Το Λαϊκό Νοσοκομείο θέτει σε δημόσια διαβούλευση τις τεχνικές προδιαγραφές για την εναρμόνιση του Γ.Ν.Α. «ΛΑΪΚΟ» με τον Ευρωπαϊκό Γενικό Κανονισμό Προστασίας των Προσωπικών Δεδομένων (General Data Protection Regulation) 679/2016 προκειμένου να δοθεί η δυνατότητα υποβολής παρατηρήσεων από τους ενδιαφερόμενους.

Η διαβούλευση θα είναι ανοικτή από την ημερομηνία ανάρτησης των τεχνικών προδιαγραφών στην ιστοσελίδα του νοσοκομείου έως 27.6.2018 ημέρα Τετάρτη και ώρα 15:00 μμ.

Οι παρατηρήσεις επί των τεχνικών προδιαγραφών μπορούν να υποβληθούν στο πρωτόκολλο του νοσοκομείου ή με τηλεομοιοτυπία στο 213.2061638.

Η υποβολή των προαναφερθέντων δεν μπορεί σε καμία περίπτωση να δεσμεύσει καθ' οιονδήποτε τρόπο καμία από τις δύο πλευρές.

ΠΡΑΚΤΙΚΟ ΣΥΝΤΑΞΗΣ ΤΕΧΝΙΚΩΝ ΠΡΟΔΙΑΓΡΑΦΩΝ

Εναρμόνιση του ΓΝΑ «ΛΑΪΚΟ» με τον Ευρωπαϊκό Γενικό Κανονισμό Προστασίας των Προσωπικών Δεδομένων (General Data Protection Regulation) 679/2016.

1) ΓΕΝΙΚΑ

Με την παρούσα μελέτη , περιγράφονται κατωτέρω οι εργασίες που απαιτούνται ώστε να εναρμονιστεί το ΓΝΑ «ΛΑΪΚΟ» με τον Ευρωπαϊκό Γενικό Κανονισμό Προστασίας των Προσωπικών Δεδομένων(General Data Protection Regulation) 679/2016.

2) ΑΝΤΙΚΕΙΜΕΝΟ

Αντικείμενο της παρούσης μελέτης είναι η εναρμόνιση του ΓΝΑ «ΛΑΪΚΟ» με τον Ευρωπαϊκό Γενικό Κανονισμό Προστασίας των Προσωπικών Δεδομένων(General Data Protection Regulation) 679/2016.

Σκοπός αυτής είναι η αναγνώριση των τεχνολογικών και οργανωτικών αναγκών του Νοσοκομείου και η κάλυψή τους , με την υλοποίηση των αντίστοιχων μέτρων για την διαμόρφωση συνεχούς συμμόρφωσης στις απαιτήσεις του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας των Προσωπικών Δεδομένων.

Το έργο θα αφορά σε όλες τις λειτουργικές μονάδες του Νοσοκομείου, οι οποίες διαχειρίζονται προσωπικά δεδομένα . Στόχος είναι η δημιουργία κουλτούρας προστασίας των προσωπικών δεδομένων στους εργαζόμενους του Νοσοκομείου, καθώς και η ενσωμάτωση της προστασίας προσωπικών δεδομένων στις λειτουργίες του Νοσοκομείου σχετικά με α)την επεξεργασία των προσωπικών δεδομένων σε όλο τον κύκλο ζωής τους, ήτοι από τη συλλογή έως και την καταστροφή τους, β)Τις προϋποθέσεις μεταφοράς τους, γ)την προστασία των δικαιωμάτων των φυσικών προσώπων, δ)την ασφάλεια όπως εμπιστευτικότητα , ακεραιότητα, διαθεσιμότητα, των προσωπικών δεδομένων και τις ενέργειες γνωστοποίησης που οφείλει να κάνει το Νοσοκομείο σε περίπτωση παραβίασης.

