ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΝΟΜΟΣ ΕΒΡΟΥ
ΔΗΜΟΣ ΣΟΥΦΛΙΟΥ

Θέμα μελέτης:	**«Παροχή υπηρεσιών συμμόρφωσης, προσαρμογής και υποστήριξης ως προς τον Νέο Κανονισμό Προστασίας Προσωπικών Δεδομένων με αριθμ. 679/2016 (General Data Protection Regulation – GDPR) του Δήμου Σουφλίου και υπηρεσίες DPO για 12 μήνες»**
Αρ. Μελέτης	**68** /2018
Ημερομηνία	01/08/2018
Κωδικός Προϋπολογισμού:	10.6117.002
Χρηματοδότηση	Ιδία έσοδα
CPV	79417000-0

ΤΕΧΝΙΚΗ ΕΚΘΕΣΗ - ΠΡΟΔΙΑΓΡΑΦΕΣ

Ι. ΓΕΝΙΚΑ

Με την παρούσα τεχνική έκθεση, εκτιμώμενης αξίας **24.000,00€** συμπεριλαμβανομένου Φ.Π.Α, περιγράφονται οι εργασίες για την παροχή υπηρεσιών συμμόρφωσης, προσαρμογής και υποστήριξης ως προς τον Νέο Κανονισμό Προστασίας Προσωπικών Δεδομένων με αριθμ. 679/2016 (General Data Protection Regulation – GDPR).
Η δαπάνη θα βαρύνει τον κωδικό **Κ.Α. 10.6117.002** του προϋπολογισμού του Δήμου έτους **2018** με το ποσό **16.800,00€** και του οικονομικού έτους **2019** με το ποσό **7.200,00€.**

Ο Δήμος Σουφλίου υπάγεται στο πλαίσιο της εφαρμογής του κανονισμού της Ε.Ε. 679/2016 του Ευρωπαϊκού Κοινοβουλίου. Ο κανονισμός Ε.Ε. 679/2016 διαμορφώνει ένα ενιαίο νομικό πλαίσιο για την επεξεργασία προσωπικών δεδομένων στα κράτη μέλη της Ευρωπαϊκής Ένωσης, που θέτει μια σειρά περιορισμών και νέων υποχρεώσεων των φορέων του Δημοσίου. Ο Δήμος Σουφλίου στα πλαίσια της άσκησης των αρμοδιοτήτων του:

- επεξεργάζεται και τηρεί δεδομένα που αφορούν στοιχεία υπαλλήλων, πολιτών, ανηλίκων, συνεργατών, προμηθευτών, ευπαθής ομάδες πληθυσμού (Κέντρο Κοινότητας)
- εκτελεί καθήκοντα και υποχρεώσεις που επιβάλλονται από το νόμο (ΔΙΑΥΓΕΙΑ)
- έχει υποχρέωση κοινολόγησης στοιχείων (εισαγγελικές παραγγελίες)
- έχει συνεργασία με πολλά τρίτα μέρη (δικηγόροι, εταιρίες πληροφορικής κλπ)

Ο Δήμος Σουφλίου δε διαθέτει εξειδικευμένο και πιστοποιημένο προσωπικό με αντίστοιχη εμπειρία για την υποστήριξη των παραπάνω υπηρεσιών, ώστε να είναι σε θέση να διεκπεραιώσει την άνω υπηρεσία, που είναι υποχρεωτική για τον Δήμο. Εξάλλου, ο Κανονισμός (679/2016) περί Προστασίας Προσωπικών Δεδομένων, εισάγει νέα δεδομένα, ειδικές διαδικασίες, μεθοδολογία και έγγραφα, τα οποία προϋποθέτουν ικανό βαθμό κατάρτισης προκειμένου να προσαρμοσθούν και εφαρμοσθούν στο Δήμο Σουφλίου.

Η ανάθεση της εργασίας θα γίνει σύμφωνα με τις διατάξεις του Ν. 4412/16 με κριτήριο ανάθεσης την πλέον συμφέρουσα από οικονομική άποψη προσφορά, μόνο βάσει τιμής, εφόσον είναι σύμφωνη με τους όρους της παρούσας και αφορά στο σύνολο των ζητούμενων υπηρεσιών.
Ο προσφέρων στον οποίο θα ανατεθεί η σύμβαση, οφείλει να προσκομίσει πριν ή κατά την έκδοση της απόφασης ανάθεσης, επιπλέον της προσφοράς του:

α) απόσπασμα ποινικού μητρώου, έκδοσης τουλάχιστον του τελευταίου τριμήνου, από το οποίο να προκύπτει ότι δεν έχει καταδικασθεί με τελεσίδικη απόφαση για αδίκημα αναφερόμενο

