ΦΥΣΙΚΟ ΑΝΤΙΚΕΙΜΕΝΟ ΕΡΓΟΥ " Σύστημα Διαχείρισης Εγγράφων & Ροών Εργασιών"

Εισαγωγή – Πεδίο εφαρμογής έργου

Ο ΕΟΠΥΥ διατηρεί και επεξεργάζεται πληθώρα δεδομένων προσωπικού χαρακτήρα, καθώς και πληροφορίες (σε ηλεκτρονικά ή / και φυσικά αρχεία), τα οποία μπορούν να ταυτοποιήσουν φυσικά πρόσωπα: ασφαλισμένους, εργαζομένους, συνεργάτες, προμηθευτές, κ.α.
Επιπλέον, η οργανωτική του δομή, απαιτεί την υποστήριξη των εσωτερικών αναγκών επικοινωνίας και διακίνησης εγγράφων με ένα σύγχρονο σύστημα διαχείρισης ροών εργασιών.
Οι εν λόγω ροές, αφενός θα πρέπει να καταγραφούν και να αποτυπωθούν σε ένα σχέδιο διασφάλισης ποιότητας για τον Οργανισμό, αφετέρου θα πρέπει να ληφθεί υπόψη και η υποχρέωση ΕΟΠΥΥ να εναρμονιστεί στον Κανονισμό GDPR (General Data Protection Regulation) που πρόκειται να εφαρμοσθεί σε όλους τους δημόσιους φορείς από τον Μάιο του 2018. Για το λόγο αυτό, ο Οργανισμός ήδη τους τελευταίους μήνες έχει προβεί σε προκαταρκτικές ενέργειες και έχει αναγάγει το θέμα σε ύψιστη προτεραιότητα.

Ο ΕΟΠΥΥ διαθέτει:

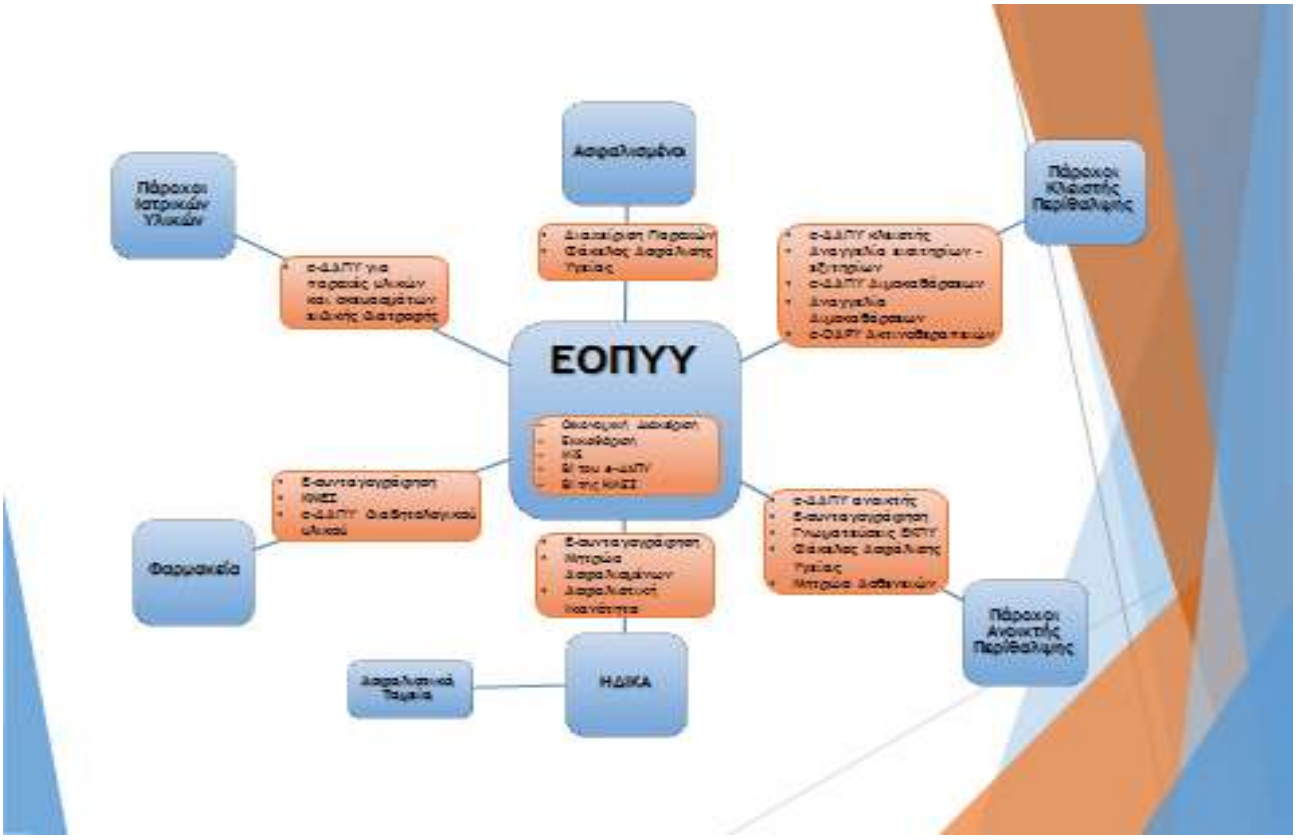
- Οργανωτική Δομή :
    - Διοίκηση
        1. Αυτοτελές Τμήμα Εσωτερικού Ελέγχου
        2. Γραφείο Διαχείρισης Παραπόνων και Καταγγελιών
        3. Αυτοτελές Τμήμα Νομικών Υποθέσεων
        4. ΥΠΕΔΥΦΚΑ
        5. Γραφείο Γραμματείας Προέδρου και ΔΣ
        6. Γραφείο Τύπου και Επικοινωνίας
    - Ανώτατο Υγειονομικό Συμβούλιο
    - Γενική Διεύθυνση Οικονομικών Υποθέσεων
        1. Διεύθυνση Οικονομικού
        2. Διεύθυνση Συμβάσεων
        3. Διεύθυνση Διεθνών Ασφαλιστικών Σχέσεων
        4. Διεύθυνση Ελέγχου και Εκκαθάρισης
    - Γενική Διεύθυνση Οργάνωσης και Σχεδιασμού Αγοράς Υπηρεσιών Υγείας
        1. Διεύθυνση Διοικητικής Υποστήριξης
        2. Διεύθυνση Πληροφορικής
        3. Διεύθυνση Φαρμάκου

