ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ ΓΙΑ ΤΟ ΕΡΓΟ

«ΕΦΑΡΜΟΓΗ ΤΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (GDPR) ΚΑΙ ΥΠΟΣΤΗΡΙΞΗΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (DPO)»

Αντικείμενο του διαγωνισμού είναι η συμμόρφωση και εναρμόνιση του Γενικού Νοσοκομείου Βενιζέλειο- Πανάνειο (εφεξής «ΦΟΡΕΑΣ ΕΦΑΡΜΟΓΗΣ») προς τον «ΓΕΝΙΚΟ ΚΑΝΟΝΙΣΜΟ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ - GDPR» - Κανονισμός (ΕΕ) 2016/679 και παροχή υπηρεσιών Data Protection Officer (DPO).

Ο Γενικός Κανονισμός για την Προστασία των δεδομένων της ΕΕ «General Data Protection Regulation - GDPR», εγκρίθηκε στις 14 Απριλίου 2016, δημοσιεύθηκε στην Επίσημη Εφημερίδα της ΕΕ στις 4 Μαΐου 2016 *και ενσωματώθηκε στην Ελληνική Νομοθεσία με το Ν. 4624/2019 (29/8/2019)*

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 συμμόρφωσης στις απαιτήσεις του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας των Προσωπικών Δεδομένων.

Το έργο θα αφορά σε όλες τις λειτουργικές μονάδες του Νοσοκομείου, οι οποίες διαχειρίζονται προσωπικά δεδομένα. Στόχος είναι η δημιουργία κουλτούρας προστασίας των προσωπικών δεδομένων στους εργαζόμενους του Νοσοκομείου, καθώς και η ενσωμάτωση της προστασίας προσωπικών δεδομένων σας λειτουργίες του Νοσοκομείου σχετικά με α) την επεξεργασία των προσωπικών δεδομένων σε όλο τον κύκλο ζωής τους, ήτοι από τη συλλογή έως και την καταστροφή τους, β) τις προϋποθέσεις μεταφοράς τους, γ) την προστασία των δικαιωμάτων των φυσικών προσώπων, 6) την ασφάλεια όπως εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα, των προσωπικών δεδομένων και τις ενέργειες γνωστοποίησης που οφείλει να κάνει το Νοσοκομείο σε περίπτωση παραβίασης.

Το έργο περιλαμβάνει υπηρεσίες για τη διενέργεια μελέτης ωριμότητας του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ έναντι του νέου Κανονισμού με σκοπό του προσδιορισμό του επιπέδου συμμόρφωσης του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ με τις διατάξεις του κανονισμού GDPR, καθώς και υπηρεσίες Διαχείρισης και Υλοποίησης του έργου συμμόρφωσης προς τον παραπάνω Κανονισμό, Η μελέτη ωριμότητας θα αξιολογεί όλους τους, τομείς δραστηριότητας του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ ως προς την ετοιμότητά τους έναντι του GDPR, θα εντοπίζει όλες τις περιοχές, όπου δεν παρατηρείται πλήρης ετοιμότητα και απαιτούνται ενέργειες συμμόρφωσης, θα εμβαθύνει στις ανωτέρω περιοχές και θα προτείνει συγκεκριμένα μέτρα, ώστε Ο ΦΟΡΕΑΣ ΕΦΑΡΜΟΓΗΣ να ξεκινήσει εγκαίρως την υλοποίηση όλων των διορθωτικών ενεργειών συμμόρφωσης. Στο αντικείμενο του έργου συμπεριλαμβάνονται η ανάπτυξη των Δραστηριοτήτων Επεξεργασίας (DataInventory and FlowMapping), η εκπόνηση Μελέτη Ανάλυσης Ελλείψεων και Αποκλίσεων (GapAnalysis), η σύνταξη Πλάνου Συμμόρφωσης (CompliancePlan) καί Ανάλυσης του Αντίκτυπου στην Προστασία Προσωπικών Δεδομένων (PrivacyImpactAssessment) και η εκπαίδευση του προσωπικού του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ, όπως ορίζονται από τον κανονισμό GDPR και τα οποία θα αποτελούν βασικά παραδοτέα του έργου (αναλύονται ακολούθως).

ΠΕΡΙΓΡΑΦΗ

Ως πρώτο βήμα, είναι απαραίτητος ο νομικός προσδιορισμός της έννοιας του φυσικού προσώπου αναφορικά με τον GDPR. Στο πλαίσιο αυτό πρέπει να προσδιοριστούν οι ρόλοι του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ που εμπίπτουν στο πεδίο του GDPR καθώς και η εθνική νομοθεσία ή οι διεθνείς συνθήκες από τις οποίες προκύπτουν οι ρόλοι αυτοί.