στην παρ. 1 του άρθρου 73 του Ν. 4412/2016 (λόγοι υποχρεωτικού αποκλεισμού). Στις περιπτώσεις εταιρειών περιορισμένης ευθύνης (Ε.Π.Ε.) και προσωπικών εταιρειών (Ο.Ε. και Ε.Ε.) και ΙΚΕ ιδιωτικών κεφαλαιουχικών εταιρειών, η υποχρέωση του αποσπάσματος ποινικού μητρώου, αφορά τους διαχειριστές. Στις περιπτώσεις ανωνύμων εταιρειών (Α.Ε.), απόσπασμα ποινικού μητρώου υποχρεούνται να προσκομίσουν όλα τα μέλη του Διοικητικού Συμβουλίου, καθώς και ο Διευθύνων Σύμβουλος. Στις περιπτώσεις Συνεταιρισμών, απόσπασμα ποινικού μητρώου υποχρεούνται να προσκομίσουν όλα τα μέλη του Διοικητικού Συμβουλίου. Σε όλες τις υπόλοιπες περιπτώσεις, η ανωτέρω υποχρέωση αφορά στους νόμιμους εκπροσώπους τους.

β) Αποδεικτικό φορολογικής ενημερότητας της εταιρείας ή του φυσικού προσώπου, κατά περίπτωση, ανάλογα με τη νομική μορφή του προσφέροντα.

γ) Αποδεικτικό καταβολής ασφαλιστικών εισφορών της εταιρείας ή του φυσικού προσώπου, κατά περίπτωση, ανάλογα με τη νομική μορφή του προσφέροντα.

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. ή οι διαχειριστές για τις Ε.Π.Ε., Ι.Κ.Ε., Ο.Ε. ή Ε.Ε. και η νόμιμη εκπροσώπηση της εταιρείας.

Δεν αποκλείεται ο προσφέρων οικονομικός φορέας, όταν έχει εκπληρώσει τις υποχρεώσεις του, είτε καταβάλλοντας τους φόρους ή τις εισφορές κοινωνικής ασφάλισης που οφείλει, είτε υπαγόμενος σε δεσμευτικό διακανονισμό για την καταβολή τους

ΙΙ. ΑΝΤΙΚΕΙΜΕΝΟ

Το αντικείμενο των υπηρεσιών της παρούσας είναι το σύνολο των υπηρεσιών και ενεργειών που θα οδηγήσουν στη συμμόρφωση του Δήμου Σουφλίου στις επιταγές του νέου κανονισμού και υπηρεσίες DPO για 12 μήνες και θα περιλαμβάνει:

- Ενέργειες έναρξης και καθορισμός διαδικασίας υλοποίησης των εργασιών
- Χαρτογράφηση της ροής των πληροφοριών του Δήμου που αφορούν τη συλλογή, διάθεση και επεξεργασία τους, κατόπιν διενέργειας επιθεώρησης, συνεντεύξεων και καταγραφής των ακολουθούμενων διαδικασιών και υφιστάμενων υποδομών του Δήμου.
- Αξιολόγηση του υφιστάμενου επιπέδου συμμόρφωσης του Δήμου με τον Κανονισμό ως προς την διαχείριση των προσωπικών δεδομένων.
- Εντοπισμός των αποκλίσεων από τον Κανονισμό
- Κατάρτιση Πολιτικών και Κωδίκων Δεοντολογίας διαχείρισης προσωπικών δεδομένων. Σύνταξη σχεδίου συμμόρφωσης για την υιοθέτηση τεχνολογικών μεθόδων και μέτρων ασφαλείας για την διαχείριση των προσωπικών δεδομένων, εναρμόνιση της λειτουργίας των οργανικών μονάδων.
- Νομική υποστήριξη που αφορά στην κατάρτιση προτάσεων για την ανάληψη διορθωτικών ενεργειών με σκοπό τη συμμόρφωση με τον Κανονισμό, καθώς και σύνταξη και παράδοση υποδειγμάτων συναινέσεων και κειμένων προς ένταξη στις ήδη υπάρχουσες συμβάσεις. Νομική αξιολόγηση της διαχείρισης των δεδομένων προσωπικού χαρακτήρα και των συμβάσεων που συνάπτει ο Δήμος υπό το φως των θεμελιωδών αρχών του Κανονισμού (Λογοδοσία, Περιορισμός του σκοπού, Διαφάνεια, Νομιμότητα και Αντικειμενικότητα, ελαχιστοποίηση δεδομένων, ακρίβεια, χρόνος διατήρησης/διαγραφή, Διαβιβάσεις, δικαιώματα δημοτών.)
- Διόρθωση διαδικασιών και πρακτικών στην διαχείριση προσωπικών δεδομένων μετά την εφαρμογή του σχεδίου συμμόρφωσης.
- Ευαισθητοποίηση της Διοίκησης, εκπαίδευση του προσωπικού που επεξεργάζεται προσωπικά δεδομένα με στόχο την συμμόρφωσή του με τις απαιτήσεις του Κανονισμού.
- Διαρκής, περιοδικός έλεγχος συμμόρφωσης του Δήμου, υποστήριξη με εξειδικευμένο στέλεχος – υπεύθυνο επεξεργασίας δεδομένων (DPO).

