

Αναζήτηση

Σελίδα 1 / 1

Σύνολο: 1

Γραμμές ανά σελίδα: 50

Γ.Ν.Κ.Υ. ΝΕΑΠΟΛΕΩΣ<<ΔΙΑΔΥΝΑΚΕΙΟ>> ΤΠ για τον «Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR)»

19DIAB000005270

Στοιχεία Διαβούλευσης

Ανενεργή

Δημοσιεύθηκε 08/07/2019 Τελευταία ανανέωση

Σχόλια 3

Σχόλια

Όνομα **I SMART**

Email **info@ismart.gr**

Άρθρο **ΤΕΧΝΙΚΕΣ
ΠΡΟΔΙΑΓΡΑΦΕΣ ΓΙΑ
ΕΝΑΡΜΟΝΙΣΗ ΜΕ GDPR ΚΑΙ
DPO**

Ημ/νία **16/07/2019**

Αξιότιμοι, Στην εν λόγω επιστολή επισυνάπτονται οι προτεινόμενες Τεχνικές Προδιαγραφές για την υλοποίηση του έργου Συμμόρφωσης με τον GDPR. ΠΡΟΣΟΝΤΑ ΥΠΟΨΗΦΙΟΥ ΕΙΔΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ → Όλες οι προτάσεις είναι απαραίτητο να βασίζονται και να λαμβάνουν υπόψη εκτός από τον Κανονισμό Γενικής Προστασίας Δεδομένων (GDPR), το υφιστάμενο Ελληνικό Νομοθετικό Πλαίσιο (συμπεριλαμβανομένης της νομολογίας), τις κατευθυντήριες γραμμές για το GDPR που δημοσιεύονται από την Ομάδα Εργασίας για την Προστασία Δεδομένων του Άρθρου 29 (WP 29), τις κατευθυντήριες οδηγίες, γνωμοδοτήσεις και αποφάσεις της Ελληνικής Αρχής Προστασίας Προσωπικών Δεδομένων (καθώς και τις κατά περίπτωση κατευθυντήριες γραμμές ή αποφάσεις άλλων Ευρωπαϊκών Αρχών Προστασίας Προσωπικών Δεδομένων) και τις βέλτιστες πρακτικές σύμφωνα με τα διεθνή πρότυπα. → Ο υποψήφιος Ανάδοχος πρέπει να συμπεριλάβει στην προσφορά του ✓ Χρονοδιάγραμμα δραστηριοτήτων – προγραμματισμό φάσεων υλοποίησης έργου → Ο υποψήφιος Ανάδοχος θα πρέπει να έχει διεκπεραιώσει τουλάχιστον δύο (2) αντίστοιχα έργα σε Δημόσια Νοσοκομεία προκειμένου να διαθέτει αποδεδειγμένη εμπειρία ολοκλήρωσης έργων αξιολόγησης έναντι του κανονισμού GDPR. → Η Ομάδα Έργου του υποψηφίου Αναδόχου θα πρέπει να περιλαμβάνει έμπειρα στελέχη που έχουν εμπλακεί σε ολοκληρωμένα έργα GDPR και τα οποία θα καλύπτουν κατ' ελάχιστο τις ακόλουθες κατηγορίες: • Ένα (1) Νομικό Σύμβουλο, με επιστημονική εξειδίκευση και εμπειρία σε προστασία δεδομένων με αποδεδειγμένη εμπειρία σε Φορείς Υγείας • Ένα (1) Εξειδικευμένο Πιστοποιημένο Διαχειριστή Κινδύνων με εμπειρία συμβουλευτικών - ελεγκτικών έργων σε Φορείς Δημόσιας Υγείας για τουλάχιστον τρία έτη. • Ένα (1) μέλος της ομάδας με εξειδίκευση στις τεχνολογικές υποδομές, τις εφαρμογές πληροφορικής και την ασφάλεια πληροφοριακών συστημάτων (IT Auditor) με αποδεδειγμένη εμπειρία σε Φορείς Υγείας • Ένα (1) Πιστοποιημένο Εσωτερικό Ελεγκτή με αποδεδειγμένη εμπειρία σε Φορείς Δημόσιας Υγείας Για το λόγο αυτό, ο υποψήφιος Ανάδοχος θα πρέπει να προσκομίσει τα αντίστοιχα έγγραφα τεκμηρίωσης, επί ποινή αποκλεισμού. Το έργο θα εκπονηθεί σε συνεργασία με τα αρμόδια στελέχη της Επιτροπής Παρακολούθησης Έργου που θα συστήσει ο ΦΟΡΕΑΣ ΕΦΑΡΜΟΓΗΣ. Η προσφορά θα περιλαμβάνει περιγραφή της μεθοδολογίας υλοποίησης, καθώς και αναφορά στις τεχνικές θα χρησιμοποιηθούν για την παροχή των σχετικών υπηρεσιών. 1.ΑΝΤΙΚΕΙΜΕΝΟ Το Νοσοκομείο 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 είναι η

