

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
7^η Υ.ΠΕ. ΚΡΗΤΗΣ
Γ.Ν. ΛΑΣΙΘΙΟΥ-Γ.Ν.-ΚΥ ΝΕΑΠΟΛΕΩΣ
«Διαλυνάκειο»

ΑΝΑΡΤΗΤΕΑ

ΑΠΟΣΠΑΣΜΑ ΠΡΑΚΤΙΚΟΥ ΣΥΝΕΔΡΙΑΣΗΣ ΤΟΥ ΔΙΟΙΚΗΤΙΚΟΥ
ΣΥΜΒΟΥΛΙΟΥ ΤΩΝ ΔΙΑΣΥΝΔΕΟΜΕΝΩΝ ΝΠΔΔ Γ.Ν.ΛΑΣΙΘΙΟΥ
Γ.Ν.ΚΥ.ΝΕΑΠΟΛΕΩΣ «ΔΙΑΛΥΝΑΚΕΙΟ» ΜΕ ΑΡΙΘΜΟ 27/17-10-2019

Στον Άγιο Νικόλαο σήμερα 17-10-2019 ημέρα Πέμπτη και ώρα 10,30π.μ. ύστερα από την με αρ.πρωτ. 2186/15-10-2019 πρόσκληση της Προέδρου, συνεδρίασε το Διοικητικό Συμβούλιο του ΝΠΔΔ με την επωνυμία <<Γενικό Νοσοκομείο Λασιθίου – Γ.Ν.-ΚΥ Νεαπόλεως «Διαλυνάκειο»>>.

Στην συνεδρίαση προεδρεύει η Κοινή Διοικήτρια κ.Σπινθούρη Μαρία και παρίστανται ο Αντιπρόεδρος κ.Μιχελάκης Εμμανουήλ Αναπληρωτής Διοικητής της Α.Ο.Μ.Σητείας, τα τακτικά μέλη Αρακαδάκης Γεώργιος Αναπληρωτής Διοικητής της Α.Ο.Μ.Ιεράπετρας, Βασιλαράς Ηλίας Αιρετός Εκπρόσωπος Ιατρών και Μανουσάκης Γεώργιος Αιρετός Εκπρόσωπος των λοιπών Εργαζομένων.

Στην συνεδρίαση παρίσταται η Γραμματέας του ΔΣ Κουμάκη Μαρία.

ΑΠΟΦΑΣΗ 725

ΘΕΜΑ 15^ο: Έγκριση σκοπιμότητας, τεχνικών προδιαγραφών, έγκριση διενέργειας συνοπτικού διαγωνισμού ανάθεσης υπηρεσιών Υπευθύνου Προστασίας Δεδομένων (DPO), με σκοπό τη Συμμόρφωση του Γ.Ν.Λασιθίου-Γ.Ν.-Κ.Υ.Νεαπόλεως «Διαλυνάκειο», με το «Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR)» – Κανονισμός (ΕΕ) 2016/679 για τις ανάγκες Γ.Ν. Λασιθίου - Γ.Ν.-Κ.Υ. Νεαπόλεως «Διαλυνάκειο», έγκριση τευχών διακήρυξης και ορισμός επιτροπής αποσφράγισης-αξιολόγησης

Το Δ/κό Σ/λιο αφού έλαβε υπόψη του

1. Την με αρ.πρωτ. 2070/8-10-2019 αναφορά της Οικονομικής Υπηρεσίας της Οργανικής Μονάδας Έδρας Αγίου Νικολάου σχετικά με έγκριση σκοπιμότητας, τεχνικών προδιαγραφών, διενέργειας του εν θέματι αναφερόμενου διαγωνισμού συνολικού προϋπολογισμού 22.473,09€ πλέον ΦΠΑ η οποία επιμερίζεται σύμφωνα με τον αριθμό των ανεπτυγμένων κλινών ανά νοσοκομείο.
2. Την εισήγηση της προέδρου του και την διαλογική συζήτηση μεταξύ των μελών του.

ΟΜΟΦΩΝΑ ΑΠΟΦΑΣΙΖΕΙ

Α. Εγκρίνει την σκοπιμότητα της ανάθεσης υπηρεσιών Υπευθύνου Προστασίας Δεδομένων (DPO), με σκοπό τη Συμμόρφωση του Γ.Ν.Λασιθίου-Γ.Ν.-Κ.Υ.Νεαπόλεως «Διαλυνάκειο», με το «Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR)» – Κανονισμός (ΕΕ) 2016/679 για τις ανάγκες των υγειονομικών μονάδων του Γ.Ν. Λασιθίου και του Γ.Ν.-Κ.Υ. Νεαπόλεως «Διαλυνάκειο» συνολικού προϋπολογισμού 22.473,09€ πλέον ΦΠΑ η οποία επιμερίζεται σύμφωνα με τον αριθμό των ανεπτυγμένων κλινών ανά νοσοκομείο.

Β. Εγκρίνει τις παρακάτω τεχνικές προδιαγραφές όπως κατατέθηκαν από την αρμόδια επιτροπή (αρ.πρωτ. 8447/13-9-2019)

ΑΝΤΙΚΕΙΜΕΝΟ ΤΟΥ ΕΡΓΟΥ

Αντικείμενο του έργου είναι η λήψη Συμβουλευτικών Υπηρεσιών με πλήρεις και ολοκληρωμένες Υπηρεσίες Υπευθύνου Προστασίας Δεδομένων (DPO), με σκοπό τη Συμμόρφωση του Γ.Ν.Λασιθίου-Γ.Ν.-Κ.Υ.Νεαπόλεως «Διαλυνάκειο», εφεξής «ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ», με το «Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR)» – Κανονισμός (ΕΕ) 2016/679 και σύμφωνα με τις κατευθυντήριες οδηγίες του Υπουργείου Υγείας. Ο Γενικός Κανονισμός για την Προστασία των δεδομένων της ΕΕ «Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR)», εγκρίθηκε στις 14 Απριλίου 2016 και δημοσιεύθηκε στην Επίσημη Εφημερίδα της ΕΕ στις 4 Μαΐου 2016. Ο GDPR εφαρμόζεται σε όλα τα κράτη μέλη της ΕΕ από τις 25 Μαΐου 2018. Συγχρόνως, καταργεί και αντικαθιστά την οδηγία 95/46/ΕΚ και τη νομοθεσία εφαρμογής των κρατών μελών της (Ν2472/1997).

Στο **Παράρτημα Α** παρατίθενται τα βασικά στοιχεία του Κανονισμού, τα οποία θα πρέπει να ληφθούν υπόψη κατά την υλοποίηση του έργου.

Το έργο περιλαμβάνει: α) Υπηρεσίες για τη διενέργεια μελέτης ωριμότητας της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ έναντι του νέου Κανονισμού, με σκοπό τον προσδιορισμό του επίπεδου συμμόρφωσης της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ με τις διατάξεις του κανονισμού GDPR, καθώς και β) Υπηρεσίες Διαχείρισης και Υλοποίησης του έργου Συμμόρφωσης προς τον παραπάνω Κανονισμό. Η μελέτη ωριμότητας θα αξιολογεί όλους τους τομείς δραστηριότητας της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ 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 η ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ 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 (Policy Gap Analysis), η Σύνταξη Πλάνου Συμμόρφωσης (Compliance Plan) και Ανάλυσης του Αντίκτυπου στην Προστασία Προσωπικών Δεδομένων (Privacy Impact Assessment), καθώς και η Εκπαίδευση της Ομάδας Εργασίας και του Προσωπικού της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ, όπως ορίζονται από τον κανονισμό GDPR και τα οποία θα αποτελούν βασικά παραδοτέα του έργου.

Οι προτεινόμενες φάσεις υλοποίησης του έργου είναι οι ακόλουθες:

ΦΑΣΗ 1: Έναρξη Έργου - Οργάνωση δράσεων

ΦΑΣΗ 2: Συγκέντρωση Δεδομένων

ΦΑΣΗ 3: Μελέτη Ανάλυσης Ελλείψεων και Αποκλίσεων (Gap Analysis & Maturity Assessment)

ΦΑΣΗ 4: Διενέργεια Privacy Impact Assessment και Ανάπτυξη Σχεδίου Διορθωτικών Ενεργειών

ΦΑΣΗ 5: Υλοποίηση των Διορθωτικών Ενεργειών - Εκπαίδευση

Σε όλη τη διάρκεια υλοποίησης των παραπάνω φάσεων, καθώς και για διάστημα ίσο με 2 (δύο) έτη από την οριστική παραλαβή του έργου, ο ΑΝΑΔΟΧΟΣ οφείλει να προσφέρει Λογισμικό με άδειες χρήσεις που θα εναρμονίσει την ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ με το «Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR)» – Κανονισμός (ΕΕ) 2016/679. Οι τεχνικές προδιαγραφές του εν λόγω λογισμικού παρατίθενται στο **ΠΑΡΑΡΤΗΜΑ Β**.

