ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΥΓΕΙΑΣ ΚΑΙ ΚΟΙΝΩΝΙΚΗΣ ΑΛΛΗΛΕΓΓΥΗΣ
ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΠΑΙΔΩΝ ΑΘΗΝΩΝ ΠΑΝ. ΚΑΙ ΑΓΛ. ΚΥΡΙΑΚΟΥ
Ν.Π.Δ.Δ.

Αθήνα: 05/02/2019
Αριθμ. Πρωτ.:

Ταχ. Διευθ.: Θηβών και Λεβαδείας, Τ.Κ. 115 27

ΠΡΟΣ :
ΤΜΗΜΑ ΠΡΟΜΗΘΕΙΩΝ

ΠΡΑΚΤΙΚΟ ΣΥΝΤΑΞΗΣ ΤΕΧΝΙΚΩΝ ΠΡΟΔΙΑΓΡΑΦΩΝ GDPR

Σήμερα, ημέρα Τρίτη 05/02/2019 οι παρακάτω, ήτοι:

1. ΚΟΛΛΙΑΣ ΑΛΕΞΙΟΣ ΤΕ ΔΙΟΙΚΗΣΗΣ ΜΟΝΑΔΩΝ ΥΓΕΙΑΣ
2. ΛΕΛΕΚΑΚΗΣ ΕΜΜΑΝΟΥΗΛ ΠΕ ΠΛΗΡΟΦΟΡΙΚΗΣ
3. ΠΗΓΗΣ ΝΙΚΟΛΑΟΣ ΔΕ Δ/ΚΟΥ – ΛΟΓ/ΚΟΥ

αποτελούντες μέλη της τριμελούς επιτροπής σύμφωνα με την 8955/29-05-18 ημερήσια απόφαση του νοσοκομείου, με την οποία ορίζονται για την σύνταξη των τεχνικών προδιαγραφών του Γενικού Κανονισμού για τα Προσωπικά Δεδομένα (**G**eneral **D**ata **P**rotection **R**egulation - **GDPR**) με σκοπό τη διενέργεια ανοικτού συνοπτικού διαγωνισμού, ολοκλήρωσαν τη επανασύνταξη των τεχνικών προδιαγραφών, καταλήγοντας στο συνημμένο κείμενο που επανυποβάλλεται.

Τα μέλη της Επιτροπής

1. ΚΟΛΛΙΑΣ ΑΛΕΞΙΟΣ ΤΕ ΔΙΟΙΚΗΣΗΣ ΜΟΝΑΔΩΝ ΥΓΕΙΑΣ

2. ΛΕΛΕΚΑΚΗΣ ΕΜΜΑΝΟΥΗΛ ΠΕ ΠΛΗΡΟΦΟΡΙΚΗΣ

3. ΠΗΓΗΣ ΝΙΚΟΛΑΟΣ ΔΕ Δ/ΚΟΥ – ΛΟΓ/ΚΟΥ

ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ

ΕΠΙΧΕΙΡΗΣΙΑΚΕΣ ΑΝΑΓΚΕΣ – ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ

ΠΑΡΟΧΗ ΣΥΜΒΟΥΛΕΥΤΙΚΩΝ ΥΠΗΡΕΣΙΩΝ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΟΝ ΓΕΝΙΚΟ ΚΑΝΟΝΙΣΜΟ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (GDPR)

1. Εισαγωγή – Πεδίο εφαρμογής έργου

Το Νοσοκομείο διατηρεί και επεξεργάζεται πληθώρα δεδομένων προσωπικού χαρακτήρα, καθώς και πληροφορίες σε ηλεκτρονικά ή/και φυσικά αρχεία, τα οποία μπορούν να ταυτοποιήσουν φυσικά πρόσωπα: ασθενείς, εργαζομένους, συνεργάτες, προμηθευτές, κ.α. Επιπλέον, η οργανωτική του δομή, απαιτεί την υποστήριξη των εσωτερικών αναγκών επικοινωνίας και διακίνησης εγγράφων. Οι εν λόγω ροές, αφενός θα πρέπει να καταγραφούν και να αποτυπωθούν σε ένα σχέδιο διασφάλισης για το Νοσοκομείο, αφετέρου θα πρέπει να ληφθεί υπόψη και η υποχρέωση του Νοσοκομείου να εναρμονιστεί στον Κανονισμό GDPR (General Data Protection Regulation) που πρέπει να εφαρμοσθεί σε όλους τους δημόσιους φορείς από τον Μάιο του 2018.

