ΚΑΛΑΜΑΤΑ 18/6/2018

ΔΗΜΟΤΙΚΗ ΕΠΙΧΕΙΡΗΣΗ

ΥΔΡΕΥΣΗΣ -ΑΠΟΧΕΤΕΥΣΗΣ

ΚΑΛΑΜΑΤΑΣ

ΠΡΟΔΙΑΓΡΑΦΕΣ ΣΥΝΤΑΞΗΣ ΜΕΛΕΤΗΣ

«ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΣΥΜΜΟΡΦΩΣΗΣ ΤΗΣ ΔΕΥΑΚ ΜΕ ΤΟΝ ΝΕΟ ΕΥΡΩΠΑΪΚΟ ΚΑΝΟΝΙΣΜΟ (GDPR) ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΦΥΣΙΚΩΝ ΠΡΟΣΩΠΩΝ ΕΝΑΝΤΙ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΚΑΙ ΥΠΗΡΕΣΙΕΣ DPO ΜΕΧΡΙ ΤΗΝ ΟΛΟΚΛΗΡΩΣΗ ΤΗΣ ΣΥΜΜΟΡΦΩΣΗΣ»
Προυπολογισμού 10.000 Euro

Οι παραπάνω τιμές ΔΕΝ συμπεριλαμβάνουν ΦΠΑ

ΠΕΡΙΕΧΟΜΕΝΑ

ΤΕΧΝΙΚΗ ΕΚΘΕΣΗ

1. ΠΕΡΙΓΡΑΦΗ

Από την **25η Μαΐου 2018** τίθεται σε εφαρμογή ο Ευρωπαϊκός Κανονισμός 2016/679 (GDPR - General Data Protection Regulation) που αφορά την Προστασία των Προσωπικών Δεδομένων (ισχύει σε όλα τα κράτη – μέλη της Ε.Ε.) και αφορά όλες τις Επιχειρήσεις και τους Οργανισμούς. Η μη συμμόρφωση με τις απαιτήσεις του κανονισμού επιφέρει πρόστιμα έως το 4% του Κύκλου Εργασιών ή 20.000.000 € (όποιο είναι μεγαλύτερο) πέρα από τις νομικές κυρώσεις του ισχύοντος Νόμου.

Η σημαντικότητα της συμμόρφωσης με τον κανονισμό, εκτός από την αποφυγή των πολύ υψηλών προστίμων και αποζημιώσεων, έγκειται και στη διατήρηση της εικόνας υψηλής ποιότητας και εμπιστοσύνης της υπηρεσίας.

Αντικείμενο της μελέτης θα είναι:

Η παροχή συμβουλευτικής υποστήριξης προς την ΔΕΥΑΚ για την «**Ανάπτυξη Ολοκληρωμένου Συστήματος Συμμόρφωσης με τον κανονισμό (ΕΕ) 2016/679 (GDPR) για την προστασία των Προσωπικών Δεδομένων»** .

Το όλο έργο πού θα υλοποιηθεί θα πρέπει να λάβει υπ' όψιν και τις τρεις πτυχές του κανονισμού, την **Τεχνική**, τη **Νομική** και την **Οργανωτική**.

Αντικείμενο των υπηρεσιών DPO θα είναι:

Η παροχή υπηρεσιών DPO, σύμφωνα με τις απαιτήσεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ στο εφεξής) , από εξειδικευμένο

επιστήμονα του αναδόχου, προς την ΔΕΥΑΚ για την έναρξη, εφαρμογή και λειτουργία για ένα έτος του υπό «**Ανάπτυξη Ολοκληρωμένου Συστήματος Συμμόρφωσης με τον κανονισμό (ΕΕ) 2016/679 (GDPR) για την προστασία των Προσωπικών Δεδομένων».**

Ως προς την μεθοδολογία της υλοποίησης του έργου καθώς και τις ποιοτικής του διασφάλισης , οι απαιτήσεις της ΔΕΥΑΚ, από τον ανάδοχο του έργου είναι:

1. Η ενημέρωση & ευαισθητοποίηση και συγκρότηση ομάδας εργασίας, πού θα έχει ως αντικείμενο:

Α) Την σύνταξη ενημερωτικού προγράμματος προς τα αρμόδια στελέχη της επιχείρησης που εμπλέκονται στη διαχείριση προσωπικών δεδομένων, για τις αρχές προστασίας προσωπικών δεδομένων GDPR.