ΔΙΑΣΤΑΣΙΟΛΟΓΗΣΗ

Το εύρος εφαρμογής του έργου περιλαμβάνει το Γενικό Νοσοκομείο Λασιθίου-Γ.Ν. Νεαπόλεως «Διαλυνάκειο», των αποκεντρωμένων Μονάδων αυτού, καθώς και το

σύνολο των Μονάδων Πρωτοβάθμιας Υγείας ευθύνης τους

ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ

- I. Οργανική Μονάδα Έδρας Αγίου Νικολάου Γενικού Νοσοκομείου Λασιθίου*
- II. Αποκεντρωμένη Οργανική Μονάδα Ιεράπετρας Γενικού Νοσοκομείου Λασιθίου*
- III. Αποκεντρωμένη Οργανική Μονάδα Σητείας Γενικού Νοσοκομείου Λασιθίου*
- IV. Γενικό Νοσοκομείο – Κέντρο Υγείας Νεαπόλεως «Διαλυνάκειο»*
- V. Περιφερειακά Ιατρεία (Π.Ι. και Π.Π.Ι.) ευθύνης τους*
- VI. Κέντρο Ψυχικής Υγείας Αγίου Νικολάου Γενικού Νοσοκομείου Λασιθίου*
- VII. Νοσοκομείο Ημέρας ΑΟΜ Σητείας Γενικού Νοσοκομείου Λασιθίου*

Κάθε νέα Μονάδα Υγείας που θα δημιουργηθεί/τεθεί σε λειτουργία κατά τη χρονική περίοδο υλοποίησης του έργου, καθώς και για διάστημα ίσο με 2 (δύο) έτη μετά την οριστική παραλαβή του.

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 της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ 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 η ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ και ειδικότερα, την αξιολόγηση των υφιστάμενων πρακτικών, των γραπτών πολιτικών και διαδικασιών, των πληροφοριακών συστημάτων (π.χ. Ολοκληρωμένο Πληροφοριακό Σύστημα Υγείας -ΟΠΣΥ Κρήτης, Ηλεκτρονική Διακίνησης Εγγράφων, ΠΣ Λογιστικής - Διαχειριστικής κίνησης ΕΛΚΕΑ, καθώς και όσα άλλα υποστηρίζουν και έχουν αναπτυχθεί ή πρόκειται να αναπτυχθούν κατά τη διάρκεια ισχύς της σύμβασης), καθώς και των δικτυακών υποδομών (π.χ. υποδομές της Μονάδας Έδρας, της ΑΟΜ Ιεράπετρας, Της ΑΟΜ Σητείας και του Γ.Ν.-Κ.Υ.Νεαπόλεως «Διαλυνάκειο») και κάθε στοιχείου που επηρεάζει την προστασία, και την ασφάλεια των προσωπικών δεδομένων σε όλες τις δραστηριότητες και τις υπηρεσιακές μονάδες της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ.*
- *Δημιουργία λεπτομερών Ροών Δεδομένων (Data Inventory and Data Flow Mapping) ανά τμήμα ή ανά κατηγορία προσωπικών δεδομένων, όπου θα απεικονίζονται όλες οι πληροφορίες σχετικά με τη διαχείριση των προσωπικών δεδομένων στην ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ 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 το βαθμό ετοιμότητας συμμόρφωσης της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ 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.*
- *Σύνταξη Ανάλυσης Επικινδυνότητας για την ασφάλεια των πληροφοριών (data) της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ (Information Security Risk Assessment).*

Ειδικότερα η αξιολόγηση που θα καταδεικνύει το βαθμό ετοιμότητας συμμόρφωσης της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ 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 της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ με Τρίτους Φορείς που εκτελούν επεξεργασία προσωπικών δεδομένων της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ.*
- *Αξιολόγηση των υφιστάμενων συμβάσεων της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ με Τρίτους Φορείς που αποστέλλουν/κοινοποιούν προσωπικά δεδομένα της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ.*
- *Αξιολόγηση της νομιμότητας και της ασφαλούς διαβίβασης προσωπικών δεδομένων.*
- *Αξιολόγηση του επιπέδου ωριμότητας και ευαισθητοποίησης της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ στα θέματα προστασίας προσωπικών δεδομένων.*
- *Αξιολόγηση των πληροφοριακών συστημάτων (όσα υποστηρίζουν και έχουν αναπτυχθεί ή πρόκειται να αναπτυχθούν κατά τη διάρκεια ισχύς της σύμβασης στην ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ).*
- *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 της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ, 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 της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ, καλύπτοντας σε αντιπροσωπευτικό επίπεδο, κάθε δραστηριότητα των Υπηρεσιακών Μονάδων της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ.
- 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, καθώς και εργαλείο λογισμικού για τον εντοπισμό των προσωπικών δεδομένων στα ψηφιακά συστήματα της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ, 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, το ελάχιστο, την τεκμηρίωση της νομικής βάσης πάνω στην οποία θα στηρίζεται η συλλογή της παρεχόμενης συναίνεσης (π.χ. λόγω εθνικής νομοθεσίας ή εποπτικού ρόλου) από τον εκάστοτε συμβαλλόμενο, των παρεχόμενων πληροφοριών, κ.ά.
- 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 της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ με Τρίτους Φορείς (Εργαστήρια, Νοσοκομεία, ΗΛΙΚΑ, ΕΟΠΥΥ κ.α.), 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.τ.λ.) και να έχουν συμφωνηθεί με την Επιτροπή Παρακολούθησης Έργου και τη Διοίκηση της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ πριν την παράδοση του πλάνου συμμόρφωσης.

ΦΑΣΕΙΣ ΤΟΥ ΕΡΓΟΥ – ΠΑΡΑΔΟΤΕΑ

ΦΑΣΗ 1: Έναρξη Έργου - Οργάνωση Δράσεων

Η φάση αυτή περιλαμβάνει τις ακόλουθες δράσεις:

- *Παρουσίαση στη Διοίκηση ολοκληρωμένης πρότασης για την οργάνωση, τη διοίκηση, καθώς και για τον προσδιορισμό των ρόλων των εμπλεκομένων στο έργο, η οποία θα περιλαμβάνει:*
 - *Καταγραφή εργασιών και αλληλεξάρτηση αυτών*
 - *Καθορισμό των παραδοτέων και των χρονικών ορόσημων*
 - *Συστηματική παρακολούθηση της προόδου του έργου και των παραδοτέων*
 - *Τρόπος παρακολούθησης της κρίσιμης διαδρομής, επισημάνση τομέων ανησυχίας και πρόταση διορθωτικών ενεργειών σε περίπτωση αποκλίσεων από το σχέδιο*
 - *Παροχή τεχνικής υποστήριξης στην Ομάδα Εργασίας και την Επιτροπή Παρακολούθησης Έργου της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ, οι οποίες θα συσταθούν στο πλαίσιο υλοποίησης του ανωτέρω έργου.*
- *Εκτίμηση απαιτούμενων ανθρωποημερών με αναφορά στην:*
 - *Αντιστοίχιση εργασιών με απαιτούμενους (ανθρώπινους) πόρους του υποψήφιου Αναδόχου και της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ*
 - *Εκτίμηση επάρκειας πόρων*
 - *Κάλυψη των αναγκών που δεν καλύπτονται από τους διαθέσιμους πόρους, με χρήση εξωπορισμού (outsourcing)*
- *Μέριμνα για την σύνταξη αναφορών προόδου*
 - *Σύνταξη αναφορών προόδου προς την Επιτροπή Παρακολούθησης Έργου της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ, οσάκις απαιτείται ad-hoc εκθέσεις σχετικά με συγκεκριμένα θέματα*
- *Οργάνωση συναντήσεων Steering Committee*
 - *Σύσταση Μικτών Ομάδων Υλοποίησης*
 - *Προγραμματισμός συναντήσεων*
 - *Πρακτικά συναντήσεων*

Παραδοτέα Φάσης 1:

- 1) *Πλάνο υλοποίησης έργου (περιγραφή του Έργου στην οποία περιγράφεται ο τρόπος προσέγγισης και εκτέλεσης του Έργου, συμπεριλαμβανομένης - ανά Φάση - της σύνθεσης της Ομάδας Έργου του υποψήφιου Αναδόχου, των επιμέρους καθηκόντων των προσώπων που θα την απαρτίζουν, το πλήθος των ανθρωποημερών (Α/Η) ανά Φάση, των παραδοτέων και του χρονοδιαγράμματος).*

ΦΑΣΗ 2: 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 της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ με έμφαση σε όλες τις κρίσιμες περιοχές επεξεργασίας.
- Εντοπισμός προσωπικών δεδομένων σε συστήματα με δομημένες και αδόμητες πληροφορίες της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ.
- 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 (π.χ. CCTV), εμπλεκόμενες εφαρμογές/εργαλεία και λόγους συλλογής τους από την ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ.

Η αποτύπωση των δεδομένων θα πρέπει να καλύπτει τις απαιτήσεις του άρθρου 30 καθώς και του άρθρου 32 παρ. Ι του Κανονισμού GDPR.

