#### ΠΙΝΑΚΕΣ ΣΥΜΜΟΡΦΩΣΗΣ

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ** | | | | | | |
| **1. Αντικείμενο του Έργου** | | | | | | |
| **α/α** | **ΠΡΟΔΙΑΓΡΑΦΕΣ** | | | **ΑΠΑΙΤΗΣΗ** | **ΑΠΑΝΤΗΣΗ** | **ΠΑΡΑΠΟΜΠΗ** |
| **Α** | **Η συμμόρφωση της ΔΕΥΑΠ με τον GDPR** | | | **ΝΑΙ** |  |  |
| **Β** | **Η Κατάρτιση Εσωτερικού Κανονισμού χρήσης και λειτουργίας του εξοπλισμού και του δικτύου πληροφορικής και επικοινωνιών** | | | **ΝΑΙ** |  |  |
| **Γ** | **Υπηρεσίες Υπεύθυνου προστασίας δεδομένων DPO (Data Protection Officer)** | | | **ΝΑΙ** |  |  |
| **2. Υλοποίηση Έργου** | | | | | | |
| **α/α** | **ΠΡΟΔΙΑΓΡΑΦΕΣ** | | | **ΑΠΑΙΤΗΣΗ** | **ΑΠΑΝΤΗΣΗ** | **ΠΑΡΑΠΟΜΠΗ** |
| **2.1** | **Μεθοδολογία Υλοποίησης Έργου**  Υπογραμμίζεται ότι δίδεται ιδιαίτερη βαρύτητα στην προσέγγιση και μεθοδολογία υλοποίησης διότι αυτή αντικατοπτρίζει σε μεγάλο βαθμό τον βαθμό κατανόησης ενός έργου και των ιδιαιτεροτήτων του. Ο Ανάδοχος υποχρεούται να υποβάλλει και περιγράψει τη μεθοδολογία υλοποίησης του έργου. | | | **ΝΑΙ** |  |  |
| **2.2** | **Χρονοδιάγραμμα Υλοποίησης**  Για την εκτέλεση του έργου, ο ανάδοχος θα πρέπει να υποβάλλει αναλυτικό χρονοδιάγραμμα, σύμφωνα με τις παρακάτω φάσεις Υλοποίησης του Έργου. | | | **ΝΑΙ** |  |  |
| **1η φάση** | **Ενημέρωση, Εκπαίδευση & Αρχικός Σχεδιασμός**  **•** Ενημέρωση και συζήτηση με τη διοίκηση και τα στελέχη του οργανισμού που επεξεργάζονται προσωπικά δεδομένα για τα βήματα που θα πρέπει να ακολουθηθούν.  • Ορισμός της ομάδας στελεχών της ΔΕΥΑΠ που θα εμπλακούν στο έργο και των τρόπων και μέσων αλληλεπίδρασης και επικοινωνίας τους με τα μέλη της ομάδας του έργου.  • Αρχική εκπαίδευση των εμπλεκομένων στελεχών και του προσωπικού στο GDPR για την εξοικείωση με τους όρους του Νέου Κανονισμού.  • Διοργάνωση σε συνεργασία με τη ΔΕΥΑΠ ημερίδας ενημέρωσης των εργαζομένων σχετικά με τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR 2016/679), σε Αίθουσα δυναμικότητας άνω των 30 ατόμων σε εγκαταστάσεις μισθωμένες από τον Ανάδοχο στην Πάτρα. | | | **ΝΑΙ** |  |  |
| **2η φάση** | **Αναλυτική καταγραφή και χαρτογράφηση των προσωπικών δεδομένων (Data Mapping)**   * Διάγνωση των υφιστάμενων νομικών, τεχνικών και οργανωτικών μέτρων ασφάλειας και προστασίας των προσωπικών δεδομένων. Εντοπισμός των εμπλεκόμενων στελεχών του οργανισμού που επεξεργάζονται προσωπικά δεδομένα. * Συνεντεύξεις με αρμόδια στελέχη των τμημάτων του