ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΥΓΕΙΑΣ
7η ΥΠΕ ΚΡΗΤΗΣ
ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΧΑΝΙΩΝ
'' Ο ΑΓΙΟΣ ΓΕΩΡΓΙΟΣ '

ΧΑΝΙΑ: 27 -05 -2019
ΑΡ. ΠΡΩΤΟΚ: 11596

ΣΥΝΟΠΤΙΚΑ ΣΤΟΙΧΕΙΑ ΔΙΑΓΩΝΙΣΜΟΥ

Το Γενικό Νοσοκομείο Χανίων « Ο Άγιος Γεώργιος» με το θέμα19/ΠΡΚ15/09-05-2019(ΑΔΑ:ΨΑ946907Τ-ΞΨΒ) του Διοικητικού Συμβουλίου και έχοντας υπόψη τις διατάξεις του Ν2286/95, Ν3329/2005, Ν2955/01,το Νόμο 4412/2016 (ΦΕΚ 147/Α/08-08-2016) Δημόσιες Συμβάσεις Έργων, Προμηθειών και Υπηρεσιών (προσαρμογή στις Οδηγίες 2014/24/ ΕΕ και 2014/25/ΕΕ). Όπως αυτός ισχύει

ΑΝΑΚΟΙΝΩΝΕΙ ΤΗΝ ΕΡΕΥΝΑ ΑΓΟΡΑΣ ΣΧΕΤΙΚΑ ΜΕ
«Εφαρμογή του γενικού κανονισμού για την προστασία των προσωπικών δεδομένων (GDPR) και υποστήριξης υπευθύνου προστασίας δεδομένων (DPO)» CPV (79417000-0)

ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ	Γενικό Νοσοκομείο Χανίων «Ο ΑΓΙΟΣ ΓΕΩΡΓΙΟΣ»
ΕΙΔΟΣ ΔΙΑΓΩΝΙΣΜΟΥ	Έρευνα Αγοράς μέσω της πλατφόρμας i-supplies
ΚΡΙΤΗΡΙΟ ΚΑΤΑΚΥΡΩΣΗΣ	Την πλέον συμφέρουσα από οικονομική άποψη προσφορά μόνο βάσει τιμής
ΗΜΕΡΟΜΗΝΙΑ ΛΗΞΗΣ ΥΠΟΒΟΛΗΣ ΠΡΟΣΦΟΡΩΝ	ΟΙ ΟΙΚΟΝΟΜΙΚΕΣ ΠΡΟΣΦΟΡΕΣ ΝΑ ΚΑΤΑΤΕΘΟΥΝ ΥΠΟΧΡΕΩΤΙΚΑ ΗΛΕΚΤΡΟΝΙΚΑ ΜΕΣΩ ΤΗΣ ΠΛΑΤΦΟΡΜΑΣ « i-supplies» εως την Δευτέρα 03-06-2019 και ώρα 12:00 μμ ΤΑ ΛΟΙΠΑ ΔΙΚΑΙΟΛΟΓΗΤΙΚΑ ΣΕ ΠΕΡΙΠΤΩΣΗ ΑΔΥΝΑΜΙΑΣ ΚΑΤΑΧΩΡΗΣΗΣ ΣΤΗΝ ΠΛΑΤΦΟΡΜΑ (ΛΟΓΩ ΟΓΚΟΥ) ΝΑ ΑΠΟΣΤΑΛΟΥΝ ΣΤΟ MAIL: apontikaki@chaniahospital.gr
ΤΟΠΟΣ ΔΙΕΝΕΡΓΕΙΑΣ	Γενικό Νοσοκομείο Χανίων «Ο ΑΓΙΟΣ ΓΕΩΡΓΙΟΣ»
ΠΕΡΙΓΡΑΦΗ ΥΠΗΡΕΣΙΑΣ	**«Εφαρμογή του γενικού κανονισμού για την προστασία των προσωπικών δεδομένων (GDPR) και υποστήριξης υπευθύνου προστασίας δεδομένων (DPO)» CPV (79417000-0)**
Κωδικός Αριθμού Εξόδου (ΚΑΕ)	0439-12.000,00 ευρώ
ΑΡΙΘΜΟΣ ΑΙΤΗΜΑΤΟΣ (REQ)	**19REQ005005936**
ΠΡΟΫΠΟΛΟΓΙΣΘΕΙΣΑ ΔΑΠΑΝΗ	Προϋπολογισμός : **12.000 ,00** ευρώ συμπ.Φ.Π.Α.24% Προϋπολογισμός: **9.677,42** ευρώ άνευ .Φ.Π.Α. 24%
ΧΡΟΝΟΣ ΚΑΙ ΤΟΠΟΣ ΠΑΡΑΔΟΣΗΣ	Γενικό Νοσοκομείο Χανίων «Ο ΑΓΙΟΣ ΓΕΩΡΓΙΟΣ»