Παραδοτέα Φάσης 2:

- 1) Αναφορές με προσωπικά δεδομένα που εντοπίστηκαν στα συστήματα προς ανάλυση.
- 2) *Data Inventory and Data Flow Mapping* που θα καλύπτουν 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 3: Μελέτη ανάλυσης Ελλείψεων και Αποκλίσεων (Gap Analysis και Maturity Assessment)

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 το χειρισμό των προσωπικών δεδομένων, ως προς:
 - τις απαιτήσεις του GDPR
 - το κανονιστικό πλαίσιο του έργου, συμπεριλαμβανομένων σχετικών δικαστικών αποφάσεων
 - τις απαιτήσεις των σχετικών διεθνών προτύπων για την ασφάλεια των πληροφοριών

- *Μελέτη ως προς τις υφιστάμενες επεξεργασίες δεδομένων (και της διαβάθμισής τους) σε συνδυασμό με τα εμπλεκόμενα συστήματα πληροφορικής της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ*
- *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 της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ 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 της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ και τις επιμέρους αποκλίσεις που παρουσιάζει σε σχέση με τις ανωτέρω απαιτήσεις.*

Παραδοτέα Φάσης 3:

1) *Μελέτη Ανάλυσης Ελλείψεων και Αποκλίσεων (GAP analysis)*

ΦΑΣΗ 4: 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 της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ, 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:*

- ι. της τροποποίησης υφιστάμενων διαδικασιών*
- ιι. της τροποποίησης του περιβάλλοντος λειτουργίας των πληροφοριακών συστημάτων και των δικτυακών υποδομών*
- ιιι. της διατήρησης στο μέλλον ικανοποιητικού επιπέδου συμμόρφωσης*
- ιiv. της συστηματικής αύξησης του επιπέδου συμμόρφωσης σε χρονικό επίπεδο που θα προσδιοριστεί σε συνεργασία με την ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ*

Παραδοτέα Φάσης 4:

- 1) Privacy Impact Assessment*
- 2) Compliance Plan που να συμπεριλαμβάνει προτάσεις αλλαγών για την ικανοποίηση των απαιτήσεων στις διαδικασίες, τα μη ψηφιακά αρχεία και τα πληροφοριακά συστήματα της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ.*

ΦΑΣΗ 5: 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 τα καθιερωμένα διεθνή πρότυπα ασφάλειας*
- *Διενέργεια Information Security Risk Assessment*
- *Υλοποίηση δράσεων ενημέρωσης και ευαισθητοποίησης*
- *Εκπαίδευση της Ομάδας Εργασίας και του προσωπικού της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ*
- *Σύνταξη πολιτικών και διαδικασιών*
 - *Προστασίας δεδομένων*
 - *Ασφάλειας δεδομένων κατά τα διεθνή πρότυπα ασφάλειας ISO 27001, ISO 27002*
- *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 5:

- 1) Information Security Risk Assessment*
- 2) Δράσεις Ευαισθητοποίησης*
- 3) Δράσεις Εκπαίδευσης και Επιμόρφωσης*
- 4) Πολιτικές και Διαδικασίες:*
 - I. προστασίας δεδομένων*
 - II. ασφάλειας δεδομένων κατά τα διεθνή πρότυπα ασφάλειας ISO 27001, ISO 27002*
- 5) Εκθέσεις, ευρήματα και προτεινόμενες διορθωτικές ενέργειες για κάθε επιθεωρούμενο τμήμα της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ μετά από το Internal Audit*

Η ημερομηνία ολοκλήρωσης του έργου ορίζεται εντός τεσσάρων μηνών από την υπογραφή της σύμβασης.

ΕΙΔΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ

- Όλες οι προτάσεις είναι απαραίτητο να βασίζονται και να λαμβάνουν υπόψη εκτός από τον Κανονισμό Γενικής Προστασίας Δεδομένων (GDPR), το ισχύον 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 του Υπουργείου Υγείας και 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
 - Αριθμό ανθρωποημερών ανά φάση του έργου, καθώς και το είδος των στελεχών ανά κατηγορία εξειδίκευσης που θα απασχοληθούν, ανά φάση του έργου
 - Αναφορά στη μεθοδολογία, τα εργαλεία και το λογισμικό που θα χρησιμοποιηθούν για την αναζήτηση των δεδομένων προσωπικού χαρακτήρα που είναι αποθηκευμένα ψηφιακά (data discovery)
 - Πρόσθετες υπηρεσίες που είναι σε θέση να αναλάβει κατά την υλοποίηση των ενεργειών του πλάνου συμμόρφωσης
- 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 κινδύνων, την αξιολόγηση ετοιμότητας και στον τομέα της ασφάλειας των πληροφοριακών συστημάτων. Το προσωπικό του ΑΝΑΔΟΧΟΥ που θα στελεχώσει το έργο πρέπει να κατέχει πιστοποιήσεις σχετικές με την ασφάλεια πληροφοριακών συστημάτων, τη διαχείριση κινδύνων και ανάλογες δεξιότητες. Όλα τα ανωτέρω να αποδεικνύονται με την επισύναψη των σχετικών εγγράφων.
- Ο υποψήφιος Ανάδοχος θα πρέπει να έχει διεκπεραιώσει παρόμοια έργα (τουλάχιστον τρία (3)) 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 κατά το ελάχιστο τις ακόλουθες κατηγορίες:
 - Project Manager και διαχείριση έργων
 - Συμβούλους οργάνωσης και διασφάλισης ποιότητας
 - Ειδικούς στην ασφάλεια πληροφοριών, την ανάλυση κινδύνων και την αξιολόγηση των ευπαθειών

- ο *Εξειδικευμένους νομικούς στην προστασία δεδομένων*
- ο *Ειδικούς στις τεχνολογικές υποδομές, τις εφαρμογές πληροφορικής και την ασφάλεια 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.

- *Ο Ανάδοχος θα πρέπει να είναι πιστοποιημένος σε διαδικασίες διαχείρισης έργων που εξασφαλίζουν την ποιότητα και να διαθέτει την πιστοποίηση ISO 9001 ή πιστοποίηση με άλλα αντίστοιχα διεθνή πρότυπα, επιτιμώντας στην προσφορά του τα σχετικά έγγραφα. Ο Ανάδοχος πρέπει να αναλάβει στο πλαίσιο του παραπάνω έργου τη χορήγηση νομικών συμβουλών προσαρμοσμένων στις ανάγκες της οργάνωσης της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ και να αναλάβει επιπλέον τη σύνταξη των νομικών εγγράφων που θα απαιτηθούν.*
- *Το έργο θα εκπονηθεί σε συνεργασία με τα αρμόδια στελέχη της Ομάδας Εργασίας και την Επιτροπή Παρακολούθησης Έργου που θα συστήσει η ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ.*
- *Η προσφορά θα περιλαμβάνει περιγραφή της μεθοδολογίας υλοποίησης, καθώς και αναφορά στις τεχνικές και τα πρότυπα που θα χρησιμοποιηθούν για την παροχή των σχετικών υπηρεσιών.*

ΥΠΗΡΕΣΙΕΣ ΥΠΟΣΤΗΡΙΞΗΣ

Αμέσως μετά την Ολοκλήρωση του Έργου, ξεκινάει η περίοδος υποστήριξης του συνόλου των διαδικασιών στο πλαίσιο εφαρμογής του GDPR, η οποία – για τη διασφάλιση συνέχειας – 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 εξωτερικού Υπευθύνου Προστασίας Δεδομένων (DPO)** που θα ορίσει ο ΥΠΟΨΗΦΙΟΣ ΑΝΑΔΟΧΟΣ και ο οποίος θα:
 - ο *Συμμετέχει/συντονίζει τις εργασίες της Ομάδας Εργασίας της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ.*
 - ο *Παρακολουθεί την εφαρμογή των πολιτικών/διαδικασιών προστασίας προσωπικών δεδομένων που έχουν αναπτυχθεί για τη συμμόρφωση του Φορέα με τον Κανονισμό με φυσική παρουσία στις εγκαταστάσεις της Αναθέτουσας Αρχής όποτε αυτό κρίνεται απαραίτητο τόσο από τον ΑΝΑΔΟΧΟ, όσο και από την ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ.*
 - ο *Προτείνει και θα εισηγείται προς τη Διοίκηση έγκριση για αναθεώρηση και βελτίωση στις πολιτικές / διαδικασίες / οδηγίες του Συστήματος Συμμόρφωσης όπου κρίνει απαραίτητο.*
 - ο *Επικαιροποιεί τις Εκτιμήσεις Αντικτύπου (DPIA) και θα δημιουργεί καινούριες για επεξεργασίες υψηλού ρίσκου σε μηνιαία βάση από την έναρξη εφαρμογής του Έργου.*
 - ο *Αναλαμβάνει την ενημέρωση του προσωπικού, καθώς και τις εσωτερικές επιθεωρήσεις, με σκοπό την επίτευξη του βέλτιστου επιπέδου συμμόρφωσης.*

- **Επιπρόσθετες υπηρεσίες συμμόρφωσης και εναρμόνισης με το GDPR:** Οι υπηρεσίες αυτές περιλαμβάνουν το σύνολο των εργασιών τις οποίες ο ΥΠΟΨΗΦΙΟΣ ΑΝΑΔΟΧΟΣ απαιτείται να παράσχει, για να αντιμετωπιστούν όλες οι οργανωσιακές αλλαγές που πρόκειται να λάβουν χώρα κατά την περίοδο υποστήριξης. **Ενδεικτικά** (μη περιοριστικά) αναφέρονται η δημιουργία/ θέση σε λειτουργία νέων Μονάδων Υγείας (π.χ. ΤΟΜΥ) και η αναμόρφωση του οργανισμού/ οργανογράμματος της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ (π.χ. αλλαγή των Διευθύνσεων από 5 σε 7 με αντίστοιχη αναδιάρθρωση των υφιστάμενων τμημάτων και λοιπών οργανικών μονάδων).