εναρμόνιση του Νοσοκομείου με τις απαιτήσεις Ευρωπαϊκού Κανονισμού Προστασίας Προσωπικών Δεδομένων ΕΕ 679/2016 (GDPR) 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 του στις απαιτήσεις του GDPR. Οι υπηρεσίες θα αφορούν 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 Αυξημένης Φροντίδας, Μονάδα Τεχνητού Νεφρού,), Διατομεακά Τμήματα, · Εργαστήρια του Εργαστηριακού Τομέα · Διοικητικές Υπηρεσίες, όπως Γραφείο Κίνησης, Λογιστήριο Ασθενών, Τμήμα Προσωπικού, Γραμματείες κλπ. · Τμήμα Πληροφορικής 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 και τα τμήματα του νοσοκομείου. · Ενημέρωση και συνεργασία (με συναντήσεις/συνεντεύξεις) με αρμόδια στελέχη Τμημάτων του Οργανισμού, καλύπτοντας κάθε μείζονα δραστηριότητα, τμήμα, εξωνοσοκομειακή δομή και γραφείο. · Δημιουργία λεπτομερών data flow maps ανά επιχειρησιακή μονάδα, τμήμα ή μείζονα κατηγορία προσωπικών δεδομένων, με σκοπό την επαρκή συμβατότητα με τις απαιτήσεις του GDPR, όπου θα απεικονίζονται όλες οι πληροφορίες σχετικά με τη διαχείριση των προσωπικών δεδομένων στο νοσοκομείο. Τα data flow maps θα καλύπτουν την απαίτηση του GDPR για το αρχείο δραστηριοτήτων επεξεργασίας δεδομένων και θα περιέχουν όλες τις επιπλέον απαραίτητες πληροφορίες, ώστε να απεικονίζεται πλήρως η τρέχουσα κατάσταση ως προς τη διαχείριση προσωπικών δεδομένων και να εντοπίζονται κενά ως προς τις απαιτήσεις του θεσμικού πλαισίου. · Εύρεση κενών ως προς την ικανοποίηση των απαιτήσεων του κανονισμού (Gap Analysis). · Ενδελεχή αξιολόγηση και σύνταξη μελέτης εκτίμησης αντικτύπου τυχόν συμβάντων παραβίασης της ιδιωτικότητας των προσωπικών δεδομένων (Data Privacy Impact Assessment). · Για κάθε κενό που εντοπίζεται, καθορισμός των απαραίτητων ενεργειών πρόληψης, αντιμετώπισης και δημιουργία ενός λεπτομερούς, προτεραιοποιημένου και ολοκληρωμένου πλάνου συμμόρφωσης (compliance plan and roadmap). · Αξιολόγηση των τρεχουσών πρακτικών επεξεργασίας προσωπικών δεδομένων και σύνταξη των απαραίτητων Πολιτικών και Διαδικασιών Προστασίας Προσωπικών Δεδομένων με βάση τα προτεινόμενα μέτρα του πλάνου συμμόρφωσης. Με σκοπό την επιτυχή υλοποίηση 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 και την προστασία των προσωπικών δεδομένων. · Διεξάγει συνεντεύξεις με τα αρμόδια στελέχη του νοσοκομείου καλύπτοντας κάθε δραστηριότητα αυτού. · Διεξάγει λεπτομερή αξιολόγηση των επιπτώσεων στην προστασία δεδομένων, 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 όλων των επιμέρους δραστηριοτήτων να είναι σε θέση να εφαρμόσουν τις απαραίτητες ενέργειες. · Παρέχει ένα λεπτομερές data flow map ανά επιχειρησιακή μονάδα, τμήμα ή ανά κατηγορία προσωπικών δεδομένων με σκοπό την πλήρη συμβατότητα με τις απαιτήσεις του κανονισμού GDPR σχετικά με τα αρχεία των δραστηριοτήτων επεξεργασίας. · Πραγματοποιήσει έλεγχο σε όλες τις εμπλεκόμενες εφαρμογές λογισμικού, σε όλα τα αποθηκευτικά μέσα (ψηφιακά, έντυπα, ηχητικά, κα) καθώς και να προτείνει με σαφήνεια τις απαιτούμενες αλλαγές και τροποποιήσεις βάσει του νέου κανονισμού. Η αξιολόγηση θα περιλαμβάνει το σύνολο 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. Ο Ανάδοχος του έργου θα 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 διαφορετικών τύπων συμβάσεων του νοσοκομείου με τρίτους, 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 το 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.) και να έχουν συμφωνηθεί με την ομάδα έργου και τους επιχειρησιακούς ιδιοκτήτες των δεδομένων του νοσοκομείου πριν την παράδοση του πλάνου συμμόρφωσης. · Να τηρεί τις αρχές εμπιστευτικότητας. Ο ανάδοχος οφείλει να αναλάβει 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. 2.ΦΑΣΕΙΣ ΕΡΓΟΥ – ΠΑΡΑΔΟΤΕΑ Φάση 1: Έναρξη Έργου - Οργάνωση Δράσεων · Πλήρης ενημέρωση της Διοίκησης και των στελεχών του Νοσοκομείου των άρθρων και των απαιτήσεων του κανονισμού. · Παρουσίαση στη Διοίκηση και τα στελέχη του νοσοκομείου του σχεδίου. · Υποβολή προτάσεων οργάνωσης της Ομάδας Έργου που θα συμμετάσχει στον Σχεδιασμό και την Υλοποίηση του Προγράμματος Προστασίας Προσωπικών Δεδομένων. 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). (ΠΕ 1.1) Φάση 2 - Συγκέντρωση δεδομένων & Υλοποίηση Ροών Εργασίας · Επισκόπηση των επιχειρησιακών, τεχνικών και λειτουργικών διαδικασιών. · Ανάπτυξη του αρχείου δραστηριοτήτων και πόρων επεξεργασίας του νοσοκομείου · Ανάπτυξη διαγραμμάτων ροής δεδομένων που θα αποτυπώνουν τις φάσεις του κύκλου ζωής των δεδομένων, από τη συλλογή, χρήση, αποθήκευση, μεταφορά μέχρι και την καταστροφή τους. · Συγκέντρωση των απαιτούμενων πληροφοριών για τη συλλογή και επεξεργασία των προσωπικών δεδομένων, μέσω της διενέργειας συνεντεύξεων με στελέχη όλων των εμπλεκόμενων τμημάτων του νοσοκομείου · Μελέτη και επισκόπηση δικτύου Παραδοτέα: · Διαγράμματα ροής δεδομένων (Data Flow Maps) που θα καλύπτουν την απαίτηση του GDPR για το αρχείο δραστηριοτήτων επεξεργασίας δεδομένων και θα περιέχουν όλες τις επιπλέον απαραίτητες πληροφορίες, ώστε να απεικονίζεται πλήρως η τρέχουσα κατάσταση ως προς τη διαχείριση προσωπικών δεδομένων. (ΠΕ 2.1) · Μελέτη αποτίμησης επικινδυνότητας (Risk Analysis) ώστε να εντοπίζονται κενά ως προς τις απαιτήσεις του θεσμικού πλαισίου (διαγράμματα ροής δεδομένων προσωπικού χαρακτήρα, με κρίσιμες πληροφορίες). (ΠΕ 2.2) Φάση 3 - Μελέτη ανάλυσης αποκλίσεων (Gap Analysis) 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. Μελέτη ως προς τις υφιστάμενες επεξεργασίες δεδομένων (και της διαβαθμίσεώς τους), καθώς και 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 περιλαμβάνει τουλάχιστον τις παρακάτω περιοχές: · Απαιτήσεις ως προς την υποχρέωση τήρησης αρχείου δραστηριοτήτων, · Συνείνηση, · Συλλογή, Χρήση, Αποθήκευση, · Διατήρηση δεδομένων/Καταστροφή, · Δικαιώματα πρόσβασης, διόρθωσης, αλλαγής, διαγραφής και λήθης, · 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. 8. Μελέτη αποτίμησης

