ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΝΟΜΟΣ ΜΕΣΣΗΝΙΑΣ
ΔΗΜΟΣ ΚΑΛΑΜΑΤΑΣ
ΔΙΕΥΘΥΝΣΗ ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ,
ΑΝΑΠΤΥΞΗΣ & ΕΥΡΩΠΑΪΚΩΝ ΘΕΜΑΤΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

ΜΕΛΕΤΗ α.α 9/2018

Κ.Α.: 70.01.7425.14

ΕΡΓΟ: Παροχή υπηρεσιών για την εφαρμογή του Γενικού Κανονισμού για την Προστασία των Προσωπικών Δεδομένων (General Data Protection Regulation)

ΠΡΟΫΠΟΛΟΓΙΣΜΟΣ: 23.994,00 € με Φ.Π.Α.

CPV: 79417000-0

ΠΕΡΙΕΧΟΜΕΝΑ:

ΚΑΛΑΜΑΤΑ ΙΟΥΛΙΟΣ 2018

1 ΤΕΧΝΙΚΗ ΕΚΘΕΣΗ – ΣΥΓΓΡΑΦΗ ΥΠΟΧΡΕΩΣΕΩΝ

1.1 Γενικά

Με την παρούσα έκθεση, προϋπολογισμού δαπάνης 23.994,00 € συμπεριλαμβανομένου του Φ.Π.Α, περιγράφονται οι εργασίες για την παροχή υπηρεσιών για την εφαρμογή του Γενικού Κανονισμού για την Προστασία των Προσωπικών Δεδομένων (General Data Protection Regulation) 679/2016 στο Δήμο Καλαμάτας. Στις υπηρεσίες αυτές συμπεριλαμβάνεται και η παροχή υπηρεσιών Υπευθύνου Προστασίας Δεδομένων(DPO).

Η δαπάνη θα βαρύνει τις Δημοτικές πιστώσεις του οικονομικού έτους 2018.

Η ανάθεση της εργασίας θα γίνει σύμφωνα με τις διατάξεις του Ν. 4412/16.

1.2 Αντικείμενο

Ο νέος Ευρωπαϊκός Κανονισμός Προστασίας Προσωπικών Δεδομένων (General Data Protection Regulation) 679/2016, που στη συνέχεια του παρόντος αναφέρεται ως GDPR ή Κανονισμός, ψηφίστηκε το 2016, και ισχύει καθολικά, υποχρεωτικά και άμεσα από την 25/05/2018.

Ο Κανονισμός έχει σχεδιαστεί κατά τέτοιο τρόπο ώστε να δώσει στους πολίτες μεγαλύτερο έλεγχο των προσωπικών τους στοιχείων στα πλαίσια του νέου «ψηφιακού κόσμου» και αφορά σε κάθε είδους επεξεργασία προσωπικών δεδομένων, αυτοματοποιημένη ή μη. Για το σκοπό αυτό, εισάγει μια σειρά διαδικασιών και υποχρεώσεων, για τους υπεύθυνους επεξεργασίας, η παραβίαση των οποίων μπορεί να προκαλέσει την επιβολή ιδιαίτερα υψηλών προστίμων.

Η υποχρεωτικότητα για τους φορείς του δημοσίου, βάσει του Κανονισμού (άρθρο 5, παράγραφος 2), είναι ρητή και αδιαπραγμάτευτη. Το άρθρο 24 καθορίζει τον τρόπο με τον οποίο οι οργανισμοί μπορούν να επιτύχουν τη συμμόρφωσή τους απαιτώντας την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων. Οι οργανισμοί οφείλουν να μπορούν να αποδείξουν ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα πραγματοποιείται σύμφωνα με τον Κανονισμό.

Τα βασικά στοιχεία του Κανονισμού που έχουν εφαρμογή στο Δήμο Καλαμάτας, είναι πολύ επιγραμματικά είναι τα εξής:

- Ιδιαίτερα αυξημένη υποχρέωση για Διαφάνεια στη διαχείριση προσωπικών δεδομένων
- Αυξημένη υποχρέωση για σαφή συγκατάθεση του υποκειμένου των δεδομένων
- Υποχρέωση γνωστοποίησης παραβιάσεων ασφάλειας
- Ιδιαίτερα αυστηρά πρόστιμα για παραβιάσεις του Κανονισμού
- Υποχρέωση ορισμού Υπεύθυνου Προστασίας Δεδομένων (Data Protection Officer - DPO)
- Υποχρέωση εκπόνησης Εκτίμησης Επιπτώσεων Προστασίας Δεδομένων
- Υποχρέωση τήρησης αρχείων δραστηριοτήτων επεξεργασίας
- Ειδικοί κανόνες για διασυνοριακή διαβίβαση δεδομένων
- Δικαίωμα στην λήθη για τα υποκείμενα των δεδομένων
- Υποχρέωση τήρησης σε συνεχή βάση από το Δήμο, όλων των αρχών νόμιμης επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που επιβάλλονται από τον Κανονισμό και το συναφές νομικό πλαίσιο
- Υποχρέωση του Δήμου να μπορεί να τεκμηριώσει τη συμμόρφωσή του με τις αρχές του κανονιστικού πλαισίου (αρχή της Λογοδοσίας)

Η συμμόρφωση με τον κανονισμό είναι μια σύνθετη διαδικασία που προϋποθέτει εξειδικευμένες γνώσεις και εκπαίδευση στη σχετική νομοθεσία, ώστε να είναι δυνατή η αποτίμηση της υφιστάμενης κατάστασης του Δήμου, ο εντοπισμός των αποκλίσεων και των κινδύνων και η διατύπωση των απαραίτητων ενεργειών για να επιτευχθεί η συμμόρφωση.

