ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ ΓΙΑ ΤΟ ΕΡΓΟ

« ΠΑΡΟΧΗ ΥΠΗΡΕΣΙΩΝ ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (D.P.O) ΓΙΑ ΤΗΝ ΚΑΛΥΨΗ ΤΩΝ ΑΝΑΓΚΩΝ ΤΟΥ ΓΕΝΙΚΟΥ ΝΟΣΟΚΟΜΕΙΟΥ ΧΙΟΥ «ΣΚΥΛΙΤΣΕΙΟ» ΣΤΟ ΠΛΑΙΣΙΟ ΕΝΑΡΜΟΝΙΣΗΣ / ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΙΣ ΑΠΑΙΤΗΣΕΙΣ ΤΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (GDPR) 679/2016 (ΕΕ)» ΠΡΟΫΠΟΛΟΓΙΣΜΟΥ 5.300,00 ΕΥΡΩ ΜΕ Φ.Π.Α.

ΕΙΣΑΓΩΓΗ

Με το Γενικό Κανονισμό για την Προστασία Δεδομένων (ΓΚΠΔ) (ΕΕ) 2016/679 θεσπίστηκε το νέο νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων όσον αφορά, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα (δ.π.χ) και στην ελεύθερη κυκλοφορία των δεδομένων αυτών, ο οποίος τέθηκε σε εφαρμογή από την 25η Μαΐου 2018, σε όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης (ΕΕ).

Ωστόσο, τα κράτη – μέλη ανέλαβαν την υποχρέωση να ενσωματώσουν στο εθνικό τους δίκαιο τον παρόντα Κανονισμό. Στις 29 Αυγούστου 2019 δημοσιεύτηκε ο ν. 4624/2019 (ΦΕΚ Α΄137), ο οποίος, όρισε τα μέτρα εφαρμογής του ΓΚΠΔ και ενσωμάτωσε στην ελληνική νομοθεσία την Οδηγία (ΕΕ) 2016/680.

Ο ΓΚΠΔ εφαρμόζεται σε κάθε είδους οργανισμό, δημόσιο ή ιδιωτικό, που παρέχει υπηρεσίες σε κράτη μέλη της ΕΕ ή συλλέγει, επεξεργάζεται και αποθηκεύει προσωπικά δεδομένα ατόμων, όπως προμηθευτών, πελατών και εργαζομένων που κατοικούν σε κράτη μέλη της Ευρωπαϊκής Ένωσης.

Ο ΓΚΠΔ επιβάλλει μια σειρά υποχρεώσεων στους υπεύθυνους επεξεργασίας, οι οποίες απορρέουν από τις βασικές αρχές και ιδίως την ενισχυμένη αρχή της διαφάνειας στον τρόπο συλλογής, επεξεργασίας και τήρησης δεδομένων και την αρχή της λογοδοσίας, σύμφωνα με την οποία ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωσή του με όλες τις αρχές που διέπουν την επεξεργασία προσωπικών δεδομένων:

- **Ευθύνη**: Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη να αποδεικνύει ότι λαμβάνει όλα τα κατάλληλα οργανωτικά και τεχνικά μέτρα προστασίας των προσωπικών δεδομένων και ότι συμμορφώνεται με τον ΓΚΠΔ.
- **Προστασία δεδομένων κατά τον σχεδιασμό («Data protection by design»)**: Ο ΓΚΠΔ επιβάλλει την εφαρμογή προϊόντων και υπηρεσιών (ηλεκτρονικών και μη) που κατά τον αρχικό σχεδιασμό τους δημιουργούν φιλικές συνθήκες για την προστασία των δπχ.
- **Προστασία δεδομένων εξ ορισμού («Data protection by default»)**: Ο ΓΚΠΔ επιβάλλει την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων που να διασφαλίζουν ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα που είναι απαραίτητα για τον σκοπό της επεξεργασίας.