οργανισμού θα καταγραφούν οι υφιστάμενες υποδομές και διαδικασίες, θα εντοπιστούν οι πρακτικές, οι πολιτικές και τα μέτρα που εφαρμόζονται κατά το χειρισμό των προσωπικών δεδομένων. * Εντοπισμός των προσωπικών ή και ειδικών (ευαίσθητων) προσωπικών δεδομένων στα συστήματα της ΔΕΥΑΠ (φυσικά αρχεία και πληροφοριακά συστήματα). * Θα καταρτιστεί διάγραμμα ροής διαδικασιών που θα αναπαριστά τη συσχέτιση των διαδικασιών σχετικά με τα προσωπικά δεδομένα. * Σύνταξη αρχείου δραστηριοτήτων (Records of ProcessingActivities) επεξεργασίας προσωπικών δεδομένων σύμφωνα με τις απαιτήσεις του άρθρου 30 και τις δραστηριότητες του οργανισμού. * Έλεγχος της αναγκαιότητας ορισμού Υπεύθυνου Προστασίας Προσωπικών Δεδομένων (DPO).   Στη περίπτωση που απαιτείται ορισμός DPO, θα γίνει έλεγχος αν έχουν δηλωθεί τα στοιχεία επικοινωνίας του στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. | | | **ΝΑΙ** |  |  |
| **3η φάση** | **Μελέτη εκτίμησης αποκλίσεων (GapAnalysis)**  **•** Με βάση τη καταγραφή και τα δεδομένα που θα προκύψουν κατά τη διάρκεια υλοποίησης της 2ηςφάσης θα πραγματοποιηθεί η συσχέτιση με τα επιμέρους άρθρα του GDPR και θα εντοπιστούν και καταγραφούν οι μη συμμορφώσεις με τις πρόνοιες του GDPR, όλων των επιχειρησιακών διαδικασιών, πολιτικών και πρακτικών μέτρων που εφαρμόζει η ΔΕΥΑΠ σχετικά με τα προσωπικά δεδομένα.  • Εντοπισμός μη συμμορφώσεων ως προς τα νομικά, τεχνολογικά μέτρα και μέτρα ασφάλειας των πληροφοριών που εφαρμόζει η ΔΕΥΑΠ σχετικά με τα προσωπικά δεδομένα.  • Καταγραφή και υπόδειξη των μέτρων που πρέπει να ληφθούν ώστε η ΔΕΥΑΠ να συμμορφωθεί με τις απαιτήσεις του GDPR (compliance) από άποψη νομική, ασφάλειας πληροφοριακών συστημάτων και φυσικών αρχείων, όσον αφορά στη χρήση προσωπικών δεδομένων και στη διακίνησή τους εντός ή εκτός του οργανισμού. | | |  |  |  |
| **4η φάση** | **Εκτίμηση επικινδυνότητας φυσικών εγκαταστάσεων, όσον αφορά στην προστασία των προσωπικών δεδομένων, από φυσικά συμβάντα ή απειλές.**  **•** Έλεγχος και καταγραφή της υφιστάμενης κατάστασης και των ελλείψεων του οργανισμού όσο αφορά τη τρωτότητα των φυσικών αρχείων και των πληροφοριακών συστημάτων όπου αποθηκεύονται και επεξεργάζονται τα προσωπικά δεδομένα.  • Υπόδειξη μέτρων ασφαλείας για συμμόρφωση του οργανισμού με το GDPR. | | | **ΝΑΙ** |  |  |
