



Ημ/νία 08/01/2020

Αρ. πρωτ. 128

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

Υπουργείο Υγείας

5ηΥ.Πε. Θεσσαλίας & Στερεάς Ελλάδας

ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΑΜΦΙΣΣΑΣ

Διεύθυνση Διοικητικού

Οικονομικό Τμήμα

Προς: Κάθε ενδιαφερόμενο

Ταχ. δ/ση: * 33100 Άμφισσα

Πληροφ.: Μήτσας Θοδωρής

Τηλ.: (22653) 50131

Fax: (22653) 22086

E-mail: diax4@gnamfissas.gr**1^η Δημόσια Διαβούλευση**

επί των Τεχνικών Προδιαγραφών για την Εκπόνηση Σχεδίου Δράσης για την συμμόρφωση των Λειτουργιών και Διαδικασιών του Νοσοκομείου με βάση τον νέο Κανονισμό Ε/Ε 2016/679 (GDPR) για τα προσωπικά δεδομένα» με κριτήριο κατακύρωσης της πλέον συμφέρουσα από οικονομική άποψη προσφορά μόνο βάσει τιμής και εκτιμώμενης αξίας:

1. Η διάρκεια της διαβούλευσης ορίζεται σε δέκα (10) ημέρες από την επομένη της ημερομηνίας ανάρτησης στον ιστότοπο της 5ης ΥΠΕ Θεσσαλίας και Στερεάς Ελλάδας (www.dypethessaly.gr) και του Νοσοκομείου: (www.gnamfissas.gr),
2. Οι ενδιαφερόμενοι μπορούν να αποστείλουν τις παρατηρήσεις τους, καθώς και να ζητήσουν διευκρινήσεις στην ηλεκτρονική διεύθυνση diax4@gnamfissas.gr

Σας ευχαριστούμε εκ των προτέρων για τη συμμετοχή σας στη διαδικασία.

- Η -

ΔΙΟΙΚΗΤΡΙΑ ΤΟΥ Γ. Ν. ΑΜΦΙΣΣΑΣ**ΑΥΓΕΡΙΝΟΥ ΕΥΦΡΟΣΥΝΗ**

ΤΕΧΝΙΚΗ ΠΕΡΙΓΡΑΦΗ

ΑΝΤΙΚΕΙΜΕΝΟ ΤΟΥ ΔΙΑΓΩΝΙΣΜΟΥ

Αντικείμενο του διαγωνισμού είναι η λήψη συμβουλευτικών υπηρεσιών με σκοπό τη συμμόρφωση του Γενικού Νοσοκομείου Άμφισσας (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 και δημοσιεύθηκε στην Επίσημη Εφημερίδα της ΕΕ στις 4 Μαΐου 2016. Ο GDPR προβλέπεται να εφαρμοστεί άμεσα σε όλα τα κράτη μέλη της ΕΕ από τις 25 Μαΐου 2018. Συγχρόνως, θα καταργήσει και θα αντικαταστήσει την οδηγία 95/46/ΕΚ και τη νομοθεσία εφαρμογής των κρατών μελών της (N2472/1997).

Το έργο περιλαμβάνει υπηρεσίες για τη διενέργεια μελέτης ωριμότητας του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ έναντι του νέου Κανονισμού με σκοπό τον 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 (Data Inventory and Flow Mapping), η εκπόνηση Μελέτης Ανάλυσης Ελλείψεων και Αποκλίσεων (Gap Analysis), η σύνταξη Πλάνου Συμμόρφωσης (Compliance Plan) και Ανάλυσης του Αντίκτυπου στην Προστασία Προσωπικών Δεδομένων (Privacy Impact Assessment) και η εκπαίδευση του προσωπικού του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ, όπως ορίζονται από τον κανονισμό GDPR και τα οποία θα αποτελούν βασικά παραδοτέα του έργου.

ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΕΡΓΟΥ

Ως πρώτο βήμα του έργου, 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 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 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 αυτή 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, Έγχαρτη/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 αυτή 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 επιπέδου 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 αυτή 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 εμπειρία εκπαίδευσης σε δημόσιους φορείς καθώς και αποδεδειγμένη εμπειρία συμβουλευτικών - ελεγκτικών έργων σε Δημόσιους Φορείς Υγείας. 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. 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.

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.

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.

Ακολουθούν τα Παραρτήματα Α, Β και Γ τα οποία αποτελούν αναπόσπαστο τμήμα των Τεχνικών Προδιαγραφών.