επικινδυνότητας Καταγραφή των σχετικών ευρημάτων σε σχέση με το βαθμό ετοιμότητας του νοσοκομείου και τις επιμέρους αποκλίσεις που παρουσιάζει σε σχέση με τις ανωτέρω απαιτήσεις. Παραδοτέα 1. Gap Analysis (ΠΕ 3.1) Φάση 4 - Ανάπτυξη σχεδίου διορθωτικών ενεργειών Καταγραφή αναλυτικού και σαφούς σχεδίου στο οποίο θα συμπεριλαμβάνονται οι προτάσεις βελτίωσης 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, όπως αναλύεται παραπάνω. Προσέγγιση και προσδιορισμός συγκεκριμένων εργασιών ώστε να βελτιωθεί κατά το δυνατόν συντομότερα το επίπεδο συμμόρφωσης. 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: 1. . Μελέτη Εκτίμησης αντικτύπου (Data Privacy Impact Assessment) & Σχέδιο διαχείρισης Επικινδυνότητας (ΠΕ 4.1) 2. Σχέδιο Συμμόρφωσης (Compliance Plan) που να συμπεριλαμβάνει προτάσεις αλλαγών. (ΠΕ 4.2) Φάση 5 – Εκπαίδευση προσωπικού/ Εσωτερικός έλεγχος Η σωστή εκπαίδευση του προσωπικού είναι πολύ κρίσιμος παράγοντας για την επιτυχία του έργου. Οι εκπαιδευτικές ανάγκες είναι σύνθετες και πρέπει να αντιμετωπιστούν με πολλαπλούς τρόπους. Ο ανάδοχος θα πρέπει να καλύπτει τουλάχιστον τις εξής εκπαιδευτικές διαδικασίες: · Εκπαίδευση κατά την διάρκεια της εργασίας (on-the-job-training) για να εξηγηθεί σε κάθε ενδιαφερόμενο πώς θα συμμετέχει στις δραστηριότητες επεξεργασίας · Μαζική εκπαίδευση/παρουσίαση (δια ζώσης, ή τηλε-εκπαίδευση) για να δοθεί μια συνολική εικόνα του νέου τρόπου λειτουργίας πάνω στα προσωπικά δεδομένα · Ενημερωτικό υλικό σε ιστοσελίδες με στόχο την συνεχή χρήση από τους ενδιαφερόμενους και εκτός του Νοσοκομείου. Ο προγραμματισμός της μαζικής εκπαίδευσης θα γίνει σε συνεργασία με το Νοσοκομείο και θα αποφασιστεί κατά την φάση της υλοποίησης του σχεδίου δράσης. Ο Ανάδοχος σε αυτή τη φάση θα πρέπει να προβεί σε ένα τελικό έλεγχο όσον αφορά στις μεθόδους διατήρησης της συμμόρφωσης των εμπλεκόμενων 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. Παραδοτέα: 1. Εκπαίδευση προσωπικού (ΠΕ 5.1) 2. Εκπαιδευτικό και ενημερωτικό υλικό (ΠΕ 5.2) Φάση 6 – Υπεύθυνος Προστασίας Δεδομένων Μετά την ολοκλήρωση της διαδικασίας συμμόρφωσης του Νοσοκομείου με τον Ευρωπαϊκό Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR), έργο που θα πρέπει να παραδοθεί σε έξι (6) μήνες από την υπογραφή της σύμβασης, ο Ανάδοχος θα παρέχει στο Νοσοκομείο κατάλληλα καταρτισμένο και πιστοποιημένο άτομο προκειμένου να αναλάβει για ένα έτος τα καθήκοντα του Υπεύθυνου Προστασίας Δεδομένων (DPO). Ο DPO θα παρακολουθεί την εφαρμογή των Πολιτικών/Διαδικασιών Προστασίας Προσωπικών Δεδομένων που έχουν αναπτυχθεί για την συμμόρφωση του Νοσοκομείου με τον Κανονισμό. Επιπλέον θα αναθεωρεί και θα βελτιώνει τις Πολιτικές / Διαδικασίες όπου κρίνει απαραίτητο. Επίσης θα επικαιροποιεί τις εκτιμήσεις αντίκτυπου (DPIA) και θα δημιουργεί καινούριες για επεξεργασίες υψηλού ρίσκου. Ακόμα θα αναλαμβάνει την ενημέρωση του προσωπικού καθώς και τις εσωτερικές επιθεωρήσεις, με σκοπό την επίτευξη του βέλτιστου επιπέδου συμμόρφωσης.

Όνομα **ΚΟΥΤΟ**
ΥΠΗΣ
ΑΝΔΡΕΑΣ

Email **andreas.koutoupis**
@knr.gr

Άρθρο **Γ.Ν-Κ.Υ.**
ΝΕΑΠΟΛΕΩΣ <<ΔΙΑΛΥΝΑ
ΚΕΙΟ>> ΤΠ για τον
<<Γενικό Κανονισμό
Προστασίας Δεδομένων
(GDPR)>>

Ημ/νία **10/07/**
2019

Αξιότιμα μέλη της επιτροπής, Παρακάτω θα βρείτε τις προτεινόμενες τεχνικές προδιαγραφές της εταιρείας μας, προκειμένου η υπηρεσία να παρασχεθεί με την βέλτιστη ποιότητα από στελέχη που διαθέτουν τεχνική