Ιδιαίτερα ως προς αυτό, πρέπει ενδεικτικά να αναφέρουμε ότι ο Δήμος Καλαμάτας, ως Οργανισμός Τοπικής Αυτοδιοίκησης, επεξεργάζεται δεδομένα που αφορούν στοιχεία υπαλλήλων, πολιτών, πελατών, προμηθευτών, ανηλίκων, κ.α. Επίσης, παρέχει πλήθος υπηρεσιών που απαιτούν επεξεργασία τόσο απλών όσο και ευαίσθητων προσωπικών δεδομένων (δημοτολόγιο, ληξιαρχείο, ΚΕΠ, ΚΑΠΗ, μονάδες μέριμνας, παιδικοί σταθμούς, κοινωνικό παντοπωλείο, ηλεκτρονικές υπηρεσίες), έχει υποχρεώσεις επεξεργασίας, κοινοποίησης και γνωστοποίησης που επιβάλλονται από το νόμο (Δι@ύγεια, μισθοδοσίες, εισαγγελικές παραγγελίες διαβιβάσεις εγγράφων), ενώ συχνά συνεργάζεται με τρίτα μέρη και αναθέτει σε αυτά μέρος των υπηρεσιών του.

Για τους παραπάνω λόγους και λόγω έλλειψης της απαραίτητης γνώσης και τεχνογνωσίας από το προσωπικό του Δήμου, καθίσταται απαραίτητη η παροχή υπηρεσιών τεχνικής υποστήριξης από εξωτερικό ανάδοχο, με στελέχη εκπαιδευμένα στις απαραίτητες διαδικασίες και τη σχετική νομοθεσία, ώστε να σχεδιάσει ένα πρόγραμμα συμμόρφωσης με το νέο Γενικό Κανονισμό Προστασίας Δεδομένων.

Η συμμόρφωση με τα προβλεπόμενα στο νέο Κανονισμό είναι το αντικείμενο αυτής της μελέτης.

Οι ενότητες των εργασιών που πρέπει να καλυφθούν φαίνονται παρακάτω. Πέραν όμως αυτών, ο ανάδοχος θα πρέπει να εκτελέσει και κάθε άλλη απαραίτητη, κατά την κρίση του Δήμου Καλαμάτας, συμβουλευτική υπηρεσία, προκειμένου ο Δήμος να εφαρμόσει με επιτυχία τον Γενικό Ευρωπαϊκό Κανονισμό Προστασίας Δεδομένων (GDPR), ακόμη και αν αυτή δεν αναφέρεται ρητά στην παρούσα. Δηλαδή, το αντικείμενο περιλαμβάνει την ουσιαστική καθοδήγηση του Δήμου Καλαμάτας στην ολοκληρωμένη εφαρμογή του Κανονισμού.

1.3 Ενότητες Εργασιών

1.3.1 Διαχείριση ενεργειών (Project Management)

Ο ανάδοχος θα αναλάβει τη διαχείριση των ενεργειών (Project Management) που απαιτούνται στο πλαίσιο υλοποίησης του έργου.

1.3.2 Ενημέρωση / Εκπαίδευση Στελεχών του Δήμου

Ενημέρωση της Διοίκησης σχετικά με τους στόχους του προγράμματος συμμόρφωσης, τη μεθοδολογία που θα ακολουθηθεί και τα εργαλεία που θα χρησιμοποιηθούν.

Εκπαίδευση των στελεχών του Δήμου στον Κανονισμό (GDPR) και στις απαιτήσεις του.

Τα στελέχη θα εκπαιδευτούν κατά ομάδες. Κατ' ελάχιστο θα γίνουν 4 τρίωρες εκπαιδεύσεις στελεχών.

Οι ενότητες εκπαίδευσης των στελεχών θα περιλαμβάνουν τα παρακάτω:

1. Εισαγωγή - Βασικές Ανάγκες & Αιτίες
2. Ευρωπαϊκός Γενικός Κανονισμός ΠΔ
3. Σύστημα Προστασίας Δεδομένων
4. Προετοιμασία Προστασίας Δεδομένων
5. Οργάνωση Προστασίας Δεδομένων
6. Εφαρμογή Μέτρων Προστασίας Δεδομένων
7. Διαχείριση Προστασίας Δεδομένων
8. Βελτίωση Προστασίας Δεδομένων

<u>Παραδοτέα:</u>

- Παρουσιολόγια εκπαίδευσης και ενημερωτικό υλικό.

1.3.3 Εκτίμηση τρέχουσας κατάστασης - αναγνώριση και καταγραφή δεδομένων

Θα καταγραφούν αναλυτικά, θα αξιολογηθούν και θα κατηγοριοποιηθούν τα δεδομένα προσωπικού χαρακτήρα και η κρισιμότητά τους σε όλο το φάσμα των λειτουργιών του Δήμου και σε όλα τα εμπλεκόμενα τμήματα.

Συγχρόνως, θα πρέπει να καταγραφούν οι χώροι και τα μέσα στα οποία διατηρούνται τα δεδομένα αυτά.

1.3.3.1 Δημιουργία λεπτομερών data flow maps

Ο ανάδοχος, σε συνεργασία με το προσωπικό του Δήμου, θα κάνει τη χαρτογράφηση των προσωπικών δεδομένων στο Δήμο και θα δημιουργήσει τα απαραίτητα αρχεία που θα πρέπει να έχει στην κατοχή του και να μπορεί να επιδεικνύει ο Δήμος.

