Χυριτση
26/4/2018
Τμ. Προμηθειων
26/4/18

4η ΔΙΟΙΚΗΣΗ ΥΓΕΙΟΝΟΜΙΚΗΣ ΠΕΡΙΦΕΡΕΙΑΣ
ΜΑΚΕΔΟΝΙΑΣ & ΘΡΑΚΗΣ

ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ
«Ι Π Π Ο Κ Ρ Α Τ Ε Ι Ο»
ΥΠΟΔΙΕΥΘΥΝΣΗ ΠΛΗΡΟΦΟΡΙΚΗΣ
Κωνσταντινουπόλεως αρ. 49, 546 42 Θεσσαλονίκη

Θεσσαλονίκη 26/4/2018

4η ΥΓΕΙΟΝΟΜΙΚΗ ΠΕΡΙΦΕΡΕΙΑ
Αρ. ΜΑΚΕΔΟΝΙΑΣ & ΘΡΑΚΗΣ
Γ.Ν.Θ. ΙΠΠΟΚΡΑΤΕΙΟ
Αριθ. Πρωτ. 22359
Ελήφθη την 26-4-2018
Αρμόδιος υπάλλ.: Αβραμίδης Α.

Προς: Τμήμα Προμηθειών

ΘΕΜΑ: Διαβίβαση προδιαγραφών για την εφαρμογή του νέου Ευρωπαϊκού Κανονισμού Προστασίας Προσωπικών Δεδομένων (GDPR)

Σχετ: Η με αρ. 384/19.4.2018 Πράξη Διοικήτριας

Σε συνέχεια του ανωτέρω σχετικού σας διαβιβάζουμε τις προδιαγραφές για την εφαρμογή του νέου Ευρωπαϊκού Κανονισμού Προστασίας Προσωπικών Δεδομένων

Η Επιτροπή

Κουντουρά Ευαγγελία

Πλιάτσικας Ιωάννης

Νάκος Δούκας

Άρθρο 1

Ο νέος Ευρωπαϊκός Κανονισμός Προστασίας Προσωπικών Δεδομένων, 679/2016 (GDPR)

Γενικά

Ο νέος Ευρωπαϊκός Κανονισμός Προστασίας Προσωπικών Δεδομένων, 679/2016 (GDPR) -*Κανονισμός*-, ψηφίστηκε στις 27.04.2016, και θα ισχύσει καθολικά, υποχρεωτικά και άμεσα από την 25/05/2018 για όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης, χωρίς την ανάγκη ψήφισης τοπικής εθνικής νομοθεσίας.

Αντικείμενο του νέου κανονισμού αποτελεί η διαμόρφωση ενός ενιαίου κανονιστικού πλαισίου για την επεξεργασία κάθε είδους προσωπικών δεδομένων, αυτοματοποιημένη ή μη, στα κράτη μέλη της Ευρωπαϊκής Ένωσης και εισάγει μια σειρά διαδικασιών και υποχρεώσεων για την:

- Συλλογή και επεξεργασία των δεδομένων προσωπικού χαρακτήρα σε όλο τον κύκλο ζωής τους.
- Την ασφάλεια (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα) των δεδομένων προσωπικού χαρακτήρα.
- Τις ενέργειες σε περίπτωση παραβίασης.

Αυξάνει επίσης σημαντικά τις απαιτήσεις που τίθενται στους οργανισμούς που επεξεργάζονται προσωπικά δεδομένα, καθώς και το μέγεθος των κυρώσεων σε περίπτωση παραβάσεων και αποκλίσεων, που μπορούν να φτάσουν μέχρι και τα 20.000.000,00€ ή το 4% του παγκόσμιου τζίρου της επιχείρησης (άρθρο 83, παράγραφος 5 & 6).

Πεδίο Εφαρμογής

Ο Κανονισμός έχει εφαρμογή σε **όλους τους οργανισμούς** (ιδιωτικές και δημόσιες επιχειρήσεις, κρατικές αρχές, συλλόγους, κλπ.) που **διαχειρίζονται, επεξεργάζονται, αποθηκεύουν και διακινούν δεδομένα προσωπικού χαρακτήρα**, εφόσον τα δεδομένα αφορούν Ευρωπαίους πολίτες ή σχετίζονται με οποιουδήποτε είδους υπηρεσίες και αγαθά προς Ευρωπαίους πολίτες.

Υποχρεώσεις Φορέα

Ο κάθε φορέας υποχρεώνεται από τον κανονισμό:

- Να μεριμνήσει για όλα τα τεχνικά και οργανωτικά μέτρα που θα διασφαλίζουν την επεξεργασία των δεδομένων προσωπικού χαρακτήρα σύμφωνα με τα οριζόμενα στον Κανονισμό
- Να αναπτύξει πολιτικές προστασίας των δεδομένων προσωπικού χαρακτήρα σύμφωνα με τα οριζόμενα στον Κανονισμό
- Να αποδείξει ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα πραγματοποιείται σύμφωνα με τον Κανονισμό

Ιδιαίτερα στην περίπτωση των προσωπικών δεδομένων ειδικής κατηγορίας (ευαίσθητα προσωπικά δεδομένα) προβλέπονται επιπλέον απαιτήσεις, όπως η υποχρέωση για τεκμηρίωση των σχετικών διαδικασιών, ο ορισμός Υπευθύνου Προστασίας Δεδομένων (DPO), η διενέργεια εκτίμησης αντικτύπου, κ.ά.