ΠΑΡΑΚΟΛΟΥΘΗΣΗ - ΠΑΡΑΛΑΒΗ ΕΡΓΟΥ

Η παραλαβή των υπηρεσιών θα γίνεται ανά Φάση από την Επιτροπή Παρακολούθησης Έργου που θα ορίσει η ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ. 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.

Η παραλαβή των υπηρεσιών του εξωτερικού DPO θα γίνεται με τη σύνταξη και κατάθεση τριμηνιαίων αναφορών στην επιτροπή Παραλαβής 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 την ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ, καθώς επίσης να αποτρέπει με κάθε νόμιμο μέσο την ανακοίνωση αυτών. Για το σκοπό αυτό θα υπογραφεί Ειδικό Συμφωνητικό Εχεμύθειας και Εμπιστευτικότητας με την έναρξη της εργασίας, το οποίο 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. Αντιθέτως, θα τους επιτραπεί να απευθύνονται για θέματα σχετικά με την εργασία μόνο στα άτομα τα οποία, σαφώς αναφέρονται στο συμφωνητικό εμπιστευτικότητας ως σύνδεσμοι στην επικοινωνία μεταξύ των τεχνικών του αναδόχου και της διοίκησης.

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

ΠΑΡΑΡΤΗΜΑ Α

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 την επεξεργασία οφείλουν να χρησιμοποιούν μεθόδους προστασίας των προσωπικών δεδομένων όπως κρυπτογράφηση, ψευδώνυμα, απόκρυψη της πληροφορίας (DataMasking) κ.τ.λ.
- **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:** Η μη συμμόρφωση με τους κανόνες προστασίας προσωπικών δεδομένων επιφέρει και πρόστιμα στις επιχειρήσεις που τον παραβιάζουν έως 20 εκατομμύρια € ή 4% του συνολικού 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 Β

ΠΕΡΙΓΡΑΦΗ ΤΕΧΝΙΚΩΝ ΠΡΟΔΙΑΓΡΑΦΩΝ ΕΦΑΡΜΟΓΗΣ

Λειτουργικά Χαρακτηριστικά

Η εφαρμογή θα πρέπει:

- Να καταγράφει και να αναλύει γενικές διαδικασίες λειτουργίας του φορέα.
- Να καταγράφει σύμφωνα με τον Κανονισμό Προστασίας Δεδομένων (GDPR):
 - τους σκοπούς συλλογής δεδομένων και το είδος των δεδομένων που συλλέγονται
 - το είδος των υποκειμένων συλλογής
 - την πηγή και το μέσο συλλογής
 - τα τμήματα που έχουν πρόσβαση στην πληροφορία
 - τα σημεία αποθήκευσης δεδομένων
 - τη μεταφορά δεδομένων τόσο εσωτερικά στο φορέα, όσο και σε εξωτερικούς αποδέκτες

- το χρόνο διατήρησης των δεδομένων και τις ενέργειες μετά το πέρας του χρόνου διατήρησης αυτών
 - τη μεταφορά δεδομένων σε Τρίτες Χώρες
 - τις νομικές βάσεις διατήρησης προσωπικών και ευαίσθητων προσωπικών δεδομένων
 - τα δικαιώματα που δίδονται στο υποκείμενο και το κατά πόσο καλύπτονται οι αρχές επεξεργασίας του κανονισμού.
- Να εξάγει το Αρχείο Δραστηριοτήτων Επεξεργασίας βάσει του άρθρου 30 του Κανονισμού και τις σχετικές αναφορές.
 - Να εξάγει Διαγράμματα Ροής για κάθε ανάλυση διαδικασίας (Data Flow Mapping).
 - Να παρουσιάζει τις αποκλίσεις από τον κανονισμό και να προτείνει μέτρα συμμόρφωσης (Gap Analysis & Maturity Assessment).
 - Να υπολογίζει την πιθανότητα απειλής των προσωπικών δεδομένων σε πληροφοριακά και άλλα τεχνολογικά συστήματα, καθώς και μεθόδους, διαδικασίες και εμπλοκή προσώπων ανά δραστηριότητα.
 - Να εξάγει τα αναγκαία Οργανωτικά και Τεχνικά Μέτρα ασφάλειας πληροφοριακών συστημάτων και φυσικών αρχείων ανάλογα με το επίπεδο του επικινδυνότητας.
 - Να διενεργεί έλεγχο σχετικά με την απαίτηση διενέργειας Εκτίμησης Αντικτύπου και την προστασία Προσωπικών Δεδομένων (DATA PROTECTION IMPACT ASSESSMENT - DPIA) και να την εξάγει ελέγχοντας την απώλεια της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων.
 - Να έχει την δυνατότητα εντοπισμού των προσωπικών δεδομένων ενός υποκειμένου, σε περίπτωση άσκησης των δικαιωμάτων από το υποκείμενο.
 - Να έχει την δυνατότητα τροποποίησης και επικαιροποίησης των διαδικασιών επεξεργασίας των προσωπικών δεδομένων.
 - Να έχει τη δυνατότητα αποθήκευσης και διατήρησης των στοιχείων συμμόρφωσης του φορέα προκειμένου να είναι άμεσα προσβάσιμα κατά τη λογοδοσία.
 - Να έχει την δυνατότητα εντοπισμού του τρόπου επεξεργασίας, των σημείων αποθήκευσης και των αποδεκτών, ανά κατηγορία προσωπικών δεδομένων και της διατήρησης ιστορικού συμμόρφωσης.

Τεχνικά Χαρακτηριστικά

Η εφαρμογή θα πρέπει:

- Να είναι δικτυακή (web based app), ώστε να είναι εφικτή η χρήση της από πολλά πλά σμεία.
- Να μην απαιτείται από την ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ πρόσθετος εξειδικευμένος εξοπλισμός σε υλικό (hardware) ή επιπλέον λογισμικό (software) για τη λειτουργία της από τους χρήστες και να δοθεί με τη μορφή αγοράς άδειας χρήσης.
- Να έχει τη δυνατότητα δημιουργίας πολλαπλών προσωποποιημένων χρηστών με κεντρική διαχείριση και δυνατότητα παραμετροποίησης χρηστών (π.χ. χρήστης με πλήρη δικαιώματα, χρήστης με δικαιώματα μόνο ανάγνωσης, απλός χρήστης).

Ο ΑΝΑΔΟΧΟΣ οφείλει να περιγράψει πλήρως τον τρόπο τήρησης αντιγράφων ασφαλείας (backup), καθώς και τον τρόπο ανάκτησης δεδομένων σε περίπτωση απώλειας αυτών.

Μετά το πέρας υλοποίησης του έργου, καθώς και για τα διάστημα ίσο με 2 (δύο) έτη μετά την οριστική παραλαβή του έργου, όλα τα δεδομένα που θα συλλεχτούν, αποθηκευτούν και επεξεργαστούν από την εν λόγω εφαρμογή, θα μεταβιβαστούν ακέραια στην ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ σε επεξεργάσιμη μορφή.

ΠΑΡΑΡΤΗΜΑ Γ ΠΡΟΫΠΟΛΟΓΙΣΜΟΣ

Α. Η προϋπολογισθείσα δαπάνη για την προμήθεια έργου «Υπηρεσιών Συμμόρφωσης με τον Ευρωπαϊκό Κανονισμό (GDPR)» εκτιμάται στο ποσό των 12.000,00€ (συμπ. ΦΠΑ).

Β. Η προϋπολογισθείσα δαπάνη για προμήθεια υπηρεσιών «Υπευθύνου Προστασίας Προσωπικών Δεδομένων (DPO)» 2 (δύο) ετών εκτιμάται στο συνολικό ποσό των 12.400,00€ (συμπ. ΦΠΑ).

Γ. Η προϋπολογισθείσα δαπάνη για την προμήθεια αδειών χρήσης ειδικού λογισμικού συμμόρφωσης (SOFTWARE) με τον Ευρωπαϊκό Κανονισμό (GDPR) στο ποσό των 3.466,64€ (συμπ. ΦΠΑ).