ΒΑΣΙΚΑ ΣΤΟΙΧΕΙΑ & ΑΡΧΕΣ ΕΡΓΟΥ

Τα βασικά στοιχεία του Κανονισμού τα οποία θα πρέπει να ληφθούν υπόψη κατά την υλοποίηση του ως άνω έργου είναι τα ακόλουθα:

- ⇒ **Πληροφόρηση και Διαφάνεια:** τα υποκείμενα φυσικά πρόσωπα να ενημερώνονται συνοπτικά, κατανοητά, εύκολα και με διαφάνεια για τις πηγές προέλευσης των προσωπικών δεδομένων, το σκοπό ή τους σκοπούς της επεξεργασίας των προσωπικών δεδομένων, τη νομική βάση ή το έννομο συμφέρον της επεξεργασίας, τους αποδέκτες των πληροφοριών, τη διαβίβαση ή / και την πρόθεση διαβίβασης σε τρίτη χώρα, τη χρήση τους ή/και την πρόθεση χρήσης για δημιουργία προφίλ ή αυτοματοποιημένης λήψης αποφάσεων, την πρόθεση ή / και τη χρήση για άλλους σκοπούς, την ταυτότητα και τα στοιχεία επικοινωνίας του ΦΟΡΕΑ ΕΦΑΡΜΟΓΗΣ, το χρονικό διάστημα της αποθήκευσης των δεδομένων, τα δικαιώματα των φυσικών προσώπων καθώς και τα δικαιώματα υποβολής καταγγελιών ή/και ανάκλησης συγκατάθεσης.
- ⇒ **Δικαίωμα στη λήθη:** Όταν εκλείπει ο λόγος της επεξεργασίας των δεδομένων ή το υποκείμενο αίρει τη συγκατάθεσή του (σε περίπτωση που αυτή είναι αναγκαία), ή όταν τα δεδομένα υποβλήθηκαν σε παράνομη επεξεργασία κ.τ.λ. το υποκείμενο έχει δικαίωμα να ζητήσει τη διαγραφή των δεδομένων και ο υπεύθυνος επεξεργασίας έχει υποχρέωση άμεσα να τα διαγράψει και, αν τα έχει δημοσιοποιήσει, να ενημερώσει και όλους τους άλλους που τα έχουν αναδημοσιεύσει, ότι το υποκείμενο ζήτησε τη διαγραφή τους .
- ⇒ **Σαφής συγκατάθεση:** Το κάθε άτομο (ενδιαφερόμενο φυσικό πρόσωπο) πρέπει να δώσει τη συγκατάθεσή του για την επεξεργασία των προσωπικών του δεδομένων
- ⇒ **Ψευδωνυμοποίηση:** Ο υπεύθυνος επεξεργασίας και οι εκτελούντες στην επεξεργασία οφείλουν να χρησιμοποιούν μεθόδους προστασίας των προσωπικών δεδομένων όπως κρυπτογράφηση, ψευδώνυμα, απόκρυψη της πληροφορίας (Data masking) κλπ.
- ⇒ **Δικαίωμα φορητότητας των δεδομένων:** Το υποκείμενο (ενδιαφερόμενο φυσικό πρόσωπο) έχει δικαίωμα να ζητά από τον υπεύθυνο επεξεργασίας να λαμβάνει τα δεδομένα σε κοινώς αναγνωρίσιμο μορφότυπο, καθώς και να ζητά την απευθείας διαβίβαση των δεδομένων του σε άλλον υπεύθυνο επεξεργασίας
- ⇒ **Προστασία των Προσωπικών Δεδομένων εκ του σχεδιασμού και εξ ορισμού (Privacy by Design & by Default):** Κάθε νέα υπηρεσία/προϊόν, λογισμικό ή διαδικασία θα πρέπει να σχεδιάζεται λαμβάνοντας υπόψη τις επιταγές του κανονισμού GDPR