Η χαρτογράφηση της ροής των προσωπικών δεδομένων (data flow maps) θα γίνει ανά τμήμα ή και ανά κατηγορία προσωπικών δεδομένων, όπου θα απεικονίζονται όλες οι πληροφορίες σχετικά με τη διαχείριση των προσωπικών δεδομένων στο Δήμο.

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.

Ενδεικτικά αναφέρονται:

- Κατάλογος δεδομένων προσωπικού χαρακτήρα (ποια προσωπικά δεδομένα συλλέγονται, ο σκοπός επεξεργασίας, η διαδικασία λήψης συγκατάθεσης, η πρόσβαση στα δεδομένα - εντός και εκτός του οργανισμού - η έγγραφη και/ή ηλεκτρονική αποθήκευσή τους, ο χρόνος διατήρησης)
- Ταξινόμηση των προσωπικών δεδομένων που έχει στην κατοχή του ο Δήμος ανά τύπο (π.χ. ευαίσθητα, εμπιστευτικά, δημόσια),
- Διατήρηση διαγραμμάτων ροής για ροές δεδομένων (π.χ. μεταξύ συστημάτων, μεταξύ διαδικασιών, μεταξύ χωρών),

Παραδοτέα:

- Μητρώο Επεξεργασιών Προσωπικών Δεδομένων

1.3.3.2 Αξιολόγηση (audit) Υποδομών & Διαδικασιών

Θα γίνει μια λεπτομερής αξιολόγηση του παρόντος επιπέδου ετοιμότητας των διαδικασιών και υποδομών ασφάλειας για τα δεδομένα προσωπικού χαρακτήρα που διατηρεί ο Δήμος, ώστε να εντοπιστούν σημεία μη συμμόρφωσης.

Η αξιολόγηση αυτή θα περιλαμβάνει και αξιολόγηση αδυναμιών (vulnerability assessment) στις πληροφοριακές υποδομές του Δήμου με χρήση εξειδικευμένου λογισμικού και προσωπικού.

Παραδοτέα:

- Ανάλυση – αξιολόγηση υφιστάμενης κατάστασης (πρακτικών, πολιτικών και διαδικασιών) που θα περιλαμβάνει και αναφορά ελέγχου πληροφοριακών συστημάτων (IT Audit Report)

1.3.3.3 Καθορισμός Νομικής Βάσης της Επεξεργασίας

Προσδιορισμός της Νομικής Βάσης στην οποία στηρίζεται η επεξεργασία των προσωπικών δεδομένων και εξέταση της πληρότητας και ορθότητάς της.

Παραδοτέα:

- Κείμενα Θεμελίωσης Νομικής Βάσης Επεξεργασίας

1.3.3.4 Μελέτη ανάλυσης αποκλίσεων

Θα πρέπει να γίνει ανάλυση των αποκλίσεων που εντοπίστηκαν κατά το χειρισμό προσωπικών δεδομένων από τοπ Δήμο, τόσο ως προς τις απαιτήσεις του Κανονισμού και του

συναφούς κανονιστικού πλαισίου όσο και ως προς τις σχετικές οδηγίες, κατευθύνσεις και αποφάσεις των Ευρωπαϊκών και Εθνικών Αρχών Προστασίας Δεδομένων.

Παραδοτέα:

- Ανάλυση αποκλίσεων

1.3.4 Εκτίμηση Αντικτύπου Προστασίας Δεδομένων

Ο ανάδοχος θα διεξάγει ανάλυση - μελέτη εκτίμησης αντικτύπου σχετικά με την προστασία των προσωπικών δεδομένων (data protection impact assessment-DPIA), η οποία θα περιλαμβάνει τουλάχιστον τα παρακάτω:

α) Συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας, της φύσης, της έκτασης και των σκοπών της επεξεργασίας, περιλαμβανομένου, κατά περίπτωση, και του έννομου συμφέροντος που επιδιώκει ο Δήμος

β) Την εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς, καθώς και τα προτεινόμενα μέτρα συμμόρφωσης

γ) Την εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων (υποκειμένων των δεδομένων).

δ) Τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας, ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα και να αποδεικνύεται η συμμόρφωση προς τον Κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερόμενων προσώπων

Η ανάλυση και αξιολόγηση των κινδύνων θα γίνει με χρήση διεθνώς αποδεκτής μεθοδολογίας, για την αξιολόγηση των παραγόντων που απειλούν τα Δεδομένα Προσωπικού Χαρακτήρα που κατέχει ο Δήμος. Η μεθοδολογία που θα ακολουθηθεί πρέπει να καλύπτει πλήρως τις απαιτήσεις του Νομικού και κανονιστικού πλαισίου και να λαμβάνει υπ’ όψιν τους εξής σημαντικούς παράγοντες:

α) Την πιθανότητα να εμφανιστεί μια συγκεκριμένη επικίνδυνη κατάσταση.

β) Τις επιπτώσεις που θα έχει στην εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα του υπό εξέταση στοιχείου.

ε) Την ευπάθεια που εμφανίζει το κάθε Δεδομένο Προσωπικού Χαρακτήρα σε σχέση με τον κίνδυνο που το απειλεί.

