ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΝΟΜΑΡΧΙΑ ΑΘΗΝΩΝ
ΔΗΜΟΣ ΑΓΙΑΣ ΒΑΡΒΑΡΑΣ

ΤΙΤΛΟΣ: «Υπηρεσίες Υποστήριξης του Δήμου Αγίας Βαρβάρας για την προετοιμασία και προσαρμογή στο νέο κανονισμό προστασίας δεδομένων (ΕΕ 2016/679)»

ΜΕΛΕΤΗ: «Παροχή υπηρεσιών για τη διαδικασία συμμόρφωσης στο Γενικό Κανονισμό Προστασίας Δεδομένων (ΕΕ 679/2016)»

ΕΝΔΕΙΚΤΙΚΟΣ ΠΡΟΫΠΟΛΟΓΙΣΜΟΣ	**ΤΙΜΗ (€)**
Παροχή υπηρεσιών υποστήριξης, συμμόρφωσης και προσαρμογής στον νέο κανονισμό προστασίας προσωπικών δεδομένων	12.400 ευρώ
Παροχή υπηρεσιών προστασίας προσωπικών δεδομένων από την υπογραφή της σύμβασης και μέχρι το τέλος του τρέχοντος έτους (31/12/2019)	5.000 ευρώ
ΦΠΑ 24%	4.176 ευρώ
ΤΕΛΙΚΟ ΣΥΝΟΛΟ	**21.576 ευρώ**

Περιεχόμενα

ΤΕΧΝΙΚΗ ΕΚΘΕΣΗ

Εισαγωγή

Η παρούσα τεχνική έκθεση αφορά την ανάθεση σε Ανάδοχο της διαδικασίας συμμόρφωσης του δήμου **Αγίας Βαρβάρας** στο «Γενικό Κανονισμό Προστασίας Δεδομένων» (ΓΚΠΔ-GDPR), (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

Η παρούσα τεχνική περιγραφή έχει συνταχθεί σύμφωνα με τις διατάξεις των άρθρων 58 και 72 του Ν. 3852 /2010, άρθρων 38, 72 και 118 του Ν. 4412/2016, παρ. 9 του άρθρου 209 του Ν. 3463/2006, όπως προστέθηκε με την παρ. 13 του άρθρου 20 του Ν. 3731/2008 και διατηρήθηκε σε ισχύ με την περίπτωση 38 της παρ. 1 του άρθρου 377 του Ν. 4412 /2016, την παρ. 4 του άρθρου 209 του Ν. 3463/2006, όπως αναδιατυπώθηκε με την παρ. 3 του άρθρου 22 του Ν. 3536/2007, το Ν. 3861/2010 Φ.Ε.Κ. 112Α/13-7-2010, το Ν. 4013/2011 «Σύσταση ενιαίας Ανεξάρτητης Αρχής Δημοσίων Συμβάσεων και Κεντρικού Ηλεκτρονικού Μητρώου Δημοσίων Συμβάσεων» όπως τροποποιήθηκε και ισχύει , τις διατάξεις του Ν. 4250/2014, άρθρο 1 παρ. 2 «Διοικητικές Απλουστεύσεις – Καταργήσεις, Συγχωνεύσεις Νομικών Προσώπων και Υπηρεσιών του Δημοσίου Τομέα – Τροποποίηση Διατάξεων του Π. . 318/1992 (Α' 161) και λοιπές ρυθμίσεις» και το Π. . 80/2016 «Ανάληψη υποχρεώσεων από τους Διατάκτες» (ΦΕΚ 145/Α'/5-8-2016).

Ο «Γενικός Κανονισμός Προστασίας Δεδομένων» (ΓΚΠΔ-GDPR), ΕΕ 2016/679, 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. Ο Κανονισμός απέκτησε τυπική ισχύ 20 ημέρες μετά τη δημοσίευσή του στην Επίσημη Εφημερίδα της ΕΕ και τέθηκε σε ισχύ στα κράτη μέλη, στις 25 Μαΐου 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 Κανονισμός έχει σχεδιαστεί κατά τέτοιο τρόπο ώστε να δώσει στους πολίτες μεγαλύτερο έλεγχο των προσωπικών τους στοιχείων.