- **Ασφάλεια επεξεργασίας**: Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία πρέπει να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το ενδεδειγμένο επίπεδο ασφάλειας.
- **Υπεύθυνος προστασίας δεδομένων**: Προβλέπεται, ο ορισμός «Υπευθύνου Προστασίας Δεδομένων» (DPO) ο οποίος, έχει εχέγγυα ανεξαρτησίας και παρακολουθεί τη συμμόρφωση με τον νόμο αποτελώντας, συγχρόνως, το σημείο επαφής με την εποπτική Αρχή.
- **Γνωστοποίηση παραβιάσεων δεδομένων**: Ο υπεύθυνος επεξεργασίας έχει υποχρέωση, μόλις αντιληφθεί παραβίαση, να ενημερώσει τις αρμόδιες εποπτικές Αρχές.
- **Εκτίμηση αντικτύπου και προηγούμενη διαβούλευση**: Όταν η επεξεργασία ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα των ατόμων, ιδίως επειδή είναι συστηματική, μεγάλης κλίμακας, αφορά ειδικές κατηγορίες δεδομένων και βασίζεται στη χρήση νέων τεχνολογιών, ο υπεύθυνος επεξεργασίας πρέπει να διενεργήσει εκτίμηση **αντικτύπου** σχετικά με την προστασία των δεδομένων (Data protection impact assessment). Όταν βάσει της διενεργηθείσας εκτίμησης αντικτύπου και παρά την πρόβλεψη μέτρων προστασίας παραμένει υψηλή επικινδυνότητα της επεξεργασίας, ο υπεύθυνος επεξεργασίας υποχρεούται να προβεί σε προηγούμενη διαβούλευση με την εποπτική Αρχή.

ΑΝΤΙΚΕΙΜΕΝΟ

Αντικείμενο του έργου είναι, η παροχή ολοκληρωμένων υπηρεσιών Υπευθύνου Προστασίας Δεδομένων (ΥΠΔ) (Data Protection Officer - DPO), σύμφωνα με τα άρθρα 37-39 του Κανονισμού (ΕΕ) 2016/679 και του ν.4624/2019.

Λόγω της φύσης του φορέα ως Δημόσιου Νοσοκομείου που, διενεργεί μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων (δεδομένα υγείας, γενετικά, βιομετρικά) η συγκρότηση θέσης DPO, είναι υποχρεωτική, βάσει του άρθρου 37 παρ. 1 (α) και (γ) του ΓΚΠΔ.

Ο DPO, στο εξής Ανάδοχος, θα λειτουργεί ως εξωτερικός συνεργάτης του Γ.Ν Χίου «ΣΚΥΛΙΤΣΕΙΟ», παρέχοντας συμβουλευτικές, εποπτικές, εκπαιδευτικές και υποστηρικτικές υπηρεσίες (GDPR, άρθρα 37-39).

Η ευθύνη λήψης αποφάσεων σχετικά με τους σκοπούς και τα μέσα επεξεργασίας προσωπικών δεδομένων καθώς επίσης και η ευθύνη υλοποίησης των οργανωτικών και τεχνικών μέτρων συμμόρφωσης, παραμένει αποκλειστικά στον Φορέα, ως Υπεύθυνο Επεξεργασίας.

Η δύναμη του Νοσοκομείου ανέρχεται στις εκατό εξήντα κλίνες (160) ενώ στην εν λόγω Μονάδα απασχολούνται συνολικά περί τους τετρακόσιους (400) εργαζόμενους.

ΣΚΟΠΟΣ

Σκοπός του έργου 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 στις απαιτήσεις του ΓΚΠΔ.

Το έργο θα αφορά 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 Εντατικής Θεραπείας, Μονάδα Εμφραγμάτων, Μονάδα Τεχνητού Νεφρού) , Διατομεακά Τμήματα κλπ.
- Εργαστήρια του Εργαστηριακού Τομέα.
- Διοικητικές Υπηρεσίες, όπως Γραφείο Κίνησης, Λογιστήριο Ασθενών, Τμήμα Προσωπικού, Γραμματείες κλπ.
- Ιατρική Υπηρεσία.
- Νοσηλευτική Υπηρεσία.
- Υποδιεύθυνση Τεχνικού.
- Τμήμα Πληροφορικής.