Με βάση τα επίπεδα επικινδυνότητας που θα προσδιοριστούν και τα αποτελέσματα της ανωτέρω αξιολόγησης, θα προσδιοριστούν οι κατάλληλες ενέργειες διαχείρισης και οι προτεραιότητες για τη διαχείριση της επικινδυνότητας των Δεδομένων Προσωπικού Χαρακτήρα. Οι επιλογές που ακολουθούνται είναι οι ακόλουθες:

- Εφαρμογή κατάλληλων ελέγχων για τον περιορισμό των κινδύνων.
- Αποδοχή κινδύνων στην περίπτωση που δεν ξεπερνούν τα καθορισμένα όρια και είναι σύμφωνοι με τις Πολιτικές Ασφαλείας.
- Αποφυγή κινδύνων.
- Μεταβίβαση πληροφόρησης κινδύνων σε εξωτερικά μέρη (π.χ. πολίτες, προμηθευτές, ασφαλιστικές εταιρείες κλπ).

Επίσης, θα πρέπει να εντοπιστούν και να καταγραφούν οι εναπομένοντες κίνδυνοι από τη διαχείριση που προηγήθηκε.

Όλα τα παραπάνω καταγράφονται στο Πλάνο Διαχείρισης Κινδύνων, που θα πρέπει να εγκριθεί από τη Διοίκηση.

Παραδοτέα:

- Μελέτη εκτίμησης αντικτύπου προστασίας δεδομένων
- Πλάνο Διαχείρισης Κινδύνων

1.3.5 Διαμόρφωση κατάλληλης πολιτικής και στόχων για την ασφάλεια, σχεδιασμός των Απαιτούμενων Πολιτικών – Διαδικασιών, Σχέδιο Συμμόρφωσης

Θα καταρτιστεί η γενική Πολιτική Ασφάλειας Πληροφοριών, η οποία θα αποτελεί τη δέσμευση για τη διασφάλιση των Δεδομένων Προσωπικού Χαρακτήρα, καθώς επίσης και οι απαιτούμενες πολιτικές και διαδικασίες διαχείρισης και προστασίας των προσωπικών δεδομένων. Με βάση αυτά, τη μελέτη εκτίμησης αντικτύπου καθώς και το Πλάνο Διαχείρισης Κινδύνων, θα δημιουργηθεί ένα πλήρες Σύστημα Διαχείρισης Δεδομένων Προσωπικού Χαρακτήρα.

Το Σύστημα, θα σχεδιαστεί με τέτοιον τρόπο, ώστε οι διαδικασίες και πολιτικές να είναι συμβατές και με το διεθνές πρότυπο ISO / IEC 27001:2013 «Διαχείριση Ασφάλειας Πληροφοριών», με το οποίο υπάρχουν αρκετά κοινά σημεία.

Θα διαμορφωθούν κατάλληλες Πολιτικές – Διαδικασίες διαχείρισης για την ασφάλεια των Δεδομένων Προσωπικού Χαρακτήρα που θα καλύπτουν τουλάχιστον τις παρακάτω περιοχές:

1. Οργάνωση Ασφάλειας Δεδομένων Προσωπικού Χαρακτήρα
2. Ασφάλεια Ανθρωπίνων Πόρων
3. Διαχείριση Δεδομένων Προσωπικού Χαρακτήρα
   (περιλαμβάνει τις διαδικασίες για την έγκυρη συναίνεση κατά την απόκτηση των προσωπικών δεδομένων καθώς και την πολιτική/διαδικασίες για ασφαλή καταστροφή προσωπικών δεδομένων)
4. Διαδικασίες ανταπόκρισης σε αιτήματα
   (πρόσβασης / διόρθωσης / εξαίρεσης / περιορισμού ή αντιρρήσεων στην επεξεργασία προσωπικών δεδομένων καθώς και διαγραφής προσωπικών δεδομένων)
5. Έλεγχος Πρόσβασης στα Συστήματα Αποθήκευσης
6. Πολιτική / διαδικασίες για την προστασία των προσωπικών δεδομένων κατά τη χρήση καμερών, συστημάτων παρακολούθησης ή καταγραφής ενεργειών, συστημάτων ελέγχου πρόσβασης, καταγραφής παρουσιών, κλπ.
7. Κρυπτογράφηση Δεδομένων Προσωπικού Χαρακτήρα
8. Φυσική Ασφάλεια & Ασφάλεια Περιβάλλοντος Χώρου
9. Ασφάλεια Λειτουργιών
10. Ασφάλεια Επικοινωνιών
11. Απόκτηση, Ανάπτυξη και Συντήρηση Πληροφοριακών Συστημάτων
    (περιλαμβάνει και την εφαρμογή του Γενικού Κανονισμού στην ιστοσελίδα του Δήμου, οδηγίες για τη χρήση των μέσων κοινωνικής δικτύωσης από το Δήμο, ειδικούς όρους για παροχή υπηρεσιών μέσω cloud, κλπ)
12. Σχέσεις με Εξωτερικούς συνεργάτες
    (περιλαμβάνει απαιτήσεις κατά την εκτέλεση συμβάσεων, όρους για δέουσα επιμέλεια, άρθρα για αντιμετώπιση περιπτώσεων μη συμμόρφωσης, κλπ)
13. Διαχείριση Περιστατικών Ασφάλειας Δεδομένων Προσωπικού Χαρακτήρα
    (διαχείριση - αντιμετώπιση παραβιάσεων ασφάλειας ή διαρροής, διατήρηση αρχείου καταγραφής με στοιχεία όπως η φύση της παραβίασης, ο κίνδυνος, η προέλευση, κλπ, διαδικασίες κοινοποίησης της παραβίασης και υποβολή αναφορών, κ.α.)