Αναλυτικά το έργο περιλαμβάνει:

- Ανάλυση της τρέχουσας κατάστασης ως προς την προστασία των προσωπικών δεδομένων που διαχειρίζεται ο ΦΟΡΕΑΣ ΕΦΑΡΜΟΓΗΣ και ειδικότερα, την αξιολόγηση των υφιστάμενων πρακτικών, των γραπτών πολιτικών και διαδικασιών, των πληροφοριακών συστημάτων και δικτυακών υποδομών και κάθε στοιχείου που επηρεάζει την προστασία, και την ασφάλεια των προσωπικών δεδομένων σε όλες τις δραστηριότητες και τις υπηρεσιακές μονάδες του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ.
- Δημιουργία λεπτομερών ροών δεδομένων (Data Flow mapping} ανά τμήμα ή ανά κατηγορία προσωπικών δεδομένων, όπου θα απεικονίζονται όλες οι πληροφορίες σχετικά με τη διαχείριση των προσωπικών δεδομένων στο ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ με σκοπό τη δημιουργία του αρχείου δραστηριοτήτων επεξεργασίας δεδομένων που αποτελεί απαίτηση του GDPR,
- Εντοπισμός κενών και ελλείψεων ως προς τις απαιτήσεις του κανονισμού (Gap Analysis), κατηγοριοποιημένα ανά θεματική περιοχή και κρισιμότητα.
- Λεπτομερής αξιολόγηση που θα καταδεικνύει τον βαθμό ετοιμότητας συμμόρφωσης του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ σε σχέση με τις απαιτήσεις του GDPR, τα βασικά κενά και τους κινδύνους. Για κάθε κενό που εντοπίζεται, είναι απαραίτητος ο καθορισμός των απαραίτητων ενεργειών αντιμετώπισης και η δημιουργία ενός λεπτομερούς, ιεραρχημένου και ολοκληρωμένου πλάνου ενεργειών συμμόρφωσης (Compliance Plan and Roadmap).
- Σύνταξη Μελέτης Εκτίμησης αντίκτυπου (Privacy Impact Assessment) με βάση τα προβλεπόμενα στον Κανονισμό.
- Εκπόνηση των απαραίτητων Πολιτικών και Διαδικασιών Προστασίας Προσωπικών Δεδομένων,

Ασφάλειας Πληροφοριών και Επιχειρησιακής Συνέχειας με βάση τα προτεινόμενα μέτρα του πλάνου συμμόρφωσης.

Ειδικότερα η αξιολόγηση που θα καταδεικνύει το βαθμό ετοιμότητας συμμόρφωσης του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ θα περιλαμβάνει, τουλάχιστον, τα εξής:

- Αξιολόγηση της νομικής βάσης, στην οποία στηρίζεται η συλλογή του συνόλου των συλλεγόμενων προσωπικών δεδομένων, της παρεχόμενης συναίνεσης από τον εκάστοτε συμβαλλόμενο, των παρεχόμενων πληροφοριών κλπ.
- Αξιολόγηση της δυνατότητας ικανοποίησης των δικαιωμάτων των φυσικών προσώπων
- Αξιολόγηση του επιπέδου ασφαλείας και επιχειρησιακής συνέχειας
- Αξιολόγηση της επάρκειας της οργανωτικής δομής
- Αξιολόγηση των υφιστάμενων συμβάσεων του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ με Τρίτους Φορείς που εκτελούν επεξεργασία προσωπικών δεδομένων του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ
- Αξιολόγηση των υφιστάμενων συμβάσεων του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ με Τρίτους φορείς που αποστέλλουν/κοινοποιούν προσωπικά δεδομένα στο ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ
- Αξιολόγηση της νομιμότητας και της ασφαλούς διαβίβασης προσωπικών δεδομένων
- Αξιολόγηση του επιπέδου ωριμότητας και ευαισθητοποίησης του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ στα θέματα προστασίας προσωπικών δεδομένων
- Αξιολόγηση των πληροφοριακών συστημάτων
- Αξιολόγηση των μέτρων προστασίας και των μηχανισμών ελέγχου (measures and controls) και διασφάλισης της συμμόρφωσης
- Αξιολόγηση σχετικών γραπτών πολιτικών και διαδικασιών

Με σκοπό την επιτυχή υλοποίηση των σκοπών του έργου, ο υποψήφιος ανάδοχος είναι απαραίτητο στη μεθοδολογία που θα ακολουθήσει να:

- Αναλύσει την τρέχουσα κατάσταση των πληροφοριακών συστημάτων και δικτυακών υποδομών, των υφιστάμενων πολιτικών, διαδικασιών και πρακτικών, οι οποίες σχετίζονται με την ασφάλεια των πληροφοριών, την επιχειρησιακή συνέχεια και την προστασία των προσωπικών δεδομένων
- Διεξάγει συνεντεύξεις με προσωπικό του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ, καλύπτοντας σε αντιπροσωπευτικό επίπεδο, κάθε δραστηριότητα των Υπηρεσιακών Μονάδων του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ,
- Παρέχει ένα λεπτομερές data flow map ανά μονάδα/τμήμα, ή ανά κατηγορία προσωπικών δεδομένων με σκοπό την πλήρη συμβατότητα με τις απαιτήσεις του κανονισμού GDPR σχετικά με τα αρχεία των δραστηριοτήτων επεξεργασίας.
- Χρησιμοποιήσει συγκεκριμένη μεθοδολογία και εργαλείο λογισμικού για τον εντοπισμό των προσωπικών δεδομένων στα ψηφιακά συστήματα του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ, τα αποτελέσματα των οποίων θα χρησιμοποιήσει, σε συνδυασμό με άλλες μεθοδολογίες, για την ανάπτυξη των Data Flow Maps και τη δημιουργία του αρχείου δραστηριοτήτων επεξεργασίας δεδομένων. Το συγκεκριμένο αρχείο θα περιλαμβάνει, κατ' ελάχιστο, την τεκμηρίωση της νομικής βάσης πάνω στην οποία στηρίζεται η συλλογή της παρεχόμενης συναίνεσης (π.χ. λόγω εθνικής νομοθεσίας ή εποπτικού ρόλου) από τον εκάστοτε συμβαλλόμενο, των παρεχόμενων πληροφοριών, κ.α.
- Πραγματοποιήσει δειγματοληπτικό έλεγχο σε όλες τις εφαρμογές και αποθηκευτικά μέσα (ψηφιακά, έντυπα, αναλογικής εικόνας και ήχου κ.α.) που τηρούν και επεξεργάζονται προσωπικά δεδομένα, καθώς και να προτείνει με σαφήνεια τις απαιτούμενες αλλαγές και τροποποιήσεις βάσει του νέου κανονισμού.
- Διεξάγει λεπτομερή αξιολόγηση των επιπτώσεων στην προστασία και ασφάλεια των δεδομένων, αξιολογώντας τους κινδύνους που σχετίζονται με θέματα ασφάλειας των πληροφοριών και με νομικά ζητήματα προστασίας δεδομένων και δίνοντας προτεραιότητα στα ευρήματα, ανάλογα με το επίπεδο κινδύνου.
- Δημιουργήσει λεπτομερές πλάνο ενεργειών αντιμετώπισης και διαχείρισης των ευρημάτων, έτσι ώστε οι επικεφαλής των αρμόδιων Τμημάτων, σε συνεργασία με την Επιτροπή Παρακολούθησης του Έργου, να είναι σε θέση να εφαρμόσουν τις ενέργειες που θα προταθούν. Πιο συγκεκριμένα, ο Ανάδοχος του έργου θα παρέχει λίστα προτάσεων σχετικά με τις αναγκαίες δράσεις αντιμετώπισης (συμπεριλαμβανομένων και των προτεινόμενων τεχνολογικών λύσεων) για κάθε κενό ή έλλειψη που προκύπτει.
- Πραγματοποιήσει έλεγχο και αξιολόγηση, κατά το εφικτό, όλων των συμβάσεων του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ με Τρίτους Φορείς, με σκοπό να εντοπίσει κενά στην προστασία και επεξεργασία προσωπικών δεδομένων και να προτείνει παράλληλα ενέργειες με σκοπό την προσαρμογή τους στον GDP

Όλες οι προτεινόμενες ενέργειες συμμόρφωσης είναι απαραίτητο να καλύπτουν ολόκληρο τον κύκλο ζωής των προσωπικών δεδομένων (δηλ. συλλογή, καταγραφή, τροποποίηση / ενημέρωση, αποθήκευση, μεταφορά, διαγραφή / καταστροφή κ.λπ.) και να έχουν συμφωνηθεί με την Επιτροπή Παρακολούθησης Έργου και τη Διοίκηση του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ πριν την παράδοση του πλάνου συμμόρφωσης.

ΦΑΣΕΙΣ ΤΟΥ ΕΡΓΟΥ - ΠΑΡΑΔΟΤΕΑ

ΦΑΣΗ 1: Συγκέντρωση δεδομένων.