3) ΤΕΧΝΙΚΗ ΠΕΡΙΓΡΑΦΗ-ΦΑΣΕΙΣ ΕΡΓΟΥ

Φάση 1: Παρουσίαση – Προετοιμασία του έργου

Η πρώτη φάση περιλαμβάνει την παρουσίαση του έργου και των επιμέρους φάσεων υλοποίησής τους στην Διοίκηση και τα βασικά στελέχη του Νοσοκομείου. Επιπλέον κατά τη φάση αυτή θα παρασχεθεί συμβουλευτική υποστήριξη για τον ορισμό της ομάδας από μέρους του Νοσοκομείου, που θα συμμετέχει στο σχεδιασμό και την υλοποίηση του Προγράμματος Προστασίας Προσωπικών Δεδομένων, στη διαχείριση της λογοδοσίας και τις διαδικασίες διαχείρισης των αναφορών.

Συγκεκριμένα, θα πρέπει να γίνουν οι παρακάτω ενέργειες: Παρουσίαση πρώτα στην Διοίκηση και στα βασικά στελέχη του Νοσοκομείου και έπειτα στους εργαζόμενους του Νοσοκομείου, των άρθρων και των απαιτήσεων του Κανονισμού. Στόχος είναι αρχικά η Διοίκηση και τα βασικά στελέχη και έπειτα οι εργαζόμενοι να ενημερωθούν πλήρως για τον Κανονισμό, τις απαιτήσεις του, τη μεθοδολογία και το χρονοπρογραμματισμό υλοποίησης της υπηρεσίας Εφαρμογής του Κανονισμού. Άλλωστε η εναρμόνιση με τον Κανονισμό δεν επιτυγχάνεται μόνο με τα τεχνολογικά και οργανωτικά μέτρα, αλλά πρωτίστως με την καλλιέργεια κουλτούρας για την προστασία των προσωπικών δεδομένων.

Προσδιορισμός όλων των ενδιαφερόμενων μερών, όσον αφορά στην Προστασία των Προσωπικών Δεδομένων. Καταγραφή των απαιτήσεών τους. Ορισμός της σύνθεσης και στελέχωσης της ομάδας που θα συμμετέχει στο σχεδιασμό και την υλοποίηση του Προγράμματος Προστασίας Προσωπικών Δεδομένων, στη διαχείριση της λογοδοσίας και τις διαδικασίες διαχείρισης των αναφορών. Αρχική παρουσίαση του Κανονισμού, των απαιτήσεών του, της μεθοδολογίας και του χρονοπρογραμματισμού υλοποίησης του έργου Εφαρμογής του Κανονισμού στην ομάδα.

Παραδοτέα φάσης 1:

Κατάθεση σχεδίου έργου

Αρχείο παρουσίασης της ενημέρωσης εφαρμογής του GDPR στην ορισμένη ομάδα εργασίας.

Φάση 2: Προσδιορισμός και Εκτίμηση της τρέχουσας κατάστασης σχετικά με τα προσωπικά δεδομένα – συλλογή Πληροφοριών.

Προκειμένου να αποτυπωθεί η τρέχουσα κατάσταση, απαιτείται να γίνει πλήρως κατανοητός ο κύκλος ζωής των προσωπικών δεδομένων στο Νοσοκομείο. Ο ανάδοχος θα πραγματοποιήσει πλήρη χαρτογράφηση των δεδομένων που θα περιλαμβάνει:

1. Στην καταγραφή των πληροφοριών σχετικά με τα δεδομένα προσωπικού χαρακτήρα που συλλέγουν και χρησιμοποιούν οι υπηρεσίες του Νοσοκομείου, καθώς και ο τρόπος χρήσης τους, ο τόπος αποθήκευσής τους, η ροή τους εντός και εκτός Νοσοκομείου καθώς και η πρόσβαση σε αυτά. Γενικά θα πρέπει να καταγραφούν λεπτομερείς πληροφορίες σχετικά με τη συλλογή, αποθήκευση, χρήση, μεταφορά, επεξεργασία και διάθεση δεδομένων σε συνεργασία με την ομάδα εργασίας. Η καταγραφή των πληροφοριών αφορά και σε έντυπα καθώς και ηλεκτρονικά μέσα στα οποία μπορούν να βρεθούν αρχεία προσωπικών δεδομένων.