14. Διαχείριση Επιχειρησιακής Συνέχειας (σχέδιο ανάκαμψης από καταστροφές, διαρροές, κλπ)

Η συγκεκριμένη ομαδοποίηση των περιοχών που αναφέρεται παραπάνω είναι ενδεικτική.

Σε κάθε Διαδικασία ή/και Πολιτική θα σχεδιαστούν και τα απαραίτητα Μητρώα, ενδεικτικά:

- Μητρώο Προσωπικών Δεδομένων Ατόμων
- Μητρώο Παραβίασης Προσωπικών Δεδομένων
- Μητρώο Συστημάτων και Μέσων, που περιέχουν Προσωπικά Δεδομένα (Systems, Servers, Files, Data Bases, Media containing Personal Data)

Τέλος, θα καταρτιστεί ένα λεπτομερές και ολοκληρωμένο σχέδιο για τη συμμόρφωση του Δήμου με τις απαιτήσεις του Κανονισμού Προστασίας Προσωπικών Δεδομένων, το οποίο θα περιλαμβάνει αναλυτικά όλες τις ενέργειες που πρέπει να γίνουν και όλα τα οργανωτικά και τεχνικά μέτρα που πρέπει να ληφθούν για την εφαρμογή στο Δήμο των πολιτικών – διαδικασιών που έχουν καθοριστεί.

Παραδοτέα:

- Πολιτική Ασφάλειας Πληροφοριών
- Εγχειρίδιο Διαδικασιών – Πολιτικών διαχείρισης και προστασίας προσωπικών δεδομένων
- Αναλυτικό Σχέδιο Συμμόρφωσης

1.3.6 Εφαρμογή Συστήματος Πολιτικών – Διαδικασιών

Ο ανάδοχος θα παραδώσει το πλήρες Σύστημα Πολιτικών – Διαδικασιών στα στελέχη του Δήμου για επεξεργασία. Κατόπιν των πιθανών τροποποιήσεων, το Σύστημα θα εγκριθεί από τη Διοίκηση του Δήμου, θα ανακοινωθεί – διανεμηθεί στο προσωπικό και θα ξεκινήσει η πλήρης λειτουργία του. Ο ανάδοχος θα υποστηρίξει το προσωπικό του Δήμου κατά τη φάση αυτή.

1.3.7 Εκπαίδευση εμπλεκόμενων υπαλλήλων του Δήμου

Στα πλαίσια του Έργου, και πριν την πλήρη λειτουργία του συστήματος Πολιτικών – Διαδικασιών, θα εκπαιδευτούν σχετικά οι εμπλεκόμενοι υπάλληλοι του Δήμου. Οι υπάλληλοι θα εκπαιδευτούν, κατά τμήματα, αντικείμενο ή διαδικασίες – πολιτικές.

Παραδοτέα:

- Πρόγραμμα και παρουσιολόγια εκπαίδευσης

1.3.8 Έλεγχος (Audit) εφαρμογής και Συμμόρφωσης

Κατά την πλήρη λειτουργία, ο ανάδοχος θα προσφέρει υπηρεσίες παρακολούθησης της ορθότητας εκτέλεσης των διαδικασιών με έγγραφες ενημερώσεις παρατηρήσεων για διάστημα ενός (1) μηνός (σε 3 τουλάχιστον, επιλεγμένες ημέρες κατόπιν συνεννόησης με το Δήμο).

Παραδοτέα:

- Καταγραφή των αποτελεσμάτων του ελέγχου ορθότητας της εκτέλεσης των σχεδιασμένων διαδικασιών

1.3.9 Υπηρεσίες Υπεύθυνου Προστασίας Δεδομένων (DPO)

Ο ανάδοχος θα ορίσει Υπεύθυνο Προστασίας Δεδομένων (DPO) του Δήμου Καλαμάτας, ο οποίος θα εκτελεί όλα τα χρέη του, τόσο με επιτόπου επισκέψεις, όσο και απομακρυσμένα.

Ο DPO θα λειτουργεί ως μια «εσωτερική» Αρχή Προστασίας Δεδομένων και θα διασφαλίζει ότι ο Δήμος Καλαμάτας τηρεί τις διατάξεις του Κανονισμού. Για την επιτέλεση των καθηκόντων του, θα είναι υπεύθυνος για την τήρηση του αρχείου των πράξεων επεξεργασίας για τις οποίες είναι αρμόδιος ο Δήμος.

Ο DPO θα συνεργάζεται με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και θα είναι προσβάσιμος από την Αρχή, το Δήμο αλλά και τα Υποκείμενα των Δεδομένων 365 ημέρες το χρόνο.

Σε όλη τη διάρκεια της θητείας του, ο DPO θα καλείται να συμμετέχει τακτικά στις συσκέψεις των ανώτερων και μεσαίων στελεχών της διοίκησης του Δήμου και να είναι παρών όταν λαμβάνονται αποφάσεις που έχουν επιπτώσεις στην προστασία των προσωπικών δεδομένων. Εφόσον ο Δήμος το θεωρήσει απαραίτητο για να διευκολυνθεί η προσβασιμότητα του DPO από το προσωπικό του, μπορεί να του ζητήσει να έχει προγραμματισμένη τακτική φυσική παρουσία στους χώρους του Δήμου, σύμφωνα με εβδομαδιαίο πρόγραμμα που θα καθοριστεί από κοινού.

Ο ανάδοχος θα πρέπει να διασφαλίσει τη διαθεσιμότητα του DPO και τη δυνατότητα επικοινωνίας των υποκειμένων των δεδομένων μαζί του, καθώς και τη δυνατότητά του να επιτελεί αποτελεσματικά όλα τα καθήκοντά του.