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

Α/Α	ΕΙΔΟΣ	CPV	ΜΟΝΑΔΑ ΜΕΤΡΗΣΗΣ	ΠΟΣΟΤΗΤ Α	ΤΙΜΗ ΜΟΝΑΔΑΣ ΧΩΡΙΣ ΦΠΑ	ΑΞΙΑ ΜΕ ΦΠΑ
1.	Έργο με υπηρεσίες συμμόρφωσης 4μηνών	79417000-0	Υπηρεσία	1	9.677,41€	12.000,00€
2.	Υπηρεσίες «Υπευθύνου Προστασίας Προσωπικών Δεδομένων (DPO)» 24 μηνών	79417000-0	Υπηρεσία	1	10.000,00€	12.400,00€
3.	Λογισμικό Συμμόρφωσης (software)	79417000-0	Άδεια χρήσης	4	698,92€	3.466,64€
Συνολική αξία με ΦΠΑ						27.866,64€

ΠΑΡΑΡΤΗΜΑ Δ

ΠΙΝΑΚΑΣ ΣΥΜΜΟΡΦΩΣΗΣ

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΙΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ ΤΕΚΜΗΡΙΟ
-----	-------------	----------	----------	--------------------

				ΙΩΣ ΗΣ
1. ΔΙΑΣΤΑΣΙΟΛΟΓΗΣΗ				
1.1	<p><i>Πεδίο εφαρμογής έργου (ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ)</i></p> <ul style="list-style-type: none"> • <i>Οργανική Μονάδα Έδρας Αγίου Νικολάου Γενικού Νοσοκομείου Λασιθίου</i> • <i>Αποκεντρωμένη Οργανική Μονάδα Ιεράπετρας Γενικού Νοσοκομείου Λασιθίου</i> • <i>Αποκεντρωμένη Οργανική Μονάδα Σητείας Γενικού Νοσοκομείου Λασιθίου</i> • <i>Γενικό Νοσοκομείο – Κέντρο Υγείας Νεαπόλεως «Διαλυνάκειο»</i> • <i>Περιφερειακά Ιατρεία (Π.Ι. και Π.Π.Ι.) ευθύνης τους</i> • <i>Κέντρο Ψυχικής Υγείας Αγίου Νικολάου Γενικού Νοσοκομείου Λασιθίου</i> • <i>Νοσοκομείο Ημέρας ΑΟΜ Σητείας Γενικού Νοσοκομείου Λασιθίου</i> <p><i>Κάθε νέα Μονάδα Υγείας που θα δημιουργηθεί /τεθεί σε λειτουργία κατά τη χρονική περίοδο υλοποίησης του έργου, καθώς και για τα διάστημα ίσο με 2 (δύο) έτη από την οριστική παραλαβή του.</i></p>	ΝΑΙ		
2. ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΕΡΓΟΥ				
2.1	<p><i>Ανάλυση της τρέχουσας κατάστασης ως προς την προστασία των προσωπικών δεδομένων που διαχειρίζεται η ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ και ειδικότερα, την αξιολόγηση των υφιστάμενων πρακτικών, των γραπτών πολιτικών και διαδικασιών, των πληροφοριακών συστημάτων (π.χ. Ολοκληρωμένο Πληροφοριακό Σύστημα Υγείας, Ηλεκτρονική Διακίνησης Εγγράφων, ΠΣ Λογιστικής-Διαχειριστικής Κίνησης ΕΛΚΕΑ, καθώς και όλα άλλα υποστηρίζουν και έχουν αναπτυχθεί ή πρόκειται να αναπτυχθούν κατά τη διάρκεια ισχύς της σύμβασης) και δικτυακών υποδομών (π.χ. υποδομές της Κεντρικής Υπηρεσίας, των Κέντρων Υγείας, των ΤΟΜΥ και του περιφερειακού Κέντρου Δεδομένων) και κάθε στοιχείου που επηρεάζει την προστασία, και την ασφάλεια των προσωπικών δεδομένων σε όλες τις δραστηριότητες και τις υπηρεσιακές μονάδες της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ.</i></p>	ΝΑΙ		
2.2	<p><i>Δημιουργία λεπτομερών ροών δεδομένων(Data inventory and data Flowmapping) ανά τμήμα ή ανά κατηγορία προσωπικών δεδομένων, όπου θα απεικονίζονται όλες οι πληροφορίες σχετικά με τη διαχείριση των προσωπικών δεδομένων στην ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ με σκοπό τη δημιουργία του αρχείου δραστηριοτήτων επεξεργασίας δεδομένων που αποτελεί απαίτηση του GDPR.</i></p>	ΝΑΙ		
2.3	<p><i>Εντοπισμός κενών και ελλείψεων ως προς τις απαιτήσεις του κανονισμού (Gap Analysis), κατηγοριοποιημένα ανά θεματική περιοχή και κρισιμότητα.</i></p>	ΝΑΙ		
2.4	<p><i>Σύνταξη Μελέτης Εκτίμησης αντίκτυπου (Privacy Impact Assessment) με βάση τα προβλεπόμενα στον Κανονισμό.</i></p>	ΝΑΙ		
2.5	<p><i>Εκπόνηση των απαραίτητων Πολιτικών και Διαδικασιών Προστασίας Προσωπικών Δεδομένων, Ασφάλειας Πληροφοριών και Επιχειρησιακής Συνέχειας με βάση τα προτεινόμενα μέτρα του πλάνου συμμόρφωσης.</i></p>	ΝΑΙ		

2.6	Σύνταξη Ανάλυσης Επικινδυνότητας για την Ασφάλεια των πληροφοριών (data) της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ (Information Security Risk Assessment).	NAI		
2.7	Λεπτομερής αξιολόγηση που θα καταδεικνύει το βαθμό ετοιμότητας συμμόρφωσης της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ 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).	NAI		
2.7.1	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 κ.τ.λ.	NAI		
2.7.2	Αξιολόγηση της δυνατότητας ικανοποίησης των δικαιωμάτων των φυσικών προσώπων.	NAI		
2.7.3	Αξιολόγηση του επιπέδου ασφαλείας και επιχειρησιακής συνέχειας	NAI		
2.7.4	Αξιολόγηση της επάρκειας της οργανωτικής δομής	NAI		
2.7.5	Αξιολόγηση των υφιστάμενων συμβάσεων της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ με Τρίτους Φορείς που εκτελούν επεξεργασία προσωπικών δεδομένων της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ.	NAI		
2.7.6	Αξιολόγηση των υφιστάμενων συμβάσεων της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ με Τρίτους Φορείς που αποστέλλουν / κοινοποιούν προσωπικά δεδομένα στην ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ.	NAI		
2.7.7	Αξιολόγηση της νομιμότητας και της ασφαλούς διαβίβασης προσωπικών δεδομένων.	NAI		
2.7.8	Αξιολόγηση του επιπέδου ωριμότητας και ευαισθητοποίησης της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ στα θέματα προστασίας προσωπικών δεδομένων	NAI		
2.7.9	Αξιολόγηση των πληροφοριακών συστημάτων (όσα υποστηρίζουν και έχουν αναπτυχθεί ή πρόκειται να αναπτυχθούν κατά τη διάρκεια ισχύς της σύμβασης στην ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ)	NAI		
2.7.10	Αξιολόγηση των μέτρων προστασίας και των μηχανισμών ελέγχου (measures and controls)	NAI		
2.7.11	Αξιολόγηση σχετικών γραπτών πολιτικών και Διαδικασιών.	NAI		
2.8. Ο υποψήφιος ανάδοχος υποχρεούται (κατ' ελάχιστον) στη μεθοδολογία που θα ακολουθήσει να:				
2.8.1	Αναλύσει την τρέχουσα κατάσταση των πληροφοριακών συστημάτων και δικτυακών υποδομών της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ, των υφιστάμενων πολιτικών, διαδικασιών και πρακτικών, οι οποίες σχετίζονται με την ασφάλεια των πληροφοριών, την επιχειρησιακή συνέχεια και την προστασία των προσωπικών δεδομένων.	NAI		
2.8.2	Διεξάγει συνεντεύξεις με προσωπικό της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ καλύπτοντας σε αντιπροσωπευτικό επίπεδο, κάθε δραστηριότητα των Υπηρεσιακών Μονάδων της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ.	NAI		