| **5η φάση** | **Μελέτη εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων (Data Protection Impact Assessment)**  • Διενέργεια εκτίμησης αντικτύπου σύμφωνα με τις πρόνοιες του άρθρου 35 του GDPR, στην περίπτωση που ένα είδος από τις χρησιμοποιούμενες τεχνολογίες του οργανισμού εκτιμηθεί ότι ενδέχεται να θέσει σε διακινδύνευση τα δικαιώματα και τις ελευθερίες των υποκειμένων της επεξεργασίας προσωπικών δεδομένων.  • Κατάρτιση κατάλληλων μέτρων και μηχανισμών ασφαλείας που θα πρέπει να υιοθετηθούν ώστε ο Οργανισμός να μπορεί να διαχειριστεί τον πιθανό αντίκτυπο μιας παραβίασης των προσωπικών δεδομένων.  • Διενέργεια διαβούλευσης με την εποπτική αρχή (εφ’ όσον κριθεί αναγκαίο). | | | **ΝΑΙ** |  |  |
| **6η φάση** | **Τελική αναφορά και σχεδιασμός πλάνου ενεργειών και σχεδίου δράσης, προς συμμόρφωση με το GDPR (Compliance Plan)**  • Λίστα αποκλίσεων που θα πρέπει να καλυφθούν.  • Σύνταξη των προτεινόμενων νομικών, οργανωτικών και τεχνολογικών μέτρων που πρέπει να ληφθούν και ενεργειών που πρέπει να ακολουθηθούν για την αντιμετώπιση των μη συμμορφώσεων με το GDPR και προτεινόμενα μέτρα ελέγχου για τον περιορισμό των κινδύνων.  • Σύνταξη τεχνικών μέτρων ελέγχου για τον περιορισμό των κινδύνων παραβίασης της ασφάλειας των πληροφοριακών συστημάτων και των φυσικών αρχείων.  • Παροχή προτάσεων για την υλοποίηση διορθωτικών ενεργειών που αφορούν στις νομικές απαιτήσεις του Κανονισμού αναφορικά με το τρόπου υλοποίηση συγκεκριμένων εργασιών.  • Καθοδήγηση και υποστήριξη για την υλοποίηση τους. | | |  |  |  |
| **7η φάση** | **Παράδοση του ολοκληρωμένου συστήματος συμμόρφωσης του οργανισμού με το GDPR (Data PrivacySystem Management).**  • Συναντήσεις με όλα τα εμπλεκόμενα στελέχη καθώς και την διοίκηση του οργανισμού, όπου θα αναλυθούν εκτενώς τα ευρήματα όλων των φάσεων του έργου συνοδευόμενα από μια έκθεση συμμόρφωσης όλων των δραστηριοτήτων του οργανισμού στις απαιτήσεις του GDPR και την ανασκόπηση όλων των παραδοτέων του έργου.  • Θα ακολουθήσει η εκπαίδευση των εμπλεκομένων στελεχών και του προσωπικού του οργανισμού στο παραδοτέο σύστημα συμμόρφωσης με το GDPR (Δυνατότητα χρηματοδότησης από το ΛΑΕΚ 0,24%). | | | **ΝΑΙ** |  |  |
| **8η φάση** | **Κατάρτιση Εσωτερικού Κανονισμού για την ορθή χρήση και τη λειτουργία του εξοπλισμού και του δικτύου πληροφορικής και επικοινωνιών από τους εργαζόμενους.**   * Συνεργασία με την Ομάδα Εργασίας που θα έχει συστήσει η ΔΕΥΑΠ για την κατάρτιση του συγκεκριμένου Κανονισμού (Συναντήσεις κάθε 2 εβδομάδες στις εγκαταστάσεις της ΔΕΥΑΠ). Τα θέματα που πρέπει να καλύπτει είναι τα ακόλουθα: | | | **ΝΑΙ** |  |  |