Ο DPO θα πρέπει να διαθέτει εμπειρογνωσία στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, σύμφωνα με το άρθρο 37 του Κανονισμού, ενώ δεν θα πρέπει να υπάρχουν συγκρούσεις συμφερόντων.

Οι υπηρεσίες του DPO θα παρέχονται από τον ανάδοχο για ένα (1) έτος από την υπογραφή της σύμβασης.

Ο DPO θα καταρτίσει ετήσια έκθεση δραστηριοτήτων στο τέλος της σύμβασης.

1.4 Χρονοδιάγραμμα εργασιών

Η συνολική διάρκεια των εργασιών θα είναι 12 μήνες, ως εξής:

1. Οι υπηρεσίες του Υπευθύνου Προστασίας Δεδομένων (DPO), θα προσφερθούν από την υπογραφή έως το τέλος της σύμβασης (για 1 έτος).

2. Οι υπόλοιπες εργασίες συμμόρφωσης του Δήμου Καλαμάτας με τον Κανονισμό, θα πρέπει να έχουν ολοκληρωθεί σε διάστημα έως τεσσάρων (4) μηνών και 15 ημερών από την ημερομηνία υπογραφής της σύμβασης, με δυνατότητα τροποποίησης του

χρονοδιαγράμματος των επιμέρους φάσεων, εφόσον η συνολική διάρκεια δεν υπερβεί τους τέσσερις (4) μήνες και 15 ημέρες.
Ενδεικτικά, οι εργασίες αυτές θα χωριστούν στις παρακάτω φάσεις:
Φάση 1:
Ενημέρωση / εκπαίδευση Στελεχών του Δήμου (ενότητα 1.3.2) στον κανονισμό (GDPR): Θα ολοκληρωθεί σε ένα (1) μήνα από την έναρξη της σύμβασης.

Φάση 2:
Περιλαμβάνονται οι εργασίες που περιγράφονται στις ενότητες 1.3.3 και 1.3.6 (εκτίμηση τρέχουσας κατάστασης, εκτίμηση αντικτύπου, σχεδιασμός πολιτικών – διαδικασιών, σχέδιο συμμόρφωσης, εφαρμογή συστήματος, κλπ): Θα έχουν ολοκληρωθεί σε τρεις (3) μήνες και 15 ημέρες από την έναρξη της σύμβασης.

Φάση 3:
Εκπαίδευση εργαζομένων (ενότητα 1.3.7) στις Διαδικασίες – Πολιτικές που θα σχεδιαστούν: Θα έχουν ολοκληρωθεί σε τρεις (3) μήνες και 15 ημέρες από την έναρξη της σύμβασης.

Φάση 4:
Περιλαμβάνεται ο έλεγχος που περιγράφεται στην ενότητα 1.3.8: Θα έχει ολοκληρωθεί σε τέσσερις (4) μήνες και 15 ημέρες από την έναρξη της σύμβασης.

1.5 Τρόπος πληρωμής

Από το συνολικό ποσό της σύμβασης, ο ανάδοχος θα μπορεί να τιμολογήσει τα παρακάτω:

- Το 10 % μετά το πέρας της 1ης φάσης
- Το 40 % μετά το πέρας της 2ης φάσης
- Το 30 % μετά το πέρας της 3ης φάσης
- Το 10 % μετά το πέρας της 4ης φάσης
- Το 10% μετά την πάροδο 8 μηνών από την έναρξη του έργου καιΤο υπόλοιπο 10% με την ολοκλήρωση του έργου

Οι πληρωμές θα γίνονται ύστερα από τους ελέγχους των παραδοτέων που θα κάνει ο Δήμος και τη βεβαίωση καλής εκτέλεσης των εργασιών από την αρμόδια επιτροπή του Δήμου.

Ο ανάδοχος βαρύνεται με όλες τις νόμιμες κρατήσεις κατά την έκδοση των αντίστοιχων τιμολογίων, εκτός του ΦΠΑ.

Κατά την υπογραφή του συμφωνητικού, ο ανάδοχος, θα καταθέσει εγγυητική επιστολή καλής εκτέλεσης της ανωτέρω υπηρεσίας, ίσης με το 5% της συμβατικής αξίας χωρίς το ΦΠΑ.

1.6 Εμπιστευτικότητα

Το σύνολο των πληροφοριών, των δεδομένων, των προκυπτόντων συμπερασμάτων και οτιδήποτε έχει σχέση με το υπό εκτέλεση έργο, είναι και θεωρούνται εμπιστευτικά και καλύπτονται από την υποχρέωση της εχεμύθειας.

Ο ανάδοχος και ο Δήμος Καλαμάτας κρατούν μυστική κάθε πληροφορία που περιέχεται στην αντίληψή τους από την εκτέλεση των εργασιών αυτής της σύμβασης και δεν αποκαλύπτουν τέτοιες πληροφορίες σε τρίτον χωρίς τη γραπτή συμφωνία του εταίρου μέρους. Ο ανάδοχος

επιβάλλει αυτή την υποχρέωση στο προσωπικό του, στην ομάδα έργου και στους τυχόν υπεργολάβους του. Ο ανάδοχος και ο Δήμος αποκαλύπτουν εμπιστευτικές πληροφορίες σε όσους υπαλλήλους ασχολούνται άμεσα με το περιεχόμενο της σύμβασης ή χρησιμοποιούν τον εξοπλισμό και το λογισμικό που περιέχει τις πληροφορίες και διασφαλίζουν ότι αυτοί οι υπάλληλοι είναι εν γνώσει και συμφωνούν με τις υποχρεώσεις εχεμύθειας, ο δε ανάδοχος μεταφέρει αυτές τις υποχρεώσεις και στους τυχόν υπεργολάβους του.