Η φάση αύτη περιλαμβάνει τις ακόλουθες δράσεις:

- Επισκόπηση των επιχειρησιακών, τεχνικών και λειτουργικών διαδικασιών.
- Συγκέντρωση των απαιτούμενων πληροφοριών για τη συλλογή και επεξεργασία των προσωπικών δεδομένων, μέσω της διενέργειας συνεντεύξεων με το αρμόδιο προσωπικό όλων των Τμημάτων,
- Δημιουργία διαγραμμάτων ροής δεδομένων που θα αποτυπώνουν τις φάσεις του κύκλου ζωής των δεδομένων, από τη συλλογή, χρήση, αποθήκευση, μεταφορά μέχρι και την καταστροφή τους,
- Δημιουργία του αρχείου δραστηριοτήτων και πόρων επεξεργασίας του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ με έμφαση σε όλες τις κρίσιμες περιοχές επεξεργασίας.
- Εντοπισμός προσωπικών δεδομένων σε συστήματα με δομημένες και αδόμητες πληροφορίες του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ.
- Εντοπισμός των κρίσιμων αποκλίσεων έναντι των απαιτήσεων του Κανονισμού GDPR.

Επισημαίνεται ότι η χαρτογράφηση των δεδομένων αναμένεται να γίνει και μέσω συνεντεύξεων και θα καλύπτει περιοχές όπως δεδομένα σε Φυσικό Αρχείο, Έντυπη /Ψηφιακή ή Αναλογική μορφή (πχ. CCTV), εμπλεκόμενες εφαρμογές/εργαλεία και λόγους συλλογής τους από το ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ.

Παραδοτέα φάσης 1:

- Αναφορές με προσωπικά δεδομένα που εντοπίστηκαν στα συστήματα προς ανάλυση.
- Data Flow Mapping που θα καλύπτει την απαίτηση του GDPR σχετικά με το αρχείο δραστηριοτήτων επεξεργασίας δεδομένων και θα περιέχουν όλες τις επιπλέον απαραίτητες πληροφορίες, ώστε να απεικονίζεται πλήρως η τρέχουσα κατάσταση ως προς τη διαχείριση προσωπικών δεδομένων και να είναι εφικτός ο εντοπισμός κενών ως προς τις απαιτήσεις του θεσμικού πλαισίου {διαγράμματα ροής δεδομένων προσωπικού χαρακτήρα, με κρίσιμες πληροφορίες).

ΦΑΣΗ 2: Μελέτη ανάλυσης Ελλείψεων και Αποκλίσεων (Gap Analysis)

Η φάση αύτη περιλαμβάνει τις ακόλουθες δράσεις:

1. Μελέτη υφιστάμενης κατάστασης ως προς τη διαχείριση προσωπικών δεδομένων από άποψη:
   - Νομική
   - Οργάνωσης, Πολιτικών Και Διαδικασιών
   - Ασφάλειας Πληροφοριών
   - Τεχνολογική
2. Εντοπισμός των πεδίων μη συμμόρφωσης στις πρακτικές και διαδικασίες που εφαρμόζονται κατά τον χειρισμό των προσωπικών δεδομένων, ως προς:
   - τις απαιτήσεις του GDPR
   - το κανονιστικό πλαίσιο του έργου, συμπεριλαμβανομένων σχετικών δικαστικών αποφάσεων
3. Μελέτη ως προς τις υφιστάμενες επεξεργασίες δεδομένων (και της διαβαθμίσεώς τους) σε συνδυασμό με τα εμπλεκόμενα συστήματα πληροφορικής του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ
4. Αναγνώριση των υφιστάμενων αποκλίσεων από τις απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων ως προς τις επιμέρους περιοχές επεξεργασίας προσωπικών δεδομένων
5. Μελέτη αποκλίσεων της υφιστάμενης κατάστασης του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ σε σχέση με τις απαιτήσεις του Κανονισμού για κάθε επεξεργασία. Η μελέτη θα πρέπει να περιλαμβάνει τουλάχιστον τις παρακάτω περιοχές:
   - Απαιτήσεις ως προς την υποχρέωση τήρησης αρχείου δραστηριοτήτων
   - Συναίνεση
   - Συλλογή, Χρήση, Αποθήκευση
   - Διατήρηση δεδομένων/Καταστροφή
   - Δικαιώματα πρόσβασης, διόρθωσης, αλλαγής, φορητότητας και διαγραφής
   - Κοινοποίηση σε Τρίτα Μέρη
   - Διαβίβαση σε τρίτες χώρες
   - Ασφάλεια επεξεργασίας προσωπικών δεδομένων
   - Έλεγχος και παρακολούθηση των οργανωτικών και τεχνολογικών μέτρων
   - Πόροι
   - Γνωστοποίηση παραβίασης Προσωπικών Δεδομένων σε εποπτική αρχή ή/και στο υποκείμενο των δεδομένων
   - Καταγραφή των σχετικών ευρημάτων σε σχέση με το βαθμό ετοιμότητας συμμόρφωσης του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ και τις επιμέρους αποκλίσεις που παρουσιάζει σε σχέση με τις ανωτέρω απαιτήσεις.