| * Διαδικασία χρήσης εξοπλισμού Πληροφορικής και επικοινωνιών | | | **ΝΑΙ** |  |  |
| * Εμπιστευτικότητα λογαριασμών χρηστών | | | **ΝΑΙ** |  |  |
| * Προστασία υπολογιστικού και τηλεπικοινωνιακού εξοπλισμού | | | **ΝΑΙ** |  |  |
| * Δικαιοδοσία και υποχρεώσεις Γραφείου Μηχανοργάνωσης | | | **ΝΑΙ** |  |  |
| * Συμμόρφωση με νομοθεσία για προστασία προσωπικών δεδομένων | | | **ΝΑΙ** |  |  |
| * Οδηγίες χρήσης | | | **ΝΑΙ** |  |  |
| * Παράδοση του Κανονισμού σε κείμενο σε μορφή WORD | | | **ΝΑΙ** |  |  |
| * Διαδικασία χρήσης εξοπλισμού Πληροφορικής και επικοινωνιών | | | **ΝΑΙ** |  |  |
| * Εμπιστευτικότητα λογαριασμών χρηστών | | | **ΝΑΙ** |  |  |
| **Φάσεις** | | **Παρεχόμενες Υπηρεσίες** | **Χρονοδιάγραμμα** | **ΑΠΑΙΤΗΣΗ** | **ΑΠΑΝΤΗΣΗ** | **ΠΑΡΑΠΟΜΠΗ** |
| **1η Φάση** | | Ενημέρωση, εκπαίδευση, σχεδιασμός & χάραξη στρατηγικής | 1η εβδομάδα | **ΝΑΙ** |  |  |
| **2η Φάση** | | Data Mapping | 2η, 3η και 4η εβδομάδα | **ΝΑΙ** |  |  |
| **3η Φάση** | | Gap Analysis | 5η,6η και 7η εβδομάδα | **ΝΑΙ** |  |  |
| **4η Φάση** | | Εκτίμηση επικινδυνότητας φυσικών εγκαταστάσεων | 8η, 9η και 10η εβδομάδα | **ΝΑΙ** |  |  |
| **5η Φάση** | | Data Protection Impact Assessment | 11η, 12η και 13η εβδομάδα | **ΝΑΙ** |  |  |
| **6η Φάση** | | Compliance Plan | 14η, 15η και 16η εβδομάδα | **ΝΑΙ** |  |  |
| **7η Φάση** | | Εκπαίδευση στο σύστημα συμμόρφωσης | 17η εβδομάδα | **ΝΑΙ** |  |  |
| **8η Φάση** | | Υποστήριξη στην εφαρμογή του Data Privacy System Management για τον πρώτο χρόνο | 18η έως 52η εβδομάδα | **ΝΑΙ** |  |  |
| **α/α** | **ΠΡΟΔΙΑΓΡΑΦΕΣ** | | | **ΑΠΑΙΤΗΣΗ** | **ΑΠΑΝΤΗΣΗ** | **ΠΑΡΑΠΟΜΠΗ** |
| **1** | Η συνολική διάρκεια του έργου ορίζεται σε **δώδεκα12μήνες** με ημερομηνία έναρξης την ημερομηνία υπογραφής της σύμβασης. | | | **ΝΑΙ** |  |  |
| **2** | Ο Ανάδοχος καλείται να συμπεριλάβει Χρονοδιάγραμμα Υλοποίησης Έργου στην Τεχνική του Προσφορά, σύμφωνα με τα ανωτέρω. | | | **ΝΑΙ** |  |  |
| **3. Σύνθεση της ομάδας του έργου** | | | | | | |
| **α/α** | **ΠΡΟΔΙΑΓΡΑΦΕΣ** | | | **ΑΠΑΙΤΗΣΗ** | **ΑΠΑΝΤΗΣΗ** | **ΠΑΡΑΠΟΜΠΗ** |
| **1** | Ο υποψήφιος Ανάδοχος υποχρεούται να υποβάλλει στην προσφορά του ολοκληρωμένη πρόταση για το σχήμα διοίκησης, την οργάνωση για την υλοποίηση του έργου και το προσωπικό που θα διαθέσει (ομάδα έργου), με αναλυτική αναφορά του αντικείμενου και του χρόνου απασχόλησης τους στο έργο. | | | **ΝΑΙ** |  |  |