ΙΙΙ. ΣΤΑΔΙΑ ΥΛΟΠΟΙΗΣΗΣ – ΠΑΡΑΔΟΤΕΑ

- **<u>ΣΤΑΔΙΟ 1 - Στάδιο προετοιμασίας – αποτύπωση υφιστάμενης κατάστασης</u>**

1.1 Δέσμευση Διοίκησης

Παρουσίαση στην Διοίκηση του Δήμου και στα στελέχη του των απαιτήσεων που θέτει ο Κανονισμός, προσδιορισμός όλων των απαραίτητων ενεργειών που απαιτούνται για την εφαρμογή του, δέσμευση της διοίκησης, προσδιορισμός πόρων και προσβάσεων που θα παρασχεθούν στην ομάδα έργου και ενημέρωση του προσωπικού του Δήμου.

Παραδοτέο:
Ενέργειες πρώτης ενημέρωσης Διοίκησης και προσωπικού συνοδευόμενο από Δήλωση Δέσμευσης της Διοίκησης.

1.2 Καταγραφή υπευθύνων ανά οργανωτική μονάδα.
Προσδιορίζονται οι διευθύνσεις και τα τμήματα του Δήμου, γίνεται καταγραφή των ανά τμήμα και ανά αρχείο δεδομένων των υπευθύνων. Η καταγραφή αποτυπώνεται στο μητρώο επεξεργασιών δεδομένων.
Παραδοτέο:
Μητρώο επεξεργασιών δεδομένων.

1.3 Καταγραφή διαθεσίμων φυσικών πόρων
Καταγραφή των διαθεσίμων ανθρώπινων πόρων ανά τμήμα που τίθενται στην διάθεση του Υπεύθυνου Προστασίας. Δημιουργία αντιπροσωπευτικής ομάδας εργασίας σε σχέση με τα υφιστάμενα δεδομένα και τις οργανωτικές μονάδες που τα επεξεργάζονται.
Παραδοτέο:
Έγγραφη αναφορά σε συμφωνία με τα μέλη της ομάδας εργασίας και προσδιορισμός αρμοδιοτήτων και υποχρεώσεων.

1.4 Καταγραφή και χαρτογράφηση των δεδομένων προσωπικού χαρακτήρα που τηρούνται στο Δήμο, της επεξεργασίας και της κυκλοφορίας τους.
Καταγραφή ανά επεξεργασία, αρχείο και είδος δεδομένων που τηρούνται και διακινούνται. Αποτύπωση ροής των προσωπικών δεδομένων (data flow map) ανά κατηγορία, ώστε να δημιουργηθούν τα Αρχεία των Δραστηριοτήτων Επεξεργασίας, κατ' απαίτηση του Κανονισμού (ΕΕ) 2016/679 (άρθρο 30) και να υπάρχει πλήρης αποτύπωση της διαχείρισης των προσωπικών δεδομένων. Καθορισμός είδους επεξεργασίας, πηγές προέλευσης δεδομένων, χρόνος τήρησής τους.
Παραδοτέο:
Αρχείο δραστηριοτήτων επεξεργασίας

1.5 Προσδιορισμός Νομικής Βάσης – έλεγχος ορθότητας
Προσδιορίζεται η Νομική Βάση που στηρίζεται η επεξεργασία των δεδομένων, εξετάζεται η ορθότητα, η πληρότητα και εγκυρότητα, η καταγραφή, τεκμηρίωση και ο τρόπος γνωστοποίησης στα υποκείμενα.
Παραδοτέο:
Πρότυπα κείμενα θεμελίωσης νομιμοποιητικής βάσης – οδηγίες ενσωμάτωσης στην κάθε μορφή επεξεργασίας, καταγραφής, τεκμηρίωσης και γνωστοποίησης.

1.6 Χαρτογράφηση του εγκατεστημένου πληροφοριακού συστήματος
Έλεγχος, αξιολόγηση, καταγραφή πληροφοριακού συστήματος και δικτυακών υποδομών και διαδικασιών λειτουργίας.
Παραδοτέο:
Σχηματικό διάγραμμα του πληροφοριακού συστήματος με τις επί μέρους λειτουργίες αυτού.