Για τον λόγο αυτό το -*Νοσοκομείο*- προχωρά στην ανάδειξη αναδόχου για την παροχή συμβουλευτικών υπηρεσιών για την εφαρμογή του Γενικού Κανονισμού για την Προστασία των Προσωπικών Δεδομένων (General Data Protection Regulation).

Άρθρο 2

Τεχνικές Προδιαγραφές

Αντικείμενο του Έργου

Αντικείμενο του αναδόχου είναι αρχικά ο προσδιορισμός της παρούσας κατάστασης του συνόλου των λειτουργιών/υπηρεσιών στα Τμήματα/Κλινικές του Νοσοκομείου σε σχέση με τον Κανονισμό και στην συνέχεια η **κατάρτιση και υλοποίηση** σχεδίου δράσεως/ενεργειών/διαδικασιών, μαζί με την απαραίτητη τεκμηρίωση, προκειμένου να επιτευχθεί η **συνεχής συμμόρφωση** του Νοσοκομείου με τον Κανονισμό.

Επιπλέον στο αντικείμενο του έργου εντάσσεται και η παροχή υπηρεσιών **Υπευθύνου Προστασίας Δεδομένων (DPO)**, καθόλη τη διάρκεια της διαδικασίας συμμόρφωσης του Νοσοκομείου με τον Κανονισμό καθώς και για έξη (6) μήνες από την ολοκλήρωση της παραπάνω διαδικασίας.

Οι προτεινόμενες ελάχιστες φάσεις υλοποίησης του έργου είναι οι ακόλουθες:

- Φάση 1 - Προετοιμασία του έργου / Παρουσίαση
- Φάση 2 - Πρώτη εκτίμηση εναρμόνισης με τον Κανονισμό
- Φάση 3 - Σχέδιο δράσης συμμόρφωσης - Ενημέρωση
- Φάση 4 - Υλοποίηση του Σχεδίου Δράσης - Εκπαίδευση
- Φάση 5 - Επιθεώρηση Συμμόρφωσης - Παρουσίαση Αποτελεσμάτων

Ο ανάδοχος μπορεί να ακολουθήσει οποιαδήποτε οργάνωση για την πρόταση του αρκεί να περιλαμβάνει κατ' ελάχιστον τις υπηρεσίες που αναφέρονται.

Φάση 1 – Προετοιμασία του έργου / Παρουσίαση

Προετοιμασία του έργου

Το έργο της εναρμόνισης του Νοσοκομείου με τις απαιτήσεις του Κανονισμού είναι πολυσύνθετο και απαιτεί σημαντικές παρεμβάσεις στην καθημερινή λειτουργία του Νοσοκομείου και στις διαδικασίες του. Παράλληλα, η πλήρης και συνεχόμενη εναρμόνιση με τον Κανονισμό δεν επιτυγχάνεται μόνο με οργανωτικά ή τεχνολογικά μέτρα αλλά πρωτίστως με την δημιουργία της κατάλληλης κουλτούρας για την προστασία των δεδομένων προσωπικού χαρακτήρα μέσα στον οργανισμό. Απαραίτητη επίσης, είναι η ρητή δέσμευση της Διοίκησης προς την κατεύθυνση της προστασίας των δεδομένων προσωπικού χαρακτήρα και της εναρμόνισης με τον κανονισμό.

Κατά το στάδιο έναρξης του έργου το Νοσοκομείο και ο ανάδοχος θα πρέπει να επιτύχουν μια κοινή καταγραφή των απαιτήσεων του έργου, της μεθοδολογίας και του χρονοδιαγράμματος υλοποίησης του έργου. Επίσης η σύνθεση και στελέχωση της ομάδας εργασίας εφαρμογής του Κανονισμού παίζει καθοριστικό ρόλο. Στην σύνθεση της θα πρέπει να συμμετέχουν εκπρόσωποι από το σύνολο των Διευθύνσεων, (Ιατρική, Νοσηλευτική, Διοικητική και Τεχνική Υπηρεσία), τη Νομική Εκπρόσωπο καθώς και από όποιες άλλες υπηρεσίες του Νοσοκομείου κριθεί απαραίτητο.

Συγκεκριμένα, σε αυτή την φάση θα πρέπει να γίνουν τουλάχιστον οι παρακάτω ενέργειες:

- Παρουσίαση στην Διοίκηση των απαιτήσεων του Κανονισμού.
- Δέσμευση και Συμμετοχή της Διοίκησης στην κατεύθυνση της προστασίας των δεδομένων προσωπικού χαρακτήρα και της εναρμόνισης με τον κανονισμό (π.χ.