ΚΑΘΗΚΟΝΤΑ – ΥΠΟΧΡΕΩΣΕΙΣ ΥΠΔ (DPO)

Τα καθήκοντα του ΥΠΔ, όπως περιγράφονται και στον ΓΚΠΔ, θα είναι τα ακόλουθα:

1. Θα ενημερώνει και θα συμβουλεύει τον Υπεύθυνο Επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους υπαλλήλους που επεξεργάζονται, τις υποχρεώσεις τους, που απορρέουν από τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) και από άλλες διατάξεις της ΕΕ ή του κράτους – μέλους σχετικά με την προστασία δεδομένων.
2. Θα παρακολουθεί τη συμμόρφωση με τον παρόντα Κανονισμό σχετικά με την προστασία δεδομένων και με τις πολιτικές του Υπεύθυνου Επεξεργασίας ή του Εκτελούντος την Επεξεργασία σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων, της ανάθεσης αρμοδιοτήτων, της ευαισθητοποίησης, και της κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας και των σχετικών ελέγχων.
3. Θα επιθεωρεί την τήρηση των συμφωνηθέντων διαδικασιών, προκειμένου να εκπληρώνεται η συμμόρφωση του Νοσοκομείου, στο Νομικό και λειτουργικό

4. πλαίσιο, το οποίο έχει οριστεί κατά τη διαδικασία της εναρμόνισης.

Συγκεκριμένα:

- Θα διενεργεί περιοδικούς ελέγχους συμμόρφωσης.
- Θα αξιολογεί τις οργανωτικές και τεχνικές διαδικασίες.
- Θα παρακολουθεί την εφαρμογή των διορθωτικών ενεργειών.
- Θα εκδίδει εκθέσεις συμμόρφωσης προς την Διοίκηση.

5. Θα παρέχει συμβουλές όσο αφορά, στην εκτίμηση αντικτύπου – DPIA – Data Protection Impact Assessment (εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα σχετικά με την προστασία των δεδομένων), θα παρακολουθεί την υλοποίηση της σύμφωνα με τον ΓΚΠΔ (GDPR, άρθρο 35) και θα καταρτίσει πρότυπο υποδείγματος Εκτίμησης Αντικτύπου.
6. Θα συνδράμει στην κατάρτιση του αρχείου δραστηριοτήτων επεξεργασίας, θα παρακολουθεί την επικαιροποίηση του και θα ελέγχει ότι, όλες οι επεξεργασίες προσωπικών δεδομένων, έχουν καταγραφεί (GDPR, άρθρο 30 & 39).
7. Θα συνεργάζεται με την εποπτική αρχή: Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) (GDPR, άρθρο 39, παρ.1 δ’ και ε΄).

Συγκεκριμένα:

- Θα αποτελεί το επίσημο σημείο επικοινωνίας με την ΑΠΔΠΧ.
- Θα συντονίζει τις απαντήσεις σε ελέγχους της ΑΠΔΠΧ.
- Θα παρέχει πληροφορίες και τεκμηρίωση της ΑΠΔΠΧ.
- Θα συμμετέχει σε συναντήσεις με την ΑΠΔΠΧ, όταν απαιτείται.

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

9. Θα συμμετέχει στον σχεδιασμό νέων υπηρεσιών ή πληροφοριακών συστημάτων, ώστε να εφαρμόζονται οι αρχές Privacy by Design και Privacy by Default (GDPR, άρθρο 25).
10. Δεσμεύεται από την τήρηση του απορρήτου ή της εμπιστευτικότητας σχετικά με την εκτέλεση των καθηκόντων του, σύμφωνα με το δίκαιο της Ευρωπαϊκής Ένωσης και του Ελληνικού Κράτους. Ο Ανάδοχος υποχρεούται, πριν από την έναρξη των εργασιών και την παροχή οποιασδήποτε πρόσβασης σε χώρους, συστήματα ή αρχεία του Νοσοκομείου, να αιτηθεί άδεια πρόσβασης. Η υποχρέωση αυτή βαραίνει εξίσου το νομικό πρόσωπο του Αναδόχου, τον ορισθέντα DPO, τον αναπληρωτή του, καθώς και το σύνολο των μελών της ομάδας έργου ή των υπαλλήλων του που θα απασχοληθούν στο έργο.
11. Θα παρέχει υποστήριξη στον Φορέα όσο αφορά, στην ικανοποίηση των δικαιωμάτων των ασθενών και εργαζομένων καθώς επίσης και στη διαχείριση περιστατικών παραβίασης δεδομένων (Data Breaches) σύμφωνα με τον ΓΚΠΔ (GDPR, άρθρα 33 & 34).
12. Θα παρέχει έγγραφες απαντήσεις και οδηγίες σε ερωτήματα του Νοσοκομείου που αφορούν σε διαχείριση αιτημάτων (GDPR, άρθρα 12 – 23):
    - Πρόσβασης.
    - Διόρθωσης.
    - Διαγραφής «δικαίωμα στη λήθη».
    - Περιορισμού.
    - Αναστολή Επεξεργασίας.
    - Εναντίωσης.
    - Αυτοματοποιημένης λήψης αποφάσεων.
13. Θα εκπαιδεύει το προσωπικό (GDPR, άρθρο 39, παρ.1’ β’).