1.7 Έλεγχος και αξιολόγηση πολιτικών και διαδικασιών.
Ελέγχονται οι πολιτικές και τα οργανωτικά μέτρα, η πολιτική ασφαλείας, οι διαδικασίες και η δυνατότητα ικανοποίησης των δικαιωμάτων των υποκειμένων ως προς την επάρκειά τους, η ύπαρξη σχεδίου σε περιστατικά παραβίασης.
Έλεγχος αξιολόγησης διαδικασιών και τήρησής τους από το προσωπικό.
Παραδοτέο: Έκθεση αξιολόγησης πολιτικών και διαδικασιών

1.8 Καταγραφή τεκμηρίωσης
Χαρτογράφηση της υπάρχουσας τεκμηρίωσης που αφορά την ασφάλεια των προσωπικών δεδομένων, εξέταση πληρότητας και ασφάλειάς της.
Παραδοτέο: Έκθεση αποτελεσμάτων

1.9 Εκτίμηση κινδύνων για τις δραστηριότητες επεξεργασίας
Παραδοτέο:

Αναφορά εκτίμησης κινδύνου για κάθε δραστηριότητα επεξεργασίας

1.10 Ανάπτυξη μεθοδολογίας για την διερεύνηση απαίτησης διεξαγωγής Μελέτης Εκτίμησης Αντικτύπου για την επεξεργασία των προσωπικών δεδομένων (Data Privacy Impact Assessment – DPIA)

Παραδοτέο:

Έκθεση αξιολόγησης για απαίτηση ή μη διεξαγωγής DPIA Μελέτη Εκτίμησης Αντικτύπου (DPIA) εφόσον προκύψει ότι απαιτείται.

1.11 Έκθεση αποκλίσεων από τον κανονισμό (Gap Analysis)

Παραδοτέο: Έκθεση αποκλίσεων (Gap Analysis)

- **<u>ΣΤΑΔΙΟ 2 - Στάδιο ολοκλήρωσης διαδικασίας συμμόρφωσης</u>**

2.1 Προτεινόμενα μέτρα – Κατάρτιση σχεδίου συμμόρφωσης

Με βάση τις διαπιστώσεις, θα υπάρξει σχεδιασμός λεπτομερούς και ολοκληρωμένου πλάνου συμμόρφωσης με τις επιταγές του κανονισμού, που θα καλύπτει όλο το φάσμα των επεξεργασιών που γίνονται σε όλο τον κύκλο της ζωής των δεδομένων και αποτελούν αντικείμενο επεξεργασίας.

Παραδοτέο:

Αναλυτικό σχέδιο συμμόρφωσης με τον κανονισμό, που θα περιλαμβάνει όλα τα οργανωτικά και τεχνικά μέτρα που θα πρέπει να λάβει ο Δήμος αλλά και πιθανές συστάσεις που θα συντείνουν στην εν γένει εύρυθμη λειτουργία του.

2.2 Συγγραφή πολιτικών συλλογής, χρήσης, επεξεργασίας, αποθήκευσης, διόρθωσης, διαγραφής δεδομένων

Παραδοτέο:

Εγχειρίδιο πολιτικών διαδικασιών συλλογής και επεξεργασίας δεδομένων που μπορεί να αποτελεί και στοιχείο της πολιτικής ασφάλειας του Δήμου.

2.3 Συγγραφή πολιτικής ασφάλειας

Η πολιτική Ασφάλειας (Security policy) αποτελεί έγγραφο του υπεύθυνου επεξεργασίας στο οποίο περιγράφονται οι στόχοι της ασφάλειας και οι αντίστοιχες διαδικασίες που πρέπει να ακολουθούνται. Καθορίζει την δέσμευση της Διοίκησης και του Δήμου αναφορικά με την ασφάλεια των πληροφοριακών συστημάτων και δικτύων και την προστασία των δεδομένων που τηρεί ο υπεύθυνος επεξεργασίας και περιγράφονται οι βασικές αρχές προστασίας προσωπικών δεδομένων και ασφάλειας που εφαρμόζονται και αφορούν α) τα οργανωτικά μέτρα ασφάλειας αναφορικά με τις αρμοδιότητες όσων εμπλέκονται στη διαχείριση και επεξεργασία προσωπικών δεδομένων, εκπαίδευση, διαχείριση περιστατικών ασφαλείας, καταστροφή προσωπικών δεδομένων β) τεχνικά μέτρα ασφαλείας αναφορικά με διαχείριση χρηστών, αναγνώριση, ασφάλεια, λειτουργία πληροφοριακού συστήματος. γ) μέτρα φυσικής ασφάλειας προσδιορίζοντας επακριβώς τον ρόλο κάθε εμπλεκόμενου εντός του Δήμου, τις αρμοδιότητες, τις ευθύνες και τα καθήκοντα που αφορούν την ασφάλεια.

Παραδοτέο:

Πλήρες κείμενο πολιτικής ασφάλειας

2.4 Συγγραφή σχεδίου ανάκαμψης από καταστροφές

Το σχέδιο ανάκαμψης από καταστροφές (disaster recovery and contingency plan) είναι το έγγραφο που αναφέρεται στα μέτρα προστασίας, ανάκαμψης και αποκατάστασης πληροφοριακών συστημάτων και τεχνολογικών υποδομών σε περίπτωση έκτακτης ανάγκης. Συμπληρώνει ή αποτελεί μέρος του σχεδίου ασφαλείας και ελέγχεται περιοδικά.

Παραδοτέο:

Πλήρες κείμενο σχεδίου ανάκαμψης από καταστροφές.