λήψη απόφασης από το Διοικητικό Συμβούλιο για την έναρξη του Προγράμματος, συγγραφή δεσμευτικής δήλωσης η οποία θα ανακοινωθεί στο προσωπικό).

- Προσδιορισμός και καταγραφή των απαιτήσεων του Νοσοκομείου όσο αφορά τα δεδομένα προσωπικού χαρακτήρα και ιδιαίτερα τα προσωπικά δεδομένα ειδικής κατηγορίας.
- Ορισμός της σύνθεσης και στελέχωση της ομάδας εργασίας εφαρμογής του Κανονισμού.
- Οριστικοποίηση του σχεδίου υλοποίησης του έργου καθώς και των χρονοδιαγραμμάτων με βάση τις απαιτήσεις του Νοσοκομείου.

Παραδοτέα Φάσης 1:

- Οριστικοποιημένο σχέδιο υλοποίησης του έργου.
- Παρουσίαση του Κανονισμού.

Φάση 2 – Πρώτη εκτίμηση εναρμόνισης με τον Κανονισμό

Προσδιορισμός και Εκτίμηση της τρέχουσας κατάστασης

Αρχικά θα πρέπει να γίνει από τον ανάδοχο μια αρχική αποτύπωση της υφιστάμενης κατάστασης σε σχέση με τις απαιτήσεις του Κανονισμού. Αυτό θα γίνει με την μορφή συνεντεύξεων ή με οποιονδήποτε άλλο τρόπο κρίνεται απαραίτητος, προκειμένου να καθοριστεί ο κύκλος ζωής των δεδομένων προσωπικού χαρακτήρα, και ιδιαίτερα των προσωπικών δεδομένων ειδικής κατηγορίας, σε όλα τα τμήματα του Νοσοκομείου. Παράλληλα θα δημιουργηθούν τα απαραίτητα *αρχεία τεκμηρίωσης* που θα πρέπει να έχει στην κατοχή του το Νοσοκομείο σε σχέση με τον Κανονισμό. Ενδεικτικά αναφέρεται:

- Κατάλογος δεδομένων προσωπικού χαρακτήρα που συλλέγονται και χρησιμοποιούνται, ο τρόπος χρήσης και αποθήκευσης τους, η ροή τους, η προστασία τους και τα δικαιώματα πρόσβασης, η διαδικασία λήψης συγκατάθεσης κλπ. Η καταγραφή των δεδομένων θα πρέπει να είναι λεπτομερής και θα αφορά τόσο τα έντυπα όσο και τα ηλεκτρονικά μέσα στα οποία μπορούν βρεθούν προσωπικά δεδομένα, όπως έγγραφα, φόρμες, κατάλογοι αρχεία κλπ.
- Ταξινόμηση των δεδομένων προσωπικού χαρακτήρα ανά τύπο (π.χ. ειδικής κατηγορίας, δημόσια κλπ).
- Διαγράμματα ροής για την διακίνηση των δεδομένων προσωπικού χαρακτήρα μέσα στο Νοσοκομείο καθώς και εκτός Νοσοκομείου (συμβόλαια συντήρησης κλπ).
- Αιτιολόγηση αναγκαιότητας λήψης και διατήρησης τους, διότι λόγω της ιδιαιτερότητας του Νοσοκομείου για την εκπλήρωση του σκοπού του απαιτείται η συλλογή και επεξεργασία πλήθους δεδομένων προσωπικού χαρακτήρα.

Απογραφή των δεδομένων προσωπικού χαρακτήρα / κατηγοριοποίηση

Ο ανάδοχος θα πρέπει να αποτυπώσει το σύνολο των δραστηριοτήτων επεξεργασίας των δεδομένων προσωπικού χαρακτήρα του Νοσοκομείου. Η αποτύπωση θα πρέπει τουλάχιστον να καλύπτει τις απαιτήσεις του άρθρου 30 και θα περιλαμβάνει κατ' ελάχιστον:

- Το όνομα και τα στοιχεία επικοινωνίας του υπεύθυνου υπαλλήλου επεξεργασίας και του υπεύθυνου προστασίας των δεδομένων
- Την θέση των δεδομένων

- Τον όγκο και την μορφή των πληροφοριών (πλήθος εγγραφών, πλήθος εγγράφων, αριθμού σελίδων κλπ, χαρτί ή ηλεκτρονικό; δομημένο ή αδόμητο)
- Τους σκοπούς της επεξεργασίας και τις ανάγκες που καλύπτουν
- Την κατηγορία των δεδομένων
- Την περιγραφή των δεδομένων (π.χ. όνομα, φυσική διεύθυνση, διεύθυνση ηλεκτρονικού ταχυδρομείου, αναγνωριστικό ταυτότητας (ΑΔΤ, ΑΦΜ, ΑΜΚΑ κλπ), ιατρικό ιστορικό, αποτελέσματα και γνωματεύσεις εξετάσεων κλπ)
- Την κατηγοριοποίηση των προσωπικών στοιχείων ταυτότητας (μη ταυτοποίηση, μερική ταυτοποίηση, ταυτοποίηση, ευαίσθητα προσωπικά δεδομένα κλπ)
- Τις κατηγορίες αποδεκτών στους οποίους έχουν διαβιβαστεί ή πρόκειται να γνωστοποιηθούν τα προσωπικά δεδομένα
- Τις προβλεπόμενες προθεσμίες για τη διαγραφή των διαφόρων κατηγοριών δεδομένων
- Γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφαλείας που αναφέρονται στο άρθρο 32 παράγραφος 1
- Υλικό τεκμηρίωσης που βασίζεται η επεξεργασία
- Όποια άλλα στοιχεία σχετίζονται με την επεξεργασία δεδομένων