	Σημείωση: Διάρκεια ισχύος των προσφορών : 120 ημέρες.
ΜΟΝΑΔΑ ΜΕΤΡΗΣΗΣ	ΥΠΗΡΕΣΙΑ
ΠΛΗΡΟΦΟΡΙΕΣ	Τηλ: 28210 22335 Ηλ. Ταχ/μείο: apontikaki@chaniahospital.gr

Ο ΔΙΟΙΚΗΤΗΣ ΤΟΥ ΓΕΝ ΝΟΣΟΚΟΜΕΙΟΥ ΧΑΝΙΩΝ

ΒΟΥΛΓΑΡΙΔΗΣ ΜΗΝΑΣ

ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ ΓΙΑ ΤΗΝ

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

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, προτεραιοποιημένου 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 ασφάλειας 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 GDPR

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:

- ⇨ Μελέτη υφιστάμενης κατάστασης ως προς τη διαχείριση προσωπικών δεδομένων από άποψη:
  - ✓ Νομική
  - ✓ Οργάνωσης, Πολιτικών Και Διαδικασιών
  - ✓ Ασφάλειας Πληροφοριών
  - ✓ Τεχνολογική
- ⇨ 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
- ⇨ Μελέτη ως προς τις υφιστάμενες επεξεργασίες δεδομένων (και της διαβαθμίσεώς τους) σε συνδυασμό με τα εμπλεκόμενα συστήματα πληροφορικής του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ
- ⇨ Αναγνώριση των υφιστάμενων αποκλίσεων από τις απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων ως προς τις επιμέρους περιοχές επεξεργασίας προσωπικών δεδομένων
- ⇨ 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

i. της τροποποίησης υφιστάμενων διαδικασιών,
ii. της τροποποίησης του περιβάλλοντος λειτουργίας των πληροφοριακών συστημάτων,
iii. της διατήρησης στο μέλλον ικανοποιητικού επίπεδου συμμόρφωσης
iv. 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 δράσεων εκπαίδευσης

⇨ Σύνταξη πολιτικών

⇨ 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

⇨ Προτεινόμενες διορθωτικές ενέργειες για κάθε επιθεωρούμενο τμήμα του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ μετά από το Internal Audit

ΥΠΗΡΕΣΙΕΣ ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ
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 1 έτος. Τα βασικά πακέτα εργασιών που θα περιλαμβάνουν οι υπηρεσίες υποστήριξης είναι τα ακόλουθα:

⇨ Πλήρεις και ολοκληρωμένες υπηρεσίες ΥΠΔ (DPO): Θα ορίσει ο υποψήφιος ανάδοχος τον (εξωτερικό) ΥΠΔ 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.

ΕΙΔΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ

⇨ 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

⇨ Ο υποψήφιος Ανάδοχος θα πρέπει να διαθέτει εμπειρία στην παροχή συμβουλευτικών υπηρεσιών ελεγκτικής, οργάνωσης, εκπόνησης πολιτικών και βελτιστοποίησης επιχειρησιακών διαδικασιών. Επίσης θα πρέπει να διαθέτει αποδεδειγμένη εμπειρία στην ανάλυση και αξιολόγηση κινδύνων. Τουλάχιστον ο Υπεύθυνος

έργου της ανάδοχης εταιρείας πρέπει να κατέχει πιστοποιήσεις σχετικές με τη διαχείριση κινδύνων και ανάλογη προϋπηρεσία σε αντίστοιχη θέση. Όλα τα ανωτέρω να αποδεικνύονται με την επισύναψη των σχετικών εγγράφων.

- ⇨ Ο υποψήφιος Ανάδοχος θα πρέπει να έχει διεκπεραιώσει παρόμοια έργα στην Ελλάδα ή το εξωτερικό και να διαθέτει αποδεδειγμένη εμπειρία ολοκλήρωσης έργων αξιολόγησης έναντι του κανονισμού GDPR. 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 που έχουν εμπλακεί σε ολοκληρωμένα έργα GDPR και τα οποία θα καλύπτουν κατ' ελάχιστο τις ακόλουθες κατηγορίες:
  - Υπεύθυνος έργου με τουλάχιστον 4ετή αποδεδειγμένη εμπειρία εκπαίδευσης σε δημόσιους φορείς καθώς και αποδεδειγμένη εμπειρία συμβουλευτικών - ελεγκτικών έργων σε Δημόσιους Φορείς Υγείας για τουλάχιστον δύο έτη. Επιπλέον απαραίτητη προϋπόθεση είναι να είναι ορισμένος DPO σε έναν τουλάχιστον οργανισμό.
  - Ένα (1) Πιστοποιημένο Εσωτερικό Ελεγκτή με αποδεδειγμένη εμπειρία σε έργα ελεγκτικά-συμβουλευτικά σε Δημόσιους Φορείς Υγείας άνω των τριών ετών. Επιπλέον απαραίτητη προϋπόθεση είναι να είναι ορισμένος DPO σε έναν τουλάχιστον οργανισμό.
  - Ένα (1) Νομικό Σύμβουλο, με επιστημονική εξειδίκευση και εμπειρία σε προστασία δεδομένων (με σχετική πιστοποίηση).
  - Ένα (1) μέλος της ομάδας με εξειδίκευση με θέματα Πληροφορικής και εμπειρία σε θέματα ασφάλειας πληροφοριακών συστημάτων.

