|  |  |  |  |
| --- | --- | --- | --- |
| **ΠΕΡΙΓΡΑΦΗ ΤΕΧΝΙΚΗΣ ΠΡΟΔΙΑΓΡΑΦΗΣ** | **ΑΠΑΙΤΗΣΗ** | **ΑΠΑΝΤΗΣΗ ΥΠΟΨΗΦΙΟΥ** | **ΠΑΡΑΠΟΜΠΗ ΣΕ  ΤΕΧΝΙΚΑ ΦΥΛΛΑΔΙΑ** |
| **Αντικείμενο του Έργου** |  |  |  |
| Αντικείμενο του αναδόχου είναι: | ΝΑΙ |  |  |
| 1. Ο έλεγχος του επιπέδου εφαρμογής του Γενικού Κανονισμού έως σήμερα. | ΝΑΙ |  |  |
| 1. Η επικαιροποίηση των σχετικών αναγκών του Νοσοκομείου και των ανάλογων πολιτικών του. | ΝΑΙ |  |  |
| 1. Η επικαιροποίηση και υλοποίηση σχεδίου δράσεως/ενεργειών/διαδικασιών, μαζί με την απαραίτητη τεκμηρίωση, προκειμένου να επιτευχθεί η συνεχής συμμόρφωση του Νοσοκομείου με τον Κανονισμό. | ΝΑΙ |  |  |
| 1. Η παροχή υπηρεσιών Υπευθύνου Προστασίας Δεδομένων (DPO) | ΝΑΙ |  |  |
| Οι προτεινόμενες ελάχιστες φάσεις υλοποίησης του έργου είναι οι ακόλουθες: | ΝΑΙ |  |  |
| Φάση 1: Προετοιμασία του έργου – Έλεγχος επιπέδου εναρμόνισης με τον   Κανονισμό- Εγκατάσταση Υπευθύνου Προστασίας Δεδομένων (DPO) | ΝΑΙ |  |  |
| Φάση 2: Ορισμός πλαισίου εργασίας – Επικαιροποίηση πολιτικών GDPR –   Ενημέρωση φορέα | ΝΑΙ |  |  |
| Φάση 3: Επικαιροποίηση και κατάθεση σχεδίου δράσης συνεχούς συμμόρφωσης -   Ενημέρωση | ΝΑΙ |  |  |
| Φάση 4: Υλοποίηση του Σχεδίου Δράσης – Συνεχής εκπαίδευση | ΝΑΙ |  |  |
| Φάση 5: Επιθεώρηση Συμμόρφωσης – Συνεχής παρουσίαση αποτελεσμάτων | ΝΑΙ |  |  |
| Υπηρεσίες DPO: Εγκατάσταση υπεύθυνου DPO | ΝΑΙ |  |  |
|  | ΝΑΙ |  |  |
| Ο ανάδοχος μπορεί να ακολουθήσει οποιαδήποτε οργάνωση για την πρόταση του αρκεί να περιλαμβάνει κατ’ ελάχιστον τις υπηρεσίες που αναφέρονται. | ΝΑΙ |  |  |
| Απαραίτητη προϋπόθεση η συνεχής επικοινωνία του αναδόχου με τον φορέα και η φυσική παρουσία του σε αυτόν τουλάχιστον 5 ημέρες /μήνα. | ΝΑΙ |  |  |
|  |  |  |  |
| **Φάση 1 - Προετοιμασία του έργου – Έλεγχος επιπέδου εναρμόνισης με τον   Κανονισμό** |  |  |  |
|  |  |  |  |
| * 1. **Ενέργειες** |  |  |  |
| Το έργο της εναρμόνισης του Νοσοκομείου με τις απαιτήσεις του Κανονισμού είναι πολυσύνθετο καθώς 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 κατεύθυνσης της προστασίας των δεδομένων προσωπικού χαρακτήρα και της εναρμόνισης με τον κανονισμό. | ΝΑΙ |  |  |
| Το Νοσοκομείο έχει ήδη εφαρμόσει πρόγραμμα ευαισθητοποίησης και εκπαίδευσης του προσωπικού και των Υπηρεσιών του, διάρκειας 18 μηνών. Κατά το διάστημα του σταδίου αυτού ο ανάδοχος θα πρέπει να ελέγξει το επίπεδο προετοιμασίας αλλά και εφαρμογής του Κανονισμού στο σύνολο του Νοσοκομείου. Σε συνεργασία με τη Διοίκηση του Νοσοκομείου θα πρέπει επιτύχουν κοινή καταγραφή και αντίληψη των απαιτήσεων του έργου, της μεθοδολογίας και του χρονοδιαγράμματος υλοποίησης του έργου. Το Νοσοκομείο θα ορίσει τη δική του ομάδα έργου σύμφωνα με τα οριζόμενα στο προοίμιο του παρόντος. | ΝΑΙ |  |  |