    Συγκεκριμένα:
    - Θα οργανώσει πρόγραμμα εκπαίδευσης για το σύνολο του προσωπικού, όλων των κλάδων και ειδικοτήτων (τεκμηριωμένο με αρχείο εκπαίδευσης).
    - Θα συντάξει εκπαιδευτικό υλικό το οποίο θα διατεθεί σε ηλεκτρονική μορφή.

- Θα αξιολογεί τεκμηριωμένα το επίπεδο συμμόρφωσης του προσωπικού.

14. Θα εκπονήσει πολιτικές και διαδικασίες με σκοπό, την εφαρμογή των απαιτήσεων του ΓΚΠΔ.

Συγκεκριμένα: Θα εισηγηθεί και θα συντάξει πολιτικές και διαδικασίες προστασίας δεδομένων οι οποίες θα διατεθούν στον Φορέα σε ηλεκτρονική μορφή.

15. Θα διενεργήσει έλεγχο των συμβάσεων (GDPR, άρθρα 28 & 44-49).

Συγκεκριμένα:

- Θα διενεργήσει έλεγχο των συμβάσεων επεξεργασίας προσωπικών δεδομένων με τους προμηθευτές του Νοσοκομείου.
- Θα ελέγχει διαβιβάσεις δεδομένων σε τρίτες χώρες.

16. Υποχρεούται, να παρέχει έγκαιρη υποστήριξη σε περιπτώσεις παραβίασης ασφάλειας δεδομένων (data breaches), συμβουλευτική και υποστηρικτική συνδρομή προς τον Φορέα με σκοπό, την τήρηση της νόμιμης προθεσμίας των 72 ωρών, αναφορικά με τη γνωστοποίηση περιστατικών παραβίασης στην ΑΠΔΠΧ.
17. Θα λογοδοτεί απευθείας στη Διοίκηση του Νοσοκομείου που αποτελεί το πρώτο σημείο επαφής με το υποκείμενο των δεδομένων και επίσης θα συνεργάζεται με το Τμήμα Πληροφορικής του Φορέα, παρέχοντας υποστηρικτική και συμβουλευτική αρωγή, δεδομένης της άμεσης εμπλοκής του με το αντικείμενο απασχόλησής του (GDPR, άρθρο 32, 38 και 39).
18. Αφότου αναλάβει καθήκοντα, θα πρέπει να έχει μεριμνήσει και για τον αναπληρωτή του. Ο αναπληρωτής θα πρέπει να πληροί τις ίδιες ελάχιστες προϋποθέσεις και να εγκριθεί από τη Διοίκηση του Νοσοκομείου
19. Δεσμεύεται από την τήρηση του απορρήτου ή της εμπιστευτικότητας σχετικά με την εκτέλεση των καθηκόντων του, σύμφωνα με το δίκαιο της Ένωσης ή του κράτους – μέλους (GDPR, άρθρο 38 παρ. 5).

20. Ο ΥΠΔ μπορεί να επιτελεί και άλλα καθήκοντα και υποχρεώσεις. Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία διασφαλίζουν ότι τα εν λόγω καθήκοντα και υποχρεώσεις δεν συνεπάγονται σύγκρουση συμφερόντων.

