλαίσιο, το οποίο έχει οριστεί κατά τη διαδικασία της εναρμόνισης.
9. Δεσμεύεται από την τήρηση του απορρήτου ή της εμπιστευτικότητας σχετικά με την εκτέλεση των καθηκόντων του, σύμφωνα με το δίκαιο της Ευρωπαϊκής Ένωσης και του Ελληνικού Κράτους.
10. Λογοδοτεί απευθείας στη Διοίκηση του Νοσοκομείου και αποτελεί το πρώτο σημείο επαφής με το υποκείμενο των δεδομένων.
11. Ο Υπεύθυνος Προστασίας Δεδομένων (DPO) αφότου αναλάβει καθήκοντα, θα πρέπει να έχει μεριμνήσει και για τον αναπληρωτή του.
12. Η Διοίκηση του Φορέα φροντίζει ώστε ο DPO να έχει ελεύθερη πρόσβαση σε δεδομένα και πράξεις επεξεργασίας και να έχει στην διάθεσή του, τους απαραίτητους πόρους για την εκπλήρωση των καθηκόντων του (π.χ. ενεργή στήριξη από τα ανώτερα διοικητικά στελέχη, υποδομές, συνεχής κατάρτιση κλπ.)
13. Απαγορεύεται ρητά η εκχώρηση των δικαιωμάτων και υποχρεώσεων του ΑΝΑΔΟΧΟΥ, που απορρέουν από τη σύμβαση σε τρίτο πρόσωπο, χωρίς προηγούμενη γραπτή συναίνεση του Νοσοκομείου.
14. Ο ανάδοχος θα πρέπει να έχει εμπειρία τουλάχιστον 3 ετών στην προμήθεια υπηρεσιών υπευθύνου προστασίας προσωπικών δεδομένων στον τομέα της υγείας. Για την απόδειξη της εμπειρίας, θα πρέπει να προσκομιστούν συμβάσεις ή δελτία παροχής υπηρεσιών, των τριών τελευταίων ετών.

Αναλυτικά το έργο θα περιλαμβάνει: ΥΠΗΡΕΣΙΕΣ ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Το πρώτο βήμα είναι η ενημέρωση της Διοίκησης και του προσωπικού του Νοσοκομείου για τον Γενικό Κανονισμό (**GDPR Awareness**), συνοπτικά:

- Χαρακτηριστικά & το νέο θεσμικό πλαίσιο
- Ορισμοί και πεδίο εφαρμογής
- Απαιτήσεις του GDPR
- Δικαιώματα των φυσικών προσώπων
- Ενημέρωση – λήψη συγκατάθεσης
- Διαβίβαση δεδομένων σε τρίτους
- Αρχεία δραστηριοτήτων επεξεργασίας
- Ο Ρόλος του Data Protection Officer (DPO)
- Υποχρεώσεις γνωστοποίησης περιστατικών παραβίασης στις αρμόδιες Αρχές και τα φυσικά πρόσωπα
- Πρόστιμα και Έλεγχοι

Να περιλαμβάνεται **εκπαίδευση** δύο ημερών (συνολικής διάρκειας 4 ωρών) στο προσωπικό του Νοσοκομείου.

Στη συνέχεια, θα πρέπει να γίνει **καταγραφή των διαδικασιών** συλλογής και διαχείρισης των προσωπικών δεδομένων, η οποία θα πραγματοποιηθεί μέσω συνεντεύξεων και ερωτηματολογίων με τις

οργανωτικές μονάδες του Νοσοκομείου. Η εμπειρία μας έχει δείξει ότι τα αποτελέσματα των συνεντεύξεων είναι πολύ καλύτερα, εάν το προσωπικό είναι ενήμερο για το σκοπό του έργου.

Έπειτα ακολουθούν οι διαδικασίες του **Legal Audit**, έτσι ώστε όλες οι απαραίτητες πληροφορίες που θα συγκεντρωθούν να οδηγήσουν σε δύο κύρια παραδοτέα:

- Καταγραφή των διαδικασιών και δραστηριοτήτων επεξεργασίας.
- Διάγνωση ελλείψεων (**Gap Analysis**) και
- Σχέδιο Αντιμετώπισης (**Remediation Plan**) σχετικά με τη συμμόρφωση με τον νέο κανονισμό και σχέδιο συμμόρφωσης.