Σε περίπτωση που υπάρξει διαρροή πληροφοριών, η οποία αποδεδειγμένα οφείλεται στον ανάδοχο, ο Δήμος Καλαμάτας διατηρεί το δικαίωμα να κάνει χρήση των διατάξεων «περί πνευματικής ιδιοκτησίας» ή όποιας άλλης πρόσφορης διάταξης και να κοστολογήσει και απαιτήσει πληρωμή για όλες τις άμεσες και έμμεσες, ζημίες που θα έχει κατά περίπτωση υποστεί, καθώς επίσης και να προβεί στη λύση της σύμβασης.

ΘΕΩΡΗΘΗΚΕ
ΚΑΛΑΜΑΤΑ 19/07/2018

Ο ΠΡΟΪΣΤΑΜΕΝΟΣ

Η ΔΙΕΥΘΥΝΤΡΙΑ

ΔΙΟΝΥΣΟΠΟΥΛΟΣ ΒΑΣΙΛΕΙΟΣ **ΚΟΥΡΑΚΛΗ ΠΑΝΑΓΙΩΤΑ**

2 ΑΠΑΙΤΟΥΜΕΝΑ ΠΡΟΣΟΝΤΑ ΑΝΑΔΟΧΟΥ

2.1 Καταλληλόλητα άσκησης επαγγελματικής δραστηριότητας

Ο υποψήφιος ανάδοχος θα πρέπει να ασκεί επαγγελματική δραστηριότητα συναφή με το αντικείμενο του προς ανάθεση έργου, ήτοι στην παροχή συμβουλευτικών υπηρεσιών, διαθέτοντας το δικό τους απαιτούμενο έμπειρο προσωπικό. Οι οικονομικοί φορείς απαιτείται να είναι εγγεγραμμένοι στο Εμπορικό ή Βιομηχανικό ή Βιοτεχνικό Επιμελητήριο για το ειδικό επάγγελμά τους.

Απαιτούνται:
Πιστοποιητικό / βεβαίωση του Εμπορικού ή Βιομηχανικού ή Βιοτεχνικού Επιμελητηρίου, ή επικυρωμένο φωτοαντίγραφο δήλωσης έναρξης επαγγέλματος, εφόσον πρόκειται για φυσικά πρόσωπα, από το οποίο να προκύπτει η δραστηριότητα της επιχείρησης/εταιρίας.

2.2 Τεχνική και επαγγελματική ικανότητα

Όσον αφορά στην τεχνική και επαγγελματική ικανότητα του αναδόχου, αυτός απαιτείται, να έχει:

1. Την κατάλληλα τεκμηριωμένη και αποδεδειγμένη επαγγελματική ικανότητα και τεχνογνωσία στο πλαίσιο υλοποίησης αντικειμένων αντίστοιχης πολυπλοκότητας με το υπό ανάθεση αντικείμενο και συγκεκριμένα:
    a. Εμπειρία στην παροχή συμβουλευτικών υπηρεσιών βελτίωσης - αναδιοργάνωσης σε Δήμους της χώρας. Για την τεκμηρίωση της ως άνω εμπειρίας, οι υποψήφιοι θα πρέπει να έχουν ολοκληρώσει επιτυχώς, τουλάχιστον δύο (2) τέτοια έργα.
    Απαιτούνται:
    Συμβάσεις και βεβαιώσεις καλής εκτέλεσης των έργων που έχουν ολοκληρωθεί επιτυχώς.

    b. Εμπειρία σε έργα συμμόρφωσης με τον GDPR. Για την τεκμηρίωση της ως άνω εμπειρίας, οι υποψήφιοι θα πρέπει να έχουν αναλάβει τουλάχιστον 10 έργα συμμόρφωσης με τον GDPR, από τα οποία, τουλάχιστον ένα να είναι σε Δήμο της χώρας και τουλάχιστον 3 θα πρέπει να έχουν ολοκληρωθεί επιτυχώς.
    Απαιτούνται:
    Συμβάσεις υλοποίησης για τα έργα που βρίσκονται σε εξέλιξη και βεβαιώσεις καλής εκτέλεσης για τα έργα που έχουν ολοκληρωθεί επιτυχώς.