2.8.3	Παρέχει ένα λεπτομερές data flowmap 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.	ΝΑΙ		
2.8.4	Χρησιμοποιήσει συγκεκριμένη μεθοδολογία και εργαλείο λογισμικού για τον εντοπισμό των προσωπικών δεδομένων στα ψηφιακά συστήματα της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ, 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.ά.	ΝΑΙ		
2.8.5	Πραγματοποιήσει δειγματοληπτικό έλεγχο σε όλες τις εφαρμογές και αποθηκευτικά μέσα (ψηφιακά, έντυπα, αναλογικής εικόνας και ήχου κ.ά.) που τηρούν και επεξεργάζονται προσωπικά δεδομένα, καθώς και να προτείνει με σαφήνεια τις απαιτούμενες αλλαγές και τροποποιήσεις βάσει του νέου κανονισμού.	ΝΑΙ		
2.8.6	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.	ΝΑΙ		
2.8.7	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.	ΝΑΙ		
2.8.8	Πραγματοποιήσει έλεγχο και αξιολόγηση, κατά το εφικτό, όλων των συμβάσεων της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ με Τρίτους Φορείς (Εργαστήρια, Νοσοκομεία, ΗΔΙΚΑ, ΕΟΠΥΥ κ.ά.), με σκοπό να εντοπίσει κενά στην προστασία και επεξεργασία προσωπικών δεδομένων και να προτείνει παράλληλα ενέργειες με σκοπό την προσαρμογή τους στον GDPR.	ΝΑΙ		
2.9	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.τ.λ.) και να έχουν συμφωνηθεί με την Επιτροπή Παρακολούθησης Έργου και τη Διοίκηση ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ πριν την παράδοση του πλάνου συμμόρφωσης.	ΝΑΙ		
3. ΔΡΑΣΕΙΣ –ΕΡΓΑΣΙΕΣ –ΠΑΡΑΔΟΤΕΑ (Κατ'ελάχιστον)				
ΦΑΣΗ 1 ΕΝΑΡΞΗ ΕΡΓΟΥ – ΟΡΓΑΝΩΣΗ ΔΡΑΣΕΩΝ				
3.1	Παρουσίαση στη Διοίκηση ολοκληρωμένης πρότασης για την οργάνωση, τη διοίκηση, καθώς και για τον προσδιορισμό των ρόλων των εμπλεκόμενων στο έργο, η οποία θα περιλαμβάνει: <ul style="list-style-type: none"> Καταγραφή εργασιών και αλληλεξάρτηση αυτών Καθορισμό των παραδοτέων και των χρονικών ορόσημων Συστηματική παρακολούθηση της προόδου του έργου και των παραδοτέων Τρόπος παρακολούθησης της κρίσιμης διαδρομής, επισήμανση τομέων ανησυχίας και πρόταση διορθωτικών ενεργειών σε περίπτωση αποκλίσεων από το σχέδιο 	ΝΑΙ		

	<ul style="list-style-type: none"> Παροχή τεχνικής υποστήριξης στην Επιτροπή Παρακολούθησης ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ, καθώς και στις επί μέρους Ομάδες Εργασίας που θα συσταθούν στο πλαίσιο υλοποίησης του ανωτέρω έργου 			
3.2	<p>Εκτίμηση απαιτούμενων ανθρωποημερών με αναφορά στην:</p> <ul style="list-style-type: none"> Αντιστοίχιση εργασιών με απαιτούμενους (ανθρώπινους) πόρους του υποψήφιου Αναδόχου και της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ Εκτίμηση επάρκειας πόρων Κάλυψη των αναγκών που δεν καλύπτονται από τους διαθέσιμους πόρους με χρήση εξωπορισμού (outsourcing) 	NAI		
3.3	<p>Μέριμνα για τη Σύνταξη Αναφορών Προόδου</p> <ul style="list-style-type: none"> Σύνταξη αναφορών προόδου προς την Επιτροπή Παρακολούθησης Έργου και τις επιμέρους ομάδες εργασίας της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ οσάκις απαιτείται αδηο εκθέσεις σχετικά με συγκεκριμένα θέματα 	NAI		
3.4	<p>Οργάνωση συναντήσεων Steering Committee:</p> <ul style="list-style-type: none"> Σύσταση Μικτών Ομάδων Υλοποίησης Προγραμματισμός συναντήσεων Πρακτικά συναντήσεων 	NAI		
3.5	<p>ΠΑΡΑΔΟΤΕΟ: Πλάνο υλοποίησης έργου (Περιγραφή του Έργου στην οποία περιγράφεται ο τρόπος προσέγγισης και εκτέλεσης του Έργου, συμπεριλαμβανομένης -ανά Φάση - της σύνθεσης της Ομάδας Έργου του υποψήφιου Αναδόχου, των επιμέρους καθηκόντων των προσώπων που θα την απαρτίζουν, το πλήθος των ανθρωποημερών (Α/Η) ανά Φάση, των παραδοτέων και του χρονοδιαγράμματος).</p>	NAI		
ΦΑΣΗ 2- ΣΥΓΚΕΝΤΡΩΣΗ ΔΕΔΟΜΕΝΩΝ				
3.6	Επισκόπηση των επιχειρησιακών, τεχνικών και λειτουργικών διαδικασιών.	NAI		
3.7	Συγκέντρωση των απαιτούμενων πληροφοριών για τη συλλογή και επεξεργασία των προσωπικών δεδομένων, μέσω της διενέργειας συνεντεύξεων με το αρμόδιο προσωπικό όλων των Τμημάτων.	NAI		
3.8	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.	NAI		
3.9	Δημιουργία του αρχείου δραστηριοτήτων και πόρων επεξεργασίας της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ με έμφαση σε όλες τις κρίσιμες περιοχές επεξεργασίας.	NAI		
3.10	Εντοπισμός προσωπικών δεδομένων σε συστήματα με δομημένες και αδόμητες πληροφορίες της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ.	NAI		
3.11	Εντοπισμός των κρίσιμων αποκλίσεων έναντι των απαιτήσεων του Κανονισμού GDPR.	NAI		
3.12	ΠΑΡΑΔΟΤΕΟ: Αναφορές με προσωπικά Δεδομένα που εντοπίστηκαν στα συστήματα προς ανάλυση.	NAI		
3.13	ΠΑΡΑΔΟΤΕΟ: Data Inventory and Data Flow Mapping που θα καλύπτουν 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).	NAI		
ΦΑΣΗ 3 – ΜΕΛΕΤΗ ΑΝΑΛΥΣΗΣ ΕΛΕΙΨΕΩΝ ΚΑΙ ΑΠΟΚΛΙΣΕΩΝ (GAP ANALYSIS AND MATURITY ASSESSMENT)				
3.14	<p>Μελέτη υφιστάμενης κατάστασης ως προς τη διαχείριση προσωπικών δεδομένων από άποψη:</p> <ul style="list-style-type: none"> Νομική Οργάνωσης, Πολιτικών Και Διαδικασιών Ασφάλειας Πληροφοριών Τεχνολογική 	NAI		

3.15	<p>Εντοπιsmός των πεδίων μη συμμόρφωσης στις πρακτικές και διαδικασίες που εφαρμόζονται κατά το χειρισμό των προσωπικών δεδομένων, ως προς:</p> <ul style="list-style-type: none"> τις απαιτήσεις του GDPR το κανονιστικό πλαίσιο του έργου, συμπεριλαμβανομένων σχετικών δικαστικών αποφάσεων τις απαιτήσεις των διεθνών προτύπων ISO 27001, ISO27002 για την ασφάλεια των πληροφοριών 	NAI		
3.16	Μελέτη ως προς τις υφιστάμενες Επεξεργασίες δεδομένων (και της διαβαθμίσεώς τους) σε συνδυασμό με τα εμπλεκόμενα συστήματα πληροφορικής της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ	NAI		
3.17	Αναγνώριση των υφιστάμενων αποκλίσεων από τις απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων ως προς τις επιμέρους περιοχές επεξεργασίας προσωπικών δεδομένων	NAI		
3.18	<p>Μελέτη αποκλίσεων της υφιστάμενης κατάστασης της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ σε σχέση με τις απαιτήσεις του Κανονισμού για κάθε επεξεργασία. Η μελέτη θα πρέπει να περιλαμβάνει τουλάχιστον τις παρακάτω περιοχές:</p> <ul style="list-style-type: none"> 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 	NAI		
3.19	Καταγραφή των σχετικών ευρημάτων σε σχέση με το βαθμό ετοιμότητας συμμόρφωσης της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ και τις επιμέρους αποκλίσεις που παρουσιάζει σε σχέση με τις ανωτέρω απαιτήσεις.	NAI		
3.20	ΠΑΡΑΔΟΤΕΟ: Gap Analysis	NAI		
ΦΑΣΗ 4: Privacy Impact Assessment και Ανάπτυξη σχεδίου διορθωτικών ενεργειών				
3.21	Διενέργεια Privacy Impact Assessment με βάση τις έγκυρες πρακτικές και μεθοδολογίες, που αναφέρθηκαν ανωτέρω	NAI		
3.22	<p>Σύνταξη αναλυτικού και σαφούς σχεδίου στο οποίο θα:</p> <ul style="list-style-type: none"> συμπεριλαμβάνονται οι προτάσεις βελτίωσης ανά τμήμα και Μονάδα της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ, 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: <ul style="list-style-type: none"> της τροποποίησης υφιστάμενων διαδικασιών της τροποποίησης του περιβάλλοντος λειτουργίας των πληροφοριακών συστημάτων και των δικτυακών υποδομών. της διατήρησης στο μέλλον ικανοποιητικού επιπέδου συμμόρφωσης της συστηματικής αύξησης του επιπέδου συμμόρφωσης σε χρονικό επίπεδο που θα προσδιοριστεί σε συνεργασία με την ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ. 	NAI		
3.23	ΠΑΡΑΔΟΤΕΟ: Privacy Impact Assessment	NAI		