Ανάλυση της συμμόρφωσης

Μετά την αποτύπωση των δραστηριοτήτων του Νοσοκομείου σε σχέση με τα δεδομένα προσωπικού χαρακτήρα ο ανάδοχος θα διενεργήσει εκτίμηση και αξιολόγηση της αποτελεσματικότητας των υπαρχόντων τεχνικών και οργανωτικών μέτρων του Νοσοκομείου σε σχέση με τις απαιτήσεις του Κανονισμού, συμπεριλαμβανομένης της ασφάλειας και των κινδύνων της επεξεργασίας. Κατά την αποτίμηση θα πρέπει να καταγραφούν τα πιθανά «κενά» συμμόρφωσης, να προσδιοριστούν και να αξιολογηθούν οι επιπτώσεις τους για το Νοσοκομείο και να τεθούν οι κατάλληλες προτεραιότητες για την αντιμετώπισή τους. Η αποτίμηση θα αφορά τόσο την «**επάρκεια**» των διαδικασιών καθώς και τον «**βαθμό υλοποίησης**» αυτών.

Η αποτίμηση της **επάρκειας** θα αξιολογήσει τις εφαρμοζόμενες πολιτικές ασφαλείας, τις υπάρχουσες διαδικασίες, πρακτικές, και οδηγίες (εγκύκλιοι, νόμοι, κανονισμοί) που επηρεάζουν τη διαχείριση των δεδομένων προσωπικού χαρακτήρα, ως προς την επάρκεια τους σε σχέση με τις *απαιτήσεις του κανονισμού ανά άρθρο*.

Η αποτίμηση του **βαθμού υλοποίησης** θα προσδιορίσει τον βαθμό της πραγματικής χρήσης των πολιτικών ασφαλείας και των διαδικασιών στα Τμήματα/Κλινικές του Νοσοκομείου.

Εκτίμηση αντικτύπου (Data Protection Impact Assessment)

Λόγω της φύσης των δεδομένων προσωπικού χαρακτήρα που διατηρούνται στο Νοσοκομείο, ο Κανονισμός επιβάλει τη διενέργεια εκτίμησης αντικτύπου (Data Protection Impact Assessment, DPIA). Η εκτίμηση αντικτύπου που θα διεξάγει ο ανάδοχος θα πρέπει να περιλαμβάνει τουλάχιστον με βάση το άρθρο 35 παρ. 7:

- Συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, περιλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει το Νοσοκομείο
- Εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς
- Εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων (υποκειμένων των δεδομένων)

- Τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας, ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα και να αποδεικνύεται η συμμόρφωση προς τον Κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερόμενων προσώπων.

Αποτίμηση Επικινδυνότητας (Risk Assessment / Treatment)

Ο ανάδοχος βασισμένος στην ανάλυση της συμμόρφωσης καθώς και στην εκτίμηση αντικτύπου, θα διεξάγει αποτίμηση επικινδυνότητας. Η αποτίμηση θα βασίζεται στις οδηγίες και τη δομή του προτύπου ISO 27005:2011, θα περιλαμβάνει την αποτίμηση της τρέχουσας κατάστασης και την εκτίμηση των κινδύνων για τα δεδομένα προσωπικού χαρακτήρα που διατηρούνται στο Νοσοκομείο, των απειλών και των ευπαθειών των εξεταζόμενων συστημάτων, ηλεκτρονικών ή μη (στα οποία είναι αποθηκευμένα τα προσωπικά δεδομένα). Η αποτίμηση θα γίνει με βάση την επίδραση που θα έχει η διαρροή, αποκάλυψη ή η μη εξουσιοδοτημένη τροποποίηση ή καταστροφή τους, στα φυσικά πρόσωπα που αφορούν και στην ομαλή λειτουργία του Νοσοκομείου.

Πιο συγκεκριμένα, θα προσδιορίζονται οι απειλές οι οποίες σχετίζονται με τα δεδομένα προσωπικού χαρακτήρα και στη συνέχεια θα εκτιμάται το επίπεδο της κάθε απειλής. Αμέσως μετά θα αποτιμάται η έκταση των ευπαθειών που μπορεί να εκμεταλλευτεί η κάθε απειλή.

Μετά την αποτίμηση επικινδυνότητας, η Διοίκηση του Νοσοκομείου, με την βοήθεια του αναδόχου, θα αποφασίσει για την διαχείριση των απειλών των δεδομένων προσωπικού χαρακτήρα, εξετάζοντας λύσεις όπως την Αποδοχή του Επιπέδου Επικινδυνότητας, την Μεταβίβαση του Επιπέδου Επικινδυνότητας, την Αντιμετώπιση του Επιπέδου Επικινδυνότητας και άλλες.