επάρκεια και εξειδίκευση στο αντικείμενο της προστασίας των προσωπικών δεδομένων. • Ο υποψήφιος Ανάδοχος θα πρέπει να είναι πιστοποιημένος κατά τα πρότυπα ISO 27001:2013 και ISO 9001:2015. • Ο υποψήφιος Ανάδοχος θα πρέπει να διαθέτει εμπειρία στην παροχή συμβουλευτικών υπηρεσιών ελεγκτικής, οργάνωσης, εκπόνησης πολιτικών και βελτιστοποίησης επιχειρησιακών διαδικασιών. Επίσης θα πρέπει να διαθέτει αποδεδειγμένη εμπειρία στην ανάλυση και αξιολόγηση κινδύνων. Τουλάχιστον ο Υπεύθυνος έργου της ανάδοχης εταιρείας πρέπει να κατέχει πιστοποιήσεις σχετικές με τη διαχείριση κινδύνων και ανάλογη προϋπηρεσία σε αντίστοιχη θέση (risk officer). Όλα τα ανωτέρω να αποδεικνύονται με την επισύναψη των σχετικών εγγράφων. • Ο υποψήφιος Ανάδοχος θα πρέπει να έχει διεκπεραιώσει παρόμοια έργα στην Ελλάδα ή το εξωτερικό και να διαθέτει αποδεδειγμένη εμπειρία ολοκλήρωσης έργων αξιολόγησης έναντι του κανονισμού GDPR (τουλάχιστον 2 σε δημόσιες Μονάδες Υγείας). Ως εκ τούτου, θα πρέπει να περιέχεται στη προσφορά, λίστα με πληροφορίες για παρόμοια έργα υλοποίησης GDPR. • Η Ομάδα Έργου του υποψηφίου Αναδόχου θα πρέπει να περιλαμβάνει εμπειρία στελέχη που έχουν εμπλακεί σε ολοκληρωμένα έργα GDPR και τα οποία θα καλύπτουν κατ' ελάχιστο τις ακόλουθες κατηγορίες: ο Υπεύθυνος έργου με τουλάχιστον τριετή αποδεδειγμένη εμπειρία εκπαίδευσης σε δημόσιους φορείς καθώς και αποδεδειγμένη εμπειρία συμβουλευτικών - ελεγκτικών έργων σε Δημόσιους Φορείς Υγείας για τουλάχιστον τέσσερα έτη. Επιπλέον απαραίτητη προϋπόθεση είναι να είναι ορισμένος DPO σε έναν τουλάχιστον οργανισμό. ο Ένα (1) Πιστοποιημένο Εσωτερικό Ελεγκτή με αποδεδειγμένη εμπειρία σε έργα ελεγκτικά-συμβουλευτικά σε Δημόσιους Φορείς Υγείας άνω των τριών ετών. Επιπλέον απαραίτητη προϋπόθεση είναι να είναι ορισμένος DPO σε μια Δημόσια Μονάδα Υγείας. ο Ένα (1) Νομικό Σύμβουλο, με επιστημονική εξειδίκευση και εμπειρία σε προστασία δεδομένων (με σχετική πιστοποίηση). Επιπλέον απαραίτητη προϋπόθεση είναι να είναι ορισμένος DPO σε έναν τουλάχιστον οργανισμό. ο Ένα (1) μέλος της ομάδας με εξειδίκευση σε θέματα Πληροφορικής και εμπειρία σε θέματα ασφάλειας πληροφοριακών συστημάτων με τουλάχιστον 3ετή εμπειρία σε Φορείς Υγείας. Για το λόγο αυτό, ο υποψήφιος Ανάδοχος θα πρέπει να προσκομίσει, μαζί με την τεχνική του προσφορά, τα αναλυτικά βιογραφικά των στελεχών που θα απαρτίσουν την ομάδα έργου του και τα αντίστοιχα έγγραφα τεκμηρίωσης. • Το έργο θα εκπονηθεί σε συνεργασία με τα αρμόδια στελέχη της Επιτροπής Παρακολούθησης Έργου που θα συστήσει ο ΦΟΡΕΑΣ ΕΦΑΡΜΟΓΗΣ. Η προσφορά θα περιλαμβάνει περιγραφή της μεθοδολογίας υλοποίησης, καθώς και αναφορά στις τεχνικές θα χρησιμοποιηθούν για την παροχή των σχετικών υπηρεσιών. Επιπλέον αναφορικά με την Τεχνική Περιγραφή του έργου θα θέλαμε να σας προτείνουμε την ανάλυση του ως εξής: ΑΝΤΙΚΕΙΜΕΝΟ ΤΟΥ ΕΡΓΟΥ Το Γενικό Ογκολογικό Νοσοκομείο Κηφισιάς "Άγιοι Ανάργυροι" 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 Γενικού Ογκολογικού Νοσοκομείου Κηφισιάς "Άγιοι Ανάργυροι" 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 των Νοσοκομείων 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 των Νοσοκομείων, 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, Μονάδα Εγκαυμάτων), Διατομεακά Τμήματα κλπ. • Εργαστήρια του Εργαστηριακού Τομέα • Διοικητικές Υπηρεσίες, όπως Γραφείο Κίνησης, Λογιστήριο Ασθενών, Τμήμα Προσωπικού, Γραμματείες κλπ. • Τμήμα Πληροφορικής 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 και τα τμήματα του νοσοκομείου. • Ενημέρωση και συνεργασία (με συναντήσεις/συνεντεύξεις) με αρμόδια στελέχη Τμημάτων του Οργανισμού, καλύπτοντας κάθε μείζονα δραστηριότητα, τμήμα, εξωνοσοκομειακή δομή και γραφείο. • Δημιουργία λεπτομερών data flow maps ανά επιχειρησιακή μονάδα, τμήμα ή μείζονα κατηγορία προσωπικών δεδομένων, με σκοπό την επαρκή συμβατότητα με τις απαιτήσεις του ΓΚΠΔ, όπου θα απεικονίζονται όλες οι πληροφορίες σχετικά με τη διαχείριση των προσωπικών δεδομένων στο νοσοκομείο. Τα data flow maps θα καλύπτουν την απαίτηση του GDPR για το αρχείο δραστηριοτήτων επεξεργασίας δεδομένων και θα περιέχουν όλες τις επιπλέον απαραίτητες πληροφορίες, ώστε να απεικονίζεται πλήρως η τρέχουσα κατάσταση ως προς τη διαχείριση προσωπικών δεδομένων και να εντοπίζονται κενά ως προς τις απαιτήσεις του θεσμικού πλαισίου. • Εύρεση κενών ως προς την ικανοποίηση των απαιτήσεων του κανονισμού (Gap Analysis). • Ενδελεχή αξιολόγηση και σύνταξη μελέτης εκτίμησης αντικτύπου τυχόν συμβάντων παραβίασης της ιδιωτικότητας των προσωπικών δεδομένων (Data Privacy Impact Assessment). • Για κάθε κενό που εντοπίζεται, καθορισμός των απαραίτητων ενεργειών πρόληψης, αντιμετώπισης και δημιουργία ενός λεπτομερούς, προτεραιοποιημένου και ολοκληρωμένου πλάνου συμμόρφωσης (compliance plan and roadmap). • Αξιολόγηση των τρεχουσών πρακτικών επεξεργασίας προσωπικών δεδομένων και σύνταξη των απαραίτητων Πολιτικών και Διαδικασιών Προστασίας Προσωπικών Δεδομένων με βάση τα προτεινόμενα μέτρα του πλάνου συμμόρφωσης. Με σκοπό την επιτυχή υλοποίηση 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 και την προστασία των προσωπικών δεδομένων. • Διεξάγει συνεντεύξεις με τα αρμόδια στελέχη του νοσοκομείου καλύπτοντας κάθε δραστηριότητα αυτού. • Διεξάγει λεπτομερή αξιολόγηση των επιπτώσεων στην προστασία δεδομένων, 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 όλων των επιμέρους δραστηριοτήτων να είναι σε θέση να εφαρμόσουν τις απαραίτητες ενέργειες. • Παρέχει ένα λεπτομερές data flow map ανά επιχειρησιακή μονάδα, τμήμα ή ανά κατηγορία προσωπικών δεδομένων με σκοπό την πλήρη συμβατότητα με τις απαιτήσεις του κανονισμού GDPR σχετικά με τα αρχεία των δραστηριοτήτων επεξεργασίας. • Πραγματοποιήσει έλεγχο σε όλες τις εμπλεκόμενες εφαρμογές λογισμικού, σε όλα τα αποθηκευτικά μέσα (ψηφιακά, έντυπα, ηχητικά, κα) καθώς και να προτείνει με σαφήνεια τις απαιτούμενες αλλαγές και τροποποιήσεις βάσει του νέου κανονισμού. Η αξιολόγηση θα περιλαμβάνει το σύνολο 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. Ο Ανάδοχος του έργου θα 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 διαφορετικών τύπων συμβάσεων του νοσοκομείου με τρίτους, να εντοπίζει 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 το 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.) και να έχουν συμφωνηθεί με την ομάδα έργου και τους επιχειρησιακούς ιδιοκτήτες των δεδομένων του νοσοκομείου πριν την παράδοση του πλάνου συμμόρφωσης • Να τηρεί τις αρχές εμπιστευτικότητας. Ο ανάδοχος οφείλει να αναλάβει 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. 2. ΦΑΣΕΙΣ ΕΡΓΟΥ – ΠΑΡΑΔΟΤΕΑ Φάση 1: Έναρξη Έργου - Οργάνωση Δράσεων 1. Πλήρης ενημέρωση της Διοίκησης και των στελεχών των Νοσοκομείων των άρθρων και των απαιτήσεων του κανονισμού. 2. Παρουσίαση στη Διοίκηση και τα στελέχη των Νοσοκομείων του σχεδίου. 3. Υποβολή προτάσεων οργάνωσης της Ομάδας Έργου που θα συμμετάσχει στον Σχεδιασμό και την Υλοποίηση του Προγράμματος Προστασίας Προσωπικών Δεδομένων. Παραδοτέα 1. 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). (ΠΕ 1.1) Φάση 2 - Συγκέντρωση δεδομένων & Υλοποίηση Ροών Εργασίας 1. Επισκόπηση των επιχειρησιακών, τεχνικών και λειτουργικών διαδικασιών. 2. Ανάπτυξη του αρχείου δραστηριοτήτων και πόρων επεξεργασίας των Νοσοκομείων 3. Ανάπτυξη διαγραμμάτων ροής δεδομένων που θα αποτυπώνουν τις φάσεις του κύκλου ζωής των δεδομένων, από τη συλλογή, χρήση, αποθήκευση, μεταφορά μέχρι και την καταστροφή τους. 4. Συγκέντρωση των απαιτούμενων πληροφοριών για τη συλλογή και επεξεργασία των προσωπικών δεδομένων, μέσω της διενέργειας συνεντεύξεων με στελέχη όλων των εμπλεκόμενων τμημάτων του νοσοκομείου 5. Μελέτη και επισκόπηση δικτύου Παραδοτέα : 1. Διαγράμματα ροής δεδομένων (Data Flow Maps) που θα καλύπτουν την απαίτηση του GDPR για το αρχείο δραστηριοτήτων επεξεργασίας δεδομένων και θα περιέχουν όλες τις επιπλέον απαραίτητες πληροφορίες, ώστε να απεικονίζεται πλήρως η τρέχουσα κατάσταση ως προς τη διαχείριση προσωπικών δεδομένων. (ΠΕ 2.1) Φάση 3 - Μελέτη ανάλυσης αποκλίσεων (Gap Analysis) 1. Μελέτη υφιστάμενης κατάστασης ως προς τη διαχείριση προσωπικών δεδομένων από: • άποψης διαδικασιών. • νομικής άποψης. • άποψης ασφάλειας πληροφοριών. • τεχνολογικής άποψης. 2. Εντοπισμός μη συμμορφώσεων στις πρακτικές και διαδικασίες που εφαρμόζονται κατά τον χειρισμό των προσωπικών δεδομένων, ως προς τις απαιτήσεις του GDPR. 3. Μελέτη ως προς τις υφιστάμενες επεξεργασίες δεδομένων (και της διαβαθμίσεώς τους), καθώς και συστημάτων πληροφορικής του νοσοκομείου. 4. Αναγνώριση των σχετικών απαιτήσεων του Γενικού Κανονισμού ως προς τις επιμέρους περιοχές επεξεργασίας προσωπικών δεδομένων. 5. Μελέτη αποκλίσεων της υφιστάμενης κατάστασης του νοσοκομείου σε σχέση με τις απαιτήσεις του Κανονισμού για κάθε επεξεργασία. Η μελέτη θα πρέπει να περιλαμβάνει τουλάχιστον τις παρακάτω περιοχές: • Απαιτήσεις ως προς την υποχρέωση τήρησης αρχείου δραστηριοτήτων, • Συνείδηση, • Συλλογή, Χρήση, Αποθήκευση, • Διατήρηση δεδομένων/Καταστροφή, • Δικαιώματα πρόσβασης, διόρθωσης, αλλαγής, διαγραφής και λήθης, • 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. 6. Μελέτη αποτίμησης επικινδυνότητας 7. Καταγραφή των σχετικών ευρημάτων σε σχέση με το βαθμό ετοιμότητας των Νοσοκομείων και τις επιμέρους αποκλίσεις που παρουσιάζει σε σχέση με τις ανωτέρω απαιτήσεις. Παραδοτέα 1. Gap Analysis (ΠΕ 3.1) Φάση 4 - Ανάπτυξη σχεδίου διορθωτικών ενεργειών 1. Καταγραφή αναλυτικού και σαφούς σχεδίου στο οποίο θα συμπεριλαμβάνονται οι προτάσεις βελτίωσης 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, όπως αναλύεται παραπάνω. 2. Προσέγγιση και προσδιορισμός συγκεκριμένων εργασιών ώστε να βελτιωθεί κατά το δυνατόν συντομότερα το επίπεδο συμμόρφωσης. 3. 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 1. Σχέδιο Συμμόρφωσης (Compliance Plan) που να συμπεριλαμβάνει προτάσεις αλλαγών. (ΠΕ 4.1) 2. Μελέτη Εκτίμησης αντικτύπου (Data Privacy Impact Assessment). (ΠΕ 4.2) Φάση 5 – Εκπαίδευση προσωπικού/ Εσωτερικός έλεγχος 1. Η σωστή εκπαίδευση του προσωπικού είναι πολύ κρίσιμος παράγοντας για την επιτυχία του έργου. Οι εκπαιδευτικές ανάγκες είναι σύνθετες και πρέπει να αντιμετωπιστούν με πολλαπλούς τρόπους. Ο ανάδοχος θα πρέπει να καλύπτει τουλάχιστον τις εξής εκπαιδευτικές διαδικασίες: • Εκπαίδευση