2.5 Έλεγχος και εφαρμογή μηχανισμού παραβιάσεων.

Έλεγχος υφιστάμενου ή εφαρμογή νέου μηχανισμού εντοπισμού παραβιάσεων (security Breaches) ή απλών περιστατικών ασφαλείας (security incident) με αυτόματη καταγραφή (Security log). Αποτελεί μέρος της υποχρεωτικής τεκμηρίωσης και απαραίτητο προαπαιτούμενο για την έγκαιρη αντίδραση σε κοινοποίηση παραβιάσεων.

Παραδοτέο: Πλήρες κείμενο εφαρμογής μηχανισμού παραβιάσεων

2.6 Κατάρτιση σχεδίου διαχείρισης συμβάντων
Το σχέδιο διαχείρισης συμβάντων είναι το έγγραφο που αναφέρεται στις διαδικασίες που θα ακολουθηθούν σε περίπτωση παραβίασης ασφαλείας. Περιγράφει δε και την κατάλληλη διαδικασία αναθεώρησής της.
Παραδοτέο:
Πλήρες κείμενο διαχείρισης συμβάντων

2.7 Κατάρτιση Σχεδίου αναγγελίας διαρροής στην Αρχή Προστασίας Προσωπικών Δεδομένων
Κατάρτιση σχεδίου ώστε να είναι δυνατή η αναγγελία της διαρροής εντός 72 ωρών, όπως προβλέπεται από τον κανονισμό.
Παραδοτέο:
Σχέδιο Αναγγελίας Διαρροής.

2.8 Δημιουργία αρχείου καταγραφής ενεργειών (Audit Log)
Αποτελεί σημαντικό αρχείο της τεκμηρίωσης της συμμόρφωσης ή της προόδου που έχει γίνει στην κατεύθυνση της συμμόρφωσης προς τις απαιτήσεις του κανονισμού. Περιλαμβάνει την καταγραφή των διαδικασιών συλλογής και επεξεργασίας των δεδομένων και το ποσοστό ολοκλήρωσης των διαφόρων σχεδίων.
Παραδοτέο:
Συλλογή αρχείων καταγραφής, αυτοματοποιημένων και μη.

2.9 Έλεγχος και προσαρμογή των συμβάσεων του οργανισμού εσωτερικά και με τρίτους
Γίνεται έλεγχος των υπαρχουσών συμβάσεων του Δήμου, τόσο με το προσωπικό όσο και με εξωτερικούς συνεργάτες. Όπου χρειάζεται γίνεται αναμόρφωσή τους. Όπου δεν υπάρχουν συγγράφονται νέες.
Παραδοτέο:
Αναμορφωμένες συμβάσεις και πρότυπα συμβάσεων προσαρμοσμένα στον κανονισμό.

2.10 Εκπαίδευση εργαζομένων
Εκπαίδευση εργαζομένων σε θέματα που αφορούν την τήρηση των προϋποθέσεων του κανονισμού. Δημιουργία κουλτούρας προστασίας προσωπικών δεδομένων.
Παραδοτέο:
Πρόγραμμα εκπαίδευσης ανά οργανωτική μονάδα με ορισμένο εκπαιδευτικό πρόγραμμα, υλικό και παρουσιολόγιο. Αποτελεί τμήμα της απαραίτητης για την συμμόρφωση τεκμηρίωσης.

2.11 Επαναξιολόγηση
Με την ολοκλήρωση του συνόλου των ενεργειών γίνεται επαναξιολόγηση του επιπέδου συμμόρφωσης του Δήμου.
Παραδοτέο:
Έκθεση επαναξιολόγησης

- **Υπηρεσίες Υπεύθυνου προστασίας δεδομένων DPO (Data ProtectionOfficer)**

Ορίζεται με ευθύνη του αναδόχου φυσικό πρόσωπο που θα διαθέτει την σχετική εκπαίδευση και Πιστοποίηση, ως Υπεύθυνος Προστασίας Δεδομένων του Δήμου. Εκτελεί όλα τα καθήκοντα του DPO σε όλο το χωρικό εύρος ανάπτυξης των υπηρεσιών του Δήμου, είναι προσβάσιμος από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα αλλά και από τα υποκείμενα των δεδομένων 24/365. **Οι υπηρεσίες του εξωτερικού DPO θα παρέχονται από τον ανάδοχο από την ημερομηνία υπογραφής της σύμβασης και για διάστημα 12 μηνών.**

- **Πιστοποίηση κατά ISO 27001**

Το πλέον διαδεδομένο και διεθνώς αναγνωρισμένο σήμερα πρότυπο για την ανάπτυξη συστημάτων διαχείρισης ασφάλειας πληροφοριών τα οποία είναι σε θέση να αντιμετωπίζουν αποτελεσματικά τους κινδύνους που διατρέχουν οι πληροφοριακοί πόροι ενός οργανισμού είναι το ISO 27001.
Η πιστοποίηση κατά ISO 27001 αποτελεί σήμερα την πιο σχετική πιστοποίηση που επιτρέπει σε επιχειρήσεις και φορείς να τεκμηριώνουν σε σημαντικό βαθμό τη συμμόρφωσή τους ως προς τις

απαιτήσεις του GDPR.
Ο ανάδοχος θα παρέχει στο Δήμο υπηρεσίες υποστήριξης στη σύνταξη πολιτικών και διαδικασιών για λήψη πιστοποίησης κατά ISO 27001.