Τέλος, στις περιπτώσεις που επιλεγεί η αντιμετώπιση του επιπέδου επικινδυνότητας, ο ανάδοχος οφείλει να προτείνει κατάλληλα μέτρα και μηχανισμούς ασφαλείας που πρέπει να υιοθετηθούν ώστε το Νοσοκομείο να δύναται να διαχειριστεί τον πιθανό αντίκτυπο μιας διαρροής, αποκάλυψης ή μη εξουσιοδοτημένης τροποποίησης ή καταστροφής.

Παραδοτέα Φάσης 2:

- Αρχεία Τεκμηρίωσης
- Αρχεία Δραστηριοτήτων Επεξεργασίας
- Ανάλυση συμμόρφωσης *ανά άρθρο του Κανονισμού*.
- Εκτίμηση αντικτύπου (Data Protection Impact Assessment)
- Αποτίμηση Επικινδυνότητας (Risk Assessment)

Φάση 3 – Σχέδιο δράσης συμμόρφωσης - Ενημέρωση

Εκπόνηση Σχεδίου Δράσης

Μετά την εκτίμηση της τρέχουσας κατάστασης, την εκτίμηση αντικτύπου και την αποτίμηση επικινδυνότητας, ο ανάδοχος θα αναλάβει να εκπονήσει και να τεκμηριώσει σχέδιο δράσης για συμμόρφωση του Νοσοκομείου με τις απαιτήσεις του Κανονισμού. Το σχέδιο θα περιλαμβάνει το σύνολο των απαιτούμενων Πολιτικών και Διαδικασιών για την αποτελεσματική προστασία των δεδομένων προσωπικού χαρακτήρα με βάση τις απαιτήσεις του Κανονισμού. Μεταξύ των άλλων θα επικεντρώνεται στον τρόπο με τον οποίο θα γίνεται η συλλογή, αποθήκευση, επεξεργασία και διαχείριση των δεδομένων

προσωπικού χαρακτήρα, καθώς και η συναίνεση του υποκειμένου, το δικαίωμα στη διαγραφή («δικαίωμα στη λήθη»), 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.

Το σχέδιο δράσης θα πρέπει να περιλαμβάνει ανά *άρθρο του Κανονισμού* όλες τις απαραίτητες πολιτικές και διαδικασίες που απαιτούνται για την συμμόρφωση του Νοσοκομείου με αυτόν.

Ενδεικτικά αναφέρονται:

- Πολιτική Προστασίας Δεδομένων Προσωπικού Χαρακτήρα που πληροί τις νομικές απαιτήσεις και αντιμετωπίζει το λειτουργικό κίνδυνο και τον κίνδυνο βλάβης των ατόμων
- Πολιτική Προστασίας Δεδομένων Προσωπικού Χαρακτήρα των εργαζομένων
- Κώδικας Δεοντολογίας που περιλαμβάνει άρθρα για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα
- Πολιτική/διαδικασίες για τη συλλογή και τη χρήση προσωπικών δεδομένων ειδικής κατηγορίας
- Πολιτική/διαδικασίες για τη συλλογή και χρήση των δεδομένων προσωπικού χαρακτήρα παιδιών και ανηλίκων
- Πολιτική/διαδικασίες για τη διατήρηση της ποιότητας των δεδομένων
- Πολιτική/διαδικασίες για τη διαγραφή των προσωπικών δεδομένων
- Πολιτική/διαδικασίες για τον έλεγχο της επεξεργασίας που διεξάγεται συνολικά ή εν μέρει με αυτοματοποιημένα μέσα
- Πολιτική/διαδικασίες για δευτερεύουσες χρήσεις των δεδομένων προσωπικού χαρακτήρα
- Πολιτική/διαδικασίες για την απόκτηση έγκυρης συναίνεσης
- Πολιτική/διαδικασίες για ασφαλή καταστροφή των δεδομένων
- Πολιτική/διαδικασίες για τη διατήρηση αρχείων
- Πολιτική/διαδικασίες - όσον αφορά τα δεδομένα προσωπικού χαρακτήρα - για άμεση επικοινωνία, ηλεκτρονικό ταχυδρομείο κλπ
- Πολιτική/διαδικασίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα σε συμβόλαια συντήρηση και υποστήριξης
- Πολιτική/διαδικασίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα σε πρακτικές πρόσληψης
- Οδηγίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα στην Ιστοσελίδα του Νοσοκομείου και στα μέσα κοινωνικής δικτύωσης
- Οδηγίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα σε πρακτικές υγείας και ασφάλειας
- Οδηγίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα στις πρακτικές παρακολούθησης και αξιολόγησης των εργαζομένων,
- Οδηγίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα σε πολιτικές / διαδικασίες σχετικά με την πρόσβαση σε λογαριασμούς εταιρικού ηλεκτρονικού ταχυδρομείου των εργαζομένων,
- Πολιτική/διαδικασίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα στη διεξαγωγή εσωτερικών επιθεωρήσεων
- Πολιτική/διαδικασίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα για την αντιμετώπιση καταγγελιών

