ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
2η ΥΓΕΙΟΝΟΜΙΚΗ ΠΕΡΙΦΕΡΕΙΑ
ΠΕΙΡΑΙΩΣ & ΑΙΓΑΙΟΥ
ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΠΕΙΡΑΙΑ «ΤΖΑΝΕΙΟ»
ΤΜΗΜΑ ΟΙΚΟΝΟΜΙΚΟ
ΓΡΑΦΕΙΟ ΠΡΟΜΗΘΕΙΩΝ
ΠΛΗΡΟΦΟΡΙΕΣ: ΜΠΑΡΓΙΑΤΑΚΗ ΓΕΩΡΓΙΑ
ΤΗΛ: 210 – 4592593
Fax: 210 - 4592597

Αριθμ. Πρωτ. : 13467

Πειραιάς: 21-09-2018

Δημόσια ανοικτή διαδικασία
συλλογής προσφορών για τις Συμβουλευτικές Υπηρεσίες συμμόρφωσης με τον κανονισμό προστασίας δεδομένων

ΑΝΤΙΚΕΙΜΕΝΟ ΤΟΥ ΔΙΑΓΩΝΙΣΜΟΥ - ΣΥΝΟΠΤΙΚΑ ΣΤΟΙΧΕΙΑ

ΕΙΔΟΣ ΔΙΑΔΙΚΑΣΙΑΣ	**Ανοικτή**
ΚΡΙΤΗΡΙΟ ΚΑΤΑΚΥΡΩΣΗΣ	**Η χαμηλότερη τιμή**
ΧΡΟΝΟΣ ΔΙΕΝΕΡΓΕΙΑΣ	**01– 10 - 2018**
ΩΡΑ:	**12:00 π.μ.,**
ΠΕΡΙΓΡΑΦΗ ΕΙΔΩΝ	**Όπως αναλυτικά αναφέρεται στα Παραρτήματα Α - Δ**

ΤΟ ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΠΕΙΡΑΙΑ «ΤΖΑΝΕΙΟ»

Έχοντας υπόψη:

1. Τις διατάξεις, όπως ισχύουν:

1.1. Του Νόμου 4412 / 2016 « Δημόσιες συμβάσεις έργου , προμηθειών και υπηρεσιών » (ΦΕΚ Α΄ 147 / 08 – 08 – 2016) .

1.2. Του Ν. 3580/2007 « Προμήθειες Φορέων εποπτευόμενων από το Υπουργείο Υγείας και Κοινωνικής Αλληλεγγύης και άλλες διατάξεις» (Φ.Ε.Κ. Α΄ 134/18-6-2007).

1.3. Του Ν. 2955/2001 « Προμήθειες Νοσοκομείων και λοιπών μονάδων υγείας των Πε.Σ.Υ. και άλλες διατάξεις » (Φ.Ε.Κ. Α΄ 256/2-11-2001), όπως τροποποιημένος ισχύει.

1.4. Του Ν. 2362/1995 «Περί Δημοσίου Λογιστικού, ελέγχου των δαπανών του Κράτους και άλλες διατάξεις» (Φ.Ε.Κ. Α΄ 247/27-11-1995), όπως ισχύει.

ΠΡΟΣΚΑΛΕΙ

1. Κάθε ενδιαφερόμενο, να καταθέσει προσφορά για την Ανάθεση : **1) Συμβουλευτικές υπηρεσίες συμμόρφωσης με τον κανονισμό προστασίας δεδομένων ,** με κριτήριο κατακύρωσης **τη χαμηλότερη τιμή η οποία θα είναι ίση ή μικρότερη του τελευταίου παρατηρητηρίου τιμών**, όπως αυτό αναρτάται στην ιστοσελίδα της Επιτροπής Προμηθειών Υγείας.

2. Περιγραφή των ζητούμενων κατηγοριών ειδών γίνεται στο **παράρτημα Α της παρούσας και στο παράρτημα Δ (Τεχνικές προδιαγραφές)** .