ΤΡΟΠΟΣ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ

Ο Ανάδοχος, ως εξωτερικός συνεργάτης του Νοσοκομείου Χίου «ΣΚΥΛΙΤΣΕΙΟ» υποχρεούται να:

- Παρέχει φυσική παρουσία στο Νοσοκομείο (συσκέψεις όταν καλείται, έλεγχος συμμόρφωσης, επιθεωρήσεις, εκπαίδευση προσωπικού) σε συγκεκριμένες ημέρες, ο αριθμός των οποίων θα οριστεί στη σύμβαση.
- Παρέχει καθημερινή εξ' αποστάσεως υποστήριξη τηλεφωνικά ή ψηφιακά σε εργάσιμες ημέρες και ώρες.
- Ανταποκρίνεται άμεσα σε έκτακτες περιπτώσεις εντός εργάσιμου ωραρίου.

ΦΑΣΕΙΣ ΥΛΟΠΟΙΗΣΗΣ ΕΡΓΟΥ - ΠΑΡΑΔΟΤΕΑ - ΧΡΟΝΟΔΙΑΓΡΑΜΜΑ

Το έργο διαρθρώνεται σε τέσσερις (4) διακριτές αλλά αλληλένδετες Φάσεις Υλοποίησης. **Ο Ανάδοχος υποχρεούται να παραθέσει, στη Διοίκηση του Φορέα, το σύνολο των αρχείων, του μητρώου (RoPa), των μελετών (DPIA) και των παραδοτέων, σε επεξεργάσιμη ψηφιακή μορφή (.docx), τα οποία θα αποτελέσουν μόνιμη ιδιοκτησία του Φορέα.**

ΦΑΣΗ 1: ΔΙΑΓΝΩΣΤΙΚΗ ΜΕΛΕΤΗ ΥΦΙΣΤΑΜΕΝΗΣ ΚΑΤΑΣΤΑΣΗΣ – ΑΝΑΛΥΣΗ ΑΠΟΚΛΙΣΕΩΝ (GAP ANALYSIS) – ΚΑΤΑΓΡΑΦΗ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ ΕΠΕΞΕΡΓΑΣΙΑΣ

1. Πλήρης ενημέρωση της Διοίκησης και των στελεχών του Νοσοκομείου σχετικά με τις απαιτήσεις του ΓΚΠΔ.
2. Συνεργασία μέσω συναντήσεων και συνεντεύξεων με αρμόδια στελέχη του Φορέα (Διοίκηση, Τμήμα Πληροφορικής και λοιπές εμπλεκόμενες υπηρεσίες του Φορέα). **Για το σύνολο των ανωτέρω συναντήσεων, συνεντεύξεων και διαβουλεύσεων, ο Ανάδοχος υποχρεούται να συντάσσει και να τηρεί**

<u>αναλυτικά Πρακτικά Συναντήσεων, τα οποία θα συνυπογράφονται από τα συμμετέχοντα μέρη.</u>

3. Ο Ανάδοχος θα προβεί σε ενδελεχή έλεγχο, χαρτογράφηση και αξιολόγηση του βαθμού συμμόρφωσης του Νοσοκομείου με τις απαιτήσεις του ΓΚΠΔ (GDPR - ΕΕ 2016/679) και του Ν. 4624/2019. Ειδικότερα, ο Ανάδοχος θα προβεί σε αναγνώριση, καταγραφή και ταξινόμηση όλων των ροών δεδομένων προσωπικού χαρακτήρα (απλών και ειδικών κατηγοριών) που, τυγχάνουν επεξεργασίας από όλες τις οργανικές μονάδες του Νοσοκομείου (Διοικητική, Ιατρική, Νοσηλευτική και Τεχνική Υπηρεσία).