- Διαδικασίες ανταπόκρισης σε αιτήματα πρόσβασης σε προσωπικά δεδομένα,
- Διαδικασίες ανταπόκρισης σε αιτήματα διόρθωσης δεδομένων προσωπικού χαρακτήρα,
- Διαδικασίες ανταπόκρισης σε αιτήματα για εξαίρεση, περιορισμό της επεξεργασίας ή αντιρρήσεις στην επεξεργασία,
- Διαδικασίες ανταπόκρισης στα αιτήματα για πληροφορίες,
- Διαδικασίες ανταπόκρισης στα αιτήματα φορητότητας δεδομένων,
- Διαδικασίες (οργανωτικές και τεχνικές) ανταπόκρισης σε αιτήματα για διαγραφή δεδομένων
- Διαδικασίες καταγραφής παραπόνων σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα
- Πολιτική/Διαδικασίες διαχείρισης των παραβιάσεων της ασφάλειας των προσωπικών δεδομένων ή της διαρροής αυτών
- Σχέδιο αντιμετώπισης περιστατικών παραβίασης, διατήρηση αρχείου καταγραφής με στοιχεία όπως η φύση της παραβίασης, ο κίνδυνος, η προέλευση
- Διαδικασίες κοινοποίησης της παραβίασης (στα ενδιαφερόμενα άτομα) και υποβολή αναφορών (σε ρυθμιστικές αρχές, πιστωτικές υπηρεσίες, κ.λπ.)
- Διαδικασία συνεχούς παρακολούθησης και ενημέρωσης για νέες απαιτήσεις συμμόρφωσης, προσδοκίες και βέλτιστες πρακτικές

Επίσης θα πρέπει να αναπτυχθούν όλες οι απαραίτητες πολιτικές και διαδικασίες σε σχέση με τους συνεργάτες (προμηθευτές / συμβούλους / εταιρίες υποστήριξης / κεντρικούς Δημόσιους φορείς κλπ) οι οποίες θα προστεθούν στα υπάρχοντα ή νέα συμβόλαια. Ενδεικτικά θα περιλαμβάνει

- Απαιτήσεις από τους συνεργάτες για την προστασία των δεδομένων προσωπικού χαρακτήρα κατά την εκτέλεση συμβάσεων ή συμφωνιών,
- Όροι για δέουσα επιμέλεια σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα
- Δυνατότητα αξιολόγησης του κινδύνου που προέρχεται από τους συνεργάτες (right to audit)

Οι παραπάνω ενέργειες του σχεδίου δράσης είναι ενδεικτικές. Το σύνολο των απαιτούμενων ενεργειών για συμμόρφωση του Νοσοκομείου με τον κανονισμό θα καθοριστούν με βάση τα αποτελέσματα της *Φάσης 2*.

Παρουσίαση του Σχεδίου Δράσης

Με την ολοκλήρωση του σχεδίου δράσης, ο ανάδοχος θα το παρουσιάσει μαζί με τα συμπεράσματα της ανάλυσής του, στην Διοίκηση και στα αρμόδια στελέχη του Νοσοκομείου. Ο στόχος της παρουσίασης είναι να ενημερωθούν και να ευαισθητοποιηθούν όλα τα εμπλεκόμενα μέρη για το σχέδιο δράσης και τις απαιτήσεις του Κανονισμού και κυρίως για τις αλλαγές στις Πολιτικές / Διαδικασίες που αυτός επιφέρει. Με τον τρόπο αυτό θα διευκολυνθεί η λήψη των απαραίτητων διοικητικών αποφάσεων για την υλοποίηση των απαιτούμενων μέτρων/ενεργειών

Ο Ανάδοχος θα πρέπει στην τελική διαμόρφωση του σχεδίου δράσης, και πριν την έγκριση του από την Διοίκηση, να λάβει υπόψη τις παρατηρήσεις και προτάσεις των στελεχών. Επίσης θα παρέχει τις ανάλογες υπηρεσίες υποστήριξης με την τεκμηρίωση της αναγκαιότητας των δράσεων.

Παραδοτέα Φάσης 3:

- Σχέδιο Δράσης Συμμόρφωσης με τις απαραίτητες πολιτικές και διαδικασίες, *ανά άρθρο* του Κανονισμού.
- Παρουσίαση του σχεδίου δράσης

Φάση 4 - Υλοποίηση του Σχεδίου Δράσης - Εκπαίδευση

Υλοποίηση του σχεδίου δράσης

Ο ανάδοχος, μετά την έγκριση από την Διοίκηση, έχει υποχρέωση να υλοποιήσει το Σχέδιο Δράσης Συμμόρφωσης. Οι υποχρεώσεις του αναδόχου αφορούν τουλάχιστον:

- Την υλοποίηση όλων των μέτρων/ενεργειών/διαδικασιών οι οποίες δεν απαιτούν την προμήθεια ή τροποποίηση εξοπλισμού/προγραμμάτων.
- Την σύνταξη όλων των Πολιτικών/Διαδικασιών που απαιτούνται για την εναρμόνιση του Νοσοκομείου με τον Κανονισμό
- Την παροχή υπηρεσιών συμβούλου στην υλοποίηση των μέτρων/ενεργειών που απαιτούν την προμήθεια ή τροποποίηση εξοπλισμού/προγραμμάτων.
- Την εκπαίδευση του προσωπικού του Νοσοκομείου που εμπλέκονται στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα.

