

Β ΦΑΣΗ ΔΙΑΒΟΥΛΕΥΣΗΣ

ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ

για την ανάδειξη αναδόχου, με σκοπό την
εναρμόνιση του Γ.Ν. Κέρκυρας με τον νέο Ευρωπαϊκό
Κανονισμό Προστασίας
Προσωπικών Δεδομένων 2016/679 (GDPR)

1. ΣΚΟΠΟΣ ΤΟΥ ΕΡΓΟΥ

Σκοπό του έργου αποτελεί ο ορισμός και η παροχή υπηρεσιών Υπευθύνου Προστασίας Δεδομένων (DPO) για τον έλεγχο των νέων διαδικασιών και την συνεχή παρακολούθηση και τήρηση της συμμόρφωσης ως προς τα οριζόμενα μέτρα – διαδικασίες που προκύπτουν από την εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΓ - General Data Protection Regulation GDPR) 2016/679 της Ε.Ε.

2. ΑΝΤΙΚΕΙΜΕΝΟ ΤΟΥ ΕΡΓΟΥ

Αντικείμενο του έργου αποτελεί ο ορισμός και η παροχή υπηρεσιών Υπευθύνου Προστασίας Δεδομένων – ΥΠΔ (DPO) στο Γ.Ν. Κέρκυρας «Αγ. Ειρήνη» και όλες τις εξωτερικές Δομές του. Οι βασικές εργασίες που θα περιλαμβάνουν οι υπηρεσίες υποστήριξης είναι τα ακόλουθες:

- Πλήρεις και ολοκληρωμένες υπηρεσίες ΥΠΔ (DPO): Θα ορίσει ο υποψήφιος ανάδοχος τον (εξωτερικό) Υπεύθυνο Προστασίας Δεδομένων, 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.

3. ΑΝΤΙΚΕΙΜΕΝΟ ΕΡΓΑΣΙΩΝ ΤΟΥ ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

1. Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία διασφαλίζουν ότι ο Υπεύθυνος Προστασίας Δεδομένων θα συμμετέχει δεόντως και εγκαίρως στη διαδικασία της λήψης αποφάσεων για όλα τα ζητήματα που σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα. Θα έχει εξουσία πρόσβασης σε δεδομένα προσωπικού χαρακτήρα και σε πράξεις επεξεργασίας και εγκαταστάσεις σχετικών υποδομών για την ορθή άσκηση των καθηκόντων του. Δεν θα λαμβάνει εντολές σχετικά με την άσκηση των καθηκόντων του. Θα δεσμεύεται

από την τήρηση του απορρήτου και της εμπιστευτικότητας σχετικά με την άσκηση των καθηκόντων του, σύμφωνα με την ισχύουσα νομοθεσία.

2. Τα υποκείμενα των δεδομένων μπορούν να επικοινωνούν με τον Υπεύθυνο Προστασίας Δεδομένων για κάθε ζήτημα σχετικά με την επεξεργασία των δεδομένων τους προσωπικού χαρακτήρα και με την άσκηση των δικαιωμάτων τους.

3. Ο υπεύθυνος προστασίας δεδομένων δεσμεύεται από την τήρηση του απορρήτου ή της εμπιστευτικότητας σχετικά με την εκτέλεση των καθηκόντων του, σύμφωνα με την ισχύουσα νομοθεσία.

4. ΚΑΘΗΚΟΝΤΑ ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (DPO support)

Ο υποψήφιος που θα επιλεγεί και θα οριστεί ΥΠΔ (DPO) θα έχει τα ακόλουθα καθήκοντα, σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων:

(α) Θα ενημερώνει και θα συμβουλεύει γραπτώς τον Υπεύθυνο Επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους υπαλλήλους του σχετικά με τις υποχρεώσεις τους, που απορρέουν από τη νομοθεσία σχετικά με την προστασία δεδομένων,

(β) Θα παρακολουθεί τη συμμόρφωση με τη νομοθεσία σχετικά με την προστασία δεδομένων και τις πολιτικές του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων: της πρότασης αναμόρφωσης διαδικασιών, της επικαιροποίησης της χαρτογράφησης δεδομένων και ροών και της ανάθεσης αρμοδιοτήτων, της ευαισθητοποίησης και της κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας και της διενέργειας των σχετικών ελέγχων,