2. Την παρουσίαση των παραπάνω δεδομένων σε μορφή πίνακα και σχεδιαστικών μοντέλων που να αποτυπώνουν με σαφήνεια την διακίνηση των προσωπικών δεδομένων στο Νοσοκομείο.

3. Την αρχική εκτίμηση της κατάστασης και των κινδύνων που σχετίζονται με τις απαιτήσεις του Κανονισμού, ώστε να αναζητηθούν οι βέλτιστες λύσεις συμμόρφωσης λαμβάνοντας υπόψη τόσο τις

ανάγκες του Νοσοκομείου όσο και το γεγονός ότι τα προσωπικά δεδομένα των ασθενών του Νοσοκομείου είναι ευαίσθητα προσωπικά δεδομένα και δημιουργούν λόγω της οργάνωσής τους διάφορα σημεία επεξεργασίας.

Επίσης, κατά τον έλεγχο, θα καταγραφούν πιθανά «κενά» συμμόρφωσης και θα προσδιοριστούν – αξιολογηθούν οι επιπτώσεις τους. Για την εύρυθμη και απρόσκοπτη λειτουργία του Νοσοκομείου, θα πρέπει να ληφθεί υπόψη από τον Ανάδοχο ότι θα πρέπει να γίνει αναλυτική καταγραφή όχι μόνο των δεδομένων αλλά και των αναγκών που καλύπτουν, ώστε να αναζητηθούν οι βέλτιστες λύσεις συμμόρφωσης. Τα αποτελέσματα θα τεκμηριωθούν και θα συζητηθούν με την ομάδα εργασίας στην οποία σε αυτή τη φάση θα γίνει και η εκπαίδευσή της στο νέο Κανονισμό και τις απαιτήσεις του.

Σε αυτή τη φάση ο ανάδοχος θα παραδώσει το σχέδιο καταγραφής του, το οποίο θα περιλαμβάνει τη μεθοδολογία και τα εργαλεία του. Οι πληροφορίες που θα συλλεχθούν θα πρέπει να καλύπτουν τις απαιτήσεις του άρθρου 30 του Κανονισμού. Επίσης σε αυτή τη φάση θα προσδιοριστούν όλοι οι διαφορετικοί τύποι προσωπικών δεδομένων που συλλέγει και επεξεργάζεται το Νοσοκομείο τα οποία στη συνέχεια θα κατηγοριοποιηθούν. Επιπλέον, θα προσδιοριστεί η προέλευσή τους και τα άτομα στα οποία κοινοποιούνται, ο τρόπος συλλογής και η συναίνεση, ο σκοπός της επεξεργασίας, ο χρόνος και ο «χώρος» αποθήκευσης, οι προσβάσεις και η διαγραφή.

Ο ανάδοχος στο τέλος της Φάσης 2, θα παραδώσει μια πρόταση που θα περιλαμβάνει:

Τις απαιτήσεις ως προς τη συμμόρφωση

Τις δράσεις που θα πρέπει να υλοποιηθούν

Τους άμεσα εμπλεκόμενους και πιθανούς νέους εμπλεκόμενους

Την εκτίμησή του ως προς το βαθμό και χρόνο υλοποίησης των απαιτήσεων

Παραδοτέα Φάσης 2:

Πρακτικό καταγραφής των δεδομένων και κατηγοριοποίησή τους

Έκθεση ανάλυσης κενών (Gap analysis)

Μελέτη εκτίμησης των επιπτώσεων (Privacy Impact Assessment)