Παραδοτέα φάσης 2:

- Gap Analysis

ΦΑΣΗ 3: Διενέργεια Privacy Impact Assessment και Ανάπτυξη σχεδίου διορθωτικών ενεργειών.

Η φάση αυτή περιλαμβάνει τις ακόλουθες δράσεις:

- Διενέργεια Privacy Impact Assessment με βάση τις έγκυρες πρακτικές και μεθοδολογίες, που αναφέρθηκαν ανωτέρω
- Σύνταξη αναλυτικού και σαφούς σχεδίου στο οποίο θα;
  -συμπεριλαμβάνονται οι προτάσεις βελτίωσης ανά τμήμα και Μονάδα του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ, με σκοπό την αντιμετώπιση των ελλείψεων ή/και αποκλίσεων σε σχέση με τις απαιτήσεις του Κανονισμού και τις απαιτήσεις του ευρύτερου κανονιστικού πλαισίου και των προτύπων, όπως αναλύεται παραπάνω
  -προσδιορίζονται συγκεκριμένες ενέργειες και εργασίες, ώστε να βελτιωθεί κατά το δυνατόν συντομότερα το επίπεδο συμμόρφωσης
  -περιλαμβάνονται προτάσεις με σκοπό τη συμμόρφωση με τον GDPR μέσω της τροποποίησης υφιστάμενων διαδικασιών, της τροποποίησης του περιβάλλοντος λειτουργίας των πληροφοριακών συστημάτων, της διατήρησης στο μέλλον ικανοποιητικού επίπεδου συμμόρφωσης και της συστηματικής αύξησης του επιπέδου συμμόρφωσης σε χρονικό επίπεδο που θα προσδιοριστεί σε συνεργασία με το ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ.

Παραδοτέα φάσης 3:

- Privacy Impact Assessment
- Compliance Plan που να συμπεριλαμβάνει προτάσεις αλλαγών για την ικανοποίηση των απαιτήσεων στις διαδικασίες, τα μη ψηφιακά αρχεία και τα Πληροφοριακά Συστήματα του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ.

ΦΑΣΗ 4: Υλοποίηση μέρους των διορθωτικών ενεργειών,

Η φάση αύτη περιλαμβάνει τις ακόλουθες δράσεις, εφόσον αυτές κριθούν απαραίτητες βάσει των παραδοτέων των προηγούμενων Φάσεων:

- Υποβολή πρόσθετων προτάσεων για την υλοποίηση πρωτοβουλιών που θα αυξήσουν το επίπεδο συμμόρφωσης με τον GDPR, λαμβάνοντας υπόψη καθιερωμένα πρότυπα ασφάλειας
- Υλοποίηση από του Ανάδοχο δράσεων εκπαίδευσης ***που θα αφορούν το σύνολα του προσωπικού του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ*** που εμπλέκεται στην επεξεργασία προσωπικών δεδομένων, τόσο κατά τη διάρκεια της εργασίας του, όσο και να παράσχει μαζική εκπαίδευση για να δοθεί μια συνολική εικόνα του νέου τρόπου λειτουργίας. Επίσης υποχρεούται να διαθέσει και ενημερωτικό υλικό προσαρμοσμένο στις ανάγκες του προσωπικού.
- Σύνταξη πολιτικών διασφάλισης προσωπικών δεδομένων
- διενέργεια πλήρους Εσωτερικής Επιθεώρησης {Internal Audit) που να καλύπτουν όλες τις παραπάνω πολιτικές και διαδικασίες, ώστε αυτές να εφαρμόζονται και να είναι πιστοποιήσιμες κατά τα αντίστοιχα πρότυπα.