(γ) Θα παρέχει συμβουλές όσον αφορά στην εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και θα παρακολουθεί την υλοποίησή της σύμφωνα με το άρθρο 35 του Γενικού Κανονισμού Προστασίας Δεδομένων,

(δ) Θα συνεργάζεται με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και θα ενεργεί ως πρόσωπο επικοινωνίας της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για τα ζητήματα που σχετίζονται με την επεξεργασία, περιλαμβανομένης και της προηγούμενης διαβούλευσης που αναφέρεται στο άρθρο 36 του Γενικού κανονισμού Προστασίας Δεδομένων και θα πραγματοποιεί διαβουλεύσεις, ανάλογα με την περίπτωση, για οποιοδήποτε άλλο θέμα συνδέεται με τις πράξεις επεξεργασίας, συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς επεξεργασίας.

(ε) Δια ζώσης εκπαίδευση των καθ' υπόδειξη στελεχών του Νοσοκομείου αναφορικά με τον Γενικό Κανονισμό Προστασίας

Δεδομένων 2016/679 της Ε.Ε., η οποία πρέπει να διεξαχθεί κατά τη διάρκεια του πρώτου τριμήνου της σύμβασης.

(στ) Κατά την εκτέλεση των καθηκόντων του, λαμβάνει δεόντως υπόψη τον κίνδυνο που συνδέεται με τις πράξεις επεξεργασίας, συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας.

(ζ) Λογοδοτεί απευθείας στο Δ.Σ. του Νοσ/μείου, στο οποίο και θα καταθέτει γραπτό μηνιαίο απολογισμό ή έκτακτα εφόσον κριθεί.

Παραδοτέα:

- Επικαιροποίηση των πολιτικών, εντύπων και διαδικασιών συμμόρφωσης με τον Κανονισμό.
- Παράδοση τριμηνιαίας έκθεσης συμμόρφωσης στην οποία θα αναλύεται ο βαθμός συμμόρφωσης του Νοσοκομείου με τα προαπαιτούμενα του Κανονισμού ή έκτακτα εφόσον κριθεί.
- Δια ζώσης εκπαίδευση των καθ' υπόδειξη στελεχών του Νοσοκομείου αναφορικά με τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΕΕ) 2016/679, η οποία πρέπει να διεξαχθεί κατά τη διάρκεια του πρώτου τριμήνου της σύμβασης.
- Υποστήριξη των υπηρεσιών σε θέματα που άπτονται στο Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων μέσω γνωμοδοτήσεων.

5. ΠΡΟΣΟΝΤΑ ΥΠΟΨΗΦΙΟΥ

Ο υποψήφιος που θα επιλεγεί και θα οριστεί ως Υπεύθυνος Προστασίας Δεδομένων – ΥΠΔ (DPO) μπορεί να είναι φυσικό ή Νομικό Πρόσωπο. Εφόσον πρόκειται για φυσικό πρόσωπο ορίζεται το ίδιο ως ΥΠΔ (DPO). Εφόσον πρόκειται για νομικό πρόσωπο, αυτό θα ορίσει με πρότασή του το φυσικό πρόσωπο εκείνου που θα αναλάβει το ρόλο του ΥΠΔ (DPO). Ο υποψήφιος μπορεί να δηλώσει ότι πλαισιώνεται από συνεργάτες φυσικά πρόσωπα, τα οποία κρίνεται απαραίτητο να δηλώνονται στην αίτησή του (στην τεχνική προσφορά), καθώς και στη σύμβαση που θα συναφθεί με το Νοσοκομείο.

Οι ενδιαφερόμενοι υποψήφιοι (φυσικά πρόσωπα ή ο εκπρόσωπος των νομικών προσώπων άλλως/ή και το υποδεικνυόμενο από το νομικό πρόσωπο άτομο ως ΥΠΔ), θα πρέπει να συγκεντρώνουν τα παρακάτω αναφερόμενα προσόντα:

- Ο υποψήφιος Ανάδοχος θα πρέπει να υλοποιεί ή να έχει υλοποιήσει τουλάχιστον 3 έργα σε αντίστοιχους οργανισμούς (Δημόσια Νοσοκομεία). Επιπλέον, θα πρέπει να περιέχεται

στην προσφορά, λίστα με πληροφορίες για παρόμοια έργα υλοποίησης GDPR.