Διάρκεια: Μήνας 1ος – 2ος

<u>ΠΑΡΑΔΟΤΕΑ</u>

Π1.1: <u>Έκθεση Αξιολόγησης Αποκλίσεων (Gap Analysis Report) και Σχέδιο Άμεσων Ενεργειών Συμμόρφωσης: Αναλυτική αποτύπωση της οργανωτικής, τεχνικής και νομικής ωριμότητας του Φορέα, με συγκεκριμένο προσδιορισμό των ελλείψεων (gaps). Η έκθεση θα συνοδεύεται υποχρεωτικά από συγκεκριμένες προτάσεις, τεχνικές προδιαγραφές και ένα Σχέδιο Άμεσων Ενεργειών (Quick-Win Actions) για την άμεση αντιμετώπιση των πλέον κρίσιμων αποκλίσεων, καθώς και από ιεραρχημένη καταγραφή των απαιτούμενων διορθωτικών ενεργειών σε βάθος χρόνου (Risk Mitigation Plan)</u>

Π1.2: Μητρώο Δραστηριοτήτων Επεξεργασίας (Record of Processing Activities - RoPA): Σύνταξη και παραμετροποίηση του Μητρώου του άρθρου 30 του Κανονισμού (ΕΕ) 2016/679, στο οποίο, θα αποτυπώνονται πλήρως οι σκοποί επεξεργασίας, οι κατηγορίες υποκειμένων και δεδομένων, οι αποδέκτες, οι χρόνοι τήρησης (retention periods) καθώς και οι διαβιβάσεις δεδομένων (π.χ. προς ΥΠΕ, ΕΟΠΥΥ, ΗΔΙΚΑ).

<u>ΦΑΣΗ 2: ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΣΧΕΔΙΟ ΔΡΑΣΗΣ (ΣΥΝΤΑΞΗ ΠΟΛΙΤΙΚΩΝ – ΔΙΑΔΙΚΑΣΙΩΝ)</u>

1. Κατά την παρούσα Φάση, ο Ανάδοχος θα εκπονήσει το γενικό πλαίσιο καθώς επίσης και τις αρχές προστασίας δεδομένων του Φορέα.

2. Ο Ανάδοχος θα εκπονήσει το «Σχέδιο Δράσης» του Φορέα με σκοπό, τη συμμόρφωσή του στις απαιτήσεις του ΓΚΠΔ. Το εν λόγω σχέδιο θα περιλαμβάνει το σύνολο των πολιτικών και διαδικασιών για την αποτελεσματική προστασία των δεδομένων προσωπικού χαρακτήρα, με βάση τις απαιτήσεις του ΓΚΠΔ. Επιπλέον, θα εστιάζει στον τρόπο με τον οποίο θα πραγματοποιείται η συλλογή, αποθήκευση, επεξεργασία και διαχείριση των δεδομένων προσωπικού χαρακτήρα. Ειδικότερα, το σχέδιο δράσης θα περιλαμβάνει:

- 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 Προστασίας 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 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 συντήρησης 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 (οργανωτικές και τεχνικές) ανταπόκρισης σε αιτήματα για διαγραφή δεδομένων.
- Διαδικασίες καταγραφής παραπόνων σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα.
- Απαιτήσεις από τους προμηθευτές 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 προμηθευτές (right to audit).

3. Ο Ανάδοχος θα συντάξει το Εγχειρίδιο Αναγνώρισης Κινδύνων και Διαχείρισης Περιστατικών Ασφαλείας (Risk Assessment) με σκοπό, την πρόληψη, αποτροπή, άμεση αντιμετώπιση και την κατά το δυνατόν, βέλτιστη διαχείριση των δεδομένων προσωπικού χαρακτήρα, σε περιπτώσεις κινδύνου. **Επιπλέον, κατά την παρούσα φάση ο Ανάδοχος θα μεριμνήσει για την άμεση θωράκιση των νομικών κειμένων του Νοσοκομείου και την εκπαίδευση του ανθρώπινου δυναμικού, ώστε να διασφαλιστεί η κατανόηση και η ορθή εφαρμογή των νέων διαδικασιών.**

Διάρκεια: Μήνας 3ος – 5ος

ΠΑΡΑΔΟΤΕΑ

Π2.1: Πολιτική Ασφάλειας & Απορρήτου Δεδομένων Φορέα.

Π2.2: Επιχειρησιακό Σχέδιο Δράσης Φορέα: Σύνταξη πολιτικών – διαδικασιών και διάθεση στον Φορέα σε ψηφιακή μορφή.