Β) Την παρουσίαση του έργου, της μεθοδολογίας και ανάλυση των ενεργειών που απαιτούνται από πλευράς των τμημάτων της επιχείρησης.

Γ) Την εκπαίδευση των στελεχών της επιχείρησης που θα συμμετέχουν στην ομάδα έργου.

2. Η συγκέντρωση δεδομένων και αξιολόγηση του υφιστάμενου επιπέδου συμμόρφωσης της επιχείρησης

Η συγκέντρωση των δεδομένων θα γίνει με βάση ειδικές φόρμες, ερωτηματολόγια και checklists αλλά και με προσωπικές συναντήσεις με στελέχη της υπηρεσίας, πού θα αποσκοπούν, στην ανασκόπηση αιτήσεων, προσφορών, συμβολαίων, λογισμικών κλπ, προκειμένου να εντοπισθούν τα προσωπικά δεδομένα τα οποία χειρίζεται η ΔΕΥΑΚ. Αποτύπωση της ροής των προσωπικών δεδομένων (data flows) και των υφιστάμενων τεχνικών και οργανωτικών μέτρων ασφάλειας, ώστε να γίνει και η εκτίμηση αντικτύπου σχετικά με την προστασία των προσωπικών δεδομένων.

3. Ο Εντοπισμός και η αξιολόγηση των αποκλίσεων **(Gap analysis)** ανάμεσα στις υφιστάμενες πρακτικές χειρισμού των προσωπικών δεδομένων και στις απαιτήσεις του κανονισμού και της σχετικής νομοθεσίας.

4. Την σύνταξη πλάνου συμμόρφωσης (Compliance Plan)

Θα περιλαμβάνει όλες τις απαιτούμενες ενέργειες, προτεραιοποιημένες, κατηγοριοποιημένες και συμφωνημένες με τα στελέχη κάθε τμήματος, ώστε να επιτευχθεί η συμμόρφωση με τον GDPR με τον πλέον έξυπνο και οικονομικό τρόπο. Περιλαμβάνεται και ο σχεδιασμός της ασφάλειας του πληροφοριακού εξοπλισμού και χρησιμοποιούμενων εφαρμογών. Με την ολοκλήρωση θα δοθούν προς τους προμηθευτές του λογισμικού που χρησιμοποιεί η υπηρεσία εκθέσεις για τις τροποποιήσεις που απαιτούνται για τη συμμόρφωση με τον GDPR.

5. Την σύνταξη των εγγράφων τεκμηρίωσης
Σύνταξη όλων των απαιτούμενων εγγράφων τεκμηρίωσης όπως εγχειρίδιο ασφάλειας δεδομένων, πολιτική προστασίας προσωπικών δεδομένων διαδικασίες, οδηγίες εργασίας, υποδείγματα συμβάσεων, υποδείγματα δηλώσεων συγκατάθεσης και ενημέρωσης των υποκειμένων κ.λ.π. Τέλος θα πρέπει να συνταχθεί ειδική έκθεση συμμόρφωσης της υπηρεσίας στον Κανονισμό GDPR.

6 Η Εκπαίδευση στελεχών και του DPO με υλοποίηση εκπαιδευτικού προγράμματος για το σύστημα ασφάλειας προσωπικών δεδομένων της υπηρεσίας, που θα απευθύνεται στα στελέχη των τμημάτων που εμπλέκονται στο χειρισμό προσωπικών δεδομένων. Θα πρέπει να περιλαμβάνει παρουσίαση του συστήματος ασφάλειας δεδομένων, των εγγράφων τεκμηρίωσης και θα αναλυθούν οι ενέργειες που απαιτούνται για την τήρηση του συστήματος. Επιπλέον εκπαίδευση τουλάχιστον εικοσιτεσσάρων (24) ωρών προς τον Υπεύθυνο επεξεργασίας δεδομένων και τον DPO της υπηρεσίας με έμφαση στις αρμοδιότητες και στον τρόπο εργασίας. Όλο το εκπαιδευτικό υλικό να παραδοθεί και σε ηλεκτρονική μορφή.

Ο συμβατικός χρόνος υλοποίησης των περιγραφόμενων υπηρεσιών από 1-6 είναι 6 μήνες από την υπογραφή της σύμβασης.