| Συγκεκριμένα, σε αυτή την φάση θα πρέπει να γίνουν τουλάχιστον οι παρακάτω ενέργειες: | ΝΑΙ |  |  |
| * Έλεγχος της υφιστάμενης κατάστασης σε όλα τα Τμήματα και Κλινικές του Νοσοκομείου | ΝΑΙ |  |  |
| * Αναφορά προς τη Διοίκηση για το επίπεδο εφαρμογής των Πολιτικών | ΝΑΙ |  |  |
| * Παρουσίαση στην Διοίκηση των αναγκών για τη συνέχεια. | ΝΑΙ |  |  |
| * Οριστικοποίηση του σχεδίου υλοποίησης του έργου καθώς και των χρονοδιαγραμμάτων με βάση τις απαιτήσεις του Νοσοκομείου. | ΝΑΙ |  |  |
|  |  |  |  |
| * 1. **Εγκατάσταση Υπευθύνου Προστασίας Προσωπικών Δεδομένων (DPO)** |  |  |  |
| Από την εκκίνηση της φάσης αυτής ο ανάδοχος θα τοποθετήσει – ενεργοποιήσει τον Υπεύθυνο Προστασίας Προσωπικών δεδομένων (DPO). Οι υποχρεώσεις-ευθύνες του DPO και της ομάδας εργασίας του αναφέρονται αναλυτικά στον Γενικό Κανονισμό. | ΝΑΙ |  |  |
|  |  |  |  |
| * 1. **Παραδοτέα** |  |  |  |
| * Έκθεση επιπέδου εφαρμογής των πολιτικών και εναρμόνισης του Νοσοκομείου με τον Κανονισμό | ΝΑΙ |  |  |
| * Παρουσίαση του Κανονισμού και των απαιτήσεων για την εφαρμογή του. | ΝΑΙ |  |  |
|  |  |  |  |
|  |  |  |  |
| **Φάση 2- Ορισμός πλαισίου εργασίας – Επικαιροποίηση πολιτικών GDPR –**  **Εγκατάσταση Υπευθύνου Προστασίας Δεδομένων (DPO) –   Ενημέρωση φορέα** |  |  |  |
|  |  |  |  |
| **2.1. Ενέργειες** |  |  |  |
| 1. Θα πρέπει από τον ανάδοχο να γίνει έλεγχος και επικαιροποίηση των πολιτικών που έχουν εγκριθεί από το Νοσοκομείο. | ΝΑΙ |  |  |
| 2. Θα πρέπει να επικαιροποιηθεί ο κύκλος ζωής των δεδομένων προσωπικού χαρακτήρα, και ιδιαίτερα των προσωπικών δεδομένων ειδικής κατηγορίας, σε όλα τα τμήματα του Νοσοκομείου. Η επικαιροποίηση θα αφορά και τα απαραίτητα αρχεία τεκμηρίωσης που πρέπει να έχει στην κατοχή του το Νοσοκομείο σε σχέση τον Κανονισμό. Σαν τέτοια, ενδεικτικά αναφέρονται: | ΝΑΙ |  |  |
| \* 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 δεδομένων, όπως έγγραφα, φόρμες, κατάλογοι αρχεία κλπ. | ΝΑΙ |  |  |
| \* Ταξινόμηση των δεδομένων προσωπικού χαρακτήρα ανά τύπο (π.χ. ειδικής κατηγορίας, δημόσια κλπ) | ΝΑΙ |  |  |
| \* Διαγράμματα ροής για την διακίνηση των δεδομένων προσωπικού χαρακτήρα μέσα στο Νοσοκομείο καθώς και εκτός Νοσοκομείου (συμβόλαια συντήρησης κλπ) | ΝΑΙ |  |  |
| \* 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. | ΝΑΙ |  |  |
|  |  |  |  |
| **Απογραφή των δεδομένων προσωπικού χαρακτήρα / κατηγοριοποίηση** |  |  |  |
| Επικαιροποίηση θα πρέπει να γίνει στο σύνολο των δραστηριοτήτων επεξεργασίας των δεδομένων προσωπικού χαρακτήρα του Νοσοκομείου. Οι ενέργειες αυτές πρέπει να καλύπτουν τουλάχιστον τις απαιτήσεις του άρθρου 30, και αποτυπώνουν κατ’ ελάχιστον: | ΝΑΙ |  |  |