2. Αντικείμενο του έργου

Αντικείμενο του έργου αυτού θα είναι μία μελέτη ωριμότητας του Νοσοκομείου έναντι του κανονισμού GDPR, η οποία θα:

- αξιολογεί όλους τους τομείς δραστηριότητας του Νοσοκομείου και όλα τα τμήματα και τις διευθύνσεις ως προς την ετοιμότητά τους έναντι του GDPR.
- εντοπίζει όλες τις περιοχές, όπου δεν παρατηρείται πλήρης ετοιμότητα και απαιτούνται ενέργειες συμμόρφωσης.
- εμβαθύνει στις ανωτέρω περιοχές και θα προτείνει αναλυτικά μέτρα, ώστε το Νοσοκομείο να ξεκινήσει εγκαίρως την υλοποίηση όλων των διορθωτικών ενεργειών συμμόρφωσης.
- ανιχνεύει έγκαιρα κάθε περιστατικό παραβίασης και θα ενημερώνει το Νοσοκομείο.

3. Τεχνική Περιγραφή

Αναλυτικά το έργο θα περιλαμβάνει :

- Ανάλυση της τρέχουσας κατάστασης ως προς την προστασία των προσωπικών δεδομένων που περιλαμβάνει την αξιολόγηση των υφιστάμενων πρακτικών, των γραπτών πολιτικών και διαδικασιών, των πληροφοριακών συστημάτων και δικτυακών υποδομών, και κάθε στοιχείου που επηρεάζει την προστασία προσωπικών δεδομένων σε όλες τις δραστηριότητες, τα τμήματα, τα παραρτήματα και τις διευθύνσεις του Νοσοκομείου. Παράλληλα θα αξιολογηθεί η υφιστάμενη κατάσταση ως προς την ασφάλεια των πληροφοριών και την επιχειρησιακή συνέχεια που αποτελούν συστατικά της προστασίας των δεδομένων.
- Εύρεση κενών ως προς την ικανοποίηση των απαιτήσεων του κανονισμού (Gap Analysis), κατηγοριοποιημένα ανά θεματική περιοχή και κρισιμότητα.

- Για κάθε κενό που εντοπίζεται, καθορισμός των απαραίτητων ενεργειών αντιμετώπισης και δημιουργία ενός λεπτομερούς, προτεραιοποιημένου και ολοκληρωμένου πλάνου συμμόρφωσης (compliance plan and roadmap).
- Σύνταξη Μελέτης Εκτίμησης αντίκτυπου (Data Privacy Impac tAssessment) με βάση τη μεθοδολογία του ISO29134, την οδηγία του WP29 και τις υφιστάμενες οδηγίες των Ευρωπαϊκών Αρχών Προστασίας.
- Παροχή υπηρεσίας διαχείρισης απειλών 24x7x365 σε πραγματικό χρόνο από εξειδικευμένο Επιχειρησιακό Κέντρο Ασφάλειας (Security Operation Center) του Αναδόχου.

Η ανωτέρω αξιολόγηση θα περιλαμβάνει τουλάχιστον τα εξής:
- Αξιολόγηση της νομικής βάσης, στην οποία στηρίζεται η συλλογή του συνόλου των συλλεγόμενων προσωπικών δεδομένων, της παρεχόμενης συναίνεσης από τον εκάστοτε συμβαλλόμενο, των παρεχόμενων πληροφοριών κ.λπ.
- Αξιολόγηση δυνατότητας ικανοποίησης των δικαιωμάτων των φυσικών προσώπων
- Αξιολόγηση επαρκούς οργανωτικής δομής
- Αξιολόγηση συμβάσεων με τρίτους που εκτελούν επεξεργασία προσωπικών δεδομένων του οργανισμού
- Αξιολόγηση μηχανισμών ελέγχου και διασφάλισης της συμμόρφωσης
- Αξιολόγηση σχετικών γραπτών πολιτικών και διαδικασιών.