- ⇒ **Υποχρέωση γνωστοποίησης παραβιάσεων ασφάλειας:** Όταν ο υπεύθυνος επεξεργασίας λάβει γνώση της παραβίασης της ασφάλειας του συστήματος οφείλει να ειδοποιήσει την ανεξάρτητη αρχή που είναι υπεύθυνη για την προστασία προσωπικών δεδομένων εντός του προβλεπόμενου χρονικού ορίου. Ο υπεύθυνος επεξεργασίας πρέπει να εξετάζει αν η γνωστοποίηση πρέπει να γίνει και στα ίδια τα υποκείμενα των δεδομένων με στόχο τη δημιουργία κλίματος εμπιστοσύνης αλλά και για λόγους υπευθυνότητας και διαφάνειας
- ⇒ **Διασυννοριακή διαβίβαση δεδομένων:** Η οδηγία περιλαμβάνει ξεκάθαρους κανόνες για τη διαβίβαση των προσωπικών δεδομένων από τις αρχές επιβολής του νόμου σε αρχές εκτός της ΕΕ, έτσι ώστε να μην υπονομεύεται το επίπεδο προστασίας των φυσικών προσώπων που είναι κατοχυρωμένο στην ΕΕ
- ⇒ **Πρόστιμα από μη συμμόρφωση:** Ημη συμμόρφωση με τους κανόνες προστασίας προσωπικών δεδομένων επιφέρει και πρόστιμα στις επιχειρήσεις που τον παραβιάζουν έως 20 εκατομμύρια € ή 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών ("τζίρος") του προηγούμενου οικονομικού έτους
- ⇒ **Αρχές ως προς την ποιότητα των δεδομένων:** Ο υπεύθυνος επεξεργασίας πρέπει να επιβεβαιώνει ότι τηρούνται οι ακόλουθες αρχές προστασίας δεδομένων:
 - ✓ **Πρώτη Αρχή: Νόμιμη Επεξεργασία (Lawful Processing):** Τα προσωπικά δεδομένα θα πρέπει να επεξεργάζονται με θεμιτό και νόμιμο τρόπο
 - ✓ **Δεύτερη Αρχή: Προσδιορισμός του Σκοπού (Purpose Specification):** Τα προσωπικά δεδομένα θα πρέπει να λαμβάνονται μόνο για έναν ή περισσότερους συγκεκριμένους και νόμιμους σκοπούς, και δεν πρέπει να υποβάλλονται σε περαιτέρω επεξεργασία με οποιονδήποτε τρόπο ασυμβίβαστο με το σκοπό ή τους σκοπούς αυτούς.
 - ✓ **Τρίτη Αρχή: Ελαχιστοποίηση και Σχετικότητα Δεδομένων (Data Relevancy):** Τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι κατάλληλα, συναφή, όχι υπερβολικά και να περιορίζονται σε αυτά που είναι απαραίτητα για την επίτευξη του σκοπού ή των σκοπών για τους οποίους υφίστανται επεξεργασία.
 - ✓ **Τετάρτη Αρχή: Ακρίβεια Δεδομένων (Data Accuracy):** Τα προσωπικά δεδομένα πρέπει να είναι ακριβή και, εφόσον χρειάζεται, να ενημερώνονται.
 - ✓ **Πέμπτη Αρχή: Περιορισμένη Διατήρηση Δεδομένων (Limited Data Retention):** Τα προσωπικά δεδομένα που έχουν τύχει επεξεργασίας για οποιονδήποτε σκοπό ή σκοπούς δεν θα πρέπει να διατηρούνται για μεγαλύτερο

χρονικό διάστημα από ότι είναι απαραίτητο για το σκοπό αυτό ή τους σκοπούς αυτούς

- ✓ **Έκτη Αρχή: Θεμιτή Επεξεργασία (Fair Processing):** Τα προσωπικά δεδομένα θα πρέπει να υποβάλλονται σε επεξεργασία με εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα, σύμφωνα με τα δικαιώματα των φυσικών προσώπων όπως αυτά προβλέπονται από τον κανονισμό
- ✓ **Έβδομη Αρχή: Λογοδοσία (Accountability):** Θα πρέπει να ληφθούν τα κατάλληλα διοικητικά, τεχνικά και οργανωτικά μέτρα, με τρόπο που να αποδεικνύονται, έναντι μη εξουσιοδοτημένης ή παράνομης επεξεργασίας δεδομένων προσωπικού χαρακτήρα και έναντι τυχαίας απώλειας ή καταστροφής, ή βλάβης, ή άλλης ζημιάς στα προσωπικά δεδομένα που τηρούνται από την επιχείρηση

ΠΑΡΑΡΤΗΜΑ ΠΡΟΫΠΟΛΟΓΙΣΜΟΣ

Η προϋπολογισθείσα **δαπάνη για το έργο υλοποίησης** εκτιμάται στο ποσό των € (**συμπ. ΦΠΑ**). Οι υπηρεσίες υποστήριξης για ένα (1) έτος.

Το κριτήριο κατακύρωσης θα είναι η οικονομικότερη προσφορά στο σύνολο των ανωτέρω.