ΠΑΡΑΡΤΗΜΑ ΙΙΙ

**ΥΠΟΔΕΙΓΜΑ ΦΥΛΛΟΥ ΣΥΜΜΟΡΦΩΣΗΣ**

(Αναλυτικό φύλλο συμμόρφωσης- τεκμηρίωσης, με το οποίο δίνονται αναλυτικές απαντήσεις με σχετικές παραπομπές σε όλα τα σημεία των «Απαιτήσεων- Τεχνικών Προδιαγραφών», καθώς και σε κάθε άλλη τεχνική απαίτηση της Αναθέτουσας Αρχής)

**Υπηρεσίες DPO**

|  |  |  |  |
| --- | --- | --- | --- |
| **ΠΕΡΙΓΡΑΦΗ ΤΕΧΝΙΚΗΣ ΠΡΟΔΙΑΓΡΑΦΗΣ** | **ΑΠΑΙΤΗΣΗ** | **ΑΠΑΝΤΗΣΗ ΥΠΟΨΗΦΙΟΥ** | **ΠΑΡΑΠΟΜΠΗ ΣΕ ΤΕΧΝΙΚΑ ΦΥΛΛΑΔΙΑ** |
| **Αντικείμενο του Έργου** |  |  |  |
| **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.  | 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 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
 | ΝΑΙ |  |  |
| * Η προτεινόμενη δική του ομάδα έργου θα πρέπει να περιλαμβάνει κατ’ ελάχιστο τις ακόλουθες ειδικότητες
 | ΝΑΙ |  |  |
| * Διαχειριστή Έργου / Project Manager
 | ΝΑΙ |  |  |
| * Information Security Consultant / IT Auditor
 | ΝΑΙ |  |  |
| * Νομικό Σύμβουλο
 | ΝΑΙ |  |  |
| * Τα μέλη της ομάδας θα πρέπει να έχουν τουλάχιστον 5ετή εμπειρία σε θέματα ασφάλειας πληροφοριών / προσωπικών δεδομένων ενώ θα πρέπει να έχουν συμμετάσχει σε δύο (2) τουλάχιστον έργα σχετικά με τον Γενικό Κανονισμό Προστασίας Δεδομένων. Η εμπειρία πιστοποιείται με την προσκόμιση των αντίστοιχων βεβαιώσεων των φορέων υλοποίησης.
 | 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 σε θέση DPO τουλάχιστον φορέα Β΄ βάθμιας φροντίδας υγείας. Η εμπειρία πιστοποιείται με την προσκόμιση των αντίστοιχων βεβαιώσεων των φορέων υλοποίησης.
 | ΝΑΙ |  |  |
| * Ως Διαχειριστής Έργου / Project Manager είναι δυνατόν να οριστεί ένα εκ των άλλων μελών της ομάδας.
 | NAI |  |  |
| **ΑΝΑΛΥΣΗ ΚΑΘΗΚΟΝΤΩΝ ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ** |  |  |  |
| * Ο σύμβουλος θα παρέχει στον Νοσοκομείο καθόλη τη διάρκεια της σύμβασης κατάλληλα καταρτισμένο και πιστοποιημένο άτομο προκειμένου να αναλάβει τα καθήκοντα του Data Protection Officer (DPO), καθώς θα ορίσει και αναπληρωτή DPO. O DPO και ο αναπληρωτής DPO θα πλαισιώνονται από κατάλληλη υποστηρικτική ομάδα.
 | NAI |  |  |
| * 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.
 | NAI |  |  |
| * 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.
 | NAI |  |  |
| **Καθήκοντα του Υπεύθυνου Προστασίας Δεδομένων:** |  |  |  |
| * Όλα τα αναφερόμενα στο Τμήμα 4 του άρθρου 37 – Υπεύθυνος προστασίας δεδομένων του 2016/679 Κανονισμού. Τουλάχιστον θα είναι τα ακόλουθα:
 | NAI |  |  |
| * θα ενημερώνει και θα συμβουλεύει το Νοσοκομείο και τους υπαλλήλους που θα διενεργούν την επεξεργασία σχετικά με τις υποχρεώσεις τους σύμφωνα με τις διατάξεις του Ν.4264/2019 και κάθε άλλης νομοθεσίας για την προστασία δεδομένων προσωπικού χαρακτήρα.
 | NAI |  |  |
| * θα παρακολουθεί την τήρηση των διατάξεων του Ν.4624/2019 και κάθε άλλης νομοθεσίας για την προστασία των προσωπικών δεδομένων και των πολιτικών του Νοσοκομείου σε σχέση με την προστασία δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων και της λογοδοσίας καθώς και των σχετικών ελέγχων
 | NAI |  |  |
| * θα καθοδηγεί για την εφαρμογή των κατάλληλων μέτρων και για την απόδειξη της συμμόρφωσης από τον υπεύθυνο επεξεργασίας και τον εκτελούντα επεξεργασία, ιδίως όσον αφορά τον προσδιορισμό των κινδύνων που συνδέονται με την επεξεργασία, την εκτίμησή τους από άποψη προέλευσης, φύσης, πιθανότητας και σοβαρότητας και τον εντοπισμό των βέλτιστων πρακτικών για τον περιορισμό των κινδύνων
 | NAI |  |  |
| * θα παρακολουθεί τη συμμόρφωση με τον Γ.Κ.Π.Δ. καθώς και κάθε άλλης νομοθεσίας σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα και με τις πολιτικές του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων τυχόν πρότασης αναμόρφωσης των διαδικασιών και επιμέρους πολιτικών, της ευαισθητοποίησης και της κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας, και της διενέργειας σχετικών ελέγχων