Με σκοπό την επιτυχή υλοποίηση των σκοπών του έργου ο υποψήφιος ανάδοχος είναι απαραίτητο να:
- Συμπεριλάβει ανάλυση της τρέχουσας κατάστασης των πληροφοριακών συστημάτων και δικτυακών υποδομών, των υφιστάμενων πολιτικών, διαδικασιών και πρακτικών, οι οποίες σχετίζονται με την ασφάλεια των πληροφοριών, την επιχειρησιακή συνέχεια και την προστασία των δεδομένων.
- Διεξάγει συνεντεύξεις με τα αρμόδια στελέχη από κάθε τμήμα του Νοσοκομείου καλύπτοντας κάθε δραστηριότητα.
- Διεξάγει λεπτομερή αξιολόγηση των επιπτώσεων στην προστασία δεδομένων, βάσει του προτύπου ISO29134, της κατευθυντήριας οδηγίας του WP29 και άλλων σχετικών διεθνών κατευθυντήριων γραμμών, οι οποίες αξιολογούν τους κινδύνους που σχετίζονται με θέματα ασφάλειας των πληροφοριών και τα νομικά ζητήματα προστασίας δεδομένων και δίνουν προτεραιότητα στα ευρήματα, ανάλογα με το επίπεδο κινδύνου.
- Δημιουργήσει λεπτομερές πλάνο ενεργειών αντιμετώπισης και διαχείρισης των ευρημάτων, έτσι ώστε οι επικεφαλής των αρμόδιων Κλινικών, Τμημάτων, Μονάδων να είναι σε θέση να εφαρμόσουν τις απαραίτητες ενέργειες.
- Πραγματοποιήσει έλεγχο σε όλες τις εμπλεκόμενες εφαρμογές λογισμικού, σε όλα τα αποθηκευτικά μέσα (ψηφιακά, έντυπα, κ.α) καθώς και να προτείνει με σαφήνεια τις απαιτούμενες αλλαγές και τροποποιήσεις βάσει του νέου κανονισμού. Η αξιολόγηση θα περιλαμβάνει την αξιολόγηση του συνόλου των συλλεγόμενων προσωπικών δεδομένων, της νομικής βάσης πάνω στην οποία στηρίζεται η συλλογή, της παρεχόμενης συναίνεσης από τον εκάστοτε συμβαλλόμενο των παρεχόμενων πληροφοριών κ.λπ.
- Παρέχει λίστα προτάσεων σχετικά με τις αναγκαίες δράσεις αντιμετώπισης (συμπεριλαμβανομένων και των προτεινόμενων τεχνολογικών λύσεων) για κάθε κενό ή έλλειψη που προκύπτει.
- Πραγματοποιήσει αξιολόγηση όλων των τύπων συμβάσεων του Νοσοκομείου με τρίτους (ιατρούς, παρόχους ιατρικών, ασφαλιστικών, ελεγκτικών και άλλων υπηρεσιών,

συνεργάτες και γενικότερα εκτελούντες την επεξεργασία), να εντοπίσει κενά και να προτείνει ενέργειες με σκοπό την προσαρμογή τους στον νέο κανονισμό.

- Πραγματοποιήσει αξιολόγηση όλων των πρακτικών που σχετίζονται με την επεξεργασία των προσωπικών δεδομένων και να παρέχει συγκεκριμένες και λεπτομερείς προτάσεις για δράσεις συμμόρφωσης με τον νέο κανονισμό.
- Παρέχει ένα λεπτομερές, προτεραιοποιημένο και ολοκληρωμένο πλάνο συμμόρφωσης
- Όλες οι προτεινόμενες ενέργειες συμμόρφωσης είναι απαραίτητο να καλύπτουν ολόκληρο τον κύκλο ζωής των προσωπικών δεδομένων (δηλ. συλλογή, καταγραφή, τροποποίηση / ενημέρωση, αποθήκευση, μεταφορά, διαγραφή / καταστροφή κ.λπ.).
- Διαθέτει την απαραίτητη υποδομή (προσωπικό, εξοπλισμό, διαδικασίες κ.λπ.) για την ανίχνευση κάθε περιστατικού παραβίασης μέσω του Διαδικτύου.

4. Φάσεις Έργου – Παραδοτέα

4.1. Φάση 1: Έναρξη έργου - Οργάνωση Δράσεων

- Παρουσίαση στη διοίκηση και τα στελέχη του Νοσοκομείου
- Υποβολή προτάσεων οργάνωσης της ομάδας έργου

Παραδοτέα

✓ Πλάνο υλοποίησης έργου (Περιγραφή του Έργου στην οποία περιγράφεται ο τρόπος προσέγγισης και εκτέλεσης του Έργου, συμπεριλαμβανομένης της σύνθεσης της Ομάδας Έργου, των επιμέρους καθηκόντων των προσώπων που θα την απαρτίζουν, των παραδοτέων και του χρονοδιαγράμματος)