Τα βασικά στοιχεία του Κανονισμού που έχουν εφαρμογή είναι τα εξής:

- **Δικαίωμα στη λήθη**: Όταν εκλείπει ο λόγος της επεξεργασίας των δεδομένων ή το υποκείμενο αίρει τη 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 τη διαγραφή των δεδομένων και ο υπεύθυνος επεξεργασίας έχει υποχρέωση άμεσα να τα διαγράψει και αν τα έχει δημοσιοποιήσει να ενημερώσει και όλους όσους τα έχουν αναδημοσιεύσει ότι το υποκείμενο ζήτησε τη διαγραφή τους.

- **Σαφής συγκατάθεση**: Το κάθε άτομο (ενδιαφερόμενο πρόσωπο) πρέπει να δώσει τη 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 για την παραβίαση της ασφάλειας του συστήματος οφείλει να ειδοποιήσει την ανεξάρτητη Αρχή 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 (*παρ. 4, 5 & 6 του άρθρου 83 του κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016*).

- **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 ζημίας 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 μία διαδικασία για τη διεξαγωγή μίας αξιολόγησης του κινδύνων προστασίας των δεδομένων (Data Protection Impact Assessment) σε όλες τις επιχειρησιακές μονάδες.

Αντικείμενο της υπηρεσίας

Με την παρούσα μελέτη προβλέπεται η παροχή υπηρεσιών συμμόρφωσης, προσαρμογής και υποστήριξης ως προς τον Νέο Κανονισμό Προστασίας Προσωπικών Δεδομένων της Ε/Ε με αριθμό 679/2016 (General Data Protection Regulation – GDPR).

Αντικείμενο του έργου που περιγράφεται στην παρούσα μελέτη, είναι το σύνολο των υπηρεσιών και ενεργειών που θα οδηγήσουν στη συμμόρφωση του δήμου στις επιταγές του νέου Ευρωπαϊκού Κανονισμού για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και θα περιλαμβάνει:

1. Αξιολόγηση όλων των τομέων δραστηριότητας του δήμου και όλων των τμημάτων και διευθύνσεών του, ως προς την ετοιμότητά τους έναντι του GDPR για όλους τους τύπους /μορφές στους οποίους αφορούν τα προσωπικά δεδομένα του κανονισμού.
2. Εντοπισμό των κενών και των ελλείψεων που πρέπει να καλυφθούν.
3. Πρόταση των αναγκαίων τεχνικών και οργανωτικών μέτρων, με κατάρτιση σχεδίου ενεργειών συμμόρφωσης, διενέργεια εκτίμησης αντικτύπου (DPIA), όπου αυτό χρειάζεται, και πρόταση σχεδιασμού της απαραίτητης τεκμηρίωσης.
4. Υπηρεσίες Υπεύθυνου Προστασίας Δεδομένων (DPO) από την υπογραφή του έργου μέχρι την ολοκλήρωση του (31/12/2019)

Η παροχή των παραπάνω υπηρεσιών, να πραγματοποιηθεί βασισμένη σε δοκιμασμένες διαδικασίες και τεχνικές, με ακριβή καθορισμό παραδοτέων και χρονοδιαγραμμάτων που θα διασφαλίσουν το άρτιο αποτέλεσμα.

Οι μελέτες που θα διενεργηθούν στο πλαίσιο του έργου θα καταγράψουν τις απαιτήσεις ασφάλειας που αρμόζουν στον οργανισμό, να αναδείξουν τις παρούσες παθογένειες των υφιστάμενων υπηρεσιών-υποδομών και να προσδιορίσουν τις ευρέως καταξιωμένες βέλτιστες πρακτικές για την πρόληψη, αποτροπή και αντιμετώπιση παραβιάσεων ασφάλειας.

Σκοπός και Αναγκαιότητα της Υπηρεσίας

Σκοπός της πρότασης αυτής είναι η παροχή υπηρεσιών εναρμόνισης, συμμόρφωσης και προσαρμογής προς τον με αριθ. 679/2016 Κανονισμό Προστασίας Δεδομένων Προσωπικού Χαρακτήρα της Ε.Ε. (GDPR). Η εναρμόνιση και η συμμόρφωση του δήμου οριοθετείται από δύο άξονες γνωστικών και διαδικαστικών προτύπων: Τον άξονα της Νομικής Εναρμόνισης και τον άξονα της Λειτουργικής Εναρμόνισης

Η **Νομική Εναρμόνιση** αφορά την αξιολόγηση των Συμβάσεων, των εντύπων και των πρακτικών διαδικασιών βάση των οποίων καθορίζονται οι σχέσεις του δήμου με τα Υποκείμενα Δεδομένων (Εργαζόμενοι, Δημότες, Προμηθευτές, Εξωτερικοί Συνεργάτες και λοιποί).