4. Διεύθυνση Στρατηγικού Σχεδιασμού

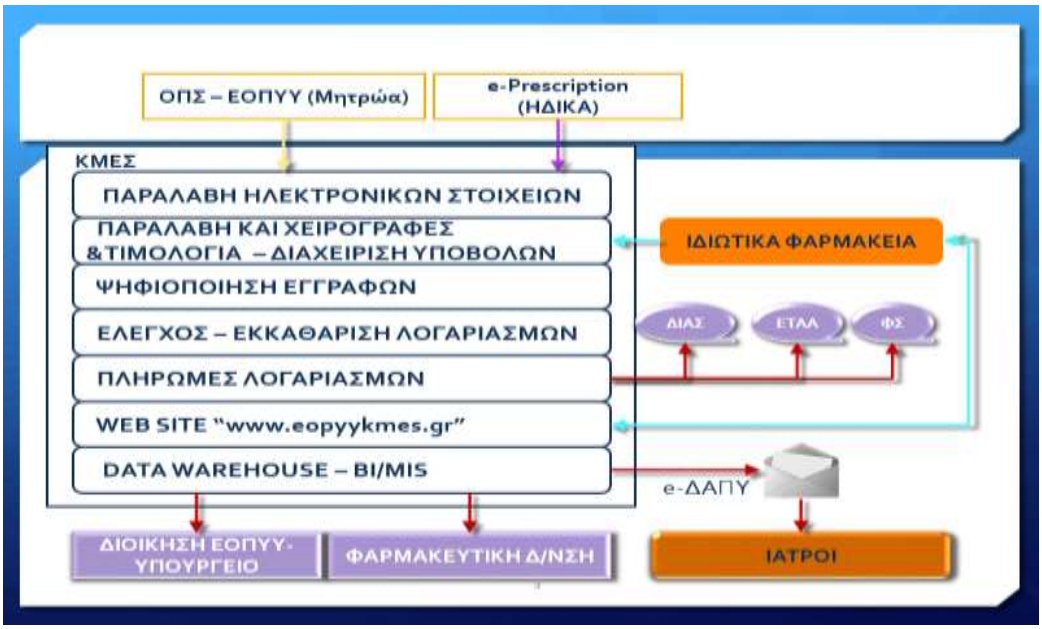
- 58 Περιφερειακές Διευθύνσεις
- 12 Υποκαταστήματα
- 6 Φαρμακεία στην Αττική, 1 στη Θεσσαλονίκη και 20 στην υπόλοιπη Ελλάδα
- δύο μεγάλα πληροφοριακά συστήματα:
    - Κεντρικό ΟΠΣ-ΕΟΠΥΥ (e-DAPY) για την Κεντρική Υπηρεσία και τις ηλεκτρονικές υπηρεσίες, και
    - Σύστημα ΚΜΕΣ για τη διαχείριση συνταγών φαρμάκου.
- Δύο data centers

Στα παρακάτω διαγράμματα φαίνεται αναλυτικά η λογική δομή των δυο συστημάτων:

Λογική αρχιτεκτονική ΟΠΣ



Λογική αρχιτεκτονική ΚΜΕΣ



Πρέπει να σημειωθεί πως τα δυο συστήματα φιλοξενούνται σε διαφορετικά datacenters, τα οποία βρίσκονται σε διαφορετικά σημεία στην Αττική. Τα δυο sites, συνδέονται με κατάλληλες τηλεπικοινωνιακές συνδέσεις,

Ο Ε.Ο.Π.Υ.Υ. στα πλαίσια του ψηφιακού εκσυγχρονισμού του και της εξοικονόμησης των σύγχρονων ψηφιακών λύσεων, αναζητά τη βέλτιστη λογισμική πλατφόρμα Διαχείρισης Εγγράφων & Ροής εργασιών με ενσωματωμένο Σύστημα Ψηφιακών Υπογραφών. Προς αυτήν την κατεύθυνση, στόχος του παρόντος έργου είναι ο προσδιορισμός του επίπεδου συμμόρφωσης του ΕΟΠΥΥ σχετικά με τις προδιαγραφές του κανονισμού General Data Protection Regulation (GDPR) 2016/679, που επικυρώθηκε στις 27.04.2016 από το Ευρωπαϊκό Κοινοβούλιο και το Ευρωπαϊκό Συμβούλιο, με σκοπό να ορίσει ο ΕΟΠΥΥ τις απαραίτητες δράσεις που συνιστούν ένα ολοκληρωμένο Πλάνο Συμμόρφωσης με τον Κανονισμό. Περαιτέρω στόχοι αυτού του έργου είναι η ανάπτυξη των Δραστηριοτήτων Επεξεργασίας (Data Flow Mapping), η εκπόνηση Μελέτης Χάσματος (Gap Analysis), η σύνταξη Πλάνου Συμμόρφωσης (Compliance Plan) και Ανάλυσης του Αντίκτυπου στην Προστασία Προσωπικών Δεδομένων (Privacy Impact Assessment), όπως ορίζονται από τον κανονισμό GDPR και τα οποία θα αποτελούν βασικά παραδοτέα του έργου.

Ο Ε.Ο.Π.Υ.Υ. είναι κάτοχος μεγάλου όγκου δεδομένων (big data), όλων των κατηγοριών, αλλά και των ειδικών κατηγοριών (π..χ υγείας) και αποτελεί το Φορέα με τον μεγαλύτερο προϋπολογισμό. Είναι προφανές ότι ένας τέτοιος Φορέας επιβάλλεται να συμμορφωθεί με τις απαιτήσεις του Κανονισμού.

Αντικείμενο Έργου

Προσδιορισμός του επίπεδου συμμόρφωσης του ΕΟΠΥΥ σχετικά με τις προδιαγραφές του κανονισμού General Data Protection Regulation (GDPR) (υποέργο 1)

Αντικείμενο του υποέργου αυτού θα είναι μία μελέτη ωριμότητας του οργανισμού έναντι του κανονισμού GDPR, η οποία θα:

- αξιολογεί όλους τους τομείς δραστηριότητας του οργανισμού και όλα τα τμήματα και τις διευθύνσεις ως προς την ετοιμότητά τους έναντι του GDPR
- εντοπίζει όλες τις περιοχές, όπου δεν παρατηρείται πλήρης ετοιμότητα και απαιτούνται ενέργειες συμμόρφωσης
- εμβαθύνει στις ανωτέρω περιοχές και θα προτείνει αναλυτικά μέτρα, ώστε ο οργανισμός να ξεκινήσει εγκαίρως την υλοποίηση όλων των διορθωτικών ενεργειών συμμόρφωσης.