3. Οι προσφορές μπορούν να κατατίθενται μέχρι και την ημερομηνία και ώρα της διαδικασίας **στο mail της Υπηρεσίας bargiataki@tzaneio.gr.**

4. Πληρωμή: Η πληρωμή θα γίνεται σε ευρώ, μετά από προηγούμενη θεώρηση των χρηματικών ενταλμάτων πληρωμής από τον αρμόδιο Επίτροπο του Ελεγκτικού Συνεδρίου.

5. Δικαίωμα Συμμετοχής στη διαδικασία έχουν οι αναφερόμενοι κατωτέρω, εφόσον ασκούν εμπορική ή βιομηχανική ή βιοτεχνική δραστηριότητα συναφή με το αντικείμενο της προμήθειας:

α) Όλα τα φυσικά ή νομικά πρόσωπα, ημεδαπά ή αλλοδαπά. β) Ενώσεις προμηθευτών που υποβάλλουν κοινή προσφορά. γ) Συνεταιρισμοί.

Κατά τα λοιπά, η διαδικασία θα διενεργηθεί και η προμήθεια θα υλοποιηθεί σύμφωνα με τα παρακάτω **ΠΑΡΑΡΤΗΜΑΤΑ** που επισυνάπτονται στην παρούσα και αποτελούν αναπόσπαστο μέρος αυτής.

1. ΠΕΡΙΓΡΑΦΗ ΖΗΤΟΥΜΕΝΩΝ ΚΑΤΗΓΟΡΙΩΝ ΕΙΔΩΝ	**ΠΑΡΑΡΤΗΜΑ Α΄**
2. ΟΡΟΙ ΣΥΜΜΕΤΟΧΗΣ	**ΠΑΡΑΡΤΗΜΑ Β΄**
3. ΥΠΟΔΕΙΓΜΑ ΠΙΝΑΚΑ	**ΠΑΡΑΡΤΗΜΑ Γ΄**
4. ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ	**ΠΑΡΑΡΤΗΜΑ Δ΄**

Οι ενδιαφερόμενοι θα έχουν δυνατότητα ελεύθερης πρόσβασης στο πλήρες κείμενο αυτής (συμπεριλαμβανομένων όλων των παραρτημάτων της), σε ηλεκτρονική μορφή, στην ιστοσελίδα του Νοσοκομείου στο διαδίκτυο (ηλεκτρονική διεύθυνση: www.tzaneio.gr).

ΠΑΡΑΡΤΗΜΑ Α'

(Αποτελεί αναπόσπαστο τμήμα της διακήρυξης)

Α.Ε.	ΑΔΑ	ΕΙΔΟΣ	ΤΕΜΑΧΙΑ	ΤΜΗΜΑ ΠΟΥ ΠΡΟΟΡΙΖΕΤΑΙ ΤΟ ΕΙΔΟΣ	ΠΛΗΡΟΦΟΡΙΕΣ
2261	**ΨΙΛΘ4 6906Κ-ΩΝΔ**	- **ΣΥΜΒΟΥΛΕΥΤΙΚΕΣ ΥΠΗΡΕΣΙΕΣ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΟΝ ΚΑΝΟΝΙΣΜΟ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ** **(Περιγραφή Τεχνικών Προδιαγραφών όπως αναλυτικά αναφέρονται στο Παράρτημα Δ΄)**	**Υπηρεσία**	**ΤΜΗΜΑ : Γραφείο Διοίκησης**	ΤΜΗΜΑ : ΤΗΛ. ΠΛΗΡΟΦΟΡΙΩΝ : Αιμοδοσία 210-4592762 (κο ΜΑΤΣΑΓΓΟ ΣΠΥΡΙΔΩΝΑ)

ΠΑΡΑΡΤΗΜΑ Β’

(Αποτελεί αναπόσπαστο τμήμα της διακήρυξης)