Ακολουθεί τον Ευρωπαϊκό Κανονισμό λαμβάνοντας όμως υπόψη τις προβλέψεις του Εθνικού Νομοσχεδίου παρότι αυτό δεν έχει ακόμη γίνει νόμος του Κράτους. Σε κάθε περίπτωση τα τελικά παραδοτέα θα είναι εναρμονισμένα με τις τυχόν αλλαγές οι οποίες θα περιλαμβάνονται στο τελικό κείμενο του Νόμου.

Συμβουλευτική Διαχείριση Συμμόρφωσης Προσωπικού με βάση το Εργατικό Δίκαιο και ειδικότερα των περιπτώσεων άρνησης συμμόρφωσης.

Η **Λειτουργική Εναρμόνιση** αφορά τις διαδικασίες Επεξεργασίας και διασφάλισης των Δεδομένων Προσωπικού Χαρακτήρα εντός της ημερήσιας πρακτικής λειτουργίας του δήμου. Ως πρότυπο Ανάλυσης και Σχεδιασμού Διαδικασιών ακολουθείται το πρότυπο διαδικασιών **ISO 27001** περί Προστασίας Πληροφοριών το οποίο είναι πλέον συμβατό με την ανάγκη της Ενδεδειγμένης Προστασίας των Προσωπικών Δεδομένων (άρθρο 5, 25γ,41,42,43 GDPR).

Εγχειρίδιο Επεξεργασίας/Προστασίας προσωπικών Δεδομένων Κώδικας/Κανονισμός Δεοντολογίας, Μελέτη Επιπτώσεων, Μητρώο Διαδικασιών, Εντύπων, Σημείων Επεξεργασίας, Σχέδιο Δράσης		
Νομική Εναρμόνιση		**Λειτουργική Εναρμόνιση**
Εγγραφή στην Αρχή Προστασίας		Νοοτροπία ασφάλειας
Συμβάσεις εργαζομένων		Κανονισμός Επικοινωνίας
Συμβάσεις Πελατών		Ατομική ευθύνη διαχείρισης πληροφορίας
Συναίνεση υποκειμένων		Διαδικασίες προστασίας προσωπικών δεδομένων

Αναλυτική περιγραφή των απαιτούμενων ενεργειών.

Το πλαίσιο των υπηρεσιών που πρέπει να προσφέρει ο ανάδοχος είναι αναλυτικά:

Προετοιμασία έργου – Ενημέρωση προσωπικού (ευαισθητοποίηση) – Οργάνωση έργου και ομάδας έργου.

Αποτύπωση της υπάρχουσας κατάστασης, ως προς την επεξεργασία δεδομένων που λαμβάνει χώρα στο φορέα μας, τα είδη των δεδομένων και των υποκειμένων τους, τις ροές των δεδομένων, τις υφιστάμενες πρακτικές, διαδικασίες και πολιτικές του φορέα, τη δυναμική των φυσικών πόρων του φορέα, τη δυναμική των τεχνικών πόρων του φορέα και τα εφαρμοζόμενα μέτρα προστασίας.

Διεξαγωγή αξιολόγησης – αποτίμησης της ασφάλειας του πληροφοριακού συστήματος του οργανισμού σε όλο το εύρος της δικτυακής υποδομής, που περιλαμβάνει συστήματα, δικτυακό εξοπλισμό, εφαρμογές, δεδομένα και υπηρεσίες. Η αξιολόγηση – αποτίμηση θα αφορά το σύνολο των υποδομών και των υπηρεσιών που παρέχει ο οργανισμός μας.

Σύνταξη έκθεσης, η οποία - λαμβάνοντας υπόψη τα αποτελέσματα της αποτύπωσης της κατάστασης - να προτείνει **εξατομικευμένο σχέδιο συμμόρφωσης**, όπου να περιγράφονται τα προτεινόμενα μέτρα προς συμμόρφωση με τον Κανονισμό, οι διορθωτικές κινήσεις που πρέπει να γίνουν, τα σημεία αναπροσαρμογής, οι νέες εφαρμοστέες διαδικασίες, η ενίσχυση με περαιτέρω τεχνικά ή οργανωτικά μέτρα, οι τρόποι υλοποίησης, τα χρονοδιαγράμματα και πιθανές εναλλακτικές.