- Ο υποψήφιος Ανάδοχος θα πρέπει να διαθέτει ομάδα έργου η οποία θα αποτελείται από τουλάχιστον έναν:
 - Πιστοποιημένο Υπεύθυνο Προστασίας Δεδομένων που κατέχει αντίστοιχη θέση τουλάχιστον σε 3 Δημόσια Νοσοκομεία
 - Εξειδικευμένο νομικό με γνώση και εμπειρία των πρακτικών περί Προστασίας και Διαχείρισης Προσωπικών Δεδομένων στο πλαίσιο υλοποίησης της συμμόρφωσης. Να αποτελεί ή να έχει αποτελέσει μέλος της ομάδας έργου σε τρία (3) τουλάχιστον παρόμοια έργα, εκ των οποίων ένα τουλάχιστον να είναι σε δημόσιο νοσοκομείο.
 - Εξειδικευμένο επιστήμονα Πληροφορικής με γνώση και Ζετή εμπειρία της ασφαλούς διαχείρισης δεδομένων μέσω πληροφοριακών συστημάτων σε φορέα παροχής υγείας. Να αποτελεί ή να έχει αποτελέσει μέλος της ομάδας έργου σε ένα (1) τουλάχιστον παρόμοιο έργο.
 - Τα μέλη της ομάδας έργου μπορούν να καλύπτουν παραπάνω της μίας ιδιότητας. 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, που θα πιστοποιούν την επιστημονική γνώση, εμπειρία και κατάρτιση στα γνωστικά αντικείμενα:
 - Ασφάλειας πληροφοριών
 - Νομικό
 - Τεχνολογικό.

Οι υποψήφιοι καλούνται να προσκομίσουν στοιχεία (βεβαιώσεις καλής εκτέλεσης, συμβάσεις, πιστοποιητικά), τα οποία θα συνεκτιμηθούν και θα αποδεικνύουν:

1. Την εξειδικευμένη επιστημονική γνώση και εμπειρογνωσία των πρακτικών περί προστασίας και διαχείρισης δεδομένων και της ικανότητας εκπλήρωσης των καθηκόντων που προβλέπονται στον ΓΚΠΔ στο πλαίσιο συμμόρφωσης και υλοποίησης αυτού, καθώς και την εμπειρία ως ΥΠΔ (DPO) ειδικά σε συνάρτηση με τον τομέα της παροχής υπηρεσιών υγείας.

2. Τη γνώση του τομέα της Υγείας και ειδικότερα των διοικητικών κανόνων που τον διέπουν.

3. Γνώση των τεχνολογιών πληροφορίας και ασφάλειας δεδομένων.

Εφόσον ο υποψήφιος (φυσικό πρόσωπο ή ο εκπρόσωπος του νομικού προσώπου ή το άτομο που αυτό θα υποδείξει και θα οριστεί και ΥΠΔ (DPO)), δηλώσει ότι πλαισιώνεται από συνεργάτες φυσικά πρόσωπα για

την αρτιότερη και ταχύτερη παροχή υπηρεσιών ΥΠΔ (DPO), θα πρέπει, για λόγους σαφήνειας και οργάνωσης και προκειμένου να αποτραπούν και συγκρούσεις συμφερόντων, να αναφέρει στην αίτησή του (στην τεχνική προσφορά) σαφώς τον καταμερισμό εργασίας στα φυσικά πρόσωπα που θα δηλώσει, τους τίτλους σπουδών αυτών και την εμπειρογνώσια τους στις πρακτικές προστασίας και διαχείρισης προσωπικών δεδομένων.

Η εμπειρία και η υλοποίηση των έργων από τον Ανάδοχο θα πρέπει να τεκμηριώνεται με Βεβαίωση Καλής Εκτέλεσης από τον πελάτη ή πρωτόκολλο οριστικής παραλαβής.