Αναλυτικά το έργο θα περιλαμβάνει :

- Ανάλυση της τρέχουσας κατάστασης ως προς την προστασία των προσωπικών δεδομένων που περιλαμβάνει την αξιολόγηση των υφιστάμενων πρακτικών, των γραπτών πολιτικών και διαδικασιών, των πληροφοριακών συστημάτων και δικτυακών υποδομών, και κάθε στοιχείου που επηρεάζει την προστασία προσωπικών δεδομένων σε όλες τις δραστηριότητες, τα τμήματα, τα παραρτήματα και τις διευθύνσεις του οργανισμού. Παράλληλα θα αξιολογηθεί η υφιστάμενη κατάσταση ως προς την ασφάλεια των πληροφοριών και την επιχειρησιακή συνέχεια που αποτελούν συστατικά της προστασίας των δεδομένων.
- Δημιουργία λεπτομερών data flow maps ανά τμήμα ή ανά κατηγορία προσωπικών δεδομένων, όπου θα απεικονίζονται όλες οι πληροφορίες σχετικά με τη διαχείριση των προσωπικών δεδομένων στον οργανισμό. Τα data flow maps θα καλύπτουν την απαίτηση του GDPR για το αρχείο δραστηριοτήτων επεξεργασίας δεομένων και θα περιέχουν όλες τις επιπλέον απαραίτητες πληροφορίες, ώστε να απεικονίζεται πλήρως η τρέχουσα κατάσταση ως προς τη διαχείριση προσωπικών δεδομένων και να εντοπίζονται κενά ως προς τις απαιτήσεις του θεσμικού πλαισίου.
- Εύρεση κενών ως προς την ικανοποίηση των απαιτήσεων του κανονισμού (Gap Analysis), κατηγοριοποιημένα ανά θεματική περιοχή και κρισιμότητα.
- Για κάθε κενό που εντοπίζεται, καθορισμός των απαραίτητων ενεργειών αντιμετώπισης και δημιουργία ενός λεπτομερούς, προτεραιοποιημένου και ολοκληρωμένου πλάνου συμμόρφωσης (compliance plan and roadmap).

- Σύνταξη Μελέτης Εκτίμησης αντίκτυπου (Data Privacy Impact Assessment) με βάση τη μεθοδολογία του ISO 29134, την οδηγία του WP 29 και τις υφιστάμενες οδηγίες των Ευρωπαϊκών Αρχών Προστασίας.
- Σύνταξη 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 πληροφοριών του οργανισμού (Information Security Risk Assessment)
- Σύνταξη Ανάλυσης Επιχειρησιακών Επιπτώσεων (Business Impact Analysis), Πλάνου Επιχειρησιακής Συνέχειας (Business Continuity Plan) και Σχεδίου Ανάκαμψης από Καταστροφή (Disaster Recovery Plan) που να εξασφαλίζουν την επιχειρησιακή συνέχεια του οργανισμού.

  Οι ανωτέρω αναλύσεις επικινδυνότητας και εκτίμησης επιπτώσεων θα πρέπει να είναι συμβατές μεταξύ τους και να μη περιέχουν αλληλεπικαλύψεις, κενά ή αλληλοσυγκρουόμενες πληροφορίες.

Η ανωτέρω αξιολόγηση 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 κ.λπ.
- Αξιολόγηση δυνατότητας ικανοποίησης των δικαιωμάτων των φυσικών προσώπων
- Αξιολόγηση ικανοποιητικού επιπέδου ασφαλείας και επιχειρησιακής συνέχειας
- Αξιολόγηση επαρκούς οργανωτικής δομής
- Αξιολόγηση συμβάσεων με τρίτους που εκτελούν επεξεργασία προσωπικών δεδομένων του οργανισμού
- Αξιολόγηση κουλτούρας και ευαισθητοποίησης στα θέματα προστασίας προσωπικών δεδομένων
- Αξιολόγηση πληροφορικών συστημάτων και πολιτικών που επιβάλλονται από την πληροφορική
- Αξιολόγηση μηχανισμών ελέγχου και διασφάλισης της συμμόρφωσης
- Αξιολόγηση σχετικών γραπτών πολιτικών και διαδικασιών.

Με σκοπό την επιτυχή υλοποίηση των σκοπών του έργου ο υποψήφιος ανάδοχος είναι απαραίτητο να:

- Συμπεριλάβει ανάλυση της τρέχουσας κατάστασης 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 δεδομένων

- Διεξάγει συνεντεύξεις με τα αρμόδια στελέχη από κάθε τμήμα του Οργανισμού καλύπτοντας κάθε δραστηριότητα, τμήμα, περιφερειακή διεύθυνση και υποκατάστημα.
- Διεξάγει λεπτομερή αξιολόγηση των επιπτώσεων στην προστασία δεδομένων, βάσει του προτύπου ISO 29134, της κατευθυντήριας οδηγίας του WP 29 και άλλων σχετικών διεθνών κατευθυντήριων γραμμών, οι οποίες αξιολογούν τους κινδύνους που σχετίζονται με θέματα ασφάλειας των πληροφοριών και τα νομικά ζητήματα προστασίας δεδομένων και δίνουν προτεραιότητα στα ευρήματα, ανάλογα με το επίπεδο κινδύνου
- Δημιουργήσει λεπτομερές πλάνο ενεργειών αντιμετώπισης και διαχείρισης των ευρημάτων, έτσι ώστε οι επικεφαλής των αρμόδιων επιχειρησιακών μονάδων να είναι σε θέση να εφαρμόσουν τις απαραίτητες ενέργειες
- Παρέχει ένα λεπτομερές data flow map ανά επιχειρησιακή 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
- Πραγματοποιήσει έλεγχο σε όλες τις εμπλεκόμενες εφαρμογές λογισμικού, σε όλα τα αποθηκευτικά μέσα (ψηφιακά, έντυπα, ηχητικά, κα) καθώς και να προτείνει με σαφήνεια τις απαιτούμενες αλλαγές και τροποποιήσεις βάσει του νέου κανονισμού. Η αξιολόγηση θα περιλαμβάνει την αξιολόγηση του συνόλου των συλλεγόμενων προσωπικών δεδομένων, της νομικής βάσης πάνω στην οποία στηρίζεται η συλλογή, της παρεχόμενης συναίνεσης από τον εκάστοτε συμβαλλόμενο, των παρεχόμενων πληροφοριών κ.λπ. 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 αξιολόγηση όλων των συμβάσεων του ΕΟΠΥΥ με τρίτους (ιατρούς, παρόχους ιατρικών, ασφαλιστικών, ελεγκτικών και άλλων υπηρεσιών, συνεργάτες και γενικότερα εκτελούντες την επεξεργασία), να εντοπίσει κενά και να προτείνει ενέργειες με σκοπό την προσαρμογή τους στον νέο κανονισμό
- Πραγματοποιήσει αξιολόγηση όλων των πρακτικών που σχετίζονται με την επεξεργασία των προσωπικών δεδομένων και να παρέχει συγκεκριμένες και λεπτομερείς προτάσεις για δράσεις συμμόρφωσης με τον νέο κανονισμό
- Παρέχει ένα λεπτομερές, προτεραιοποιημένο και ολοκληρωμένο πλάνο συμμόρφωσης
- 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 ομάδα έργου και τους επιχειρησιακούς ιδιοκτήτες των δεδομένων του ΕΟΠΥΥ πριν την παράδοση του πλάνου συμμόρφωσης