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.

- ⇨ Το έργο θα εκπονηθεί σε συνεργασία με τα αρμόδια στελέχη της Επιτροπής Παρακολούθησης Έργου που θα συστήσει ο ΦΟΡΕΑΣ ΕΦΑΡΜΟΓΗΣ.

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

ΔΙΚΑΙΟΛΟΓΗΤΙΚΑ ΔΙΑΓΩΝΙΣΜΟΥ

Ο οικονομικός φορέας που λαμβάνει μέρος στον παραπάνω διαγωνισμό οφείλει να υποβάλει ηλεκτρονικά τα εξής έγγραφα δικαιολογητικά τα οποία αποσφραγίζονται και ελέγχονται κατά την **διαδικασία της αξιολόγησης** της προσφοράς .

α) Όσον αφορά την παράγραφο 1 του άρθρου73, Απόσπασμα του σχετικού μητρώου, όπως του ποινικού μητρώου ή, ελλείψει αυτού, ισοδύναμου εγγράφου που εκδίδεται από αρμόδια δικαστική ή διοικητική αρχή του κράτους-μέλους ή της χώρας καταγωγής ή της χώρας όπου είναι εγκατεστημένος ο εν λόγω οικονομικός φορέας, από το οποίο προκύπτει ότι πληρούνται αυτές οι προϋποθέσεις. Η υποχρέωση προσκόμισης του ως άνω αποσπάσματος αφορά και τα πρόσωπα του δεύτερου εδαφίου της παραγράφου 1 του άρθρου 73.

β) Όσον αφορά την παράγραφο 2 του άρθρου 73, πιστοποιητικό που εκδίδεται από την αρμόδια αρχή του οικείου κράτους - μέλους ή χώρας, από το οποίο να προκύπτει ότι είναι ενήμεροι ως προς τις υποχρεώσεις τους που αφορούν τις εισφορές κοινωνικής ασφάλισης (κύριας και επικουρικής) και ως προς τις φορολογικές τους υποχρεώσεις.

γ) Όσον αφορά την παράγραφο 4, περίπτωση β' του άρθρου 73, πιστοποιητικό που εκδίδεται από την αρμόδια αρχή του οικείου κράτους - μέλους ή χώρας, από το οποίο να προκύπτει ότι δεν τελεί υπό πτώχευση ή έχει υπαχθεί σε διαδικασία εξυγίανσης ή ειδικής εκκαθάρισης ή τελεί υπό αναγκαστική διαχείριση από εκκαθαριστή ή από το δικαστήριο ή έχει υπαχθεί σε διαδικασία πτωχευτικού συμβιβασμού ή έχει αναστείλει τις επιχειρηματικές του δραστηριότητες ή εάν βρίσκεται σε οποιαδήποτε ανάλογη κατάσταση προκύπτουσα από παρόμοια διαδικασία, προβλεπόμενη σε εθνικές διατάξεις νόμου

Αν το κράτος-μέλος ή η χώρα του οικονομικού φορέα δεν εκδίδει τα έγγραφα ή πιστοποιητικά ή όπου το έγγραφα ή το πιστοποιητικά δεν καλύπτουν όλες τις ως άνω περιπτώσεις α) – γ) (όπως αυτά αναφέρονται και στις παράγραφος 1 και 2 και στην περίπτωση β' της παραγράφου 4 του άρθρου 73), τα έγγραφα ή τα πιστοποιητικά μπορεί να αντικαθίσταται από ένορκη βεβαίωση ή, στα κράτη - μέλη ή στις χώρες όπου δεν προβλέπεται ένορκη βεβαίωση, από υπεύθυνη δήλωση του ενδιαφερομένου ενώπιον αρμόδιας δικαστικής ή διοικητικής αρχής, συμβολαιογράφου ή αρμόδιου επαγγελματικού ή εμπορικού οργανισμού του κράτους -μέλους ή της χώρας καταγωγής ή της χώρας όπου είναι εγκατεστημένος ο οικονομικός φορέας.

δ) Για την απόδειξη της απαίτησης της παραγράφου 1α) και 2 του άρθρου 75, Πιστοποιητικό/βεβαίωση του οικείου επαγγελματικού μητρώου του Παραρτήματος XI του Προσαρτήματος Α' του Ν. 4412/2016, με το οποίο πιστοποιείται η εγγραφή του οικονομικού φορέα σε αυτό. Για την απόδειξη άσκησης γεωργικού ή κτηνοτροφικού επαγγέλματος, οι οικονομικοί φορείς προσκομίζουν σχετική βεβαίωση άσκησης επαγγέλματος, από αρμόδια διοικητική αρχή ή αρχή Οργανισμού Τοπικής Αυτοδιοίκησης.