✓ Πλάνο ποιότητας έργου

4.2. Φάση 2 - Συγκέντρωση Δεδομένων

- Επισκόπηση των επιχειρησιακών, τεχνικών και λειτουργικών διαδικασιών.
- Ανάπτυξη του αρχείου δραστηριοτήτων και πόρων επεξεργασίας για όλες τις κρίσιμες περιοχές επεξεργασίας.
- Συγκέντρωση των απαιτούμενων πληροφοριών για τη συλλογή και επεξεργασία των προσωπικών δεδομένων, μέσω της διενέργειας συνεντεύξεων με στελέχη όλων των τμημάτων, και των διευθύνσεων.
- Εντοπισμός των κρίσιμων αποκλίσεων έναντι των απαιτήσεων του Κανονισμού GDPR

Παραδοτέα :

✓ Αρχείο δραστηριοτήτων επεξεργασίας δεδομένων

4.3. Φάση 3 - Μελέτη Ανάλυσης Αποκλίσεων (Gap Analysis και Maturity Assessment)

- Μελέτη υφιστάμενης κατάστασης ως προς τη διαχείριση προσωπικών δεδομένων από:
  ✓ άποψης διαδικασιών

  ✓ νομικής άποψης

  ✓ άποψης ασφάλειας πληροφοριών

  ✓ τεχνολογικής άποψης

- Εντοπισμός μη συμμορφώσεων στις πρακτικές και διαδικασίες που εφαρμόζονται κατά τον χειρισμό των προσωπικών δεδομένων, ως προς:
  ✓ τις απαιτήσεις του GDPR

  ✓ του κανονιστικού πλαισίου του έργου, συμπεριλαμβανομένων σχετικών δικαστικών αποφάσεων

  ✓ των οδηγιών, κατευθύνσεων και αποφάσεων του WP29, της ΑΠΔΠΧ και των Ευρωπαϊκών Αρχών Προστασίας Δεδομένων

  ✓ τις απαιτήσεις του ISO27001, ISO27002 για την ασφάλεια πληροφοριών

- Μελέτη ως προς τις υφιστάμενες επεξεργασίες δεδομένων (και της διαβαθμίσεώς
- τους), καθώς και των συστημάτων πληροφορικής του Νοσοκομείου.
- Αναγνώριση των σχετικών απαιτήσεων του Γενικού Κανονισμού ως προς τις επιμέρους περιοχές επεξεργασίας προσωπικών δεδομένων.
- Μελέτη αποκλίσεων της υφιστάμενης κατάστασης του Νοσοκομείου σε σχέση με τις απαιτήσεις του Κανονισμού για κάθε επεξεργασία. Η μελέτη θα πρέπει να περιλαμβάνεις τουλάχιστον τις παρακάτω περιοχές:
  ✓ Απαιτήσεις ως προς την υποχρέωση τήρησης αρχείου δραστηριοτήτων,

  ✓ Συναίνεση,

  ✓ Συλλογή, Χρήση, Αποθήκευση,

  ✓ Διατήρηση δεδομένων/Καταστροφή,

  ✓ Δικαιώματα πρόσβασης, διόρθωσης, αλλαγής και διαγραφής,

  ✓ Κοινοποίηση σε Τρίτα Μέρη,

  ✓ Διαβίβαση σε τρίτες χώρες,

  ✓ Ασφάλεια επεξεργασίας προσωπικών δεδομένων,

  ✓ Έλεγχος και παρακολούθηση των οργανωτικών και τεχνολογικών μέτρων,

  ✓ Πόροι

  ✓ Γνωστοποίηση παραβίασης Προσωπικών Δεδομένων σε εποπτική αρχή ή/και στο υποκείμενο των δεδομένων.

- Καταγραφή των σχετικών ευρημάτων σε σχέση με το βαθμό ετοιμότητας του Οργανισμού και τις επιμέρους αποκλίσεις που παρουσιάζει σε σχέση με τις ανωτέρω απαιτήσεις.