Φάση 3 – Σχέδιο Δράσης – Παρουσίαση

Μετά την ανάλυση των κενών, ο Ανάδοχος θα πρέπει να προβεί σε κατάθεση αναλυτικού σχεδίου δράσης συμμόρφωσης προτείνοντας τα κατάλληλα μέτρα ανάλογα με το Τμήμα του Νοσοκομείου, με στόχο τη βέλτιστη κάλυψη των κενών. Ειδικότερα, θα αναπτύξει Πολιτική Προστασίας Προσωπικών Δεδομένων που θα επικεντρώνεται στον τρόπο με τον οποίο θα γίνεται η συλλογή, αποθήκευση, επεξεργασία και διαχείριση των προσωπικών δεδομένων, καθώς και η συναίνεση του υποκειμένου, το δικαίωμα να διαγραφεί (right to be forgotten), η καταγραφή και γνωστοποίηση παραβιάσεων (διαδικασία γνωστοποίησης της παραβίασης δεδομένων & σχέδιο απόκρισης σε περίπτωση συμβάντων) και των πολιτικών και διαδικασιών για ενημερώσεις, επιθεωρήσεις και συνεχή βελτίωση. Επίσης θα ενημερώσει

όλα τα εμπλεκόμενα μέρη για το σχέδιο δράσης και τις αλλαγές στις οποίες πρέπει να προβούν με στόχο τη λήψη αποφάσεων από τη Διοίκηση του Νοσοκομείου και την εμπέδωση των αλλαγών. Ο Ανάδοχος υποχρεούται να υλοποιήσει τα μέτρα που τον αφορούν και να παρέχει συμβουλευτικές υπηρεσίες για τις ενέργειες που θα υλοποιήσει το Νοσοκομείο. Για την κατάρτιση του Σχεδίου Δράσης συμμόρφωσης, ο Ανάδοχος θα πρέπει δώσει έμφαση και στους εξωτερικούς συνεργάτες (προμηθευτές, υπεργολάβους κ.α.). Θα αναπτυχθεί Πολιτική Συνεργατών, θα γίνει αξιολόγηση των υπαρχόντων συνεργατών και έλεγχος των υφιστάμενων συμβάσεων (όπου απαιτείται) και θα προστεθούν κατάλληλοι όροι στα Συμβόλαια, συμπεριλαμβανομένων των παρακάτω: Απαιτήσεις από τους συνεργάτες για την Προστασία των Προσωπικών Δεδομένων κατά την εκτέλεση συμβάσεων ή συμφωνιών, άρθρα για την αντιμετώπιση περιπτώσεων μη συμμόρφωσης με συμβάσεις και συμφωνίες ή τους όρους προστασίας προσωπικών δεδομένων που επιβάλλει ο GDPR κ.α.

Το Σχέδιο Δράσης θα παρουσιαστεί αρχικά στην Διοίκηση και στα βασικά στελέχη του Νοσοκομείου και κατόπιν σε διαδοχικές ημερίδες σε όλο το εμπλεκόμενο προσωπικό. Ο Ανάδοχος υποχρεούται να λάβει υπόψη του τις παρατηρήσεις που τυχόν θα κατατεθούν από τα στελέχη του Νοσοκομείου κατά τη διάρκεια των ημερίδων.

Παραδοτέα Φάσης 3:

Κατάθεση Αναλυτικού Σχεδίου Δράσης

Παρουσίαση του Σχεδίου Δράσης

Προγραμματισμός ενεργειών κάλυψης κενών και προτεινόμενες διαδικασίες συμμόρφωσης

Φάση 4 - Υλοποίηση των μέτρων και εκπαίδευση

Σε αυτή τη Φάση ο Ανάδοχος υποχρεούται να παρέχει εκπαίδευση στο προσωπικό του Νοσοκομείου που εμπλέκεται στην επεξεργασία των προσωπικών δεδομένων, την σύνταξη όλων των διαδικασιών και πολιτικών διασφάλισης των προσωπικών δεδομένων, την παροχή υπηρεσιών συμβούλου στην υλοποίηση των ενεργειών που θα πρέπει να προβεί το Νοσοκομείο, αλλά και να υλοποιήσει όλα τα μέτρα για τα οποία είναι υπεύθυνος αυτός.

Εκπαίδευση

Ο ανάδοχος υποχρεούται να εκπαιδεύσει το εμπλεκόμενο προσωπικό τόσο κατά τη διάρκεια της εργασίας του, όσο και να παράσχει μαζική εκπαίδευση για να δοθεί μια συνολική εικόνα του νέου τρόπου λειτουργίας. Επίσης υποχρεούται να διαθέσει και ενημερωτικό υλικό προσαρμοσμένο στις ανάγκες του προσωπικού.