Παραδοτέα Φάσης 4:

- Δράσεις εκπαίδευσης και επιμόρφωσης συνοδευόμενες από εκπαιδευτικό και ενημερωτικό υλικό
- Προτεινόμενες διορθωτικές ενέργειες για κάθε επιθεωρούμενα τμήμα του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ μετά από το Internal Audit

ΦΑΣΗ 5: Συνεχιζόμενη διενέργεια εσωτερικών επιθεωρήσεων (Internal Audit) και ενδυνάμωση κουλτούρας προσωπικού αναφορικά με την ασφάλεια και προστασία των προσωπικών δεδομένων

- Η τελευταία φάση περιλαμβάνει προγραμματισμό και εσωτερικές επιθεωρήσεις σε μηνιαία βάση που συνοδεύονται εκάστη με αναλυτικές εκθέσεις και οδηγίες για βελτιωτικές δράσεις και ενέργειες, και θα ελέγχεται το επίπεδο γνώσης και συμμόρφωσης των εργαζομένων. Θα επιθεωρούνται όλοι οι εργαζόμενοι, οι χώροι εργασίας τους, τα σημεία αποθήκευσης των προσωπικών δεδομένων, έγγραφων και ηλεκτρονικών, η πρόσβαση σε αυτά, καθώς και ο τρόπος επικοινωνίας με τους συνεργάτες, το είδος της πληροφορίας που ανταλλάσσεται (στην περίπτωση που ανταλλάσσονται προσωπικά δεδομένα) και η αποθήκευσή της.

Παραδοτέα Φάσης 5:

- Μηνιαίες αναλυτικές εκθέσεις εσωτερικών επιθεωρήσεων με προτεινόμενες διορθωτικές δράσεις

ΥΠΗΡΕΣΙΕΣ ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΑΝΑΠΛΗΡΩΤΗ ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΕΟΜΕΝΩΝ

- Με την υπογραφή της σύμβασης, ξεκινάει η περίοδος υποστήριξης του συνόλου των διαδικασιών στο πλαίσιο εφαρμογής του GDPR, η οποία θα έχει χρονική διάρκεια ίση με 2 έτη. Τα βασικά πακέτα εργασιών που θα περιλαμβάνουν οι υπηρεσίες υποστήριξης είναι τα ακόλουθα:
- Πλήρεις και ολοκληρωμένες υπηρεσίες ΥΠΔ (DPO) (αντίστοιχα και του Α.Υ,Π.Δ.): Θα ορίσει ο υποψήφιος ανάδοχος τον (εξωτερικό) ΥΠΔ (ΚΑΙ ΑΝΑΠΛΗΡΩΤΗ ΤΟΥ) 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.

ΠΡΟΫΠΟΘΕΣΕΙΣ ΣΥΜΜΕΤΟΧΗΣ

- Ο υποψήφιος Ανάδοχος πρέπει να διαθέτει τις ακόλουθες δεξιότητες και εμπειρογνωμοσύνη:
  - ✓ Εμπειρογνωσία στον τομέα Δικαίου και των πρακτικών περί προστασίας δεδομένων, τόσο σε εθνικό όσο και σε ευρωπαϊκό επίπεδο, καθώς και άριστη γνώση του ΓΚΠΔ, ν' Γνώση των πράξεων επεξεργασίας που διενεργούνται,
  - ✓ Γνώση του τομέα τεχνολογιών πληροφοριών και της ασφάλειας δεδομένων,
  - ✓ Γνώση του τομέα δραστηριότητας του οργανισμού,
  - ✓ Ικανότητα ανάπτυξης νοοτροπίας προστασίας των δεδομένων στους κόλπους του οργανισμού.

- Όλες οι προτάσεις είναι απαραίτητο να βασίζονται και να λαμβάνουν υπόψη εκτός από τον Κανονισμό Γενικής Προστασίας Δεδομένων (GDPR), το υφιστάμενο Ελληνικό Νομοθετικό Πλαίσιο (συμπεριλαμβανομένης της νομολογίας), τις κατευθυντήριες γραμμές για το GDPR που δημοσιεύονται από την Ομάδα Εργασίας για την Προστασία Δεδομένων του Άρθρου 29 (WP 29), τις κατευθυντήριες οδηγίες, γνωμοδοτήσεις και αποφάσεις της Ελληνικής Αρχής Προστασίας Προσωπικών Δεδομένων (καθώς και τις κατά περίπτωση κατευθυντήριες γραμμές ή αποφάσεις άλλων Ευρωπαϊκών Αρχών Προστασίας Προσωπικών Δεδομένων) και τις βέλτιστες πρακτικές σύμφωνα με τα διεθνή πρότυπα.

- Ο υποψήφιος Ανάδοχος πρέπει να συμπεριλάβει στην προσφορά ***του Χρονοδιάγραμμα δραστηριοτήτων*** - προγραμματισμό φάσεων υλοποίησης έργου (σύμφωνα με τα ανωτέρω των επιμέρους φάσεων).