Ο ανάδοχος είναι υπεύθυνος για την υλοποίηση του σχεδίου δράσης.

Εκπαίδευση

Η σωστή εκπαίδευση του προσωπικού του Νοσοκομείου είναι κρίσιμη για την διαφύλαξη της ασφάλειας των δεδομένων προσωπικού χαρακτήρα. Για τον λόγο αυτόν, το προσωπικό του Νοσοκομείου θα πρέπει να εκπαιδευτεί κατάλληλα από τον ανάδοχο ώστε:

- Να είναι ενήμερο για τον Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR), τις απαιτήσεις του και την υποχρέωση του Νοσοκομείου να συμμορφώνεται με αυτόν.
- Να είναι γνώστης των Πολιτικών Προστασίας των δεδομένων προσωπικού χαρακτήρα καθώς και των διαδικασιών εφαρμογής τους και να τις αποδέχεται
- Να καταλαβαίνει πλήρως το ρόλο και τις ευθύνες που του έχουν ανατεθεί σχετικά με τη συμμόρφωση με τον Κανονισμό,
- Να γνωρίζει λεπτομερώς τις διαδικασίες αντιμετώπισης συμβάντων αλλά και τις υπόλοιπες κρίσιμες διαδικασίες.

Λόγω του μεγέθους του Νοσοκομείου οι εκπαιδευτικές ανάγκες είναι σύνθετες και πρέπει να αντιμετωπιστούν με πολλούς τρόπους. Ο ανάδοχος θα πρέπει να καλύπτει τουλάχιστον τις εξής εκπαιδευτικές διαδικασίες:

- Εκπαίδευση κατά την διάρκεια της εργασίας (on-the-job-training)
- Μαζική εκπαίδευση
- Εκπαιδευτικό και ενημερωτικό υλικό.

Παραδοτέα Φάσης 4:

- Τεκμηρίωση της υλοποίησης από τον ανάδοχο του Σχεδίου Δράσης.
- Διαδικασίες και πολιτικές συμμόρφωσης με τον Κανονισμό.

- Εκπαίδευση και ενημέρωση προσωπικού καθώς και εκπαιδευτικό και ενημερωτικό υλικό

Φάση 5 – Επιθεώρηση Συμμόρφωσης – Παρουσίαση Αποτελεσμάτων

Επιθεώρηση Συμμόρφωσης

Η διαδικασία συμμόρφωσης του Νοσοκομείου με τον Κανονισμό θα πρέπει να ολοκληρωθεί με την τελική επιθεώρηση συμμόρφωσης από τον ανάδοχο για τη διατήρηση της συμμόρφωσης και την τήρηση των προβλεπόμενων αρχείων που μπορούν να χρησιμοποιηθούν τόσο για εσωτερική όσο και για εξωτερική αναφορά.

Κατά τη φάση της επιθεώρησης συμμόρφωσης από τον ανάδοχο θα επιθεωρηθούν οι εργαζόμενοι, οι χώροι εργασίας τους, τα σημεία αποθήκευσης των προσωπικών δεδομένων - έγγραφων και ηλεκτρονικών-, η πρόσβαση σε αυτά, οι χρησιμοποιούμενες πολιτικές και διαδικασίες καθώς επίσης και οι συμφωνίες εμπιστευτικότητας που έχουν υπογραφεί, ώστε να επιβεβαιωθεί η διαφύλαξη της ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας των δεδομένων προσωπικού χαρακτήρα και των απαιτήσεων του Κανονισμού.

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 οι Συμφωνίες Εμπιστευτικότητας και τα Συμβόλαια Συντήρησης/Υποστήριξης που έχουν υπογραφεί με τους συνεργάτες, καθώς και το είδος της εκπαίδευσης / ενημέρωσης που έχουν λάβει, όσον αφορά την προστασία των προσωπικών δεδομένων.

Μετά την ολοκλήρωση της επιθεώρησης συμμόρφωσης, ο ανάδοχος θα πρέπει να επικαιροποιήσει:

- Αρχεία Τεκμηρίωσης
- Αρχεία Δραστηριοτήτων Επεξεργασίας
- Ανάλυση του επιπέδου συμμόρφωσης του Νοσοκομείου, *ανά άρθρο του Κανονισμού*.
- Εκτίμηση αντικτύπου (Data Protection Impact Assessment)
- Αποτίμηση Επικινδυνότητας (Risk Assessment)
- Σχέδιο Δράσης Συμμόρφωσης με τα συμπληρωματικά μέτρα και διαδικασίες, *ανά άρθρο* του Κανονισμού που θα πρέπει να υλοποιηθούν

Ο ανάδοχος αναλαμβάνει να εκτελέσει όποιο συμπληρωματικό μέτρο / ενέργεια προκύψει και στη συνέχεια να συντάξει τελική έκθεση με τα αποτελέσματα του εσωτερικού ελέγχου.