Παραδοτέα

✓ Gap Analysis

4.4. Φάση 4 - Ανάπτυξη Σχεδίου Διορθωτικών Ενεργειών

- Καταγραφή αναλυτικού και σαφούς σχεδίου στο οποίο θα συμπεριλαμβάνονται οι προτάσεις στη βελτίωση ανά Τμήμα/Κλινική/Μονάδα του Νοσοκομείου, με σκοπό την αντιμετώπιση των ελλείψεων ή/και αποκλίσεων σε σχέση με τις απαιτήσεις του Κανονισμού και τις απαιτήσεις του ευρύτερου κανονιστικού πλαισίου και των προτύπων, όπως αναλύεται παραπάνω.
- Προσέγγιση και προσδιορισμός συγκεκριμένων εργασιών ώστε να βελτιωθεί κατά το δυνατόν συντομότερα το επίπεδο συμμόρφωσης.
- Κατάθεση προτάσεων για τη διατήρηση στο μέλλον ικανοποιητικού επίπεδου συμμόρφωσης με τις απαιτήσεις του Κανονισμού.
- Κατάθεση προτάσεων αναφορικά με την πραγματοποίηση συγκεκριμένων εργασιών, σχετικά με την τροποποίηση υφιστάμενων διαδικασιών, καθώς και το περιβάλλον λειτουργίας των πληροφοριακών συστημάτων, με σκοπό τη συμμόρφωση με τον Κανονισμό.

Παραδοτέα

✓ Compliance Plan που να συμπεριλαμβάνει προτάσεις αλλαγών

✓ Privacy Impact Assessment

4.5. Φάση 5 – Παροχή Υπηρεσίας Διαχείρισης Απειλών 24x7x365 σε πραγματικό χρόνο

- Ετήσια περιμετρική παρακολούθηση και διαχείριση περιστατικών παραβίασης σε πραγματικό χρόνο 24x7 με σκοπό τον εντοπισμό και την αναφορά των περιστατικών παραβίασης των προσωπικών δεδομένων στο Νοσοκομείο.
- Δημιουργία προσαρμοσμένων σεναρίων επίθεσης στα πληροφοριακά συστήματα του Νοσοκομείου βάση των οποίων θα εντοπίζονται τα περιστατικά παραβίασης από το Διαδίκτυο.
- Κάθε κρίσιμο περιστατικό θα πρέπει να αναφέρεται εντός 15 λεπτών.
- Ενημέρωση για κάθε Περιστατικό Ασφαλείας μέσω e-mail, SMS, τηλεφωνική κλήση. Για κάθε περιστατικό θα πρέπει τουλάχιστον να αναφέρεται η ώρα και ημερομηνία, η κρισιμότητα, οι ενέργειες εξάλειψης.
- Υπηρεσίες Forensics
- Threat Intelligence
- WebPortal στο οποίο θα αναφέρονται οι απαραίτητες πληροφορίες ανά περιστατικό.

Παραδοτέα

✓ Μηνιαία Αναφορά Περιστατικών Ασφαλείας

5. Ελάχιστες Προϋποθέσεις Συμμετοχής

Ο υποψήφιος Ανάδοχος θα πρέπει:

- Να έχει εμπειρία στην παροχή συμβουλευτικών υπηρεσιών στον τομέα της ασφάλειας πληροφοριών.
- Να διαθέτει σχετική προϋπηρεσία περιλαμβανομένης τυχόν έργων αξιολόγησης έναντι του κανονισμού GDPR στον κλάδο υπηρεσιών και ιδιαίτερα στον κλάδο υπηρεσιών Υγείας π.χ. Νοσοκομεία, (1 συναφές έργο).
- Να κατέχει Σύστημα Διαχείρισης της Ασφάλειας Πληροφοριών πιστοποιημένο κατά ISO/IEC 27001:2013.
- Να έχει και να διαχειρίζεται Επιχειρησιακό Κέντρο Ασφάλειας (Security Operation Center) με τουλάχιστον ένα (1)συναφές έργο στον χώρο της Υγείας.
- Να παρέχει υπηρεσίες DPO σε εταιρίες του χώρου της Υγείας.

6. Ομάδες και Συντελεστές Κριτηρίων Τεχνικής Αξιολόγησης

Η αξιολόγηση των προσφορών των υποψηφίων Αναδόχων, για την επιλογή του καταλληλότερου, θα γίνει με βάση τα ακόλουθα κριτήρια:

1.	**Κριτήρια**	Συντελεστής Βαρύτητας
1.1.	***Φάση 1: Έναρξη έργου - Οργάνωση δράσεων***	8%
1.2.	***Φάση 2 - Συγκέντρωση δεδομένων & Υλοποίηση Ροών Εργασίας***.	20%
1.3.	Φάση 3 - Μελέτη ανάλυσης αποκλίσεων (Gap Analysis και Maturity Assessment)	30%
1.4.	Φάση 4 - Ανάπτυξη σχεδίου διορθωτικών ενεργειών.	22%
1.5.	Φάση 5 – Παροχή υπηρεσίας διαχείρισης απειλών 24x7x365 σε πραγματικό χρόνο	20%