Π2.3: Επιχειρησιακό Εγχειρίδιο Αναγνώρισης Κινδύνων & Διαχείρισης Περιστατικών Ασφαλείας (Data Breach & Risk Playbook):

Πρακτικός οδηγός (βήμα-βήμα) που περιλαμβάνει:

- Μητρώο Πιθανών Κινδύνων (Risk Register): Φυσικοί κίνδυνοι (π.χ. πρόσβαση σε φυσικούς ιατρικούς φακέλους), τεχνικοί κίνδυνοι (Ransomware, συστήματα τηλεϊατρικής) και ανθρώπινα σφάλματα.
- Διαδικασία Κλιμάκωσης (Escalation): Σαφές οργανόγραμμα σήμανσης εσωτερικού συναγερμού.
- Σχέδιο Δράσης 72 ωρών: Έτοιμα πρότυπα και φόρμες γνωστοποίησης προς την Αρχή Προστασίας Δεδομένων (ΑΠΔΠΧ).

Π2.4: Πρότυπα Κείμενα & Υποδείγματα Συμβάσεων (DPA): Τυποποιημένες ρήτρες συμμόρφωσης για τις συμβάσεις του Νοσοκομείου με εξωτερικούς αναδόχους και εκτελούντες την επεξεργασία (π.χ. εταιρείες συντήρησης λογισμικού, security).

Π2.5: Υλοποίηση Προγραμμάτων Εκπαίδευσης και Ευαισθητοποίησης: Πραγματοποίηση δύο σεμιναρίων για το σύνολο του προσωπικού (ένα διήμερο σεμινάριο με φυσική παρουσία και ένα Webinar δύο ωρών καθώς και μια επανάληψη αυτών).

Π2.6: Εκπαιδευτικό Υλικό: Σύνταξη και διάθεση του εκπαιδευτικού υλικού σε ψηφιακή μορφή.

ΦΑΣΗ 3: ΔΙΕΝΕΡΓΕΙΑ ΕΚΤΙΜΗΣΗΣ ΑΝΤΙΚΤΥΠΟΥ (DPIA)

Αξιολόγηση των κινδύνων σε κρίσιμες ψηφιακές υποδομές.

Διάρκεια: Μήνας 6ος – 7ος

ΠΑΡΑΔΟΤΕΑ

Π3.1: Μελέτη Εκτίμησης Αντικτύπου σχετικά με την Προστασία Δεδομένων (DPIA): Διενέργεια πλήρους και εξειδικευμένης μελέτης DPIA (βάσει του άρθρου 35 του GDPR) για τα πληροφοριακά συστήματα: HIS, LIS, PACS/RIS, ERP/MIS και το Σύστημα Τηλεϊατρικής του Νοσοκομείου.

ΦΑΣΗ 4: ΕΠΙΘΕΩΡΗΣΗ ΣΥΜΜΟΡΦΩΣΗΣ – ΠΑΡΟΥΣΙΑΣΗ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

1. Ο Ανάδοχος θα πραγματοποιήσει έλεγχο συμμόρφωσης του Φορέα που, θα περιλαμβάνει επιθεώρηση εργαζομένων, χώρου εργασίας, σημεία αποθήκευσης προσωπικών δεδομένων, έγγραφων και ηλεκτρονικών, η πρόσβασή τους καθώς επίσης και οι συμφωνίες εμπιστευτικότητας που, έχουν υπογραφεί με σκοπό, να επιβεβαιωθεί η διαφύλαξη της ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας των προσωπικών δεδομένων και των απαιτήσεων του ΓΚΠΔ.
2. Ο Ανάδοχος θα παρουσιάσει στη Διοίκηση και τα στελέχη του Φορέα τα αποτελέσματα της επιθεώρησης συμμόρφωσης με προτεινόμενες διορθωτικές ενέργειες.

Διάρκεια: Μήνας 8ος έως τη Λήξη της Σύμβασης

ΠΑΡΑΔΟΤΕΑ

Π4.1: Εξαμηνιαίες Εκθέσεις Πεπραγμένων και Ελέγχου Συμμόρφωσης.