| * Το όνομα και τα στοιχεία επικοινωνίας του υπεύθυνου υπαλλήλου επεξεργασίας και του υπεύθυνου προστασίας των δεδομένων | ΝΑΙ |  |  |
| * Την θέση των δεδομένων | ΝΑΙ |  |  |
| * Τον όγκο και την μορφή των πληροφοριών (πλήθος εγγραφών, πλήθος εγγράφων, αριθμού σελίδων κλπ, χαρτί ή ηλεκτρονικό; δομημένο ή αδόμητο) | ΝΑΙ |  |  |
| * Τους σκοπούς της επεξεργασίας και τις ανάγκες που καλύπτουν | ΝΑΙ |  |  |
| * Την κατηγορία των δεδομένων | ΝΑΙ |  |  |
| * 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) | ΝΑΙ |  |  |
| * Την κατηγοριοποίηση των προσωπικών στοιχείων ταυτότητας (μη ταυτοποίηση, μερική ταυτοποίηση, ταυτοποίηση, ευαίσθητα προσωπικά δεδομένα κλπ) | ΝΑΙ |  |  |
| * Τις κατηγορίες αποδεκτών στους οποίους έχουν διαβιβαστεί ή πρόκειται να γνωστοποιηθούν τα προσωπικά δεδομένα | ΝΑΙ |  |  |
| * Τις προβλεπόμενες προθεσμίες για τη διαγραφή των διαφόρων κατηγοριών δεδομένων | ΝΑΙ |  |  |
| * Γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφαλείας που αναφέρονται στο άρθρο 32 παράγραφος 1 | ΝΑΙ |  |  |
| * Υλικό τεκμηρίωσης που βασίζεται η επεξεργασία | ΝΑΙ |  |  |
| * Όποια άλλα στοιχεία σχετίζονται με την επεξεργασία δεδομένων | ΝΑΙ |  |  |
|  |  |  |  |
| **Ανάλυση της συμμόρφωσης** |  |  |  |
| Μετά την επικαιροποίηση των πιο πάνω 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. | ΝΑΙ |  |  |
| Η αποτίμηση της επάρκειαςθα 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. | ΝΑΙ |  |  |
| Η αποτίμηση τουβαθμού υλοποίησηςθα προσδιορίσει τον βαθμό της συμμόρφωσης του Νοσοκομείου με τον Κανονισδμό. | ΝΑΙ |  |  |
|  |  |  |  |
| **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: | ΝΑΙ |  |  |
| * Συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, περιλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει το Νοσοκομείο | ΝΑΙ |  |  |
| * Εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς | ΝΑΙ |  |  |
| * Εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων (υποκειμένων των δεδομένων) | ΝΑΙ |  |  |
| * 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. | ΝΑΙ |  |  |
|  |  |  |  |
| **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. | ΝΑΙ |  |  |
| 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. | ΝΑΙ |  |  |
| 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. | ΝΑΙ |  |  |
| 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 εξουσιοδοτημένη τροποποίηση ή καταστροφής. | ΝΑΙ |  |  |
|  |  |  |  |
| **2.2. Ενημέρωση φορέα** |  |  |  |
|  |  |  |  |
| **2.3. Παραδοτέα** |  |  |  |
| * Αρχεία Τεκμηρίωσης | ΝΑΙ |  |  |
| * Αρχεία Δραστηριοτήτων Επεξεργασίας | ΝΑΙ |  |  |
| * Ανάλυση συμμόρφωσης ανά άρθρο του Κανονισμού. | ΝΑΙ |  |  |
| * Εκτίμηση αντικτύπου (Data Protection Impact Assessment) | ΝΑΙ |  |  |
| * Αποτίμηση Επικινδυνότητας (Risk Assessment) | ΝΑΙ |  |  |