| **2** | Ο Ανάδοχος του έργου θα πρέπει να διαθέτει προσωπικό επαρκές σε πλήθος και δεξιότητες για την εκτέλεση του έργου, με τα εξής χαρακτηριστικά κατ’ελάχιστον: | | | **ΝΑΙ** |  |  |
| **3** | * **1 Επιστημονικό Υπεύθυνο Έργου** με τουλάχιστον 10ετή αποδεδειγμένη επιστημονική και επαγγελματική εμπειρία σε αντικείμενα συναφή με Δίκαιο Πληροφορικής ή Cybercrime ή Cyberlaw ή Ασφάλεια Πληροφοριακών Συστημάτων. | | | **ΝΑΙ** |  |  |
| **4** | * **1 ProjectManager Έργου** – Διπλωματούχο Μηχανικό της ημεδαπής ή ισότιμης Σχολής της Αλλοδαπής, με τουλάχιστον δεκαετή εμπειρία αποδεδειγμένη στη Διοίκηση Projects. | | | **ΝΑΙ** |  |  |
| **5** | * **2 Εξειδικευμένους Νομικούς Συμβούλους** (τουλάχιστον ένας εκ των οποίων θα πρέπει να βρίσκεται ακόμα και σε καθημερινή βάση, στη διάθεση της ΔΕΥΑΠ, προκειμένου για την εντός χρονοδιαγράμματος διεκπεραίωση του εν λόγω έργου) **–** Αποδεδειγμένα Εξειδικευμένους στην Ασφάλεια πληροφοριακών Συστημάτων ή Πιστοποιημένους Υπεύθυνους Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Cert. Data Protection Officers - DPO) | | | **ΝΑΙ** |  |  |
| **6** | * **2 Εξειδικευμένους ΙΤ Experts -** (**τουλάχιστον ένας εκ των οποίων** θα πρέπει να **βρίσκεται ακόμα και σε καθημερινή βάση**, στη διάθεση της ΔΕΥΑΠ, προκειμένου για την εντός χρονοδιαγράμματος διεκπεραίωση του εν λόγω έργου) | | | **ΝΑΙ** |  |  |
| **7** | * **Ο Υπεύθυνος προστασίας δεδομένων DPO (Data Protection Officer),** ορίζεται με ευθύνη του αναδόχου φυσικό πρόσωπο **(απαραίτητα ένας εκ των ανωτέρω)** που θα διαθέτει την σχετική εκπαίδευση και Πιστοποίηση, ως Υπεύθυνος Προστασίας Δεδομένων της ΔΕΥΑ ΠΑΤΡΑΣ. | | | **ΝΑΙ** |  |  |
| **8** | Στις αρμοδιότητές του θα είναι η εκτέλεση όλων των καθηκόντων του DPO σε όλο το χωρικό εύρος ανάπτυξης των υπηρεσιών της ΔΕΥΑΠ. **Είναι επιβεβλημένο να:** | | | **ΝΑΙ** |  |  |
| **9** | * + είναι **προσβάσιμος** από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, αλλά και από τα υποκείμενα των δεδομένων 24/365. | | | **ΝΑΙ** |  |  |
| **10** | * + **συνεργάζεται** **άμεσα** με τον οριζόμενο από την ΔΕΥΑΠ DPO - Data Protection Officer (ο οποίος θα διαθέτει την σχετική Πιστοποίηση ως DPO). | | | **ΝΑΙ** |  |  |
| **11** | * + παραδίδει στον οριζόμενο DPO υπάλληλο από την ΔΕΥΑΠ οποιοδήποτε υλικό χρησιμοποιείται για την υλοποίηση της υπηρεσίας του σε επεξεργάσιμη ηλεκτρονική μορφή καθ’ όλη την διάρκεια της σύμβασης | | | **ΝΑΙ** |  |  |