  - ✓ Ο υποψήφιος ανάδοχος θα πρέπει να διαθέτει αποδεδειγμένη εξειδίκευση, επιστημονική γνώση και τουλάχιστον 4/ετή εμπειρία σε έργα ασφάλειας πληροφοριακών συστημάτων και προστασίας δεδομένων. Επίσης τετραετή εμπειρία στην παροχή συμβουλευτικών υπηρεσιών οργάνωσης, ελεγκτικής εκπόνησης πολιτικών και βελτιστοποίησης επιχειρησιακών διαδικασιών σε δημόσιους φορείς υγείας που διαθέτουν κλίνες νοσηλείας. Επίσης θα πρέπει να διαθέτει αποδεδειγμένη 2/ετή τουλάχιστον εμπειρία στην ανάλυση και αξιολόγηση κινδύνων με πιστοποιήσεις σχετικές με το αντικείμενο. Όλα τα ανωτέρω να αποδεικνύονται με την επισύναψη των σχετικών εγγράφων.
    Επιπλέον ο Υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία, ήτοι ο φορέας Γ.Ν.Β.Π. ,θα διασφαλίσει ότι η άσκηση των καθηκόντων του ΥΠΔ δεν οδηγεί σε σύγκρουση συμφερόντων.

  - ✓ Ο υποψήφιος Ανάδοχος θα πρέπει να έχει διεκπεραιώσει τουλάχιστον πέντε (5) παρόμοια έργα έναντι του κανονισμού **GDPR** στην Ελλάδα και ένα (1) τουλάχιστον από αυτά να αφορά δημόσιο ή ιδιωτικό Νοσοκομείο με προσωπικό άνω των 400 εργαζομένων. Ως εκ τούτου, θα πρέπει να περιέχεται στη προσφορά, λίστα με πληροφορίες για παρόμοια έργα υλοποίησης GDPR,

  - ✓ Η Ομάδα Έργου του υποψηφίου Αναδόχου θα πρέπει να περιλαμβάνει έμπειρα στελέχη, πτυχιούχων Πανεπιστημιακής εκπαίδευσης, με πιστοποιημένα καλή γνώση της Αγγλικής γλώσσας, που έχουν εμπλακεί σε ολοκληρωμένα έργα GDPR και τα οποία θα καλύπτουν κατ' ελάχιστο τις ακόλουθες κατηγορίες:

    1. Υπεύθυνος έργου – Υπεύθυνος Προστασίας Δεδομένων με αποδεδειγμένη εμπειρία συμβουλευτικών έργων σε Δημόσιους φορείς Υγείας για τουλάχιστον δύο έτη. Επιπλέον απαραίτητη προϋπόθεση είναι να είναι πιστοποιημένος & ορισμένος DPO σε πέντε (5) τουλάχιστον Δημόσιους ή ιδιωτικούς οργανισμούς, οι τέσσερεις (4) εκ των οποίων σε Δημόσιους φορείς υγείας που διαθέτουν κλίνες νοσηλείας.
    2. Ένα πιστοποιημένο Αναπληρωτή Υπεύθυνο Προστασίας Δεδομένων με αντίστοιχα προσόντα.
    3. Ένα (1) Νομικό Σύμβουλο, με επιστημονική εξειδίκευση και εμπειρία σε προστασία

δεδομένων (με σχετική πιστοποίηση). Απαραίτητη προϋπόθεση είναι να είναι ορισμένος DPO σε τουλάχιστον ένα οργανισμό.

4. Ένα (1) μέλος της ομάδας με εξειδίκευση με θέματα Πληροφορικής και εμπειρία σε θέματα ασφάλειας πληροφοριακών συστημάτων τουλάχιστον τεσσάρων (4) ετών, σε φορείς υγείας άνω των 3 ετών.

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. Απαραίτητη προϋπόθεση για να συμμετέχει υποψήφιος ανάδοχος είναι να διαθέτει Σύστημα Διαχείρισης Ποιότητας και πιστοποίηση κατά το πρότυπο ISO9001:2015.

Απαραίτητη επιπλέον προϋπόθεσή είναι η πιστοποίηση του Αναδόχου σύμφωνα με το πρότυπο ISO27001:2013, αναφορικά με την ασφάλεια των πληροφοριακών συστημάτων.

Το έργο θα εκπονηθεί σε συνεργασία με τα αρμόδια στελέχη της Επιτροπής Παρακολούθησης Έργου που θα συστήσει ο ΦΟΡΕΑΣ ΕΦΑΡΜΟΓΗΣ, αμέσως μετά την υπογραφή σύμβασης με τον ΑΝΑΔΟΧΟ.