3.24	ΠΑΡΑΔΟΤΕΟ: <i>Compliance Plan</i> που να συμπεριλαμβάνει προτάσεις αλλαγών για την ικανοποίηση των απαιτήσεων στις διαδικασίες, τα μη ψηφιακά αρχεία και τα Πληροφοριακά Συστήματα της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ	NAI		
ΦΑΣΗ 5: ΥΛΟΠΟΙΗΣΗ ΜΕΡΟΥΣ ΔΙΟΡΘΩΤΙΚΩΝ ΕΝΕΡΓΕΙΩΝ				
3.25	Υποβολή πρόσθετων προτάσεων για την υλοποίηση πρωτοβουλιών που θα αυξήσουν το επίπεδο συμμόρφωσης με τον GDPR, λαμβάνοντας υπόψη καθιερωμένα πρότυπα ασφάλειας	NAI		
3.26	Διενέργεια <i>Information Security Risk Assessment</i>	NAI		
3.27	Υλοποίηση δράσεων ενημέρωσης και ευαισθητοποίησης	NAI		
3.28	Εκπαίδευση της Ομάδας Εργασίας και του προσωπικού της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ	NAI		
3.29	Σύνταξη πολιτικών και διαδικασιών: <ul style="list-style-type: none"> ■ προστασίας δεδομένων ■ ασφάλειας δεδομένων κατά ISO 27001, ISO 27002 	NAI		
3.30	Διενέργεια πλήρους Εσωτερικής Επιθεώρησης (<i>Internal Audit</i>) που να καλύπτουν όλες τις παραπάνω πολιτικές και διαδικασίες, ώστε αυτές να εφαρμόζονται και να είναι πιστοποιήσιμες κατά τα αντίστοιχα πρότυπα.	NAI		
3.31	ΠΑΡΑΔΟΤΕΟ: <i>Information Security Risk Assessment</i>	NAI		
3.32	ΠΑΡΑΔΟΤΕΟ: Δράσεις ευαισθητοποίησης	NAI		
3.33	ΠΑΡΑΔΟΤΕΟ: Δράσεις εκπαίδευσης και επιμόρφωσης	NAI		
3.34	ΠΑΡΑΔΟΤΕΟ: Πολιτικές και διαδικασίες: <ul style="list-style-type: none"> ■ προστασίας δεδομένων ■ ασφάλειας δεδομένων κατά ISO27001, ISO27002 	NAI		
3.35	ΠΑΡΑΔΟΤΕΟ: Εκθέσεις, ευρήματα και προτεινόμενες διορθωτικές ενέργειες για κάθε επιθεωρούμενο τμήμα της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ μετά από το <i>Internal Audit</i>	NAI		
4. ΕΙΔΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ				
4.1	Όλες οι προτάσεις είναι απαραίτητο να βασίζονται και να λαμβάνουν υπόψη εκτός από τον Κανονισμό Γενικής Προστασίας Δεδομένων (GDPR), το ισχύον 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 αποφάσεις του Υπουργείου Υγείας και άλλων Ευρωπαϊκών Αρχών Προστασίας Προσωπικών Δεδομένων και τις βέλτιστες πρακτικές σύμφωνα με τα διεθνή πρότυπα.	NAI		
4.2	Ο υποψήφιος Ανάδοχος πρέπει να συμπεριλάβει στην προσφορά του: <ul style="list-style-type: none"> ■ Χρονοδιάγραμμα δραστηριοτήτων προγραμματισμό φάσεων υλοποίησης έργου ■ Αριθμό ανθρωποημερών ανά φάση του έργου, καθώς και το είδος των στελεχών ανά κατηγορία εξειδίκευσης που θα απασχοληθούν, ανά φάση του έργου ■ Αναφορά στην μεθοδολογία, τα εργαλεία και το λογισμικό που θα χρησιμοποιηθούν για την αναζήτηση των δεδομένων προσωπικού χαρακτήρα που είναι αποθηκευμένα ψηφιακά (<i>data discovery</i>) ■ Πρόσθετες υπηρεσίες που είναι σε θέση να αναλάβει κατά την υλοποίηση των ενεργειών του πλάνου συμμόρφωσης 	NAI		
4.3	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 κινδύνων, την αξιολόγηση ετοιμότητας και στον τομέα της ασφάλειας των πληροφοριακών συστημάτων. Το προσωπικό της ανάδοχης εταιρείας που θα στελεχώσει το έργο πρέπει να κατέχει πιστοποιήσεις σχετικές με τη ασφάλεια πληροφοριακών συστημάτων, τη	NAI		

	διαχείριση κινδύνων και ανάλογες δεξιότητες. Όλα τα ανωτέρω να αποδεικνύονται με την επισύναψη των σχετικών εγγράφων.			
4.4	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.	ΝΑΙ		
4.5	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: <ul style="list-style-type: none"> ▪ Project Manager και διαχείριση έργων ▪ Συμβούλους οργάνωσης και διασφάλισης ποιότητας ▪ Ειδικούς στην ασφάλεια πληροφοριών και την ανάλυση κινδύνων και αξιολόγηση των ευπαθειών ▪ Εξειδικευμένους νομικούς στην προστασία δεδομένων ▪ Ειδικούς στις τεχνολογικές υποδομές ,τις εφαρμογές πληροφορικής και την ασφάλεια πληροφοριακών συστημάτων 	ΝΑΙ		
4.6	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.	ΝΑΙ		
4.7	Ο Ανάδοχος θα πρέπει να είναι πιστοποιημένος σε διαδικασίες διαχείρισης έργων που εξασφαλίζουν την ποιότητα και να διαθέτει την πιστοποίηση ISO9001 ή πιστοποίηση με άλλα αντίστοιχα διεθνή πρότυπα, επισυνάπτοντας στην προσφορά του τα σχετικά έγγραφα. Ο Ανάδοχος πρέπει να αναλάβει στο πλαίσιο του παραπάνω έργου τη χορήγηση νομικών συμβουλών προσαρμοσμένων στις ανάγκες της οργάνωσης της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ και να αναλάβει επιπλέον τη σύνταξη των νομικών εγγράφων που θα απαιτηθούν.	ΝΑΙ		
4.8	Το έργο θα εκπονηθεί σε συνεργασία με τα αρμόδια στελέχη της Ομάδας Εργασίας και της Επιτροπής Παρακολούθησης Έργου που θα συστήσει η ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ.	ΝΑΙ		
4.9	Η προσφορά θα περιλαμβάνει περιγραφή της μεθοδολογίας υλοποίησης, καθώς και αναφορά στις τεχνικές και τα πρότυπα που θα χρησιμοποιηθούν για την παροχή των σχετικών υπηρεσιών.	ΝΑΙ		
5.	ΥΠΗΡΕΣΙΕΣ ΣΥΜΒΟΥΛΟΥ ΣΥΜΜΟΡΦΩΣΗΣ (DPO)			
5.1	Χρονική διάρκεια ίση με 2 (δύο) έτη από την ολοκλήρωση του Έργου	ΝΑΙ		
5.2. Βασικά Πακέτα Εργασιών των Υπηρεσιών Υποστήριξης				
5.2.1	Πλήρεις και ολοκληρωμένες υπηρεσίες εξωτερικού Υπεύθυνου Προστασίας Δεδομένων (DPO) που θα ορίσει ο ΥΠΟΨΗΦΙΟΣ ΑΝΑΔΟΧΟΣ και ο οποίος θα: <ul style="list-style-type: none"> ▪ Συμμετέχει/συντονίζει τις εργασίες της Ομάδας Εργασίας της ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ. ▪ Παρακολουθεί την εφαρμογή των Πολιτικών/Διαδικασιών Προστασίας Προσωπικών Δεδομένων που έχουν αναπτυχθεί για την συμμόρφωση του Φορέα με τον Κανονισμό, με φυσική παρουσία στις εγκαταστάσεις της Αναθέτουσας Αρχής όποτε αυτό κρίνεται απαραίτητο τόσο από τον ΑΝΑΔΟΧΟ, όσο και από την ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ. ▪ Προτείνει και θα εισηγείται προς τη Διοίκηση έγκριση για αναθεώρηση και βελτίωση στις πολιτικές / διαδικασίες / οδηγίες του συστήματος συμμόρφωσης όπου κρίνει απαραίτητο. ▪ Επικαιροποιεί τις εκτιμήσεις αντικτύπου (DPIA) και θα δημιουργεί καινούργιες για επεξεργασίες υψηλού ρίσκου σε μηνιαία βάση από 	ΝΑΙ		