| * Επικαιροποιημένα κείμενα πολιτικών GDRP | ΝΑΙ |  |  |
|  |  |  |  |
| **Φάση 3 - Επικαιροποίηση και κατάθεση σχεδίου δράσης συνεχούς συμμόρφωσης-   Ενημέρωση** |  |  |  |
|  |  |  |  |
| **3.1. Ενέργειες** |  |  |  |
| **Εκπόνηση Σχεδίου Δράσης** |  |  |  |
| Βάση της εκτίμησης επιπέδου συμμόρφωσης, την εκτίμηση αντικτύπου και την αποτίμηση επικινδυνότητας, ο ανάδοχος θα εκπονήσει και θα τεκμηριώσει σχέδιο δράσης για επικαιροποίηση της συμμόρφωσης 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/επικαιροποίηση. | ΝΑΙ |  |  |
| 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. | ΝΑΙ |  |  |
| Ενδεικτικά τέτοιες αναφέρονται: | ΝΑΙ |  |  |
| * Πολιτική Προστασίας Δεδομένων Προσωπικού Χαρακτήρα που πληροί τις νομικές απαιτήσεις και αντιμετωπίζει το λειτουργικό κίνδυνο και τον κίνδυνο βλάβης των ατόμων | ΝΑΙ |  |  |
| * Πολιτική Προστασίας Δεδομένων Προσωπικού Χαρακτήρα των εργαζομένων | ΝΑΙ |  |  |
| * Κώδικας Δεοντολογίας που περιλαμβάνει άρθρα για την Προστασίας Δεδομένων Προσωπικού Χαρακτήρα | ΝΑΙ |  |  |
| * Πολιτική/διαδικασίες για τη συλλογή και τη χρήση προσωπικών δεδομένων ειδικής κατηγορίας | ΝΑΙ |  |  |
| * Πολιτική/διαδικασίες για τη συλλογή και χρήση των δεδομένων προσωπικού χαρακτήρα παιδιών και ανηλίκων | ΝΑΙ |  |  |
| * Πολιτική/διαδικασίες για τη διατήρηση της ποιότητας των δεδομένων, | ΝΑΙ |  |  |
| * Πολιτική/διαδικασίες για τη διαγραφή των προσωπικών δεδομένων, | ΝΑΙ |  |  |
| * Πολιτική/διαδικασίες για τον έλεγχο της επεξεργασίας που διεξάγεται συνολικά ή εν μέρει με αυτοματοποιημένα μέσα | ΝΑΙ |  |  |
| * Πολιτική/διαδικασίες για δευτερεύουσες χρήσεις των δεδομένων προσωπικού χαρακτήρα | ΝΑΙ |  |  |
| * Πολιτική/διαδικασίες για την απόκτηση έγκυρης συναίνεσης | ΝΑΙ |  |  |
| * Πολιτική/διαδικασίες για ασφαλή καταστροφή των δεδομένων | ΝΑΙ |  |  |
| * Πολιτική/διαδικασίες για τη διατήρηση αρχείων | ΝΑΙ |  |  |
| * Πολιτική/διαδικασίες -όσον αφορά τα δεδομένα προσωπικού χαρακτήρα - για άμεση επικοινωνία, ηλεκτρονικό ταχυδρομείο κλπ | ΝΑΙ |  |  |
| * Πολιτική/διαδικασίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα σε συμβόλαια συντήρηση και υποστήριξης | ΝΑΙ |  |  |
| * Πολιτική/διαδικασίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα σε πρακτικές πρόσληψης | ΝΑΙ |  |  |
| * Οδηγίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα στην Ιστοσελίδα του Νοσοκομείου και στα μέσα κοινωνικής δικτύωσης | ΝΑΙ |  |  |
| * Οδηγίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα σε πρακτικές υγείας και ασφάλειας | ΝΑΙ |  |  |
| * Οδηγίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα στις πρακτικές παρακολούθησης και αξιολόγησης των εργαζομένων, | ΝΑΙ |  |  |
| * Οδηγίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα σε πολιτικές / διαδικασίες σχετικά με την πρόσβαση σε λογαριασμούς εταιρικού ηλεκτρονικού ταχυδρομείου των εργαζομένων, | ΝΑΙ |  |  |
| * Πολιτική/διαδικασίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα στη διεξαγωγή εσωτερικών επιθεωρήσεων | ΝΑΙ |  |  |
| * Πολιτική/διαδικασίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα για την αντιμετώπιση καταγγελιών | ΝΑΙ |  |  |
| * Διαδικασίες ανταπόκρισης σε αιτήματα πρόσβασης σε προσωπικά δεδομένα, | ΝΑΙ |  |  |
| * Διαδικασίες ανταπόκρισης σε αιτήματα διόρθωσης δεδομένων προσωπικού χαρακτήρα, | ΝΑΙ |  |  |
| * Διαδικασίες ανταπόκρισης σε αιτήματα για εξαίρεση, περιορισμό της επεξεργασίας ή αντιρρήσεις στην επεξεργασία, | ΝΑΙ |  |  |
| * Διαδικασίες ανταπόκρισης στα αιτήματα για πληροφορίες, | ΝΑΙ |  |  |
| * Διαδικασίες ανταπόκρισης στα αιτήματα φορητότητας δεδομένων, | ΝΑΙ |  |  |
| * Διαδικασίες (οργανωτικές και τεχνικές) ανταπόκρισης σε αιτήματα για διαγραφή δεδομένων | ΝΑΙ |  |  |
| * Διαδικασίες καταγραφής παραπόνων σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα | ΝΑΙ |  |  |
| * Πολιτική/Διαδικασίες διαχείρισης των παραβιάσεων της ασφάλειας των προσωπικών δεδομένων ή της διαρροής αυτών | ΝΑΙ |  |  |
| * Σχέδιο αντιμετώπισης περιστατικών παραβίασης, διατήρηση αρχείου καταγραφής με στοιχεία όπως η φύση της παραβίασης, ο κίνδυνος, η προέλευση | ΝΑΙ |  |  |
| * Διαδικασίες κοινοποίησης της παραβίασης (στα ενδιαφερόμενα άτομα) και υποβολή αναφορών (σε ρυθμιστικές αρχές, πιστωτικές υπηρεσίες, κ.λπ.) | ΝΑΙ |  |  |
| * Διαδικασία συνεχούς παρακολούθησης και ενημέρωσης για νέες απαιτήσεις συμμόρφωσης, προσδοκίες και βέλτιστες πρακτικές | ΝΑΙ |  |  |
|  | ΝΑΙ |  |  |
| Επίσης θα πρέπει να αναπτυχθούν όλες οι απαραίτητες πολιτικές και διαδικασίες σε σχέση με τους συνεργάτες (προμηθευτές / συμβούλους / εταιρίες υποστήριξης κλπ) οι οποίες θα προστεθούν στα υπάρχοντα ή νέα συμβόλαια. Ενδεικτικά θα παραλαμβάνει | ΝΑΙ |  |  |
| * Απαιτήσεις από τους συνεργάτες για την προστασία των δεδομένων προσωπικού χαρακτήρα κατά την εκτέλεση συμβάσεων ή συμφωνιών, | ΝΑΙ |  |  |
| * Όροι για δέουσα επιμέλεια σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα | ΝΑΙ |  |  |
| * Δυνατότητα αξιολόγησης του κινδύνου που προέρχεται από τους συνεργάτες (right to audit) | ΝΑΙ |  |  |
|  | ΝΑΙ |  |  |
| 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 1. | ΝΑΙ |  |  |
|  | ΝΑΙ |  |  |
| **Παρουσίαση του Σχεδίου Δράσης** | ΝΑΙ |  |  |
| 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 | ΝΑΙ |  |  |
| Ο Ανάδοχος θα πρέπει στην τελική διαμόρφωση/επικαιροποίηση 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. | ΝΑΙ |  |  |
|  |  |  |  |
| **3.2. Παραδοτέα** |  |  |  |