- Αναλάβει το Project Management της υλοποίησης των ενεργειών που θα περιέχει το ολοκληρωμένο πλάνο συμμόρφωσης έως το Μάιο του 2018.

Ευρωπαϊκός Γενικός Κανονισμός Προστασίας Δεδομένων

Ο Γενικός Κανονισμός Προστασίας δεδομένων είναι ένα νομοθέτημα άμεσης εφαρμογής: κατισχύει των εθνικών νομοθεσιών των κρατών μελών για την προστασία προσωπικών δεδομένων, χωρίς να χρειάζεται να εισαχθεί με νόμο στην εσωτερική έννομη τάξη. Αυτό σημαίνει ότι η θέση σε ισχύ του Κανονισμού εκτοπίζει ουσιαστικά τον δικό μας Ν.2472/1997, τουλάχιστον ως προς το πεδίο εφαρμογής του Κανονισμού και ως προς τις διατάξεις του που βρίσκονται τυχόν σε αντίθεση με τις διατάξεις του Κανονισμού. Ο Κανονισμός απέκτησε τυπική ισχύ 20 ημέρες μετά την δημοσίευσή του στην Επίσημη Εφημερίδα της ΕΕ και θα ισχύει στα κράτη μέλη 2 χρόνια μετά, δηλαδή το Μάιο του 2018. Καταργεί επίσης την Οδηγία 95/46 που ήταν εδώ και 20 χρόνια το βασικό νομοθέτημα για την προστασία προσωπικών δεδομένων σε επίπεδο Ευρωπαϊκών Κοινοτήτων.. Ο νέος, γενικός κανονισμός έχει σχεδιαστεί κατά τέτοιο τρόπο ώστε να δώσει στους πολίτες μεγαλύτερο έλεγχο των προσωπικών τους στοιχείων στα πλαίσια του νέου, ψηφιακού κόσμου των "έξυπνων" κινητών τηλεφώνων (smartphones), των κοινωνικών μέσων δικτύωσης, των ηλεκτρονικών τραπεζικών συναλλαγών (internet banking) και των διεθνών συναλλαγών (global transfers). **Τα βασικά στοιχεία του Κανονισμού που έχουν εφαρμογή στον ΕΟΠΠΥ είναι τα εξής:**

- **Δικαίωμα στην λήθη**: Όταν εκλείπει ο λόγος της επεξεργασίας των δεδομένων ή το υποκείμενο αίρει την 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 την 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 την διαγραφή τους.
- **Σαφής συγκατάθεση**: Το κάθε άτομο (ενδιαφερόμενο πρόσωπο) πρέπει να δώσει την συγκατάθεσή του για την επεξεργασία των προσωπικών του δεδομένων.
- **Δικαίωμα φορητότητας των δεδομένων**: Το υποκείμενο (ενδιαφερόμενο πρόσωπο) έχει δικαίωμα να ζητά από τον υπεύθυνο επεξεργασίας να λαμβάνει τα δεδομένα σε κοινώς αναγνωρίσιμο μορφότυπο, καθώς και την απευθείας διαβίβαση των δεδομένων του σε άλλον υπεύθυνο επεξεργασίας.
- **Υποχρέωση γνωστοποίησης παραβιάσεων ασφάλειας**: Όταν ο υπεύθυνος λάβει γνώση την παραβίαση της ασφάλειας του συστήματος οφείλει να ειδοποιήσει την

ανεξάρτητη αρχή που είναι υπεύθυνη για την προστασία προσωπικών δεδομένων. Η γνωστοποίηση πρέπει να γίνεται και στο ίδιο το υποκείμενο των δεδομένων

- **Διασυνοριακή 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.
- **Ενημέρωση για Δεδομένα Προσωπικού Χαρακτήρα**: Ο υπεύθυνος επεξεργασίας πρέπει να παρέχει όλες τις εξηγήσεις για τις πολιτικές απορρήτου σε σαφή και κατανοητή γλώσσα.
- **Πρόστιμα από μη συμμόρφωση**: Η μη συμμόρφωση με τους κανόνες προστασίας προσωπικών δεδομένων επιφέρει και πρόστιμα στις επιχειρήσεις που τον παραβιάζουν έως 20 εκατομ. € 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 ακόλουθες αρχές προστασίας δεδομένων τηρούνται:
    - **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: Σχετικότητα Δεδομένων (Data Relevancy):** Τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι κατάλληλα, συναφή και όχι υπερβολικά σε σχέση με το σκοπό ή τους σκοπούς 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 επεξεργασθεί για οποιονδήποτε σκοπό ή σκοπούς δεν θα πρέπει να διατηρούνται για μεγαλύτερο χρονικό διάστημα από ό, τι 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 σύμφωνα με τα δικαιώματα των υποκειμένων των δεδομένων δυνάμει του παρόντος νόμου.
    - **Έβδομη Αρχή: Λογοδοσία (Accountability):** Θα πρέπει να ληφθούν τα κατάλληλα διοικητικά, τεχνικά και οργανωτικά μέτρα 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.