- ✓ Απαραίτητη προϋπόθεση είναι η αυτοπρόσωπη παρουσία μία με δυο φορές την εβδομάδα και η δυνατότητα επικοινωνίας μέσω τηλεδιάσκεψης με στελέχη του φορέα για οποιοδήποτε θέμα προκύπτει του ορισμένου DPO (Υ.Π.Π.Δ.), (αντίστοιχα του Α.Υ.Π.Δ.)
- ✓ Ο ορισμένος DPO (Υ.Π.Δ.), (αντίστοιχα ο Α.Υ.Π.Δ.) θα παρέχει γραπτή γνωμοδότηση επί θεμάτων Γ.Κ.Π.Δ. όταν του ζητηθεί από τις ομάδες εργασίας του φορέα.

Η προσφορά θα περιλαμβάνει περιγραφή της μεθοδολογίας υλοποίησης, καθώς και αναφορά στις τεχνικές θα χρησιμοποιηθούν για την παροχή των σχετικών υπηρεσιών.

ΠΑΡΑΚΟΛΟΥΘΗΣΗ - ΠΑΡΑΛΑΒΗ ΕΡΓΟΥ

Η παραλαβή των υπηρεσιών θα γίνεται ανά φάση από την Επιτροπή Παρακολούθησης Έργου που θα ορίσει ο ΦΟΡΕΑΣ ΕΦΑΡΜΟΓΗΣ. Με την παράδοση από τον Ανάδοχο του μέρους του έργου που αντιστοιχεί στη συγκεκριμένη Φάση, η Επιτροπή Παρακολούθησης συντάσσει πρακτικό οριστικής παραλαβής, το οποίο επιβεβαιώνει ότι τα παραδοτέα της Φάσης αυτής πληρούν τις προδιαγραφές της σχετικής σύμβασης.
Μετά την επιτυχή ολοκλήρωση του συνόλου των Φάσεων του Έργου, συντάσσεται από την Επιτροπή Παρακολούθησης το Πρακτικό Ολοκλήρωσης, το οποίο επιβεβαιώνει την οριστική παραλαβή του συνόλου του έργου.

ΧΡΟΝΟΔΙΑΓΡΑΜΜΑ ΥΛΟΠΟΙΗΣΗΣ

Το έργο θα πρέπει να έχει ολοκληρωθεί συνολικά σε δύο (2) έτη από την υπογραφή της σύμβασης και με το ακόλουθο χρονοδιάγραμμα υλοποίησης φάσεων:

- ✓ Φάση 1, εντός δύο μηνών από την ημερομηνία υπογραφής της σύμβασης.
- ✓ Φάση 2, εντός 1 μήνα από την ολοκλήρωση της Φάσης 1.
- ✓ Φάση 3, εντός 1 μήνα από την ολοκλήρωση της Φάσης 2,
- ✓ Φάση 4 εντός 2 μηνών από την ολοκλήρωση της Φάσης 3 και τέλος.
- ✓ Φάση 5 μέχρι την ολοκλήρωση της διετίας της ισχύος της σύμβασης.

ΕΧΕΜΥΘΕΙΑ, ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ

Ο Ανάδοχος οφείλει τόσο κατά τη διάρκεια ισχύος της σύμβασης όσο και μετά τη λήξη αυτής, χωρίς χρονικό περιορισμό, να μην αποκαλύπτει ή με οποιονδήποτε τρόπο αφήνει να διαρρεύσουν σε τρίτους και να μη χρησιμοποιεί, με κανένα τρόπο ή μέσο, οποιαδήποτε στοιχεία σχετικά με το ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ, καθώς επίσης να αποτρέπει με κάθε νόμιμο μέσο την ανακοίνωση αυτών. Κατά τη διάρκεια των υπηρεσιών ο Ανάδοχος απαιτείται να χειριστεί ευαίσθητα προσωπικά δεδομένα του φορέα Εφαρμογής. Θα πρέπει να εγγυηθεί την εχεμύθεια των αποτελεσμάτων, καθώς επίσης και όσων δεδομένων συλλεχθούν κατά την υλοποίηση της εργασίας, μέσω Ειδικού Συμφωνητικού Εχεμύθειας και Εμπιστευτικότητας που θα συντάξει και θα υπογράφει με την έναρξη της εργασίας και θα καλύπτει όλα τα αποτελέσματα, καθώς και όλες τις πληροφορίες που πρέπει να ανακτηθούν κατά τη διάρκεια της εργασίας. Αναλαμβάνει την ευθύνη για τη διασφάλιση της εμπιστευτικότητας των εμπλεκόμενων συμβούλων και τεχνικών, όσον αφορά τη μη διαρροή πληροφοριών του είδους, του βαθμού διεκπεραίωσης της εργασίας καθώς και τις λεπτομέρειες αυτού, σε οιοδήποτε άτομο ή ομάδα ατόμων.