| * Επικαιροποιημένο Σχέδιο Δράσης Συμμόρφωσης με τις απαραίτητες πολιτικές και διαδικασίες, ανά άρθρο του Κανονισμού. | ΝΑΙ |  |  |
| * Σχέδιο συνεχούς συμμόρφωσης-επικαιροποίησης με τον Κανονισμό | ΝΑΙ |  |  |
| * Παρουσίαση του σχεδίου δράσης | ΝΑΙ |  |  |
|  |  |  |  |
| **Φάση 4 - Υλοποίηση του Σχεδίου Δράσης – Συνεχής Εκπαίδευση** |  |  |  |
|  |  |  |  |
| * 1. **Ενέργειες** |  |  |  |
|  |  |  |  |
| **Υλοποίηση του σχεδίου δράσης** |  |  |  |
| Ο ανάδοχος, μετά την έγκριση από την Διοίκηση, έχει υποχρέωση να υλοποιήσει στο Σχέδιο Δράσης Συμμόρφωσης. Οι υποχρεώσεις του αναδόχου αφορούν τουλάχιστον: | ΝΑΙ |  |  |
| * Την υλοποίηση όλων των μέτρων/ενεργειών/διαδικασιών οι οποίες δεν απαιτούν την προμήθεια ή τροποποίηση εξοπλισμού/προγραμμάτων. | ΝΑΙ |  |  |
| * Την σύνταξη/επικαιροποίηση όλων των Πολιτικών/Διαδικασιών που απαιτούνται για την εναρμόνιση του Νοσοκομείου με τον Κανονισμό | ΝΑΙ |  |  |
| * Την παροχή υπηρεσιών συμβούλου στην υλοποίηση των μέτρων/ενεργειών που απαιτούν την προμήθεια ή τροποποίηση εξοπλισμού/προγραμμάτων. | ΝΑΙ |  |  |
| * Την εκπαίδευση του προσωπικού του Νοσοκομείου που εμπλέκονται στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα. | ΝΑΙ |  |  |
| Ο ανάδοχος είναι υπεύθυνος για την υλοποίηση του σχεδίου δράσης. | ΝΑΙ |  |  |
|  |  |  |  |
| **Συνεχής Εκπαίδευση** |  |  |  |
| Η σωστή εκπαίδευση του προσωπικού του Νοσοκομείου είναι κρίσιμη για την διαφύλαξη της ασφάλειας των δεδομένων προσωπικού χαρακτήρα. Για τον λόγο το προσωπικό του Νοσοκομείου θα πρέπει να εκπαιδευτεί κατάλληλα από τον ανάδοχο ώστε: | ΝΑΙ |  |  |
| * Να είναι ενήμερο για τον Κανονισμό, τις απαιτήσεις του και την υποχρέωση του Νοσοκομείου να συμμορφώνεται με αυτόν. | ΝΑΙ |  |  |
| * Να είναι γνώστες των Πολιτικών Προστασίας των δεδομένων προσωπικού χαρακτήρα καθώς και των διαδικασιών εφαρμογής τους και να τις αποδέχεται | ΝΑΙ |  |  |
| * Να καταλαβαίνει πλήρως το ρόλο και τις ευθύνες που του έχουν ανατεθεί σχετικά με τη συμμόρφωση με τον Κανονισμό, | ΝΑΙ |  |  |
| * Να γνωρίζουν λεπτομερώς τις διαδικασίες αντιμετώπισης συμβάντων αλλά και τις υπόλοιπες κρίσιμες διαδικασίες. | ΝΑΙ |  |  |
| 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: | ΝΑΙ |  |  |
| * Εκπαίδευση κατά την διάρκεια της εργασίας (on-the-job-training) | ΝΑΙ |  |  |
| * Μαζική εκπαίδευση | ΝΑΙ |  |  |
| * Εκπαιδευτικό και ενημερωτικό υλικό. | ΝΑΙ |  |  |
|  |  |  |  |
| * 1. **Παραδοτέα** |  |  |  |
| * Τεκμηρίωση της υλοποίησης από τον ανάδοχο του Σχεδίου Δράσης. | ΝΑΙ |  |  |
| * Επικαιροποιημένες διαδικασίες και πολιτικές συμμόρφωσης με τον Κανονισμό. | ΝΑΙ |  |  |
| * Πρόγραμμα συνεχούς εκπαίδευσης και ενημέρωσης προσωπικού καθώς και σχετικό εκπαιδευτικό και ενημερωτικό υλικό | ΝΑΙ |  |  |