Παράλληλα με τα ανωτέρω, θα πρέπει πραγματοποιείται το **Legal Audit**. Ο σκοπός αυτού του σταδίου είναι να διερευνήσει τη νομική βάση για την επεξεργασία των προσωπικών δεδομένων, να εξετάσει τις αρχές προστασίας προσωπικών δεδομένων σε κάθε τύπο της επεξεργασίας των δεδομένων, και να παρασχεθούν νομικές κατευθύνσεις για την εξισορρόπηση των δικαιωμάτων των υποκειμένων των δεδομένων.

Επιπλέον θα πρέπει να περιλαμβάνει την αποσαφήνιση της **νομικής βάσης της συλλογής και επεξεργασίας προσωπικών δεδομένων**, τη δημιουργία **σύμβασης συγκατάθεσης** των φυσικών προσώπων και τη δημιουργία προσαρτημάτων **συμβάσεων για πελάτες, προμηθευτές και προσωπικό**.

Αξιολόγηση εάν η επεξεργασία είναι πιθανό να έχει ως αποτέλεσμα **ψηλό κίνδυνο** για το υποκείμενο των δεδομένων.

Μελέτη της επεξεργασίας, ιεράρχηση των κινδύνων και μεταχείριση τους κατά τρόπο ανάλογο, ώστε να βελτιστοποιηθεί το κόστος και να ληφθούν αποφάσεις.

Η επεξεργασία κάθε κατηγορίας προσωπικών δεδομένων θα εξεταστεί σύμφωνα με τις απαιτήσεις του GDPR, έτσι ώστε να επιτευχθεί το απαραίτητο επίπεδο συμμόρφωσης. Τα θέματα που θα εξετασθούν ενδεικτικά περιλαμβάνουν κατά πόσο τα προσωπικά δεδομένα υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο («νομιμότητα, αντικειμενικότητα και διαφάνεια»), τον «περιορισμό του σκοπού της επεξεργασίας», την «ελαχιστοποίηση των δεδομένων», τη «συγκατάθεση» των υποκειμένων των δεδομένων, τον «περιορισμό αποθήκευσης των δεδομένων», τα μέτρα προστασίας δεδομένων κλπ.

Επιπλέον, θα πρέπει να αναλυθεί η ετοιμότητα του Νοσοκομείου να ανταποκριθεί στα δικαιώματα των υποκειμένων των δεδομένων, όπως ενδεικτικά: «δικαίωμα πρόσβασης», «δικαίωμα στη διόρθωση», «δικαίωμα στη λήθη», «δικαίωμα περιορισμού της επεξεργασίας», «δικαίωμα μεταφοράς δεδομένων», «δικαίωμα εναντίωσης».

Ακολουθεί η επικαιροποίηση της υφιστάμενης **διάγνωσης ελλείψεων (Gap Analysis)**, η εκπόνηση των κατάλληλων οργανωτικών μέτρων, η εισήγηση των κατάλληλων τεχνικών μέτρων και η εκπόνηση σχεδίου και χρονοδιαγράμματος για την υλοποίηση αυτών.

Επιγραμματικά, ως κατάλληλα οργανωτικά μέτρα θεωρούνται:

Η εκπαίδευση του προσωπικού στον GDPR.

Η σαφής κατανομή ρόλων και αρμοδιοτήτων του προσωπικού για την επεξεργασία των προσωπικών δεδομένων.

Οι πολιτικές και διαδικασίες προστασίας προσωπικών δεδομένων.

Τα σχέδια Disaster Recovery και Business Continuity, τα οποία μπορούν να εξασφαλίσουν τη συνεχή διαθεσιμότητα της πληροφορίας [προαιρετικά].