Χρονοδιάγραμμα Υλοποίησης

Στάδια	**Εργασίες**	**Διάρκεια (Ημερολογιακοί μήνες)**
Στάδιο 1	**Στάδιο προετοιμασίας – αποτύπωση υφιστάμενης κατάστασης** 1.1 Δέσμευση Διοίκησης 1.2 Καταγραφή υπευθύνων ανά οργανωτική μονάδα 1.3 Καταγραφή διαθεσίμων φυσικών πόρων 1.4 Καταγραφή και χαρτογράφηση των δεδομένων προσωπικού χαρακτήρα που τηρούνται στο Δήμο, της επεξεργασίας και της κυκλοφορίας τους. 1.5 Προσδιορισμός Νομικής Βάσης – έλεγχος ορθότητας 1.6 Χαρτογράφηση του εγκατεστημένου πληροφοριακού συστήματος 1.7 Έλεγχος και αξιολόγηση πολιτικών και διαδικασιών. 1.8 Καταγραφή τεκμηρίωσης 1.9 Εκτίμηση κινδύνων για τις δραστηριότητες επεξεργασίας 1.10 Ανάπτυξη μεθοδολογίας για την διερεύνηση απαίτησης διεξαγωγής Μελέτης Εκτίμησης Αντικτύπου 1.11 Έκθεση αποκλίσεων από τον κανονισμό (Gap Analysis)	3 Μήνες
Στάδιο 2	**Στάδιο ολοκλήρωσης διαδικασίας συμμόρφωσης** 2.1 Προτεινόμενα μέτρα – Κατάρτιση σχεδίου συμμόρφωσης 2.2 Συγγραφή πολιτικών συλλογής, χρήσης, επεξεργασίας, αποθήκευσης, διόρθωσης, διαγραφής δεδομένων 2.3 Συγγραφή πολιτικής ασφάλειας 2.4 Συγγραφή σχεδίου ανάκαμψης από καταστροφές 2.5 Έλεγχος και εφαρμογή μηχανισμού παραβιάσεων 2.6 Κατάρτιση σχεδίου διαχείρισης συμβάντων 2.7 Κατάρτιση Σχεδίου αναγγελίας διαρροής στην Αρχή Προστασίας Προσωπικών Δεδομένων 2.8 Δημιουργία αρχείου καταγραφής ενεργειών (Audit Log) 2.9 Έλεγχος και προσαρμογή των συμβάσεων του οργανισμού εσωτερικά και με τρίτους 2.10 Εκπαίδευση εργαζομένων 2.11 Επαναξιολόγηση	
	Υπηρεσίες Υπεύθυνου προστασίας δεδομένων DPO (Data Protection Officer)	12 μήνες από την υπογραφή της σύμβασης
	Πιστοποίηση κατά ISO 27001	6 μήνες από την υπογραφή της σύμβασης

IV.ΕΛΑΧΙΣΤΕΣ ΠΡΟΫΠΟΘΕΣΕΙΣ ΣΥΜΜΕΤΟΧΗΣ – ΦΑΚΕΛΟΣ ΠΡΟΣΦΟΡΑΣ

Ο υποψήφιος ανάδοχος προκειμένου να αναλάβει την εργασία απαιτείται:

1. κατά τη διάρκεια της τελευταίας 2ετίας, να έχει εκτελέσει ή να εκτελεί τουλάχιστον 2 έργα που αφορούν το σύνολο του προγράμματος συμμόρφωσης GDPR σε εταιρείες ή οργανισμούς. Προς απόδειξη της εμπειρίας θα πρέπει να προσκομίσει υπεύθυνη δήλωση του Ν.1599/86 συμπληρωμένη από τον ανάδοχο στην οποία θα περιλαμβάνεται ένας πίνακας με τα εξής πεδία συμπληρωμένα για

κάθε σχετικό έργο: επωνυμία φορέα υλοποίησης, τίτλος έργου, περιεχόμενο έργου, χρονική διάρκεια (από – έως), υπεύθυνος φορέα και στοιχεία επικοινωνίας υπευθύνου.