Παρουσίαση Αποτελεσμάτων Επιθεώρησης Συμμόρφωσης

Ο ανάδοχος θα παρουσιάσει στην Διοίκηση του Νοσοκομείου τα αποτελέσματα της επιθεώρησης συμμόρφωσης καθώς και του επικαιροποιημένου Data Protection Impact Assessment και Risk Assessment.

Επίσης, θα αναλυθούν οι μεγαλύτεροι κίνδυνοι που αντιμετωπίζει το Νοσοκομείο όσον αφορά τα δεδομένα προσωπικού χαρακτήρα και ιδιαίτερα όσο αφορά τα προσωπικά δεδομένα ειδικής κατηγορίας.

Παραδοτέα Φάσης 5:

- Επικαιροποιημένο ΑρχείοΤεκμηρίωσης

- Επικαιροποιημένα Αρχεία Δραστηριοτήτων Επεξεργασίας
- Επικαιροποιημένη Ανάλυση του επιπέδου συμμόρφωσης του Νοσοκομείου, *ανά άρθρο του Κανονισμού*.
- Επικαιροποιημένη Εκτίμηση αντικτύπου (Data Protection Impact Assessment)
- Επικαιροποιημένη Αποτίμηση Επικινδυνότητας (Risk Assessment)
- Σχέδιο Δράσης Συμμόρφωσης με τα συμπληρωματικά μέτρα και διαδικασίες, *ανά άρθρο* του Κανονισμού

6. Υπεύθυνος Προστασίας Δεδομένων - Data Protection Officer (DPO)

Ο ανάδοχος θα παρέχει στον Νοσοκομείο καθόλη τη διάρκεια της διαδικασίας συμμόρφωσης του Νοσοκομείου με τον Κανονισμό καθώς και για έξι (6) μήνες από την ολοκλήρωση της παραπάνω διαδικασίας κατάλληλα καταρτισμένο και πιστοποιημένο άτομο προκειμένου να αναλάβει τα καθήκοντα του Υπεύθυνου Προστασίας Δεδομένων (DPO). Ο DPO θα πλαισιώνεται από κατάλληλη υποστηρικτική ομάδα, η οποία θα περιλαμβάνει κατ' ελάχιστο έναν Information Security Consultant, έναν IT Auditor και έναν Νομικό με εμπειρία πάνω σε θέματα ασφάλειας πληροφοριών / προσωπικών δεδομένων.

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 αντικτύπου (DPIA) και θα δημιουργεί καινούργιες για επεξεργασίες υψηλού ρίσκου. Ακόμα θα αναλαμβάνει την ενημέρωση του προσωπικού καθώς και τις εσωτερικές επιθεωρήσεις, με σκοπό την επίτευξη του βέλτιστου επιπέδου συμμόρφωσης.

Άρθρο 3

Τεχνική και Επαγγελματική Ικανότητα

Ο ανάδοχος απαιτείται να

- Έχει υλοποιήσει ή υλοποιεί τουλάχιστον πέντε (5) έργα GDPR
- Να διαθέτει πιστοποίηση κατά ISO 9001 και ISO 27001
- Η προτεινόμενη ομάδα έργου θα πρέπει να περιλαμβάνει κατ' ελάχιστο τις ακόλουθες ειδικότητες:
    - Project Manager
    - Information Security Consultant
    - IT Auditor
    - Νομικό Σύμβουλο
- Τα μέλη της ομάδας θα πρέπει να έχουν συμμετάσχει σε δύο (2) τουλάχιστον έργα με αντικείμενο θέματα ασφάλειας πληροφοριών / προσωπικών δεδομένων
- Ένα μέλος της ομάδας θα πρέπει να είναι πιστοποιημένος κατά ISO 27001 auditor.
- Ένα μέλος της ομάδας θα πρέπει να είναι πιστοποιημένος Data Protection Officer (DPO)

Άρθρο 4

Χρονοδιάγραμμα Υλοποίησης

Το χρονοδιάγραμμα Υλοποίησης του έργου Συμμόρφωσης είναι 12 μήνες με προτεινόμενο χρόνο υλοποίησης ανά φάση:

Μήνες	1	2	3	4	5	6	7	8	9	10	11	12
Φάση 1												
Φάση 2												
Φάση 3												
Φάση 4												
Φάση 5												

Επιπλέον μετά την ολοκλήρωση της διαδικασίας συμμόρφωσης συμμόρφωσης θα παρέχονται υπηρεσίες DPO για έξι (6) μήνες.

Άρθρο 5

Προϋπολογισμός

58.000€ με ΦΠΑ.

Η επιτροπή

Κουνταυρά Ευαγγελία

Πλιάτσικας Ιωάννης

Νάκος Δούκας