2. Προσωπικό επαρκές σε πλήθος και δεξιότητες (επαγγελματικά προσόντα) για την ανάληψη του εν λόγω έργου και συγκεκριμένα απαιτείται να δηλώσει Ομάδα Έργου που κατ' ελάχιστο θα περιλαμβάνει:
    - Υπεύθυνο Έργου: Κάτοχο πανεπιστημιακού διπλώματος που να διαθέτει, είτε μεταπτυχιακό τίτλο σπουδών σχετικό με τη διοίκηση οργανισμών, τη διοίκηση πληροφοριακών συστημάτων ή τη διαχείριση έργων, είτε πιστοποίηση στη διαχείριση έργων κατά PMI ή PRINCE2. Επίσης, να διαθέτει τουλάχιστον 10ετή επαγγελματική εμπειρία στην παροχή συμβουλευτικών υπηρεσιών στην οποία να περιλαμβάνεται εμπειρία τουλάχιστον 2 ετών σε θέματα οργάνωσης φορέων του δημοσίου τομέα, καθώς και εμπειρία σε τουλάχιστον πέντε (5) έργα GDPR.
    - Σύμβουλο Οργάνωσης: Κάτοχο πανεπιστημιακού διπλώματος με 5ετή εμπειρία σε Έργα Οργάνωσης στον ευρύτερο δημόσιο τομέα και συμμετοχή σε πέντε (5) τουλάχιστον έργα GDPR.
    - Ειδικό στην Ασφάλεια Πληροφορικής: Κάτοχο πανεπιστημιακού διπλώματος, να κατέχει πιστοποίηση ως ISO 27001 auditor, και να έχει τουλάχιστον 5ετή εμπειρία στον τομέα της Ασφάλειας Πληροφοριακών Συστημάτων
    - IT Auditor: να κατέχει πιστοποίηση ως ISO 27001 auditor, και να έχει τουλάχιστον 5ετή εμπειρία στον τομέα της Ασφάλειας Πληροφοριακών Συστημάτων
    - Νομικός Σύμβουλος: Δικηγόρος, μέλος Δικηγορικού Συλλόγου με νόμιμη άδεια ασκήσεως επαγγέλματος στην Ελλάδα και επαγγελματική εμπειρία στο γνωστικό αντικείμενο της προστασίας δεδομένων με συμμετοχή σε τουλάχιστον τρία (3) έργα GDPR.

    Απαιτούνται:
    Αναλυτικά Βιογραφικά Σημειώματα, όλων των μελών της Ομάδας Έργου από τα οποία να αποδεικνύονται οι παραπάνω προϋποθέσεις ευθέως, τίτλοι σπουδών και βεβαιώσεις προϋπηρεσίας.

2.3 Πρότυπα διασφάλισης ποιότητας

Οι οικονομικοί φορείς για την παρούσα διαδικασία σύναψης σύμβασης οφείλουν, επί ποινή αποκλεισμού, να διαθέτουν σε ισχύ κατά το χρόνο διενέργειας του Διαγωνισμού:

- Πρότυπο πιστοποίησης συστημάτων διαχείρισης ποιότητας ISO 9001:2008 ή ισοδύναμο.
- Πρότυπο πιστοποίησης διαχείρισης ασφάλειας πληροφοριακών συστημάτων ISO 27001:2013 ή ισοδύναμο

Για την απόδειξη της συμμόρφωσης με πρότυπα διασφάλισης ποιότητας, ο υποψήφιος ανάδοχος πρέπει να υποβάλλει τα ανωτέρω ζητούμενα πρότυπα διασφάλισης ποιότητας και διαχείρισης ασφάλειας πληροφοριακών συστημάτων, τα οποία να βρίσκονται σε ισχύ κατά το χρόνο διενέργειας του Διαγωνισμού.

ΘΕΩΡΗΘΗΚΕ

Ο ΠΡΟΪΣΤΑΜΕΝΟΣ **ΚΑΛΑΜΑΤΑ 19/07/2018**
Η ΔΙΕΥΘΥΝΤΡΙΑ

ΔΙΟΝΥΣΟΠΟΥΛΟΣ ΒΑΣΙΛΕΙΟΣ **ΚΟΥΡΑΚΛΗ ΠΑΝΑΓΙΩΤΑ**

3 ΠΡΟΜΕΤΡΗΣΗ – ΠΡΟΫΠΟΛΟΓΙΣΜΟΣ ΜΕΛΕΤΗΣ

α/α	Είδος	CPV	Μονάδα μέτρησης	Ποσότητα	Τιμή μονάδας	Αξία
1.	Εφαρμογή του Γενικού Κανονισμού για την Προστασία των Προσωπικών Δεδομένων (General Data Protection Regulation)	79417000-0	Υπηρεσία	1	19.350,00 €	19.350,00 €
					ΑΞΙΑ	**19.350,00 €**
					Φ.Π.Α	**4.644,00 €**
					ΣΥΝΟΛΟ	**23.994,00 €**

ΘΕΩΡΗΘΗΚΕ
ΚΑΛΑΜΑΤΑ 19/07/2018

Ο ΠΡΟΪΣΤΑΜΕΝΟΣ

Η ΔΙΕΥΘΥΝΤΡΙΑ

ΔΙΟΝΥΣΟΠΟΥΛΟΣ ΒΑΣΙΛΕΙΟΣ

ΚΟΥΡΑΚΛΗ ΠΑΝΑΓΙΩΤΑ

4 ΤΙΜΟΛΟΓΙΟ - ΠΡΟΫΠΟΛΟΓΙΣΜΟΣ ΠΡΟΣΦΟΡΑΣ

α/α	Είδος	CPV	Μονάδα μέτρησης	Ποσότητα	Τιμή μονάδας	Αξία
1.	Εφαρμογή του Γενικού Κανονισμού για την Προστασία των Προσωπικών Δεδομένων (General Data Protection Regulation)	79417000-0	Υπηρεσία	1		
					ΑΞΙΑ	
					Φ.Π.Α	
					ΣΥΝΟΛΟ	

Έλαβα υπόψη όλους τους όρους της μελέτης 9/2018 του Τμήματος Ηλεκτρονικής Διακυβέρνησης του Δήμου Καλαμάτας και αποδέχομαι αυτούς ανεπιφύλακτα και αμετάκλητα.

Η προσφορά ισχύει για 60 ημέρες από την επόμενη της διενέργειας της διαδικασίας της Ανάθεσης.

Ο υποβάλλων

Καλαμάτα / / 2018