| **12** | * + παρέχονται από τον ανάδοχο οι υπηρεσίες του DPO από την ημερομηνία υπογραφής της σύμβασης και για διάστημα 12 μηνών. | | | **ΝΑΙ** |  |  |
| **13** | Για κάθε μέλος της ομάδας του έργου θα παρατίθεται αναλυτικό βιογραφικό σημείωμα και τα ανάλογα αποδεικτικά εμπειρίας. | | | **ΝΑΙ** |  |  |
| **ΟΛΕΣ ΟΙ ΠΡΟΣΦΕΡΟΜΕΝΕΣ ΥΠΗΡΕΣΙΕΣ ΝΑ ΑΝΑΛΥΟΝΤΑΙ ΜΕ ΣΑΦΕΙΣ ΠΑΡΑΠΟΜΕΣ ΚΑΙ ΝΑ ΑΝΑΦΕΡΟΝΤΑΙ ΣΕ ΣΥΓΚΕΚΡΙΜΕΝΕΣ ΣΕΛΙΔΕΣ ΚΑΙ ΠΑΡΑΓΡΑΦΟΥΣ Ή ΑΛΛΟ ΣΥΓΚΕΚΡΙΜΕΝΟ ΣΗΜΕΙΟ ΤΗΣ ΠΡΟΣΦΟΡΑΣ ΤΟΥΣ.**  **ΣΕ ΚΑΘΕ ΑΠΑΝΤΗΣΗ ΤΟΥ ΑΝΑΔΟΥΧΟΥ ΝΑ ΥΠΑΡΧΕΙ ΚΑΙ ΠΑΡΑΠΟΜΠΗ ΤΗΣ.** | | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ΒΙΟΓΡΑΦΙΚΟ ΣΗΜΕΙΩΜΑ** | | | | | | | | | | | |
|  | | | | | | | | | | | |
| **ΠΡΟΣΩΠΙΚΑ ΣΤΟΙΧΕΙΑ** | | | | | | | | | | | |
| Επώνυμο: |  | | | | | | Όνομα: |  | | | |
| Πατρώνυμο: |  | | | | | | Μητρώνυμο: |  | | | |
| Ημερομηνία Γέννησης: | \_\_ /\_\_ / \_\_\_\_ | | | | | | Τόπος Γέννησης: |  | | | |
| Τηλέφωνο: |  | | | | | | E-mail: |  | | | |
| Fax: |  | | | | | |  |
| Διεύθυνση Κατοικίας: | |  | | | | | | | | | |
|  | | | | | | | | | | | |
| **ΕΚΠΑΙΔΕΥΣΗ** | | | | | | | | | | | |
| Όνομα Ιδρύματος | | | Τίτλος Πτυχίου | | | Ειδικότητα | | | | Ημερομηνία Απόκτησης Πτυχίου | |
|  | | |  | | |  | | | |  | |
|  | | |  | | |  | | | |  | |
|  | | |  | | |  | | | |  | |
|  | | |  | | |  | | | |  | |
|  | | |  | | |  | | | |  | |
| **ΚΑΤΗΓΟΡΙΑ ΣΤΕΛΕΧΟΥΣ**  (στο προτεινόμενο, από τον υποψήφιο Ανάδοχο, σχήμα διοίκησης Έργου) | | | |  | | | | | | | |
| **ΕΠΑΓΓΕΛΜΑΤΙΚΗ ΕΜΠΕΙΡΙΑ** | | | | | | | | | | | |
| **Έργο** | **Εργοδότης** | | | | **Θέση και Καθήκοντα στο Έργο** | | | | **Απασχόληση στο Έργο** | |
| **Περίοδος**  (από **-** έως)  **Α/Μ** | |
|  |  | | | |  | | | | \_\_ /\_\_ / \_\_\_  \_\_ /\_\_ / \_\_\_ | |
|  |  | | | |  | | | | \_\_ /\_\_ / \_\_\_  \_\_ /\_\_ / \_\_\_ | |
|  |  | | | |  | | | | \_\_ /\_\_ / \_\_\_  \_\_ /\_\_ / \_\_\_ | |
|  |  | | | |  | | | | \_\_ /\_\_ / \_\_\_  \_\_ /\_\_ / \_\_\_ | |
|  |  | | | |  | | | | \_\_ /\_\_ / \_\_\_  \_\_ /\_\_ / \_\_\_ | |
|  |  | | | |  | | | | \_\_ /\_\_ / \_\_\_  \_\_ /\_\_ / \_\_\_ | |
|  |  | | | |  | | | | \_\_ /\_\_ / \_\_\_  \_\_ /\_\_ / \_\_\_ | |
|  |  | | | |  | | | | \_\_ /\_\_ / \_\_\_  \_\_ /\_\_ / \_\_\_ | |
|  |  | | | |  | | | | \_\_ /\_\_ / \_\_\_  \_\_ /\_\_ / \_\_\_ | |