Το σχέδιο Αντιμετώπισης Περιστατικών Ασφαλείας και Παραβίασης προσωπικών δεδομένων (Incident Response Plan & Data Breach Response Plan), το οποίο θα επιτρέπει την οργανωμένη και συστηματική αντιμετώπιση περιστατικών παραβίασης.

Ως κατάλληλα τεχνικά μέτρα που θα προταθούν θεωρούνται (επίσης επιγραμματικά):

- Η ασφάλεια των πληροφοριακών συστημάτων (IT security).
- Μηχανισμοί ελέγχου προσβάσεων στα πληροφοριακά συστήματα.
- Η προστασία των προσωπικών δεδομένων (ενδεικτικά: κρυπτογράφηση, ψευδωνυμοποίηση, DLP-Data Loss Prevention).
- Η αποτελεσματική πρόληψη και αντίδραση σε απειλές παραβίασης.

Παραδοτέα:

1. Πολιτική Προστασίας Προσωπικών Δεδομένων (Personal Data Protection Policy).

Πρόκειται για την πολιτική που θα θέσει σε ισχύ και εφαρμόζει στο εξής το Νοσοκομείο για την προστασία των προσωπικών δεδομένων, σε συνάρτηση προς άλλες πολιτικές ασφάλειας που ενδεχομένως διαθέτει και τηρεί. Η ύπαρξη πολιτικής προσωπικών δεδομένων ενθαρρύνει το σεβασμό των θεμελιωδών αρχών προστασίας των προσωπικών δεδομένων από το προσωπικό και αποτελεί μέσο απόδειξης της συμμόρφωσης του Ταμείου προς τον GDPR. Τυχόν επιμέρους «πολιτικές» ανά δραστηριότητα ή κατηγορία δεδομένων ενδέχεται να προκύψουν στην πορεία υλοποίησης του έργου. Εκπροσώπηση του Νοσοκομείου σε κανονιστικά ζητήματα και ζητήματα προστασίας προσωπικών δεδομένων.

Παροχή συμβουλών αναφορικά με τις υποχρεώσεις συμμόρφωσης με το εκάστοτε ισχύον κανονιστικό πλαίσιο προστασίας δεδομένων αλλά και στη σύνταξη πολιτικών Προστασίας Δεδομένων, των απαιτούμενων συμβάσεων, των ρητρών συγκατάθεσης.

2. Πολιτική τήρησης δεδομένων (Data Retention Policy), Privacy Policy & Cookies Policy

Πρόκειται για το πλάνο προσδιορισμού της χρονικής περιόδου τήρησης των προσωπικών δεδομένων ανά κατηγορία και σκοπό επεξεργασίας.

3. Περιγραφή Ρόλου Υπευθύνου Προστασίας

Επεξήγηση του ρόλου και των ευθυνών του υπευθύνου προστασίας δεδομένων.

4. Απογραφή των Αρχείων των Δραστηριοτήτων Επεξεργασίας

Η καταγραφή των ζητούμενων στοιχείων σε αρχείο, σύμφωνα με τις απαιτήσεις του **άρθρου 30 του Κανονισμού (GDPR)**. Η καταγραφή αυτή είναι μείζονος σημασίας για την απόδειξη της προσπάθειας συμμόρφωσης με τον GDPR.

5. Συγκατάθεση

Η συγκατάθεση πρέπει να είναι σαφής, συγκεκριμένη, έγγραφη και εν πλήρη επίγνωση, δήλωση με την οποία το υποκείμενο των δεδομένων δηλώνει ότι συμφωνεί, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα που το αφορούν. Τα αιτούμενα προσωπικά δεδομένα πρέπει να τυγχάνουν αυτοματοποιημένης επεξεργασίας επί τη βάση της συγκατάθεσης του υποκειμένου των δεδομένων ή προς εκπλήρωση της σύμβασης. Διαδικασία και έντυπα για τη λήψη συγκατάθεσης από το υποκείμενο των δεδομένων για την επεξεργασία των προσωπικών δεδομένων του, όπου η επεξεργασία έχει ως νομική βάση τη συγκατάθεση.