κατά την διάρκεια της εργασίας (on-the-job-training) για να εξηγηθεί σε κάθε ενδιαφερόμενο πώς θα συμμετέχει στις δραστηριότητες επεξεργασίας • Μαζική εκπαίδευση/παρουσίαση (δια ζώσης, ή τηλε-εκπαίδευση) για να δοθεί μια συνολική εικόνα του νέου τρόπου λειτουργίας πάνω στα προσωπικά δεδομένα • Ενημερωτικό υλικό σε ιστοσελίδες με στόχο την συνεχή χρήση από τους ενδιαφερόμενους και εκτός των Νοσοκομείων Ο προγραμματισμός της μαζικής εκπαίδευσης θα γίνει σε συνεργασία με τους φορείς και θα αποφασιστεί κατά την φάση της υλοποίησης του σχεδίου δράσης. Ο Ανάδοχος σε αυτή τη φάση θα πρέπει να προβεί σε ένα τελικό έλεγχο όσον αφορά στις μεθόδους διατήρησης της συμμόρφωσης των εμπλεκόμενων 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. Παραδοτέα 1. Εκπαίδευση στο προσωπικό του ιδρύματος (ΠΕ 5.1) 2. Εκπαιδευτικό και ενημερωτικό υλικό (ΠΕ 5.2) 3. Πολιτικές και διαδικασίες προστασίας προσωπικών δεδομένων. (ΠΕ 5.3) ΥΠΗΡΕΣΙΕΣ ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ Με την υπογραφή της σύμβασης, ξεκινάει η περίοδος υποστήριξης του συνόλου των διαδικασιών στο πλαίσιο εφαρμογής του GDPR, η οποία θα έχει χρονική διάρκεια ίση με 1 έτος. Τα βασικά πακέτα εργασιών που θα περιλαμβάνουν οι υπηρεσίες υποστήριξης είναι τα ακόλουθα: • Πλήρεις και ολοκληρωμένες υπηρεσίες ΥΠΔ (DPO): Θα ορίσει ο υποψήφιος ανάδοχος τον (εξωτερικό) ΥΠΔ ο οποίος θα συμμετέχει/συντονίζει τις εργασίες της ομάδας των ΥΠΔ του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ. • Επιπρόσθετες υπηρεσίες συμμόρφωσης και εναρμόνισης με το GDPR: Οι υπηρεσίες αυτές περιλαμβάνουν το σύνολο των εργασιών τις οποίες ο υποψήφιος ανάδοχος απαιτείται να παράσχει, για να αντιμετωπιστούν όλες οι οργανωτικές αλλαγές που πρόκειται να λάβουν χώρα κατά την περίοδο υποστήριξης. Με εκτίμηση, Ανδρέας Κουτούπης

Όνομα **NIMD**
A
DYNAMICS

Email info@nimdynamics.com

Άρθρο **ΔΙΑΒΟΥΛΕΥΣ**
Η ΤΕΧΝΙΚΩΝ
ΠΡΟΔΙΑΓΡΑΦΩΝ

Ημ/via **15/07/20**
19

Πρόταση Τεχνικών Προδιαγραφών για την Ανάδειξη Παρόχου Συμβουλευτικών Υπηρεσιών για την εφαρμογή του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων 679/2016 (GDPR), με παράλληλη παροχή υπηρεσιών Υπευθύνου Προστασίας Δεδομένων (DPO) Αναλυτικά, το έργο θα περιλαμβάνει: • Αποτύπωση της υπάρχουσας κατάστασης, ως προς την επεξεργασία δεδομένων που λαμβάνει χώρα στο φορέα, τα είδη των δεδομένων και των υποκειμένων τους, τις ροές των δεδομένων, τις υφιστάμενες πρακτικές, διαδικασίες και πολιτικές του φορέα, τη δυναμική των φυσικών πόρων του φορέα, τη δυναμική των τεχνικών πόρων του φορέα και τα εφαρμοζόμενα μέτρα προστασίας. • Σύνταξη έκθεσης, η οποία - λαμβάνοντας υπόψη τα αποτελέσματα της αποτύπωσης της κατάστασης - θα προτείνει εξατομικευμένο σχέδιο συμμόρφωσης, όπου θα περιγράφονται τα προτεινόμενα μέτρα προς συμμόρφωση με τον Κανονισμό, οι διορθωτικές κινήσεις που πρέπει να γίνουν, τα σημεία αναπροσαρμογής, οι νέες εφαρμοστέες διαδικασίες, η ενίσχυση με περαιτέρω τεχνικά ή οργανωτικά μέτρα, οι τρόποι υλοποίησης, τα χρονοδιαγράμματα και πιθανές εναλλακτικές. • Υλοποίηση των παραπάνω διορθωτικών ενεργειών και εφόσον απαιτείται διενέργεια Privacy Impact Assessment με βάση τις έγκυρες πρακτικές – μεθοδολογίες και υλοποίηση των οργανωτικών - τεχνικών μέτρων που θα προταθούν. • Υλοποίηση δράσεων εκπαίδευσης – ευαισθητοποίησης και σύνταξη ειδικού ενημερωτικού, περιληπτικού και σαφούς εγχειριδίου με τα βασικά στοιχεία του ΓΚΠΔ και τα σημεία που χρήζουν ιδιαίτερης προσοχής ανά κατηγορία προσωπικού. • Υπηρεσίες του Υπευθύνου Προστασίας Δεδομένων (DPO) μέχρι την ολοκλήρωση του έργου. Η παροχή των παραπάνω υπηρεσιών, θα πραγματοποιηθεί βασισμένη σε δοκιμασμένες διαδικασίες και τεχνικές, και με τον ακριβή καθορισμό παραδοτέων και χρονοδιαγραμμάτων που θα διασφαλίσουν το άρτιο αποτέλεσμα. Οι μελέτες που