	<p>την έναρξη εφαρμογής του Έργου.</p> <ul style="list-style-type: none"> Αναλαμβάνει την ενημέρωση του προσωπικού, καθώς και τις εσωτερικές επιθεωρήσεις, με σκοπό την επίτευξη του βέλτιστου επιπέδου συμμόρφωσης. 			
5.2.2	<p>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 οργανωσιακές αλλαγές που πρόκειται να λάβουν χώρα κατά την περίοδο υποστήριξης.</p>	NAI		
6. Λογισμικό Συμμόρφωσης (software)				
6.1	<ul style="list-style-type: none"> Να καταγράφει και να αναλύει γενικές διαδικασίες λειτουργίας του φορέα. 	NAI		
6.2	<ul style="list-style-type: none"> Να καταγράφει σύμφωνα με τον Κανονισμό Προστασίας Δεδομένων (GDPR): <ul style="list-style-type: none"> τους σκοπούς συλλογής δεδομένων και το είδος των δεδομένων που συλλέγονται το είδος των υποκειμένων συλλογής την πηγή και το μέσο συλλογής τα τμήματα που έχουν πρόσβαση στην πληροφορία τα σημεία αποθήκευσης δεδομένων τη μεταφορά δεδομένων τόσο εσωτερικά στο φορέα, όσο και σε εξωτερικούς αποδέκτες το χρόνο διατήρησης των δεδομένων και τις ενέργειες μετά το πέρας του χρόνου διατήρησης αυτών τη μεταφορά δεδομένων σε Τρίτες Χώρες τις νομικές βάσεις διατήρησης προσωπικών και ευαίσθητων προσωπικών δεδομένων τα δικαιώματα που δίδονται στο υποκείμενο και το κατά πόσο καλύπτονται οι αρχές επεξεργασίας του κανονισμού. 	NAI		
6.3	<ul style="list-style-type: none"> Να εξάγει το Αρχείο Δραστηριοτήτων Επεξεργασίας βάσει του άρθρου 30 του Κανονισμού και τις σχετικές αναφορές. 			
6.4	<ul style="list-style-type: none"> Να εξάγει Διαγράμματα Ροής για κάθε ανάλυση διαδικασίας (Data Flow Mapping). 	NAI		
6.5	<ul style="list-style-type: none"> Να παρουσιάζει τις αποκλίσεις από τον κανονισμό και να προτείνει μέτρα συμμόρφωσης (Gap Analysis & Maturity Assessment). 	NAI		
6.6	<ul style="list-style-type: none"> Να υπολογίζει την πιθανότητα απειλής των προσωπικών δεδομένων σε πληροφοριακά και άλλα τεχνολογικά συστήματα, καθώς και μεθόδους, διαδικασίες και εμπλοκή προσώπων ανά δραστηριότητα. 	NAI		
6.7	<ul style="list-style-type: none"> Να εξάγει τα αναγκαία Οργανωτικά και Τεχνικά Μέτρα ασφάλειας πληροφοριακών συστημάτων και φυσικών αρχείων ανάλογα με το επίπεδο επικινδυνότητας. 	NAI		

6.8	<ul style="list-style-type: none"> Να διενεργεί έλεγχο σχετικά με την απαίτηση διενέργειας Εκτίμησης Αντικτύπου και την προστασία προσωπικών δεδομένων (DATA PROTECTION IMPACT ASSESSMENT - DPIA) και να την εξάγει ελέγχοντας την απώλεια της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων. 	ΝΑΙ		
6.9	<ul style="list-style-type: none"> Να έχει την δυνατότητα εντοπισμού των προσωπικών δεδομένων ενός υποκειμένου, σε περίπτωση άσκησης των δικαιωμάτων από το υποκείμενο. 	ΝΑΙ		
6.10	<ul style="list-style-type: none"> Να έχει την δυνατότητα τροποποίησης και επικαιροποίησης των διαδικασιών επεξεργασίας των προσωπικών δεδομένων. 	ΝΑΙ		
6.11	<ul style="list-style-type: none"> Να έχει την δυνατότητα εντοπισμού του τρόπου επεξεργασίας, των σημείων αποθήκευσης και των αποδεκτών, ανά κατηγορία προσωπικών δεδομένων και της διατήρησης ιστορικού συμμόρφωσης. 	ΝΑΙ		
6.12	<ul style="list-style-type: none"> Να έχει τη δυνατότητα αποθήκευσης και διατήρησης των στοιχείων συμμόρφωσης του φορέα προκειμένου να είναι άμεσα προσβάσιμα κατά τη λογοδοσία. 	ΝΑΙ		
6.13	<ul style="list-style-type: none"> Να είναι δικτυακή (webbasedapp), ώστε να είναι εφικτή η χρήση της από πολλαπλά σημεία. 	ΝΑΙ		
6.14	<ul style="list-style-type: none"> Να μην απαιτείται από την ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ πρόσθετος εξειδικευμένος εξοπλισμός σε υλικό (hardware) ή επιπλέον λογισμικό (software) για τη λειτουργία της από τους χρήστες και να δοθεί με τη μορφή αγοράς άδειας χρήσης. 	ΝΑΙ		
6.15	<ul style="list-style-type: none"> Να έχει τη δυνατότητα δημιουργίας πολλαπλών προσωποποιημένων χρηστών με κεντρική Διαχείριση και δυνατότητα παραμετροποίησης χρηστών (π.χ. χρήστης με πλήρη δικαιώματα, χρήστης με δικαιώματα μόνο ανάγνωσης, απλός χρήστης). 	ΝΑΙ		
6.16	<ul style="list-style-type: none"> Ο ΑΝΑΔΟΧΟΣ οφείλει να περιγράψει πλήρως τον τρόπο τήρησης αντιγράφων ασφαλείας (backup), καθώς και τον τρόπο ανάκτησης δεδομένων σε περίπτωση απώλειας αυτών. 	ΝΑΙ		
6.17	<ul style="list-style-type: none"> Μετά το πέρας υλοποίησης του έργου, καθώς και για τα διάστημα ίσο με 2 (δύο) έτη μετά την οριστική παραλαβή του έργου, όλα τα δεδομένα που θα συλλεχτούν, αποθηκευτούν και επεξεργαστούν από την εν λόγω εφαρμογή, θα μεταβιβαστούν ακέραια στην ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ σε επεξεργάσιμη μορφή. 	ΝΑΙ		

Γ. Εγκρίνει την διενέργεια του διαγωνισμού με τα εξής στοιχεία, και με ένταξή του στον Πίνακα Προγραμματισμού του Γ.Ν. Λασιθίου-Γ.Ν.-Κ.Υ. Νεαπόλεως «Διαλυνάκειο» των ετών 2019-2020.

Κωδικός CPV	Περιγραφή CPV	Μ.Μ.	Ποσοτ.	τρόπος προμήθειας	Κριτ. Α-ξιολ.	ΚΑΕ	ΠΡ/ΣΘΕΙ ΣΑ ΔΑ-ΠΑΝΗ ΠΛΕΟΝ Φ.Π.Α.	ΠΡ/ΣΘΕΙΣ Α ΔΑ-ΠΑΝΗ ΣΥΜΠ/ΝΟ Υ Φ.Π.Α.	ΔΙΚΑΙΟΥΧΟΣ ΠΡΟΜΗΘΕΙΑΣ	ΔΙΑΡΚΕΙΑ
79417 000-0	Υπηρεσίες Παροχής Συμβουλών σε θέματα ασφαλείας	ΥΠΗΡΕΣΙ Α	1	Συνοπτικός διαγωνισμός	πλέον συμφέρουσα από οικονομική ή άποψη προσφορά μόνο βάσει τιμής	0439	10.306,13	12.779,60	Ο.Μ. ΕΔΡΑΣ-ΑΓΙΟΣ ΝΙΚΟΛΑΟΣ-ΚΨΥ-ΨΥΧΑΓΓΩΣ	28 ΜΗΝΕΣ
			1				5.367,78	6.656,04	Α.Ο.Μ. ΙΕΡΑΠΕΤΡΑΣ	

			1				5.367,78	6.656,04	Α.Ο.Μ. ΣΗΤΕΙΑΣ	
			1				1.431,41	1.774,94	Γ.Ν.-Κ.Υ. Νεαπόλεως «Διαλυνάκειο»	
					<u>ΣΥΝΟΛΟ</u>		<u>22.473,09</u>	<u>27.866,64</u>		

Δ. Εγκρίνει τα επισυναπτόμενα τεύχη της διακήρυξης.

Ε. Ορίζει τριμελή επιτροπή αποσφράγισης – αξιολόγησης του παραπάνω διαγωνισμού, όπως και κάθε τυχόν επαναληπτικού αυτού αποτελούμενη από τους:

- Κουφάκη Θεόδωρο (Ο.Μ.Έδρας Αγίου Νικολάου) με αναπληρωτή τον Δηλαβεράκη Μηνά (Α.Ο.Μ.Ιεράπετρας).
 - Δρετάκη Ουρανία (Α.Ο.Μ.Σητείας) με αναπληρώτρια την Μπαλίδου Παρασκευή (Α.Ο.Μ.Σητείας).
 - Λιανά Ειρήνη (Γ.Ν.-ΚΥ Νεαπόλεως) με αναπληρωτή τον Καντιδάκη Γεώργιο (Γ.Ν.-ΚΥ Νεαπόλεως).
-