- **Υπεύθυνος Προστασίας Δεδομένων:** Σε κάθε δημόσιο φορέα (εκτός από τα δικαστήρια στο πλαίσιο των δικαιοδοτικών τους αρμοδιοτήτων, εάν τα κράτη επιλέξουν να τα εξαιρέσουν) και σε κάθε ιδιωτικό φορέα που λόγω της φύσης των δραστηριοτήτων τους παρακολουθούν υποκείμενα δεδομένων σε μεγάλη κλίμακα ή επεξεργάζονται ευαίσθητα δεδομένα, ορίζεται ένα πρόσωπο ως ΥΠΔ. Ο ΥΠΔ λειτουργεί ως μια εσωτερική Αρχή Προστασίας Δεδομένων που διασφαλίζει ότι η δημόσια υπηρεσία ή ο ιδιωτικός φορέας τηρεί τις διατάξεις του Κανονισμού και συνεργάζεται με την Εθνική Αρχή Προστασίας για την τήρηση των διατάξεων.
- **Εκτίμηση Επιπτώσεων Προστασίας Δεδομένων**: Ο υπεύθυνος επεξεργασίας πρέπει να επιβεβαιώνει ότι εφαρμόζεται μια διαδικασία για τη διεξαγωγή μιας αξιολόγησης του κινδύνων προστασίας των δεδομένων (Data Protection Impact Assessment) σε όλες τις επιχειρησιακές μονάδες.

Υλοποίηση Συστήματος Διαχείρισης Εγγράφων & Ροών Εργασίας (υποέργο 2)

Αντικείμενο του υποέργου είναι η :

- Μελέτη – σχεδιασμός, ανάπτυξη, εγκατάσταση & θέση σε λειτουργία (συμπεριλαμβανομένης της εσωτερικής εκπαίδευσης του προσωπικού) Συστήματος Διαχείρισης Εγγράφων και Ροών Εργασίας με χρήση του λογισμικού Microsoft Sharepoint.

Αναλυτικά το έργο περιλαμβάνει:

- Καταγραφή τύπων εγγράφων και άλλου περιεχομένου του Οργανισμού
- Επιλογή κατάλληλου προτύπου για κάθε έγγραφο
- Καταγραφή απαραίτητων μεταδεδομένων για κάθε τύπο εγγράφου
- Προδιαγραφές πρόσβασης εγγράφων σε κάθε φάση της ζωής τους
- Υλοποίηση ροών εργασίας εγγράφων μέσα στον Οργανισμό (δημιουργία, επισκόπηση, έγκριση, έκδοση, καταστροφή)

Για την υλοποίηση του υποέργου, ο Οργανισμός θα διαθέσει τις κατάλληλες υποδομές (hardware & system software). Ο ανάδοχος καλείται να παρέχει αποκλειστικά τις υπηρεσίες μελέτης, σχεδιασμού, ανάπτυξης, εγκατάστασης & θέσης σε λειτουργία του συστήματος.

Για την καταγραφή των σχετικών ροών εργασίας, θα πρέπει να ακολουθηθούν τα εξής βήματα:

Αναγνώριση ρόλων διαχείρισης εγγράφων
Θα πρέπει να διασφαλιστεί ότι ο σχεδιασμός θα λαμβάνει υπόψη τις προτεραιότητες του Οργανισμού και θα αναγνωρίζει το σύνολο των εμπλεκόμενων στη διαδικασία διακίνησης εγγράφων.

Ανάλυση χρήσης εγγράφων
Μετά την αναγνώριση των εργαζόμενων στα έγγραφα, θα πρέπει να αναγνωριστεί το είδος των εγγραφών και πώς χρησιμοποιούνται.

Οργάνωση εγγράφων
Θα πρέπει να παρέχονται πολλαπλές δυνατότητες οργάνωσης των εγγράφων σε δομές όπως συλλογές ή βιβλιοθήκες.

Ροή περιεχομένου
Θα πρέπει να μπορούν να μεταφερθούν ή να αντιγραφούν έγγραφα από μία δομή στην άλλη, σε διαφορετικές φάσης της ζωής των εγγράφων.

Καθορισμός τύπων περιεχομένου
Θα μπορούν να καθοριστούν τύποι περιεχομένου σχετικά με τα έγγραφα, όπως μεταδεδομένα, πρότυπα εγγράφων, και διαδικασίες ροών εργασιών. Με τον τρόπο αυτό θα πρέπει να οργανωθούν τα έγγραφα και να επιβληθεί η συνοχή στον Οργανισμό.

Καθορισμός ροών εργασίας
Κατά τον σχεδιασμό ροών εργασίας στον Οργανισμό, θα πρέπει να ελεγχθεί και να εντοπιστεί ο τρόπος κίνησης των δεδομένων μεταξύ των εμπλεκόμενων.

Καθορισμός διαβάθμισης εγγράφων
Θα πρέπει να σχεδιαστεί το επίπεδο ελέγχου που βασίζεται σε παραμέτρους όπως ο τύπος του εγγράφου ή ο τόπος αποθήκευσης.

Καθορισμός πολιτικών
Για κάθε τύπο εγγράφων, θα πρέπει να σχεδιάζονται πολιτικές διαχείρισης ώστε για τα δεδομένα να καταγράφονται, να κρατούνται και γενικά να τυγχάνουν διαχείρισης βάσει του κανονισμού GDPR.

Βασικές Αρχές Υποβολής Προσφορών

Όλες οι προτάσεις είναι απαραίτητο να βασίζονται και να λαμβάνουν υπόψη εκτός από τον Κανονισμό Γενικής Προστασίας Δεδομένων, 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, τις κατευθυντήριες γραμμές της Ελληνικής Αρχής Προστασίας Προσωπικών Δεδομένων (καθώς και τις κατά περίπτωση Κατευθυντήριες γραμμές άλλων Ευρωπαϊκών Αρχών Προστασίας Προσωπικών Δεδομένων) και τις βέλτιστες πρακτικές σύμφωνα με τα διεθνή πρότυπα.
Επίσης, ο υποψήφιος Ανάδοχος θα συμπεριλάβει στην προσφορά του :

- Χρονοδιάγραμμα δραστηριοτήτων – προγραμματισμό φάσεων υλοποίησης έργου
- Προτεινόμενες τεχνολογίες για τις υπηρεσίες αυτοματοποιημένου data discovery
- Πρόσθετες υπηρεσίες που είναι σε θέση να αναλάβει κατά την υλοποίηση των ενεργειών του πλάνου συμμόρφωσης
- Ανάλυση του κανονιστικού πλαισίου που θα λάβει υπόψη κατά την εκτέλεση του έργου.