ΟΡΟΙ ΣΥΜΜΕΤΟΧΗΣ

1. Η προσφορά θα πρέπει να έχει τη μορφή του πίνακα που επισυνάπτεται στο Παράρτημα ΄Γ.
2. Υποχρεωτικά να δηλώνονται κωδικός Παρατηρητηρίου Τιμών, GMDN και κωδικός ΕΚΑΠΤΥ
3. Η οικονομική προσφορά θα κατατίθεται αποκλειστικά σε **EURO**.
4. Γλώσσα: **Ελληνική**

Οι υποψήφιοι υποβάλλουν επί ποινή απόρριψης την προσφορά τους ηλεκτρονικά :

1. Σε περίπτωση μη υποβολής ή μη προσήκουσας υποβολής των αναφερόμενων πιο πάνω, η προσφορά απορρίπτεται ως απαράδεκτη.

ΠΑΡΑΡΤΗΜΑ ΄Γ

ΑΡΙΘΜΟΣ ΕΝΤΟΛΗΣ	ΠΕΡΙΓΡΑΦΗ ΕΙΔΟΥΣ	ΤΙΜΗ ΠΡΟΣΦΟΡΑΣ ΧΩΡΙΣ ΦΠΑ	ΚΩΔΙΚΟΣ ΠΑΡΑΤΗΡΗΤΗΡΙΟΥ	ΤΙΜΗ ΠΑΡΑΤΗΡΗΤΗΡΙΟΥ	ΚΩΔΙΚΟΣ ΕΜΠΟΡΙΟΥ	GMDN	ΕΚΑΠΤΥ
			-	-	-	-	-

ΥΠΟΔΕΙΓΜΑ ΠΙΝΑΚΑ

ΠΑΡΑΡΤΗΜΑ Δ

- Τεχνικές Προδιαγραφές ανάθεσης σε σύμβουλο ή εταιρεία συμβούλων, του έργου συμμόρφωσης του Νοσοκομείου με τον νέο Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου

Ο υποψήφιος Ανάδοχος εναρμόνισης του Νοσοκομείου με τον ΓΚΠΔ, οφείλει αρχικά, να παραδώσει στη Διοίκηση, στον Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ) (αν έχει ορισθεί κατά την έναρξη ανάληψης του έργου) και στην επιτροπή ελέγχου υλοποίησης του έργου που θα ορίσει η Διοίκηση του Νοσοκομείου, πλάνο και ενδεικτικό χρονοδιάγραμμα υλοποίησης του έργου στο οποίο να περιγράφεται αναλυτικά ο τρόπος προσέγγισης και εκτέλεσης του έργου καθώς και να καθορίζεται ο χρόνος υλοποίησης ο οποίος δεν θα ξεπερνάει τους οκτώ (8) μήνες. Ο Ανάδοχος θα αναλάβει την ολοκληρωμένη συμμόρφωση του Νοσοκομείου και τον έλεγχο αυτής, προς τις επιταγές του νέου ΓΚΠΔ που θα περιλαμβάνει υποχρεωτικά ως παραδοτέες τις παρακάτω διαδικασίες:

- **Ενημέρωση και ευαισθητοποίηση της Διοίκησης** του νοσοκομείου με σκοπό την πλήρη κατανόηση των απαιτήσεων που θα προκύψουν από τις ενέργειες συμμόρφωσης με τον ΓΚΠΔ.

- **Χαρτογράφηση αρχείων και δεδομένων (έντυπα και ηλεκτρονικά) καθώς και της ροής των δεδομένων**: που θα καλύπτουν την απαίτηση του ΓΚΠΔ για την σύνταξη αρχείου δραστηριοτήτων. Καταγραφή ανά δραστηριότητα/σκοπό των προσωπικών δεδομένων που τυγχάνουν επεξεργασίας, και της ροής αυτών, δηλ. οι διαδικασίες συλλογής, επεξεργασίας και τήρησης τους, αξιοποιώντας τυχόν υπάρχουσες καταγραφές των διαδικασιών, συστημάτων και προσώπων που προβαίνουν σε επεξεργασία αυτών .