θα διενεργηθούν στο πλαίσιο του έργου θα καταγράψουν τις απαιτήσεις συμμόρφωσης που αρμόζουν στον οργανισμό, θα αναδείξουν τις παρούσες παθογένειες των υφιστάμενων υπηρεσιών – υποδομών – πρακτικών και θα προσδιορίσουν τις ευρέως καταξιωμένες βέλτιστες πρακτικές για την πρόληψη, αποτροπή και αντιμετώπιση παραβιάσεων ασφάλειας. ΔΙΑΡΚΕΙΑ ΕΡΓΟΥ Το έργο έχει συνολική διάρκεια ένα (1) χρόνο και χωρίζεται σε τέσσερις (4) φάσεις διάρκειας έξι (6) μηνών από την υπογραφή της σύμβασης και στην Φάση 5 που αφορά τις υποστηρικτικές υπηρεσίες διάρκειας έξι (6) μηνών. ΦΑΣΗ 1: Αποτύπωση της υπάρχουσας κατάστασης ΦΑΣΗ 2: Μελέτη ανάλυσης Ελλείψεων και Αποκλίσεων (Gap Analysis) ΦΑΣΗ 3: Διενέργεια Privacy Impact Assessment και υλοποίηση διορθωτικών ενεργειών ΦΑΣΗ 4: Εκπαίδευση – ευαισθητοποίηση προσωπικού ΦΑΣΗ 5: Υπηρεσίες Υποστήριξης ΦΑΣΗ 1: Αποτύπωση της υπάρχουσας κατάστασης 1. Δέσμευση της Διοίκησης: Στο στάδιο αυτό, παρουσιάζονται στον Φορέα οι απαιτήσεις του Κανονισμού και οι ενέργειες προς τη συμμόρφωση, τα χρονοδιαγράμματα και προσδιορίζονται οι πόροι και οι προσπάθειες που θα παρασχεθούν στην ομάδα έργου. Εν συνεχεία πραγματοποιείται η δέσμευση του φορέα με τη δρομολόγηση και την προετοιμασία των αποφάσεων που θα κοινοποιηθούν στο προσωπικό. Παραδοτέο: • Απόφαση δέσμευση του Νοσοκομείου και ενημέρωσης του προσωπικού – εξουσιοδοτήσεις πρόσβασης. 2.1 Ορισμός υπευθύνων ανά τμήμα: Γίνεται ορισμός και καταγραφή των ανά τμήμα και ανά αρχείο δεδομένων υπευθύνων. Η καταγραφή αυτή αποτυπώνεται στο Μητρώο Επεξεργασιών Δεδομένων. 2.2 Καταγραφή διαθέσιμων φυσικών πόρων: Καταγραφή των διαθέσιμων πόρων (ανθρώπων ανά τμήμα), που τίθενται στην διάθεση του Υπεύθυνου Προστασίας Δεδομένων για την περάτωση των εργασιών, προς την επίτευξη συμμόρφωσης και δημιουργία ομάδας εργασίας, με ανάθεση ρόλων και αρμοδιοτήτων, κατόπιν συναξιολόγησης με τους υπευθύνους των Τμημάτων. Η ομάδα εργασίας πρέπει να είναι αντιπροσωπευτική και να καλύπτει όλα τα Τμήματα του φορέα και τις μορφές της επεξεργασίας προσωπικών δεδομένων. Παραδοτέο: • Έγγραφο αναφορά με τα μέλη της ομάδας εργασίας και προσδιορισμός αρμοδιοτήτων και υποχρεώσεων. 3. Καταγραφή και χαρτογράφηση των Δεδομένων Προσωπικού Χαρακτήρα, που τηρούνται από τον Φορέα, της επεξεργασίας και της κυκλοφορίας τους. Στο στάδιο αυτό, γίνεται καταγραφή, ανά επεξεργασία και ανά αρχείο δεδομένων, του είδους των δεδομένων που τηρούνται, των υποκειμένων, των ρόλων και περιλαμβάνονται όλες οι απαραίτητες πληροφορίες που απαιτεί ο Κανονισμός στα πλαίσια της υποχρέωσης για τήρηση αρχείου επεξεργασίας, ώστε να αποτυπώνεται πλήρως η κατάσταση επί της διαχείρισης των προσωπικών δεδομένων. Στο πλαίσιο αυτό καθορίζονται τα είδη της επεξεργασίας που πραγματοποιεί ο φορέας, τα δεδομένα που αφορούν κάθε είδος επεξεργασίας, τα υποκείμενα που αφορούν κάθε είδος επεξεργασίας, ο σκοπός και η νομική βάση της επεξεργασίας, οι πηγές προέλευσης των δεδομένων, ο χρόνος τήρησης των δεδομένων, ο τόπος (φυσικός ή ηλεκτρονικός) τήρησης των δεδομένων, τα τεχνικά και οργανωτικά μέτρα (επιγραμματικά) και οι πιθανές διαβιβάσεις ή αναθέσεις σε τρίτους μέρους της επεξεργασίας. Παραδοτέο : • Μητρώο Επεξεργασιών Δεδομένων. ΦΑΣΗ 2: Μελέτη ανάλυσης Ελλείψεων και Αποκλίσεων (Gap Analysis) 4.1 Έλεγχος και αξιολόγηση πολιτικών και διαδικασιών. Στο στάδιο αυτό ελέγχονται οι πολιτικές, τα τεχνικά και τα οργανωτικά μέτρα του οργανισμού, ως προς την επάρκειά τους για τον Κανονισμό. Ελέγχεται και αξιολογείται αν υπάρχει πολιτική ασφαλείας που προβλέπει διαδικασίες και δυνατότητα ικανοποίησης των δικαιωμάτων των υποκειμένων, διαδικασίες για την άμεση και εντός των προβλεπόμενων χρονοδιαγραμμάτων ανταπόκριση σε αιτήματα των υποκειμένων, λήψης συγκατάθεσης των υποκειμένων, εκπαίδευση και δημιουργία κουλτούρας στο ανθρώπινο δυναμικό. Ελέγχεται αν υπάρχει επαρκές σχέδιο επιχειρησιακής συνέχειας και ανταπόκρισης σε περιστατικά παραβίασης καθώς και αν προβλέπονται μηχανισμοί ανίχνευσης περιστατικών παραβίασης. Ελέγχεται αν υπάρχουν διαδικασίες, γίνεται αξιολόγηση των διαδικασιών, της τήρησής τους, της εμπέδωσής τους από το προσωπικό σε σχέση με την πολιτική προστασίας προσωπικών δεδομένων. 4.2 Έλεγχος Συμβάσεων. Ελέγχονται οι συμβάσεις του οργανισμού με τρίτους των οποίων προσωπικά δεδομένα επεξεργάζεται ή οι οποίοι επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του, όσο και με τρίτους στους οποίους διαβιβάζονται δεδομένα προσωπικού χαρακτήρα. 4.3 Σύμβαση έκθεσης αποκλίσεων-κατάρτιση σχεδίου συμμόρφωσης Έκθεση