Φάσεις Έργου – Παραδοτέα

Φάση 1 : Έναρξη έργου - Οργάνωση δράσεων (15 ημέρες από την υπογραφή της σύμβασης)

- παρουσίαση στη διοίκηση και τα στελέχη του Οργανισμού
- υποβολή προτάσεων οργάνωσης της ομάδας έργου
- **Παραδοτέα**
  - ✓ Πλάνο υλοποίησης έργου (Περιγραφή του Έργου στην οποία περιγράφεται ο τρόπος προσέγγισης και εκτέλεσης του Έργου, συμπεριλαμβανομένης της σύνθεσης της Ομάδας Έργου, των επιμέρους καθηκόντων των προσώπων που θα την απαρτίζουν, των παραδοτέων και του χρονοδιαγράμματος)
  - ✓ Πλάνο ποιότητας έργου

Φάση 2 - Συγκέντρωση δεδομένων & Υλοποίηση Ροών Εργασίας (2 μήνες από την ολοκλήρωση της Φάσης 1)

- Επισκόπηση των επιχειρησιακών, τεχνικών και λειτουργικών διαδικασιών.
- Ανάπτυξη του αρχείου δραστηριοτήτων και πόρων επεξεργασίας του Οργανισμού
- Ανάπτυξη του αρχείου δραστηριοτήτων και πόρων επεξεργασίας για όλες τις κρίσιμες περιοχές επεξεργασίας.
- Ανάπτυξη διαγραμμάτων ροής δεδομένων που θα αποτυπώνουν τις φάσεις του κύκλου ζωής των δεδομένων, από τη συλλογή, χρήση, αποθήκευση, μεταφορά μέχρι και την καταστροφή τους.

- Συγκέντρωση των απαιτούμενων πληροφοριών για τη συλλογή και επεξεργασία των προσωπικών δεδομένων, μέσω της διενέργειας συνεντεύξεων με στελέχη όλων των τμημάτων, των διευθύνσεων και των υποκαταστημάτων.
- εντοπισμός των κρισίμων αποκλίσεων έναντι των απαιτήσεων του Κανονισμού GDPR
- παραμετροποιήση και προσαρμογή αυστήματος διαχείρισης εγγράφων και ροών εργασίας
- **Παραδοτέα :**
  - ✓ Data Flow Maps που θα καλύπτουν την απαίτηση του GDPR για το αρχείο δραστηριοτήτων επεξεργασίας δεομένων και θα περιέχουν όλες τις επιπλέον απαραίτητες πληροφορίες, ώστε να απεικονίζεται πλήρως η τρέχουσα κατάσταση ως προς τη διαχείριση προσωπικών δεδομένων και να εντοπίζονται κενά ως προς τις απαιτήσεις του θεσμικού πλαισίου (διαγράμματα ροής δεδομένων προσωπικού χαρακτήρα, με κρίσιμες πληροφορίες)
  - ✓ Σύστημα διαχείρισης εγγράφων και ροών εργασίας με εγκατεστημένες τις καταγεγραμμένες ροές εργασίας

Φάση 3 - Μελέτη ανάλυσης αποκλίσεων (Gap Analysis και Maturity Assessment) – 1 μήνας από την ολοκλήρωση της Φάσης 2

- Μελέτη υφιστάμενης κατάστασης ως προς τη διαχείριση προσωπικών δεδομένων από:
  - ✓ άποψης διαδικασιών
  - ✓ νομικής άποψης
  - ✓ άποψης ασφάλειας πληροφοριών
  - ✓ τεχνολογικής άποψης
- εντοπισμός μη συμμορφώσεων στις πρακτικές και διαδικασίες που εφαρμόζονται κατά τον χειρισμό των προσωπικών δεδομένων, ως προς:
  - ✓ τις απαιτήσεις του GDPR
  - ✓ του κανονιστικού πλαισίου του έργου, συμπεριλαμβανομένων σχετικών δικαστικών αποφάσεων
  - ✓ των οδηγιών, κατευθύνσεων και αποφάσεων του WP29, της ΑΠΔΠΧ και των Ευρωπαϊκών Αρχών Προστασίας Δεδομένων
  - ✓ τις απαιτήσεις του ISO 27001, ISO 27002 και ISO 27799 για την ασφάλεια πληροφοριών
  - ✓ τις απαιτήσεις του ISO 22301 και ISO 27031 για την επιχειρησιακή συνέχεια
- Μελέτη ως προς τις υφιστάμενες επεξεργασίες δεδομένων (και της διαβαθμίσεώς τους), καθώς και συστημάτων πληροφορικής του Οργανισμού.
- Αναγνώριση των σχετικών απαιτήσεων του Γενικού Κανονισμού ως προς τις επιμέρους περιοχές επεξεργασίας προσωπικών δεδομένων.

- Μελέτη αποκλίσεων της υφιστάμενης κατάστασης του Οργανισμού σε σχέση με τις απαιτήσεις του Κανονισμού για κάθε επεξεργασία. Η μελέτη θα πρέπει να περιλαμβάνεις τουλάχιστον τις παρακάτω περιοχές:
  - ✓ Απαιτήσεις ως προς την υποχρέωση τήρησης αρχείου δραστηριοτήτων,
  - ✓ Συναίνεση,
  - ✓ Συλλογή, Χρήση, Αποθήκευση,
  - ✓ Διατήρηση δεδομένων/Καταστροφή,
  - ✓ Δικαιώματα πρόσβασης, διόρθωσης, αλλαγής 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 του Οργανισμού και τις επιμέρους αποκλίσεις που παρουσιάζει σε σχέση με τις ανωτέρω απαιτήσεις
- **Παραδοτέα**
  - ✓ Gap Analysis

Φάση 4 - Ανάπτυξη σχεδίου διορθωτικών ενεργειών – Εκπαίδευση Προσωπικού – Πιλοτική Λειτουργία (1 μήνας από την ολοκλήρωση της Φάσης 3)

- Καταγραφή αναλυτικού και σαφούς σχεδίου στο οποίο θα συμπεριλαμβάνονται οι προτάσεις εμπειρία στη βελτίωσης ανά περιοχή/ μονάδα του Οργανισμού, 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.
- Προσέγγιση και προσδιορισμός συγκεκριμένων εργασιών ώστε να βελτιωθεί κατά το δυνατόν συντομότερα το επίπεδο συμμόρφωσης.
- Κατάθεση προτάσεων για τη διατήρηση στο μέλλον ικανοποιητικού επίπεδου συμμόρφωσης με τις απαιτήσεις του Κανονισμού.
- Κατάθεση προτάσεων αναφορικά με την πραγματοποίηση συγκεκριμένων εργασιών, σχετικά με την τροποποίηση υφιστάμενων διαδικασιών, καθώς και το περιβάλλον λειτουργίας των πληροφοριακών συστημάτων, με σκοπό τη συμμόρφωση με τον Κανονισμό.
- Εκπόνηση ενδοεπιχειρησιακών σεμιναρίων και ηλεκτρονικών μαθημάτων