- **Αξιολόγηση κινδύνου περί ιδιωτικότητας και Μελέτη ανάλυσης ελλείψεων-αποκλίσεων και κινδύνου:** Με γνώμονα την αρχική χαρτογράφηση ο σύμβουλος ή η ομάδα συμβούλων θα αξιολογήσει τις υφιστάμενες διαδικασίες πρακτικών συλλογής, επεξεργασίας και τήρησης των προσωπικών δεδομένων. Στη συνέχεια θα συντάξει έκθεση των αποκλίσεων με τον ΓΚΠΔ και αξιολόγηση του βαθμού επικινδυνότητας αυτών.

- **<u>Έκθεση Εκτίμησης Αντικτύπου (DPIA):</u>** Σύνταξη Μελέτης Εκτίμησης Αντικτύπου για το σύνολο των επεξεργασιών εντός του νοσοκομείου αλλά και εξωτερικά (ιδίως για την περίπτωση μεταφοράς δεδομένων εντός και εκτός Ευρωπαϊκής Ένωσης) έτσι ώστε να εξασφαλίζεται τόσο το "Privacy by Design" όσο και το "Privacy by Default".

- **<u>Έλεγχος και Πρόταση Τροποποίησης Εντύπων:</u>** επιθεώρηση του συνόλου των εντύπων που απευθύνονται σε ασθενείς, εργαζόμενους, προμηθευτές του νοσοκομείου και πρόταση τροποποίησης τους ή και ψηφιοποίησης τους καθώς και ένταξη νέων (όπου χρειάζεται) για την εναρμόνιση τους με τις διατάξεις του ΓΚΠΔ.

- **<u>Αναθεώρηση των πολιτικών Ασφάλειας και Προστασίας δεδομένων και συγγραφή εγχειριδίων</u>:** Διαμόρφωση προγράμματος συμμόρφωσης (πρόταση τεχνικών και οργανωτικών μέτρων) και ανάπτυξη πρότυπων διαδικασιών για την επεξεργασία προσωπικών δεδομένων, υπό τη μορφή έντυπου και ηλεκτρονικού εγχειριδίου για την διευκόλυνση του προσωπικού κατά την άσκηση των καθηκόντων του. Στις αναθεωρημένες πολιτικές ασφάλειας και προστασίας πρέπει τουλάχιστον να περιλαμβάνονται τα εξής:
  - Προσδιορισμός νομικών βάσεων επεξεργασίας προσωπικών δεδομένων συμπεριλαμβανομένης της συναίνεσης του υποκειμένου και έλεγχος συμβάσεων και διατυπώσεων σε έντυπα ή ψηφιακές φόρμες Ενημέρωσης και χορήγησης συγκατάθεσης.
  - Ανάπτυξη σχεδίου του χειρισμού αιτημάτων των υποκειμένων (πρόσβασης, διαγραφής, φορητότητας κλπ)
  - Ανάπτυξη σχεδίου αναγνώρισης και έγκαιρης απόκρισης σε περίπτωση παραβίασης δεδομένων και επεξεργασία πρωτοκόλλου γνωστοποίησης παραβίασης δεδομένων στην εποπτεύουσα αρχή (ΑΠΔΠΧ) και σχετικής ανακοίνωσης στα υποκείμενα.

- **<u>Αξιολόγηση πλαισίου Ασφαλείας των πληροφοριακών συστημάτων:</u>** Έκθεση αξιολόγησης ασφάλειας σε επίπεδο hardware και software. Επίσης, θα πρέπει να ελεγχθεί η ασφάλεια των υποδομών των υπολογιστικών συστημάτων καθώς και των δικτυακών υποδομών. Έλεγχος του συνόλου των χρησιμοποιούμενων εφαρμογών λογισμικού καθώς και των σχετικών συμβάσεων έργου με τους συνεργαζόμενους παρόχους λογισμικού, ως προς την συμμόρφωση τους με τον ΓΚΠΔ. Αξιοποίηση των ήδη εγκατεστημένων συστημάτων ή και πρόταση διαμόρφωσης ή επανασχεδιασμού τους ή και πρόταση προμήθειας νέων, **(Firewalls/AVs, CRMs/Work Flow Applications, Encryption, Cloud…)** με σκοπό τη διασφάλιση της προστασίας των δεδομένων και αλλά και την παρακολούθηση της συμμόρφωσης.