7. Η παροχή υπηρεσιών DPO για ένα έτος με δυνατότητα επέκτασης στα δύο (2) έτη. Το στέλεχος του αναδόχου που οριστεί DPO θα πρέπει να είναι εξειδικευμένος και να διαθέτει εμπειρία στο ρόλο αυτό. Θα πρέπει να κάνει κατ΄ελάχιστο έξι (6) επισκέψεις το έτος στη Δ.Ε.Υ.Α.Κ. για τη συνεργασία και την επίλυση θεμάτων σχετικά με το GDPR, με τα αρμόδια στελέχη της υπηρεσίας και τον Υπεύθυνο Επεξεργασίας Δεδομένων. Τα προαναφερόμενα καθήκοντά του είναι επιπρόσθετα σε αυτά που απαιτεί η ΑΠΔΠΧ .

8. Απαιτούμενα ποιοτικά κριτήρια Αναδόχου

Α. Να διαθέτει εμπειρία στην εκτέλεση έργων στον τομέα ασφάλειας πληροφοριών και προστασίας προσωπικών δεδομένων που να αποδεικνύεται από την συμμετοχή σε τουλάχιστον δύο (2) έργα παροχής υπηρεσιών για προσαρμογή στον GDPR

Β. Να φροντίσει ώστε να οριστεί μέλος της Ομάδας Έργου σε ρόλο Υπευθύνου Έργου (Project Manager), ο οποίος να διαθέτει εμπειρία στον τομέα προστασίας προσωπικών δεδομένων που αποδεικνύεται από τη συμμετοχή του ως υπευθύνου στην υλοποίηση τουλάχιστον ενός (1) έργου προσαρμογής στον GDPR, ο οποίος θα πρέπει να διαθέτει και Πιστοποιητικό Συμμόρφωσης σύμφωνα με το Πρότυπο ISO/IEC 17024.

Γ. Να διατεθεί Ομάδα Έργου που να απαρτίζεται κατ' ελάχιστο από δύο (2) μέλη (εκτός από τον Υπεύθυνο Έργου).

Ο μειοδότης θα πρέπει να προσκομίσει, προς απόδειξη της μη συνδρομής των λόγων αποκλεισμού από διαδικασίες σύναψης δημοσίων συμβάσεων των παρ 1 και του 2 του άρθρου 73 Ν.4412/2016, τα παρακάτω δικαιολογητικά.
Α. Απόσπασμα ποινικού μητρώου. Η υποχρέωση αφορά ιδίως αα) στις περιπτώσεις εταιριών περιορισμένης ευθύνης (Ε.Π.Ε), Ι.Κ.Ε και προσωπικών εταιριών (Ο.Ε. και Ε.Ε.), τους διαχειριστές, ββ) στις περιπτώσεις ανώνυμων εταιριών (Α.Ε.) , τον Διευθύνοντα Σύμβουλο, καθώς και όλα τα μέλη του Δ.Σ.
Β. Φορολογική ενημερότητα.
Γ. Ασφαλιστική ενημερότητα (άρθρο 80 παρ. 2 του Ν.4412/2016
Δ. Τα αποδεικτικά έγγραφα νομιμοποίησης της εταιρείας, δηλαδή νομιμοποιητικά έγγραφα σύστασης και τελευταίας τροποποίησης από τα οποία προκύπτει η τρέχουσα σύνθεση του Δ.Σ για τις Α.Ε η οι διαχειριστές για τις Ε.Π.Ε., Ι.Κ.Ε., Ο.Ε η Ε.Ε και η νόμιμη εκπροσώπηση της εταιρείας. ΄Όλα τα παραπάνω θα πρέπει να αποδεικνύονται από επίσημα έγραφα τα οποία μπορούν να είναι φωτοαντίγραφα αλλά οποιαδήποτε στιγμή θα μπορούν να ζητηθούν επικυρωμένα αντίγραφα ή τα πρωτότυπα, επί ποινή αποκλεισμού εάν δεν προσκομισθούν εντός οκτώ (8) εργασίμων ημερών

Οι τιμές για την μελέτη και για τις υπηρεσίες DPO θα είναι διακριτές διότι θα είναι στην ευχέρεια της υπηρεσίας μας αν τελικά θα ληφθούν οι υπηρεσίες DPO.

ΠΑΝΑΓΙΩΤΗΣ ΚΟΥΦΑΛΑΚΟΣ
ΠΡΟΙΣΤΑΜΕΝΟΣ ΟΙΚΟΝΟΜΙΚΗΣ ΚΑΙ ΔΙΟΙΚΗΤΙΚΗΣ ΥΠΗΡΕΣΙΑΣ