 | NAI |  |  |
| * θα παρέχει συμβουλές, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και παρακολουθεί την υλοποίησή της σύμφωνα με το άρθρο 35 του Κανονισμού και το άρθρο 65 του Ν.4624/2019.
 | NAI |  |  |
| * θα συνεργάζεται με την Αρχή Προστασίας Προσωπικών Δεδομένων
 | NAI |  |  |
| * θα ενεργεί ως σημείο επαφής με την Αρχή Προστασίας Προσωπικών Δεδομένων σε θέματα που αφορούν την επεξεργασία, συμπεριλαμβανομένης της προηγούμενης διαβούλευσης που αναφέρεται στο άρθρο 67 του Ν.4264/2019, και τη συμβουλεύεται, κατά περίπτωση, σχετικά με οποιοδήποτε άλλο θέμα.
 | NAI |  |  |
| * θα απαντά σε ερωτήματα σχετικά με την νομοθεσία περί προστασίας προσωπικών δεδομένων τα οποία θα υποβάλλονται στον Δήμο ηλεκτρονικά είτε με οποιοδήποτε πρόσφορο τρόπο.
 | NAI |  |  |
| * θα απαντά σε καταγγελίες που σχετίζονται με ζητήματα προστασίας προσωπικών δεδομένων.
 | NAI |  |  |
| * θα βρίσκεται στην διάθεση του Νοσοκομείου σε περίπτωση παραβίασης προσωπικών δεδομένων για τα οποία θα ενημερώνεται άμεσα από τον υπεύθυνο επεξεργασίας ή τον εκτελών την επεξεργασία προκειμένου να γίνει άμεση εκτίμηση επικινδυνότητας και θα ακολουθεί χωρίς καθυστέρηση την διαδικασία γνωστοποίησης της παραβίασης στην Αρχή σύμφωνα με τις ισχύουσες διατάξεις.
 | NAI |  |  |
| * θα συνεργάζεται άμεσα με το Νοσοκομείο για την καταγραφή, ανάλυση και εξέταση τυχόν περιστατικών παραβίασης προσωπικών δεδομένων ώστε να ακολουθηθεί διαδικασία αποκατάστασης και λήψης μέτρων αποτροπής στο μέλλον παρόμοιων περιστατικών.
 | NAI |  |  |
| * θα μεριμνά για την ευαισθητοποίηση και την εκπαίδευση του προσωπικού σε θέματα προστασίας προσωπικών δεδομένων.
 | NAI |  |  |
| * θα λαμβάνει υπόψη του τον κίνδυνο που σχετίζεται με την επεξεργασία . τη φύση , το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας.
 | NAI |  |  |
| * θα συμμετέχει, δεόντως και εγκαίρως, στη διαδικασία λήψης αποφάσεων για τα ζητήματα τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα.
 | NAI |  |  |
| * θα έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα και σε πράξεις επεξεργασίας και εγκαταστάσεις σχετικών υποδομών, εφόσον κρίνεται απολύτως απαραίτητη, με σκοπό την ορθή ενάσκηση των καθηκόντων του.
 | NAI |  |  |
| * θα λογοδοτεί απευθείας στον Διοικητή ή στο πρόσωπο/όργανο που ο Διοικητής πιθανώς ορίσει, όπου θα καταθέτει, όποτε είναι αναγκαίο, γραπτό απολογισμό καθώς δεν θα λαμβάνει εντολές για την άσκηση των καθηκόντων του. Η διασφάλιση της αυτονομίας του ΥΠΔ δεν σημαίνει ότι θα αποκτά εξουσίες λήψης αποφάσεων καθ’ υπέρβαση των καθηκόντων του.
 | NAI |  |  |
| * θα διαχειρίζεται τα αιτήματα υποκειμένων.
 | NAI |  |  |
| * θα συμβάλει στην τήρηση και επικαιροποίηση του αρχείου δραστηριοτήτων.
 | NAI |  |  |
| **Υποβολή Ερωτημάτων** |  |  |  |
| * Ο Υ.Π.Δ οφείλει να απαντά σε ερωτήματα του υπευθύνου επεξεργασίας ή του εκτελούντα την επεξεργασία, του υποκειμένου των δεδομένων ή των υπαλλήλων, καθώς και σε καταγγελίες που αφορούν ζητήματα σχετικά με τα προσωπικά δεδομένα. Τα υποκείμενα των δεδομένων θα μπορούν να επικοινωνούν με τον Υπεύθυνο Προστασίας Δεδομένων για κάθε ζήτημα σχετικό με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα τους και με την άσκηση των δικαιωμάτων τους που απορρέουν από το ισχύον νομοθετικό πλαίσιο περί προστασίας προσωπικών δεδομένων.
 | NAI |  |  |
| **Παραδοτέο** |  |  |  |
| * Τριμηνιαία Αναφορά Εργασιών
 | NAI |  |  |
| **Διάρκεια Υπηρεσίας:** * 12 μήνες
 | NAI |  |  |