6. ΔΙΑΡΚΕΙΑ

Η διάρκεια της σύμβασης θα πρέπει είναι για ένα (1) έτος και να δύναται να παραταθεί για ένα (1) ακόμη έτος κατά μέγιστο, με τη σύμφωνη γνώμη και των δύο συμβαλλόμενων μερών.

7. ΑΠΑΣΧΟΛΗΣΗ – ΠΡΟΓΡΑΜΜΑ ΕΡΓΑΣΙΑΣ

Ο υποψήφιος ΥΠΔ (DPO) που θα επιλεγεί και θα υπογράψει σύμβαση θα παρέχει τις υπηρεσίες του εντός και εκτός των Δομών του Γ.Ν. Κέρκυρας. Για την εκτέλεση των ΓΚΠΔ υπηρεσιών ο συμβασιούχος ΥΠΔ και η τυχόν υπάρχουσα ομάδα του έχουν πλήρη πρόσβαση στις δομές του Νοσ/μείου από τις 07.00 έως 20.00 κάθε εργάσιμη ημέρα της εβδομάδας.

Για τη διευκόλυνση της παροχής υπηρεσιών ΥΠΔ (DPO) το Νοσ/μείο θα παρέχει ειδικό χώρο που θα διατεθεί για το σκοπό αυτό. Ο ΥΠΔ (DPO) υποχρεούται να πραγματοποιεί τουλάχιστον δύο (2) επισκέψεις ανά δεκαπενθήμερο στο χώρο του Νοσ/μείου για την άσκηση των καθηκόντων του, διάρκειας όχι μικρότερης των έξι (6) πλήρων ωρών σε πρωινή και εργάσιμη ώρα και επιπλέον να παρέχει συμβουλές τηλεφωνικά ή μέσω ηλεκτρονικού ταχυδρομείου, όποτε αυτό ζητηθεί. Ο συμβασιούχος ΥΠΔ (DPO) θα συνεργάζεται άμεσα με όλους τους Διευθυντές των Υπηρεσιών και το Διοικητικό Συμβούλιο του Νοσοκομείου.

8. ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ – ΕΧΕΜΥΘΕΙΑ

α) Όλες οι εκθέσεις και τα συναφή στοιχεία, όπως διαγράμματα, πλάνα, στατιστικά στοιχεία και κάθε άλλο σχετικό έγγραφο ή στοιχείο που αποκτάται, συγκεντρώνεται ή καταρτίζεται από τον συμβασιούχο ΥΠΔ (DPO) κατά την εκτέλεση του έργου της παρούσας σύμβασης, είναι εμπιστευτικά και ανήκουν στην απόλυτη ιδιοκτησία του Νοσ/μείου.

β) Ο συμβασιούχος, χωρίς την προηγούμενη γραπτή συναίνεση της Διοίκησης του Νοσ/μείου, δεν αποκαλύπτει καμία πληροφορία που του δόθηκε, ούτε κοινοποιεί στοιχεία ή έγγραφα των οποίων έλαβε γνώση σε σχέση με το αντικείμενο της εργασίας του.

γ) Σε περίπτωση αθέτησης από τον συμβασιούχο της ως άνω υποχρέωσής του, το Νοσ/μείο δικαιούται να απαιτήσει:

- Την αποκατάσταση κάθε ζημίας του, που ενδεχομένως προκύψει, συνεπεία της κοινοποίησης εγγράφων – στοιχείων, σε τρίτους, και
- την άμεση και στο διηνεκές παύση κοινοποίησης εγγράφων – στοιχείων, σε τρίτους, στο μέλλον.

δ) Ο συμβασιούχος, με κανένα τρόπο, δεν δύναται να προβαίνει σε δημόσιες δηλώσεις, σχετιζόμενες με την εν γένει κατάσταση του Νοσ/μείου, χωρίς την προηγούμενη γραπτή άδεια της Διοίκησης του Νοσ/μείου.

ε) Ο συμβασιούχος δεσμεύεται από την τήρηση απορρήτου και εμπιστευτικότητας σχετικά με την άσκηση των καθηκόντων του, ευθυνόμενος και για τυχόν συναφείς παραβάσεις των μελών της οργανωμένης ομάδας του (εφόσον έχει τέτοια) κατά τον ΓΚΠΔ.