αποκλίσεων Με την ολοκλήρωση των ανωτέρω σταδίων, αξιολογούνται οι υφιστάμενες διαδικασίες και πολιτικές σε συνάρτηση με το νέο νομικό πλαίσιο για την προστασία των δεδομένων προσωπικού χαρακτήρα. Εντοπίζονται οι αποκλίσεις των υπαρχουσών πρακτικών και πολιτικών με το νέο νομικό πλαίσιο. Προτεινόμενα μέτρα - Κατάρτιση σχεδίου συμμόρφωσης Παράλληλα με την έκθεση αποκλίσεων, σχεδιάζεται λεπτομερές και ολοκληρωμένο πλάνο συμμόρφωσης του οργανισμού με τις επιταγές του Κανονισμού. Βάσει των αποτελεσμάτων της έκθεσης αποκλίσεων, προτείνονται πιθανές συμπληρώσεις, αλλαγές ή νέα μέτρα. Οι προτεινόμενες ενέργειες θα καλύπτουν όλο το φάσμα των επεξεργασιών που γίνονται και όλο τον κύκλο ζωής των προσωπικών δεδομένων που αποτελούν αντικείμενο επεξεργασίας. Ο σχεδιασμός θα γίνει από την ομάδα έργου, σύμφωνα με τα ευρήματα του σταδίου της αποτύπωσης και πάντα σύμφωνα με τη φιλοσοφία του οργανισμού και των ανθρώπων του. Παραδοτέο: • Έκθεση Αποκλίσεων και σχέδιο συμμόρφωσης, το οποίο περιλαμβάνει όλα τα Οργανωτικά μέτρα, που θα πρέπει να λάβει ο Οργανισμός για να συμμορφωθεί με τις απαιτήσεις του Κανονισμού, όλες τις συμπληρώσεις ή προσαρμογές που πρέπει να κάνει σε σχέση με τα υπάρχοντα μέτρα, όπου χρειάζεται, γίνεται αναμόρφωση των συμβάσεων με τρίτους, με βάση τις απαιτήσεις του Κανονισμού, όπου δεν υπάρχουν συμβάσεις συγγράφονται νέες και δημιουργούνται πρότυπα συμβάσεων για μελλοντική χρήση. ΦΑΣΗ 3: Διενέργεια Privacy Impact Assessment και υλοποίηση διορθωτικών ενεργειών 5. Συγγραφή πολιτικής προστασίας δεδομένων Η Πολιτική Προστασίας Δεδομένων σκοπό έχει να περιγράψει τις διαδικασίες και της πρακτικές που εφαρμόζει ο οργανισμός για την προστασία των προσωπικών δεδομένων που διαχειρίζεται. Περιλαμβάνει, ενδεικτικά, διαδικασίες για την προστασία των δεδομένων των εργαζομένων και συναλλασσόμενων, την προστασία των δεδομένων των ανηλίκων, τη διατήρηση της ποιότητας των δεδομένων, τον αποχαρακτηρισμό προσωπικών δεδομένων (ψευδωνυμοποίηση / ανωνυμοποίηση), τον διαρκή έλεγχο συμμόρφωσης κλπ. Παραδοτέο Π5: • Πολιτική Προστασίας Δεδομένων, συμπεριλαμβανομένων, ενδεικτικά, διαδικασιών για την προστασία των δεδομένων των εργαζομένων και συναλλασσόμενων, την προστασία των δεδομένων των ανηλίκων, τη διατήρηση της ποιότητας των δεδομένων, τον αποχαρακτηρισμό προσωπικών δεδομένων (ψευδωνυμοποίηση / ανωνυμοποίηση), τον διαρκή έλεγχο συμμόρφωσης κλπ 6. Συγγραφή πρότυπων ρητρών ή/και συμβάσεων Θα αναπτυχθούν και θα εφαρμοσθούν πρότυπες ρήτρες ή/και πρότυπες συμβάσεις, κατά περίπτωση, οι οποίες θα χρησιμοποιούνται από τον οργανισμό στις σχέσεις του με τρίτους των οποίων προσωπικά δεδομένα επεξεργάζεται ή οι οποίοι επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του, όσο και με τρίτους στους οποίους διαβιβάζονται δεδομένα προσωπικού χαρακτήρα. Παραδοτέο: • Πρότυπες ρήτρες ή/και συμβάσεις κατά περίπτωση για την προστασία των προσωπικών δεδομένων που διαχειρίζεται ο οργανισμός 7. Συγγραφή εγγράφων ενημέρωσης Όπου απαιτείται βάσει της καταγραφής των δραστηριοτήτων επεξεργασίας, θα συνταχθούν και θα παραδοθούν στον οργανισμό έγγραφα ενημέρωσης των υποκειμένων των δεδομένων, τα οποία θα πληρούν τους όρους συμμόρφωσης του νέου νομικού πλαισίου για την προστασία των προσωπικών δεδομένων. Παραδοτέο : • Έγγραφα ενημέρωσης των υποκειμένων των δεδομένων (άδειες, βεβαιώσεις, εργαζόμενοι, συναλλασσόμενοι κτλ.) 8. Συγγραφή εγγράφων συγκατάθεσης Κατόπιν της ολοκλήρωσης της καταγραφής των δραστηριοτήτων επεξεργασίας του οργανισμού και, εφόσον παρατηρηθεί ότι υφίστανται επεξεργασίες με νομική βάση τη συγκατάθεση των υποκειμένων των δεδομένων, θα συνταχθούν και θα παραδοθούν στον οργανισμό έγγραφα συγκατάθεσης, τα οποία θα πληρούν τους όρους συμμόρφωσης του νέου νομικού πλαισίου για την προστασία των προσωπικών δεδομένων. Παραδοτέο Π8 (εφόσον προκύψει τέτοια ανάγκη μετά την ολοκλήρωση της καταγραφής των δραστηριοτήτων επεξεργασίας του οργανισμού): • Έγγραφα συγκατάθεσης των υποκειμένων των δεδομένων 9. Κατάρτιση διαδικασίας διαχείρισης αιτημάτων των υποκειμένων των δεδομένων Θα καταρτισθεί διαδικασία διαχείρισης αιτημάτων των υποκειμένων των δεδομένων με σκοπό την κατάλληλη προετοιμασία του οργανισμού για να ανταποκρίνεται σε αιτήματα που ενδέχεται να προβάλλουν τα υποκείμενα των δεδομένων και σχετίζονται με τα δικαιώματα που τους απονέμει το νέο νομικό πλαίσιο για την προστασία των δεδομένων (πρόσβαση, διόρθωση, δικαίωμα διαγραφής, περιορισμός, φορητότητα, εναντίωση, αίτημα ανθρωπίνης παρέμβασης). Εκτός από την διαδικασία