2. Η προτεινόμενη ομάδα έργου του υποψηφίου αναδόχου θα πρέπει να περιλαμβάνει κατ' ελάχιστο:
   - Έναν (01) Data Protection Officer (DPO)
   - Έναν (01) Σύμβουλο ασφάλειας πληροφοριών
   - Έναν (01) Νομικό Σύμβουλο με αποδεδειγμένη εμπειρία σε νομικά θέματα προστασίας προσωπικών δεδομένων

Για την απόδειξη των ανωτέρω ο υποψήφιος ανάδοχος θα πρέπει να προσκομίσει τα αναλυτικά βιογραφικά των στελεχών που θα απαρτίσουν την ομάδα έργου του.

3. Στο φάκελο της προσφοράς να καταθέσει χρονοδιάγραμμα υλοποίησης εργασιών
4. Στο φάκελο της προσφοράς να καταθέσει έντυπο οικονομικής προσφοράς παρόμοιο με τον πίνακα ενδεικτικού προϋπολογισμού της παρούσας.

ΕΝΔΕΙΚΤΙΚΟΣ ΠΡΟΫΠΟΛΟΓΙΣΜΟΣ

Α/Α	**ΠΕΡΙΓΡΑΦΗ**	**ΜΟΝ. ΜΕΤΡ**	**ΠΟΣ.**	**ΤΙΜΗ ΜΟΝΑΔΑΣ**	**ΔΑΠΑΝΗ €**
1	Παροχή υπηρεσιών συμμόρφωσης, προσαρμογής και υποστήριξης ως προς τον Νέο Κανονισμό Προστασίας Προσωπικών Δεδομένων με αριθμ. 679/2016 (General Data Protection Regulation – GDPR) του Δήμου Σουφλίου και υπηρεσίες DPO για 12 μήνες	Υπηρεσία	1	19.354,84€	19.354,84€
				ΚΑΘΑΡΗ ΑΞΙΑ	**19.354,84€**
				Φ.Π.Α. 24%	**4.645,16€**
				ΣΥΝΟΛΟ:	**24.000,00€**

Σουφλί 01/08/2018

Συντάχθηκε

Κύρτσιου Τριανταφυλλιά
ΠΕ Πληροφορικής

Θεωρήθηκε
Ο Προϊστάμενος Διεύθυνσης
Διοικητικών & Οικονομικών Υπηρεσιών

Πιστόλας Νικόλαος

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΝΟΜΟΣ ΕΒΡΟΥ

ΔΗΜΟΣ ΣΟΥΦΛΙΟΥ

Αρ.Μελέτης: **68** /2018

Θέμα: «Παροχή υπηρεσιών συμμόρφωσης, προσαρμογής και υποστήριξης ως προς τον Νέο Κανονισμό Προστασίας Προσωπικών Δεδομένων με αριθμ. 679/2016 (General Data Protection Regulation – GDPR) του Δήμου Σουφλίου και υπηρεσίες DPO για 12 μήνες

Κ.Α. :10.6117.002
CPV : 79417000-0

ΓΕΝΙΚΗ ΣΥΓΓΡΑΦΗ ΥΠΟΧΡΕΩΣΕΩΝ

Άρθρο 1° : Αντικείμενο εργασιών.
Η παρούσα συγγραφή υποχρεώσεων αφορά την Παροχή υπηρεσιών συμμόρφωσης, προσαρμογής και υποστήριξης ως προς τον Νέο Κανονισμό Προστασίας Προσωπικών Δεδομένων με αριθμ. 679/2016 (General Data Protection Regulation – GDPR) του Δήμου Σουφλίου και υπηρεσίες DPO για 12 μήνες..

Άρθρο 2° : Ισχύουσες διατάξεις.
Για την εκτέλεση των υπηρεσιών της παρούσας μελέτης ισχύουν οι κάτωθι διατάξεις:

- τις διατάξεις του Ν. 3852/2010 (ΦΕΚ Α΄ 87) «Νέα Αρχιτεκτονική της Αυτοδιοίκησης και της Αποκεντρωμένης Διοίκησης – Πρόγραμμα Καλλικράτης».
- Το Ν. 3463/2006 (Κώδικας Δήμων και Κοινοτήτων) και ιδιαίτερα των άρθρων 103 και 209, όπως αναδιατυπώθηκε με την παρ. 3 του άρθρου 22 του ν. 3536/2007.
- Το Ν. 4412/2016 «Δημόσιες Συμβάσεις Έργων, Προμηθειών & Υπηρεσιών»(προσαρμογή στις οδηγίες 2014/14/ΕΕ και 2014/25/ΕΕ).

Άρθρο 3ο : Συμβατικά στοιχεία
Τα συμβατικά στοιχεία κατά σειρά ισχύος είναι:
α. Ο προϋπολογισμός της μελέτης
β. Η συγγραφή υποχρεώσεων
γ. Τεχνική περιγραφή - Προδιαγραφές

Άρθρο 4ο : Χρόνος εκτέλεσης εργασιών
Οι αναφερόμενες στην παρούσα μελέτη εργασίες παροχής υπηρεσιών θα ξεκινήσουν να εκτελούνται τμηματικά σύμφωνα με το χρονοδιάγραμμα και η έναρξη ισχύος της σύμβασης θα είναι **άμεση** κατόπιν υπογραφής της, από τα δύο συμβαλλόμενα μέρη.