Παραδοτέα Φάσης 4:

Τεκμηρίωση της υλοποίησης των ενεργειών του αναδόχου

Διαδικασίες και πολιτικές διασφάλισης των προσωπικών δεδομένων

Εκπαιδευτικό και ενημερωτικό υλικό

ΦΑΣΗ 5 – Εσωτερικός έλεγχος – συνεχής συμμόρφωση

Ο ανάδοχος στην πέμπτη φάση θα πρέπει να προβεί σε ένα τελικό έλεγχο όσον αφορά στις μεθόδους διατήρησης της συμμόρφωσης των εμπλεκομένων προκειμένου να ελεγχθεί το επίπεδο γνώσης και συμμόρφωσης των εργαζομένων. Θα επιθεωρηθούν όλοι οι εργαζόμενοι, οι χώροι εργασίας τους, τα σημεία αποθήκευσης των προσωπικών δεδομένων, έγγραφων και ηλεκτρονικών, η πρόσβαση σε αυτά, καθώς επίσης και οι συμφωνίες εμπιστευτικότητας που έχουν υπογραφεί, ώστε να επιβεβαιωθεί η διαφύλαξη της ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας των προσωπικών δεδομένων και των απαιτήσεων του GDPR. Επιπλέον, θα επιθεωρηθούν ο τρόπος επικοινωνίας με τους συνεργάτες, το είδος της πληροφορίας που ανταλλάσσεται (στην περίπτωση που ανταλλάσσονται προσωπικά δεδομένα) και η αποθήκευσή της. Σημαντικό στοιχείο ελέγχου είναι και οι Συμφωνίες Εμπιστευτικότητας και τα Συμβόλαια Συνεργασίας που έχουν υπογραφεί με τους εξωτερικούς συνεργάτες, καθώς και το είδος της εκπαίδευσης/ενημέρωσης που έχουν λάβει, όσον αφορά στην προστασία των προσωπικών δεδομένων. Ο ανάδοχος υποχρεούται να προβεί σε συμπληρωματικά μέτρα που τυχόν θα προκύψουν και στη συνέχεια να συντάξει μια τελική έκθεση με τα αποτελέσματα του ελέγχου του. Η έκθεσή του θα περιλαμβάνει τον τρόπο εκτέλεσης του εσωτερικού ελέγχου στον οποίο προέβη. Ολοκληρώνοντας το πρόγραμμα, θα σχεδιαστεί και θα παραδοθεί μια σφραγίδα για τη δέσμευση του Νοσοκομείου στην προστασία προσωπικών δεδομένων ή ενός σήματος αξιοπιστίας (trustmark) στην ιστοσελίδα του, για την ενίσχυση της εμπιστοσύνης των πολιτών.

Παραδοτέα Φάσης 5:

Έκθεση εσωτερικού ελέγχου

Επικαιροποιημένο σχέδιο δράσης

Παράδοση σφραγίδας – σήματος

IV. ΧΡΟΝΟΔΙΑΓΡΑΜΜΑ ΥΛΟΠΟΙΗΣΗΣ - ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ Χρονοδιάγραμμα Υλοποίησης

Σο έργο θα πρέπει να έχει ολοκληρωθεί συνολικά σε έξι (6) μήνες από την υπογραφή της σύμβασης.

Πιο αναλυτικά:

Οι Φάσεις 1 και 2 θα πρέπει να έχουν ολοκληρωθεί σε χρονικό διάστημα δύο (2) μηνών από την υπογραφή της σύμβασης

Η Φάση 3 σε χρονικό διάστημα δύο (2) μηνών από το τέλος της Φάσης 2

Οι Φάσεις 4 και 5 θα πρέπει να έχουν ολοκληρωθεί σε χρονικό διάστημα δύο (2) μηνών από το τέλος της Φάσης 3

Εμπιστευτικότητα

Κατά τη διάρκεια των υπηρεσιών ο Ανάδοχος απαιτείται να χειριστεί ευαίσθητα προσωπικά δεδομένα του Γ.Ν.Α. «ΛΑΪΚΟ». Θα πρέπει να εγγυάται την εχεμύθεια των αποτελεσμάτων, καθώς επίσης και όσων δεδομένων συλλεχθούν κατά την υλοποίηση της εργασίας, **μέσω Ειδικού Συμφωνητικού Εχεμύθειας και Εμπιστευτικότητας** που θα υπογραφεί με την έναρξη της εργασίας και θα καλύπτει όλα τα αποτελέσματα, καθώς και όλες τις πληροφορίες που πρέπει να ανακτηθούν κατά τη διάρκεια της εργασίας.