|  | ΝΑΙ |  |  |
| **Φάση 5 – Επιθεώρηση Συμμόρφωσης – Παρουσίαση Αποτελεσμάτων** |  |  |  |
|  |  |  |  |
| **5.1. Ενέργειες** |  |  |  |
| Η διαδικασία συμμόρφωσης του Νοσοκομείου με τον Κανονισμό θα πρέπει να αποτελεί διαρκή και ανοιχτή δραστηριότητα τόσο του αναδόχου όσο και του Νοσοκομείου. Κατά τη φάση της επιθεώρησης συμμόρφωσης από τον ανάδοχο θα επιθεωρούνται 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 επιβεβαιώνεται η διαφύλαξη της ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας των δεδομένων προσωπικού χαρακτήρα και των απαιτήσεων του Κανονισμού. | ΝΑΙ |  |  |
| Επιπλέον, θα επιθεωρούνται 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/Υποστήρικης που έχουν υπογραφεί με τους συνεργάτες, καθώς και το είδος της εκπαίδευσης / ενημέρωσης που έχουν λάβει, όσον αφορά την προστασία των προσωπικών δεδομένων. | ΝΑΙ |  |  |
| Ορόσημα της διαδικασίας τοποθετούνται στο τέλος κάθε φάσης του έργου. Με την συμπλήρωση κάθε ορόσημου ο ανάδοχος θα πρέπει να επικαιροποιεί εάν απαιτείται κα τα παραδοτέα προηγούμενων φάσεων. | ΝΑΙ |  |  |
|  | ΝΑΙ |  |  |
| Ο ανάδοχος αναλαμβάνει να εκτελέσει όποιο συμπληρωματικό μέτρο / ενέργεια προκύψει και στη συνέχεια να συντάξει τελική έκθεση με τα αποτελέσματα του εσωτερικού ελέγχου. | ΝΑΙ |  |  |
| Τα αποτελέσματα κάθε επιθεώρησης καταγράφονται και φυλάσσονται στο αρχείο του έργου τόσο από τον ανάδοχο όσο και από το Νοσοκομείο, αποτελούν δε περιουσιακό στοιχείο και του Νοσοκομείου. | ΝΑΙ |  |  |
|  |  |  |  |
| **Παρουσίαση Αποτελεσμάτων Επιθεώρησης Συμμόρφωσης** |  |  |  |
| Ο ανάδοχος έχει υποχρέωση παρουσίασης προς τη Διοίκηση του Νοσοκομείου, των αποτελεσμάτων της επιθεώρησης συμμόρφωσης καθώς και του επικαιροποιημένου Data Protection Impact Assessment και Risk Assessment, με γραπτή έκθεση. Η Διοίκηση του Νοσοκομείου διατηρεί τη δυνατότητα να ζητήσει αυτοπρόσωπη παρουσίαση από τον ανάδοχο. | ΝΑΙ |  |  |
|  |  |  |  |
| **Τελική Επιθεώρηση υλοποίησης του έργου** |  |  |  |
| Ο ανάδοχος υποχρεούται σε παρουσίαση προς τη Διοίκηση του Νοσοκομείου, της τελικής εικόνας πορείας του έργου, τρείς (3) μήνες πριν τη λήξη της σύμβασης. | ΝΑΙ |  |  |
|  |  |  |  |
| * 1. **Παραδοτέα** |  |  |  |
| * Επικαιροποιημένο Αρχείο Τεκμηρίωσης | ΝΑΙ |  |  |
| * Επικαιροποιημένα Αρχεία Δραστηριοτήτων Επεξεργασίας | ΝΑΙ |  |  |
| * Επικαιροποιημένη Ανάλυση του επιπέδου συμμόρφωσης του Νοσοκομείου, ανά άρθρο του Κανονισμού. | ΝΑΙ |  |  |
| * Επικαιροποιημένη Εκτίμηση αντικτύπου (Data Protection Impact Assessment) | ΝΑΙ |  |  |
| * Επικαιροποιημένη Αποτίμηση Επικινδυνότητας (Risk Assessment) | ΝΑΙ |  |  |
| * Επικαιροποιημένο Σχέδιο Δράσης Συμμόρφωσης με τα συμπληρωματικά μέτρα και διαδικασίες, ανά άρθρο του Κανονισμού | ΝΑΙ |  |  |