διαχείρισης αιτημάτων, θα καταρτισθεί ειδική φόρμα υποβολή αιτημάτων των υποκειμένων των δεδομένων καθώς και υποδείγματα απαντήσεων των εν λόγω αιτημάτων για την ενημέρωση και κατάλληλη προετοιμασία των στελεχών του οργανισμού. Παραδοτέο : • Διαδικασία διαχείρισης αιτημάτων των υποκειμένων των δεδομένων • Φόρμα υποβολής αιτήματος υποκειμένου των δεδομένων • Υποδείγματα απαντήσεων σε αιτήματα υποκειμένων των δεδομένων 10. Διενέργεια Εκτίμησης Αντικτύπου για προστασία των Προσωπικών Δεδομένων (DPIA) Θα προδιαγραφεί και θα εφαρμοστεί μία διαδικασία εκτίμησης αντικτύπου (DataProtection- ή Privacy ImpactAssessment) σε όποιες επεξεργασίες δεδομένων αυτό χρειάζεται και τα αποτελέσματα θα αποτυπωθούν σε έκθεση αξιολόγησης. Ο σκοπός είναι να αναδειχθεί το αντίκτυπο που ενδέχεται να έχουν συγκεκριμένες επεξεργασίες προσωπικών δεδομένων στην προστασία της ιδιωτικής ζωής και να προταθούν, εφόσον χρειάζεται, νέες διαδικασίες και πρακτικές. Παραδοτέο: • Έκθεση Εκτίμησης Αντικτύπου για προστασία των Προσωπικών Δεδομένων (DPIA), η οποία θα περιγράφει τις δραστηριότητες επεξεργασίας με τον υψηλότερο κίνδυνο, τις απειλές και τυχόν επιπτώσεις τους στην προστασία της ιδιωτικής ζωής. ΦΑΣΗ 4: Εκπαίδευση – ευαισθητοποίηση προσωπικού 10. Δημιουργία κουλτούρας προστασίας προσωπικών δεδομένων στον Οργανισμό - Εκτεταμένη εκπαίδευση του προσωπικού (όσο κριθεί απαραίτητη από τον Οργανισμό) πάνω στην Πολιτική Ασφαλείας του Οργανισμού, αλλά και γενικότερα, σε θέματα προσωπικών δεδομένων και της ασφάλειάς τους, με σκοπό να δημιουργηθεί στον οργανισμό κουλτούρα ασφάλειας προσωπικών δεδομένων. Να αναγνωρίζονται αυτά από τους εργαζομένους, ως πολύτιμο περιουσιακό στοιχείο του οργανισμού, το οποίο χρήζει προστασίας. Παραδοτέο: • Πρόγραμμα εκπαίδευσεων κατά τμήμα με αναλυτικό, εκπαιδευτικό πρόγραμμα, υλικό και παρουσιολόγιο ΦΑΣΗ 5: Υπηρεσίες Υποστήριξης Εξωτερικός Υπεύθυνος Προστασίας Δεδομένων: Ορίζεται άτομο του παρόχου, ως Υπεύθυνος Προστασίας Δεδομένων του Οργανισμού, ο οποίος και εκτελεί όλα τα χρέη του DPO (π.χ. και σε περιπτώσεις καταγγελιών), τόσο με επιτόπου επισκέψεις, όσο και εξ αποστάσεως, μέχρι και την ημερομηνία ολοκλήρωσης της υλοποίησης των προτεινόμενων οργανωτικών μέτρων σύμφωνα με τα παραπάνω. Είναι δε προσβάσιμος από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, τον Οργανισμό αλλά και τα Υποκείμενα των Δεδομένων, 24/365. Αφού ολοκληρωθεί η λήψη των Οργανωτικών και Τεχνικών Μέτρων, γίνεται επαναξιολόγηση του επιπέδου συμμόρφωσης του Οργανισμού από τον Υπεύθυνο Προστασίας Δεδομένων. Ειδικές Απαιτήσεις Ο υποψήφιος Ανάδοχος πρέπει να συμπεριλάβει στην προσφορά του : • Χρονοδιάγραμμα δραστηριοτήτων – προγραμματισμό φάσεων υλοποίησης έργου. • Πρόσθετες υπηρεσίες που είναι σε θέση να αναλάβει κατά την υλοποίηση των ενεργειών του πλάνου συμμόρφωσης. Την Ομάδα Έργου η οποία θα περιλαμβάνει έμπειρα στελέχη που να έχουν αποδεδειγμένη εμπειρία στην ασφάλεια πληροφοριών, διαχείριση δεδομένων προσωπικού χαρακτήρα και αποδεδειγμένη εμπειρογνώσια σε θέματα προστασίας προσωπικών δεδομένων και τα οποία θα καλύπτουν κατ' ελάχιστο τις ακόλουθες κατηγορίες: • Πιστοποιημένος Σύμβουλος οργάνωσης και ελεγκτής διαδικασιών και συμμόρφωσης (CIA/CFSA/CCSA/CISA) με αποδεδειγμένη εμπειρία σε Φορείς Δημόσιας Υγείας • Ειδικός στην ανάλυση/διαχείριση κινδύνων και αξιολόγηση των ευπαθειών, με τριετή εμπειρία σε αντίστοιχη θέση (Risk Officer – CRMA) • Εξειδικευμένος νομικός στην προστασία δεδομένων, κάτοχος μεταπτυχιακού τίτλου με σχετική πιστοποίηση DPO με αποδεδειγμένη εμπειρία σε Φορείς Δημόσιας Υγείας • Ειδικός στις τεχνολογικές υποδομές, τις εφαρμογές πληροφορικής και την ασφάλεια πληροφοριακών συστημάτων (IT Auditor) με αποδεδειγμένη εμπειρία σε Φορείς Δημόσιας Υγείας Ένας από τη ομάδα θα οριστεί Project Manager και διαχειριστής του έργου. Όλα τα ανωτέρω να αποδεικνύονται με την επισύναψη των σχετικών επίσημων εγγράφων (βεβαιώσεις πελατών, Συμβάσεις πελατών). Ο Ανάδοχος θα πρέπει να είναι πιστοποιημένος σε διαδικασίες διαχείρισης έργων που εξασφαλίζουν την ποιότητα και να διαθέτει την πιστοποίηση ISO 9001 και την πιστοποίηση 27001, επισυνάπτοντας στην προσφορά του τα σχετικά έγγραφα στην ελληνική γλώσσα ή συνοδευόμενα από επίσημη μετάφραση. Ειδικότερα για τον Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ) που θα υποδείξει θα πρέπει να προσκομίσει στοιχεία (βεβαιώσεις, πιστοποιητικά), τα οποία να αποδεικνύουν τις εξειδικευμένες επιστημονικές γνώσεις σχετικά με τις πρακτικές περί προστασίας και διαχείρισης προσωπικών δεδομένων και

της ικανότητας εκπλήρωσης των καθηκόντων που προβλέπονται στον ΓΚΠΔ στο πλαίσιο συμμόρφωσης και υλοποίησης αυτού. Επιπλέον να έχει αναλάβει το ρόλο του Data Protection Officer (DPO) σε τουλάχιστον τρεις (3) Δημόσιες Μονάδες Υγείας. Επιπλέον υποχρεούται να παρέχει συμβουλευτικές υπηρεσίες όποτε και αν απαιτηθεί εγγράφως μέσω e- mail ή fax εντός εύλογου χρονικού διαστήματος ανάλογα με τη φύση του προβλήματος. Ο ΥΠΔ θα συνεργάζεται άμεσα με την Διοίκηση του Νοσοκομείου καθώς και τις επιμέρους Ο Νόμιμος Εκπρόσωπος Πρόδρομος Νικολαΐδης