Αναλαμβάνει την ευθύνη για τη διασφάλιση της εμπιστευτικότητας των εμπλεκόμενων συμβούλων και τεχνικών, όσον αφορά τη μη διαρροή πληροφοριών του είδους, του βαθμού διεκπεραίωσης της εργασίας καθώς και τις λεπτομέρειες αυτού, σε οιοδήποτε άτομο ή ομάδα ατόμων. Αντιθέτως, θα τους επιτραπεί να απευθύνονται για θέματα σχετικά με την εργασία μόνο στα άτομα τα οποία, σαφώς αναφέρονται στο συμφωνητικό εμπιστευτικότητας ως σύνδεσμοι στην επικοινωνία μεταξύ των τεχνικών του αναδόχου και της διοίκησης.

VI. ΠΡΟΥΠΟΘΕΣΕΙΣ ΣΥΜΜΕΤΟΧΗΣ

Κάθε υποψήφιος πρέπει να διαθέτει, επί ποινή αποκλεισμού, τα κάτωθι:

Αποδεδειγμένη εξειδικευμένη επιστημονική γνώση και υπερδεκαετή εμπειρία σε έργα ασφάλειας πληροφοριακών συστημάτων και προστασίας δεδομένων.

Αποδεδειγμένη εξειδικευμένη επιστημονική γνώση και εμπειρία σε νομικά και τεχνικά θέματα προστασίας δεδομένων σε νοσοκομεία, διοικητικές δομές υγείας (πχ. υγειονομικές περιφέρειες) και φορείς κοινωνικής ασφάλισης (πχ. ασφαλιστικά ταμεία).

Εμπειρία στην προσαρμογή φορέων και οργανισμών στο ΓΚΠΣ, έχοντας εκτελέσει ή να εκτελεί τουλάχιστον 3 έργα που αφορούν το σύνολο του προγράμματος συμμόρφωσης GDPR σε εταιρείες ή οργανισμούς κατά τη διάρκεια της τελευταίας 2ετίας .

Η ομάδα έργου πρέπει να περιλαμβάνει, επί ποινή αποκλεισμού, εξειδικευμένα επιστημονικά στελέχη, ως εξής:

Έναν (1) Διευθυντή Έργου, με υπερδεκαετή και διακεκριμένη επιστημονική εξειδίκευση και εμπειρία σε ασφάλεια πληροφοριακών συστημάτων και προστασία δεδομένων, μεταξύ άλλων σε νοσοκομεία, διοικητικές δομές υγείας και φορείς κοινωνικής ασφάλισης.

Ένα (1) Νομικό Σύμβουλο, με υπερδεκαετή και διακεκριμένη επιστημονική εξειδίκευση και εμπειρία ειδικά σε προστασία δεδομένων και δικαίου πληροφορικής.

Τουλάχιστον τέσσερις (4) Ειδικούς Επιστήμονες, με μεταπτυχιακή ή διδακτορική επιστημονική εξειδίκευση σε γνωστική περιοχή της Πληροφορικής και εμπειρία σε θέματα ασφάλειας πληροφοριακών συστημάτων ή προστασίας δεδομένων, μεταξύ άλλων σε νοσοκομεία ή διοικητικές δομές υγείας ή φορείς κοινωνικής ασφάλισης.

Η προαναφερόμενη εμπειρία θα πρέπει να τεκμηριώνεται με αντίστοιχη σύμβαση έργου ή αντίστοιχες βεβαιώσεις καλής εκτέλεσης» .