6. Διαδικασία Λήψης & Ικανοποίησης Αιτημάτων Υποκειμένου των Δεδομένων

Η διαδικασία που πρέπει να έχει η εταιρία σας για να ανταποκρίνεται σε αιτήματα των υποκειμένων των δεδομένων να έχουν πρόσβαση και να λάβουν αντίγραφα των δεδομένων τους.

7. Εκτίμηση Αντίκτυπου σχετικά με την προστασία δεδομένων – DPIA [προαιρετικά ή σε μεταγενέστερη φάση]

Πρόκειται για τη μεθοδολογία βάσει της οποίας το Νοσοκομείο θα εκτιμά το ρίσκο μιας σχεδιαζόμενης επεξεργασίας και θα προσδιορίζει τα μέτρα απαλοιφής των πιθανών ρίσκων που θα επηρέαζαν αρνητικά τα δικαιώματα και τις ελευθερίες των υποκείμενων των δεδομένων. Η εκτίμηση αντίκτυπου θα πρέπει να αναθεωρείται περιοδικά και σε κάθε περίπτωση όταν επέρχεται κάποια σημαντική αλλαγή. Περιλαμβάνει μία αρχική αξιολόγηση με την χρήση ερωτηματολογίου και προσωπικών συνεντεύξεων.

8. Προσδιορισμός, Ανάλυση Παρούσας και Επιθυμητής Θέσης (GAP Analysis).

Ο οργανισμός συγκρίνει την τρέχουσα κατάσταση με την προσδοκώμενη για να προσδιορίσει τα κενά, σε μία προσπάθεια βελτιστοποίησης της ασφαλείας των προσωπικών δεδομένων. Στη συνέχεια προτείνεται ένα σχέδιο δράσης, με καταγραφή των ενεργειών που επιβάλλεται ή είναι σκόπιμο να πραγματοποιηθούν κατά σειρά προτεραιότητας, καθώς και των απαιτούμενων πόρων για την αντιμετώπιση αυτών των κενών με ανάλυση κόστους / οφέλους, σε συνδυασμό με την κατανόηση του κινδύνου και την επίτευξη των στόχων. Η χρήση της μεθοδολογίας δίνει τη δυνατότητα στο Νοσοκομείο να λάβει τεκμηριωμένες αποφάσεις σχετικά με τις δραστηριότητες στον τομέα της ασφάλειας και να υποστηρίξει τη διαχείριση κινδύνου.

9. Πολιτική Ασφάλειας Πληροφοριακών Συστημάτων [προαιρετικά ή σε μεταγενέστερη φάση]

Η πολιτική που θα υποδείξουμε θα περιγράφει τις βασικές έννοιες και οδηγίες ασφαλείας φυσικής προστασίας και ασφάλεια πληροφορικής. Ενδεικτικά περιλαμβάνονται: Πολιτική Ελέγχου Πρόσβασης, Κανόνες ασφαλείας για την προστασία της υποδομής πληροφοριακών συστημάτων, Πολιτική “Bring Your Own Device” (BYOD), Πολιτική Κινητών Συσκευών και Τηλεργασία κ.ά.)

10. Διαδικασία Ενημέρωσης της Εθνικής Αρχής Προστασίας Δεδομένων (DPA) και των Υποκειμένων σε περίπτωση παραβίασης Προσωπικών Δεδομένων

Καθορισμός των βημάτων που ακολουθούνται και των ενδεδειγμένων μέτρων σε περίπτωση που υπάρξει διαρροή, αλλοίωση, καταστροφή ή άλλη αθέμιτη επεξεργασία των προσωπικών δεδομένων, με αφετηρία την ενημέρωση της Εποπτεύουσα Αρχής και των Υποκειμένων και στόχο να μετριασθούν οι συνέπειες. Ο Κανονισμός υποχρεώνει σε γνωστοποίηση της παραβίασης δεδομένων προσωπικού χαρακτήρα στην αρμόδια εποπτική αρχή, ενώ συγκεκριμενοποιεί την υποχρέωση του υπευθύνου επεξεργασίας απαιτώντας η γνωστοποίηση να λαμβάνει χώρα μέσα σε 72 ώρες.