| * Εκθέσεις επιθεωρήσεων | ΝΑΙ |  |  |
| * Τελική παρουσίαση αποτελεσμάτων του έργου | ΝΑΙ |  |  |
|  |  |  |  |
|  |  |  |  |
| **ΥΠΗΡΕΣΙΕΣ DPO** |  |  |  |
|  |  |  |  |
| Ο ανάδοχος θα παρέχει στον Νοσοκομείο καθόλη τη διάρκεια της σύμβασης κατάλληλα καταρτισμένο και πιστοποιημένο άτομο προκειμένου να αναλάβει τα καθήκοντα του Data Protection Officer (DPO). O 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. | ΝΑΙ |  |  |
| O 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. | ΝΑΙ |  |  |
| Η δραστηριότητα του DPO θα πρέπει να βρίσκεται σε συνεχή συντονισμό με την Ομάδα Έργου του Νοσοκομείου και το ΑΤΕΠΕΣΕ ως υπεύθυνης υπηρεσίας συντονισμού αυτής. | ΝΑΙ |  |  |
|  |  |  |  |
| **Άρθρο 3** |  |  |  |
| **Χρονοδιάγραμμα Υλοποίησης** |  |  |  |
| Το χρονοδιάγραμμα Υλοποίησης του έργου Συμμόρφωσης είναι 12 μήνες με προτεινόμενο χρόνο υλοποίησης ανά φάση: | ΝΑΙ |  |  |
|  |  |  |  |
| |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | ΜΗΝΕΣ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | | Φάση 1 | Χ | Χ | Χ |  |  |  |  |  |  |  |  |  | | Φάση 2 |  | Χ | Χ | Χ |  |  |  |  |  |  |  |  | | Φάση 3 |  |  | Χ | Χ | Χ |  |  |  |  |  |  |  | | Φάση 4 |  |  |  |  | Χ | Χ | Χ | Χ |  |  |  |  | | Φάση 5 |  |  |  |  |  |  | Χ | Χ | Χ | Χ | Χ | Χ | | Υπηρεσίες DPO | Χ | Χ | Χ | Χ | Χ | Χ | Χ | Χ | Χ | Χ | Χ | Χ | | ΝΑΙ |  |  |
|  |  |  |  |
| **Προϋπολογισμός** |  |  |  |
|  |  |  |  |
| 15.000€ πλέον ΦΠΑ. | ΝΑΙ |  |  |
|  |  |  |  |
| **Άρθρο 4** |  |  |  |
| **Τεχνική και Επαγγελματική Ικανότητα αναδόχου** |  |  |  |
|  |  |  |  |
| Ο ανάδοχος απαιτείται να | ΝΑΙ |  |  |
| * Έχει υλοποιήσει ή υλοποιεί τουλάχιστον πέντε (5) έργα GDPR | ΝΑΙ |  |  |
| * Να διαθέτει πιστοποίηση κατά ISO 9001 και ISO 27001 | ΝΑΙ |  |  |
| * Η προτεινόμενη δική του ομάδα έργου θα πρέπει να περιλαμβάνει κατ’ ελάχιστο τις ακόλουθες ειδικότητες | ΝΑΙ |  |  |
| * Project Manager | ΝΑΙ |  |  |
| * Information Security Consultant | ΝΑΙ |  |  |
| * IT Auditor | ΝΑΙ |  |  |
| * Νομικό Σύμβουλο | ΝΑΙ |  |  |
| * Τα μέλη της ομάδας θα πρέπει να έχουν τουλάχιστον τουλάχιστον 5ετή εμπειρία σε θέματα ασφάλειας πληροφοριών / προσωπικών δεδομένων ενώ θα πρέπει να έχουν συμμετάσχει σε δύο (2) τουλάχιστον έργα με αντικείμενο θέματα ασφάλειας πληροφοριών/προσωπικών δεδομένων. | ΝΑΙ |  |  |
| * Ο Information Security Consultant, θα πρέπει να είναι πιστοποιημένος ISO 27001 auditors. | ΝΑΙ |  |  |
| Ένα μέλος της ομάδας θα πρέπει να διαθέτει βεβαίωση ως Data Protection Officer (DPO) από εταιρία πιστοποιήσεων ή αντίστοιχη βεβαίωση άλλου φορέα καθώς και εμπειρία με εμπειρία σε ανάλογη θέση φορέα Β΄ βάθμιας φροντίδας υγείας. | ΝΑΙ |  |  |