- **Σύνταξη πλάνου επιχειρησιακής συνέχειας και σχεδίου ανάκαμψης από καταστροφή.**

- **Εκπαίδευση του προσωπικού του νοσοκομείου** σε όλα τμήματα και τις μονάδες του Νοσοκομείου ξεχωριστά και κατά περίπτωση (Διοικητικό-Ιατρονοσηλευτικό-Τεχνικό προσωπικό, κλπ). Ο σύμβουλος μετά την ολοκλήρωση της εκπαίδευσης οφείλει να ζητήσει ενυπόγραφη δήλωση συμμετοχής στην εκπαίδευση από το προσωπικό των εκάστοτε τμημάτων.

- **Δοκιμαστικοί έλεγχοι συστημάτων και διαδικασιών** θα πρέπει να πραγματοποιηθούν κατά περίπτωση, προκειμένου να εξακριβωθεί η αποτελεσματικότητα των νέων εφαρμοζόμενων διαδικασιών καθώς και ο βαθμός συμμόρφωσης με τον νέο κανονισμό.

- **Διαρκής παρακολούθηση** αλλά και επικαιροποίηση των νέων εφαρμοσμένων διαδικασιών και συστημάτων κατά τη διάρκεια της σύμβασης.

Προϋποθέσεις συμμετοχής

Η ομάδα έργου των ενδιαφερομένων υποψηφίων αναδόχων θα πρέπει να αποτελείται από στελέχη εξειδικευμένα επιστημονικά, τα οποία να διαθέτουν εμπειρογνωσία στον τομέα της υγείας και των διοικητικών κανόνων που τον διέπουν καθώς και στα πρότυπα συστημάτων διαχείρισης ασφάλειας των πληροφοριών.

Πιο συγκεκριμένα, στην ομάδα των εξειδικευμένων στελεχών θα πρέπει να περιλαμβάνονται κατά το ελάχιστο οι κάτωθι:

1. Εξειδικευμένος νομικός με γνώση και εμπειρία των πρακτικών περί Προστασίας και διαχείρισης προσωπικών δεδομένων στο πλαίσιο υλοποίησης της συμμόρφωσης, ειδικά στον τομέα της παροχής υπηρεσιών υγείας.
2. Εξειδικευμένος επιστήμονας Πληροφορικής με γνώση και εμπειρία της ασφαλούς διαχείρισης δεδομένων μέσω πληροφοριακών συστημάτων, την ασφάλεια υποδομών πληροφορικής και δικτύων (π.χ. ανάπτυξη σχεδίων ασφάλειας, συστήματα διαχείρισης ασφάλειας των πληροφοριών όπως ISO/IEC 27001:2013 κλπ)

Τα παραπάνω αναφερόμενα προσόντα θα πρέπει να τεκμηριώνονται με τις σχετικές βεβαιώσεις-πιστοποιητικά-πτυχία-βιογραφικά σημειώματα, κλπ.

Βιβλιογραφικές Αναφορές

Για τη σύνταξη των τεχνικών προδιαγραφών χρησιμοποιήθηκαν οι παρακάτω πηγές:

1. «Οδηγός Συμμόρφωσης με ΓΚΠΔ» της ιστοσελίδας της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (http://www.dpa.gr/portal/page?_pageid=33,209418&_dad=portal&_schema=PORTAL)
2. Γενικός Κανονισμός Προστασίας Δεδομένων: Το νέο τοπίο και οι υποχρεώσεις της Δημόσιας Διοίκησης. Έκθεση Συμπερασμάτων. ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ (Υπ. Αριθμ. 8125/27-11-2017 Απόφαση Προέδρου ΕΚΔΔΑ) Εθνικό Κέντρο Δημόσιας Διοίκησης και Αυτοδιοίκησης. http://www.ekdd.gr/ekdda/images/seminaria/GDPR.pdf
3. Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016. https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EL