- Βελτιώσεις των εφαρμογών, Επίλυση προβλημάτων – υποστήριξη χρηστών
- On the job training στους χρήστες του συστήματος
- **Παραδοτέα**
  - ✓ Compliance Plan που να συμπεριλαμβάνει προτάσεις αλλαγών για ικανοποίηση απαιτήσεων στα Π.Σ. του ΕΟΠΥΥ (e-dapy, ΚΜΕΣ, BI)
  - ✓ Privacy Impact Assessment
  - ✓ Infromation Security Risk Assessment
  - ✓ Business Continuity Risk Assessmnet
  - ✓ Business Impact Analysis
  - ✓ Business Continuity Plans
  - ✓ Disaster Recovery Plans
  - ✓ Δράσεις ευαισθητοποίησης
  - ✓ Δράσεις εκπαίδευσης
  - ✓ Σύνταξη πολιτικών και διαδικασιών
    (1) προστασίας δεομένων
    (2) ασφάλειας δεδομένων κατά ISO 27001, ISO 27002 και ISO 27799
    (3) επιχειρησιακής συνέχειας κατά ISO 22301 και ISO 27031
  - ✓ Internal Audit για τις παραπάνω πολιτικές και διαδικασίες, ώστε αυτές να είναι πιστοποιήσιμες
  - ✓ Εκπαιδευτικό Υλικό εκπαιδευομένων ανά κατηγορία εκπαιδευομένου σε έντυπη και ηλεκτρονική μορφή συμπεριλαμβανομένων των Εκπαιδευτικών Παρουσιάσεων
  - ✓ Αναφορά Πιλοτικής Λειτουργίας, η οποία θα περιλαμβάνει παρουσίαση των Προβλημάτων και των τρόπων Επίλυσης τους

Ελάχιστες προδιαγραφές Υπηρεσιών

Υπηρεσίες Εκπόνησης Πλάνου Υλοποίησης Έργου

Το πλάνο αφορά στην οριστικοποίηση των τεχνικών προδιαγραφών του πληροφοριακού συστήματος, του τρόπου κωδικοποίησης, εισαγωγής και ομογενοποίησης των δεδομένων αυτών στη νέα Βάση Δεδομένων, τα επίπεδα της διαβαθμισμένης πρόσβασης στη πληροφορία από πλευράς χρηστών και στην οριστικοποίηση των τεχνικών προδιαγραφών του μοντέλου διαχείρισης αυτών. Συγκεκριμένα, περιλαμβάνει την αναλυτική καταγραφή των απαιτήσεων, δημιουργία μοντέλου του συστήματος και περιγραφή αυτού με κάποια από τις υπάρχουσες μεθόδους.

Η ανάλυση θα περιλαμβάνει κατ' ελάχιστον τα παρακάτω:

- Τον πλήρη σχεδιασμό του συνολικού συστήματος (αρχιτεκτονική συστήματος, ρόλοι χρηστών, ασφάλεια συστήματος, μηχανισμοί ελέγχου, μηχανισμοί αναφορών και παραγωγής εκθέσεων κτλ.).
- Αναλυτικό χρονοδιάγραμμα υλοποίησης με πρόβλεψη για όλα τα παραδοτέα και τον απαιτούμενο χρόνο ελέγχου/αποδοχής τους.
- Τον προσδιορισμό της μεθοδολογίας και των αρχικών σεναρίων ελέγχου αποδοχής καθώς και τον καθορισμό της μεθόδου καταγραφής δεικτών απόδοσης των συστημάτων και εφαρμογών.

Υπηρεσίες Εκπαίδευσης

Στα πλαίσια παροχής της συγκεκριμένης υπηρεσίας θα πρέπει να παρασχεθεί η κατάλληλη τεχνική εκπαίδευση σε επιλεγμένες ομάδες χρηστών της αναθέτουσας αρχής, με σκοπό να επιτευχθούν οι παρακάτω στόχοι:

- Η επίλυση προβλημάτων που σχετίζονται με την αρχική εξοικείωση των χρηστών του συστήματος και η υποστήριξη της προσαρμογής τους.
- Η μεταφορά τεχνογνωσίας προς τα στελέχη του Φορέα και των υπηρεσιών του, που θα αναλάβουν μετά το πέρας του έργου την ενημέρωση, διαχείριση και υποστήριξη του συστήματος.

- Η ανάληψη του καθήκοντος της εκπαίδευσης από επιλεγμένα στελέχη του Φορέα, προς τους υπόλοιπους τη διαχείριση του προμηθευόμενου συστήματος, εξοπλισμού, καθώς και λογισμικού συστημάτων και εφαρμογών που θα χρησιμοποιηθεί στο πλαίσιο του έργου και για την δοκιμαστική λειτουργία του και των εφαρμογών που θα αναπτυχθούν.
- Εκπαιδευτές, με σκοπό την ενημέρωση και διαρκή εκπαίδευση του υπόλοιπου προσωπικού του Φορέα, αναφορικά με τις διαδικασίες που θα τηρούνται κατά την παροχή ηλεκτρονικών υπηρεσιών από το Φορέα. Η συγκεκριμένη τεχνική επιλογή αποσκοπεί στη μείωση του προϋπολογισμού του έργου και είναι σύμφωνη με διαδεδομένες πρακτικές σε έργα ΤΠΕ (Teach the teachers).

Ο υποψήφιος ανάδοχος, θα πρέπει να παρουσιάσει στην προσφορά του ολοκληρωμένο προτεινόμενο πρόγραμμα κατάρτισης ανά κατηγορία εκπαιδευομένων και γνωστικό αντικείμενο καθώς επίσης αναλυτικό χρονοδιάγραμμα εκπαίδευσης ανά ομάδα εκπαιδευομένων και εκπαιδευτικό κύκλο.

Υπηρεσίες Πιλοτικής Λειτουργίας

Μετά την επιτυχή ολοκλήρωση όλων των ελέγχων και την αποδοχή τους από την Επιτροπή Παρακολούθησης και Παραλαβής του Έργου, αρχίζει η Περίοδος Πιλοτικής Λειτουργίας. Στην περίοδο αυτή το σύστημα θα εγκατασταθεί και θα λειτουργήσει σε πραγματικές συνθήκες εργασίας.