Π4.2: Έλεγχος Συμμόρφωσης επικαιροποιημένος

Π4.3: Ετήσια Έκθεση Πεπραγμένων DPO: Τελική απολογιστική έκθεση προς τη Διοίκηση του Νοσοκομείου

ΣΥΝΟΠΤΙΚΟΣ ΠΙΝΑΚΑΣ ΠΑΡΑΔΟΤΕΩΝ & ΧΡΟΝΟΔΙΑΓΡΑΜΜΑΤΟΣ

Φάση	**Κωδικός Παραδοτέου**	**Τίτλος Παραδοτέου**	**Ορόσημο Παράδοσης (Milestone)**
Φάση 1	Π1.1, Π1.2	Έκθεση Gap Analysis & Σχέδιο Άμεσων Ενεργειών Μητρώο Δραστηριοτήτων (RoPA)	Τέλος 2ου Μήνα
Φάση 2	Π2.1, Π2.2, Π2.3, Π2.4, Π2.5, Π2.6	Πολιτικές Ασφαλείας, Επιχειρησιακό Σχέδιο, Playbook Κινδύνων, Πρότυπα Συμβάσεων, Υλοποίηση Εκπαιδευτικών Σεμιναρίων & Ψηφιακό Υλικό	Τέλος 5ου Μήνα
Φάση 3	Π3.1	Μελέτη-DPIA	Τέλος 7ου Μήνα
Φάση 4	Π4.1 Π4.2	Εξαμηνιαίες Αναφορές, Ετήσια Έκθεση DPO &	Λήξη Έργου

Φάση	Κωδικός Παραδοτέου	Τίτλος Παραδοτέου	Ορόσημο Παράδοσης (Milestone)
	Π4.3	Επικαιροποιημένος Έλεγχος Συμμόρφωσης	

ΔΙΚΑΙΩΜΑ ΣΥΜΜΕΤΟΧΗΣ – ΑΠΑΙΤΗΣΕΙΣ – ΚΡΙΤΗΡΙΑ ΕΠΙΛΟΓΗΣ

Δικαίωμα συμμετοχής έχει, **οποιαδήποτε εταιρεία ή φυσικό πρόσωπο που δραστηριοποιείται στο αντικείμενο (GDPR**, **με τεκμηριωμένη ικανότητα εκπλήρωσης των καθηκόντων που**, **αναφέρονται στο άρθρο 39 του εν λόγω Κανονισμού) με την προϋπόθεση ότι**:

1. Αποδέχεται τις απαιτήσεις που αφορούν, στην εκτέλεση καθηκόντων και υποχρεώσεων του παρόντος.
2. πληροί τις προϋποθέσεις *όσο* αφορά, στα κριτήρια επιλογής υποψήφιου Αναδόχου βάσει τεχνικής και επαγγελματικής επάρκειας, όπως περιγράφονται στο παρόν.

ΤΕΧΝΙΚΗ ΚΑΙ ΕΠΑΓΓΕΛΜΑΤΙΚΗ ΕΠΑΡΚΕΙΑ ΑΝΑΔΟΧΟΥ

Ο Ανάδοχος απαιτείται να:

1. Διαθέτει (σε ισχύ) Σύστημα Διαχείρισης Ποιότητας (ΣΔΠ) και πιστοποίηση κατά ISO 9001:2015 με πεδίο εφαρμογής, την παροχή υπηρεσιών υπεύθυνου Προστασίας Προσωπικών Δεδομένων (DPO).
2. Διαθέτει (σε ισχύ) Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών και πιστοποίηση κατά ISO 27001: 2022 ή νεότερο, με πεδίο εφαρμογής, την παροχή υπηρεσιών υπεύθυνου Προστασίας Προσωπικών Δεδομένων (DPO).
3. Διαθέτει τεκμηριωμένη εμπειρία τουλάχιστον τριών ετών (3) και υλοποίηση τουλάχιστον (3) έργων συμμόρφωσης με τον ΓΚΠΔ, σε δευτεροβάθμιο ή τριτοβάθμια δημόσιο φορέα υγείας, ως Υπεύθυνος Προστασίας Προσωπικών Δεδομένων (DPO). Η υλοποίηση τεκμηριώνεται με την προσκόμιση των αντίστοιχων βεβαιώσεων / συμβάσεων των φορέων υλοποίησης.