Άρθρο 5ο : Υποχρεώσεις του αναδόχου
Πριν την υπογραφή της σύμβασης ο ανάδοχος υποχρεούται να καταθέσει εγγυητική επιστολή καλής εκτέλεσης που ορίζεται σε ποσοστό 5% της αξίας της σύμβασης χωρίς Φ.Π.Α. και θα ισχύει για (1) χρόνο από την υπογραφή της σύμβασης.
Επιστρέφεται δε μετά το πέρας της ισχύος της σύμβασης και την υλοποίηση-ολοκλήρωση των υπηρεσιών.
Παράλληλα είναι υποχρεωμένος να συγκροτήσει τα συνεργεία διεξαγωγής της εργασίας και ευθύνεται για την ακρίβεια των στοιχείων και για την καλή και σωστή εκτέλεση της εργασίας.

Άρθρο 6ο : Υποχρεώσεις του εντολέα
Είναι υποχρεωμένος για την παροχή όλων των μέσων και στοιχείων τα οποία κρίνονται απαραίτητα για την υλοποίηση της ανατιθέμενης εργασίας.

Άρθρο 7ο : Ανωτέρα βία
Ως ανωτέρα βία θεωρείται κάθε απρόβλεπτο και τυχαίο γεγονός που είναι αδύνατο να προβλεφθεί έστω και εάν για την πρόβλεψη και αποτροπή της επέλευσης του καταβλήθηκε υπερβολική

επιμέλεια και επιδείχθηκε η ανάλογη σύνεση. Ενδεικτικά γεγονότα ανωτέρας βίας είναι : εξαιρετικά και απρόβλεπτα φυσικά γεγονότα, πυρκαγιά που οφείλεται σε φυσικό γεγονός ή σε περιστάσεις για τις οποίες ο εντολοδόχος ή ο εντολέας είναι ανυπαίτιοι, αιφνιδιαστική απεργία προσωπικού, πόλεμος, ατύχημα, αιφνίδια ασθένεια του προσωπικού του εντολοδόχου κ.α. στην περίπτωση κατά την οποία υπάρξει λόγος ανωτέρας βίας ο εντολοδόχος οφείλει να ειδοποιήσει αμελλητί τον εντολέα και να καταβάλει κάθε δυνατή προσπάθεια σε συνεργασία με το άλλο μέρος για να υπερβεί τις συνέπειες και τα προβλήματα που ανέκυψαν λόγω της ανωτέρας βίας.
Ο όρος περί ανωτέρας βίας εφαρμόζεται ανάλογα και για τον εντολέα προσαρμοζόμενος ανάλογα.

Άρθρο 8ο : Τρόπος πληρωμής
Με την ολοκλήρωση της διαδικασίας συμμόρφωσης και τη συμμόρφωση του Δήμου, (Στάδια 1 και 2) θα καταβληθεί το 70% της συνολικής δαπάνης, ενώ το υπόλοιπο 30% θα καταβληθεί με την ολοκλήρωση του συνόλου των υποχρεώσεων του αναδόχου. Η καταβολή των ανωτέρω ποσών γίνεται ύστερα από έκδοση σχετικού δελτίου παροχής υπηρεσιών του αναδόχου, τη σύνταξη βεβαίωσης καλής εκτέλεσης εργασιών από το Δήμο και την έκδοση σχετικών ενταλμάτων πληρωμής.
Στο ποσό της αμοιβής συμπεριλαμβάνονται οι βαρύνοντες τον εντολοδόχο φόροι και βάρη. Η αμοιβή δεν υπόκειται σε καμία αναθεώρηση για οποιοδήποτε λόγο και αιτία και παραμένει σταθερή και αμετάβλητη καθ' όλη την διάρκεια ισχύος της εντολής.

Άρθρο 9ο : Φόροι, τέλη, κρατήσεις
Ο εντολοδόχος σύμφωνα με τις ισχύουσες διατάξεις βαρύνεται με όλους ανεξαιρέτως τους φόρους, τέλη, δασμούς και εισφορές υπέρ του δημοσίου, δήμων και κοινοτήτων ή τρίτων που ισχύουν κατά την ημέρα της δημοπρασίας.

Άρθρο 10ο : Επίλυση διαφορών
Οι διαφορές που θα εμφανισθούν κατά την εφαρμογή της σύμβασης, επιλύονται σύμφωνα με τις ισχύουσες διατάξεις.

Σουφλί 01/08/2018

Συντάχθηκε	**Θεωρήθηκε**
	Ο Προϊστάμενος Διεύθυνσης Διοικητικών & Οικονομικών Υπηρεσιών
Κύρτσιου Τριανταφυλλιά ΠΕ Πληροφορικής	Πιστόλας Νικόλαος