Ο Ανάδοχος υποχρεούται να υποστηρίξει την λειτουργία του συστήματος και τους χρήστες κάτω από πραγματικές συνθήκες λειτουργίας εξασφαλίζοντας την απαιτούμενη διαθεσιμότητα. Κατά την περίοδο αυτή ο Ανάδοχος θα βρίσκεται σε συνεχή συνεργασία με τους υπεύθυνους του Φορέα Υλοποίησης.

Στη φάση της Πιλοτικής λειτουργίας ο Ανάδοχος υποχρεούται να προσφέρει τις εξής υπηρεσίες:

Άμεση τηλεφωνική υποστήριξη Help-desk

Άμεση υποστήριξη σε όλους τους χρήστες Συστήματος που χρησιμοποιούν το Πληροφοριακό Σύστημα μέσω τηλεφώνου κατά το ωράριο λειτουργίας 08:00-18:00. Ο Ανάδοχος υποχρεούται να παρέχει τις ακόλουθες υπηρεσίες:

- Τηλεφωνική υποστήριξη σχετικά με τη χρήση του συστήματος
- Τηλεφωνική υποστήριξη για την αντιμετώπιση προβλημάτων κατά την χρήση

Υπηρεσίες Τεχνικής Υποστήριξης της Πιλοτικής Λειτουργίας

Ο Ανάδοχος για όλη τη διάρκεια της δοκιμαστικής λειτουργίας, καλείται να διαθέσει εξειδικευμένο προσωπικό τουλάχιστον ένα (1) άτομο στο χώρο εγκατάστασης του Συστήματος (on – the – job) με στόχο την υποστήριξη των χρηστών του φορέα στη λειτουργία των εφαρμογών.

Η υποστήριξη κατά την δοκιμαστική λειτουργία του συστήματος θα πρέπει να περιλαμβάνει:

A1. Συνεχής τεχνική υποστήριξη για την απρόσκοπτη λειτουργία συστημάτων και υποδομών.
A2. Τεχνική υποστήριξη των διαδικασιών τεκμηρίωσης
A1. Βελτιώσεις / Διορθώσεις των εφαρμογών
A2. Επίλυση προβλημάτων – υποστήριξη χρηστών
A3. Συλλογή παρατηρήσεων από τους χρήστες
A4. Διόρθωση / Διαχείριση λαθών
A5. Υποστήριξη στον χειρισμό και λειτουργία των υπολογιστών, και λοιπού προσφερόμενου εξοπλισμού.
A6. Επικαιροποίηση (update) τεκμηρίωσης.

Από τη συλλογή των παρατηρήσεων και των εκκρεμοτήτων ενδέχεται να δημιουργηθεί η ανάγκη για συγκεκριμένες παρεμβάσεις ή διορθώσεις στη λειτουργία του συστήματος. Ο Ανάδοχος μετά από συνεννόηση με την αρμόδια Επιτροπή, θα προχωρήσει στις απαραίτητες διορθωτικές κινήσεις, οι οποίες θα πρέπει να ολοκληρωθούν μέσα στο χρονικό διάστημα της δοκιμαστικής λειτουργίας.

Σε περίπτωση που κατά την περίοδο της δοκιμαστικής λειτουργίας, εμφανισθούν σοβαρά κατά την κρίση της Επιτροπής Παρακολούθησης Παραλαβής Έργου προβλήματα ή διαπιστωθεί ότι

δεν πληρούνται κάποιες από τις προδιαγραφόμενες απαιτήσεις, διακόπτεται η περίοδος δοκιμαστικής λειτουργίας και καλείται ο Ανάδοχος να αποκαταστήσει το πρόβλημα μέσα στους προβλεπόμενους από τους πίνακες συμμόρφωσης χρόνους.

Ο Ανάδοχος πρέπει να ειδοποιήσει εγγράφως την ΕΠΠΕ ότι αποκατέστησε τη δυσλειτουργία ή βλάβη και τον τρόπο που το πραγματοποίησε. Η αρμόδια επιτροπή μετά από έλεγχο πιστοποιεί την αποκατάσταση της δυσλειτουργίας. Ο χρόνος της δοκιμαστικής λειτουργίας επιμηκύνεται αντίστοιχα για όσο χρόνο μεσολάβησε από την διαπίστωση της βλάβης μέχρι την πιστοποίηση της αποκατάστασής της.

Με την ολοκλήρωση της δοκιμαστικής λειτουργίας και πριν από την οριστική παραλαβή του έργου ο Ανάδοχος είναι υποχρεωμένος να παραδώσει επικαιροποιημένη έκδοση του συνόλου της τεχνικής και λειτουργικής τεκμηρίωσης.

Ελάχιστες Προϋποθέσεις Συμμετοχής

Ο υποψήφιος Ανάδοχος θα πρέπει να διαθέτει τα παρακάτω χαρακτηριστικά:

- εμπειρία στην παροχή συμβουλευτικών υπηρεσιών οργάνωσής και ιδιαίτερα στον τομέα της ασφάλειας πληροφοριών, της επιχειρησιακής συνέχειας και της βελτιστοποίησης επιχειρησιακών διαδικασιών
- Να διαθέτει αποδεδειγμένη αποδεδειγμένη γνώση των νομικών και τεχνικών θεμάτων των προσωπικών δεδομένων και σχετική προϋπηρεσία περιλαμβανομένης τυχόν έργων αξιολόγησης έναντι του κανονισμού GDPR και ιδιαίτερα στον κλάδο υπηρεσιών (2 συναφή έργα).
- Η ομάδα έργου να περιλαμβάνει:
  - συμβούλους οργάνωσης,
  - ειδικούς στην ασφάλεια πληροφοριών
  - εξειδικευμένους νομικούς στην προστασία δεδομένων,
  - και ειδικούς στις τεχνολογικές υποδομές πληροφορικής
  - ειδικούς Ιατρικής Πληροφορικής
  - ειδικού Πληροφορικής

  και οι οποίοι να έχουν εμπλακεί σε ολοκληρωμένα έργα GDPR.
- Να έχει υλοποιήσει σημαντικό αριθμό έργων Διαχείρισης Ασφάλειας Πληροφοριών σύμφωνα με το πρότυπο ISO27001 ή άλλα διεθνή πρότυπα ασφάλειας.
- Να διαθέτει ISO 27001

ΔΙΑΡΚΕΙΑ ΚΑΙ ΠΡΟΥΠΟΛΟΓΙΣΜΟΣ

Το έργο θα έχει διάρκεια 5,5 μήνες από την υπογραφή της σύμβασης και ο προϋπολογισμός ανέρχεται στο ποσό των 350.000€ συμπεριλαμβανομένου του ΦΠΑ