Υπηρεσίες Υπευθύνου Προστασίας Δεδομένων (DPO) από την υπογραφή της σύβασης μέχρι την ολοκλήρωση του έργου.

Διαδικασία υλοποίησης υπηρεσιών- <u>ΠΑΡΑΔΟΤΕΑ</u>

Η ολοκλήρωση της παρούσας Υπηρεσίας καταλήγει στην δημιουργία του Εγχειριδίου Προστασίας Προσωπικών Δεδομένων το οποίο αποτελείται από το σύνολο των παρακάτω παραδοτέων.

1. Σύνταξη Κανονισμού Δεοντολογίας και Πολιτική Προστασίας ΔΠΧ (άρθρο 41 GDPR)
2. Σύνταξη Μητρώου Διαδικασιών στα πλαίσια του Γενικού Κανονισμού (Εγχειρίδιο)
3. Μητρώο Σημείων Επεξεργασίας

4. Μητρώο πρότυπων Εντύπων για κάθε χρήση σχετικά με την εφαρμογή του Γενικού Κανονισμού
5. Μελέτη Κινδύνων Παραβίασης Δεδομένων και Αντίκτυπος αυτών
6. Σχέδιο Δράσης για την Λειτουργική Εναρμόνιση στα πρότυπα του ISO 27001
7. Εκπαιδευτικό Υλικό για νεοεισερχόμενους εργαζομένους
8. Παρουσίαση Έργου στα διευθυντικά στελέχη του δήμου Αγ. Βαρβάρας.

5. Σύμφωνα με τις απαιτήσεις του Κανονισμού Προστασίας Προσωπικών Δεδομένων, οι υπηρεσίες που θα παρασχεθούν αφορούν στα παρακάτω:

- Κατάλληλη εκπαίδευση για το ανθρώπινο δυναμικό του δήμου
- Κατάλληλα μέτρα ασφαλείας και απαραίτητες πολιτικές για την προστασία των πληροφοριών
- Συγκεκριμένες αναλύσεις των επιπτώσεων που μπορούν να προκύψουν λόγω παραβίασης ιδιωτικότητας (Privacy Impact Assessment)
- Ενημέρωση στις Αρμόδιες Αρχές εντός 72 ωρών από τον εντοπισμό συμβάντος παραβίασης συστημάτων και απώλειας δεδομένων
- Ειδικό πλάνο αντιμετώπισης περιστατικών παραβίασης συστημάτων και απώλειας δεδομένων
- (Incident Response Plan)
- Εγγύηση ανάληψης ευθύνης κάθε ζημίας, απώλειας, κόστους και δαπάνης που μπορεί να υποστεί ο δήμος στην περίπτωση που υπάρξει αποτυχία στην επισήμανση κινδύνου και στις πρακτικές οι οποίες μπορεί να οδηγήσουν σε παραβίαση των διατάξεων του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων

Πλάνο Υλοποίησης

Στάδιο 1ο: Ενημέρωση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

- Εγγραφή του δήμου στο Μητρώο Υπεύθυνων Επεξεργασίας της Ανεξάρτητης Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και ορισμός προσωρινού Υπεύθυνου Προστασίας Δεδομένων έτσι ώστε να διασφαλίζεται άμεσα η Νομιμότητα Λειτουργίας του δήμου.

Η ενέργεια αυτή πραγματοποιείται την επόμενη ημέρα από την ανάθεση του έργου. Στο τέλος της ενημέρωσης θα εκπονηθεί σχετικό πρακτικό με τα αποτελέσματα υλοποίησης του 1ου σταδίου.

Στάδιο 2ο: Συντονισμός και προγραμματισμός έργου

- Παρουσιάζονται στη Διοίκηση και τα στελέχη οι απαιτήσεις του Κανονισμού.
- Ορίζονται ονομαστικά τα άτομα κομβικής σημασίας στην λειτουργία του δήμου.
- Ορίζεται χώρος εργασίας για την ομάδα εργασίας του Ανάδοχου και του εξοπλισμού της.
- Ορίζεται το χρονοδιάγραμμα εργασίας και η ημερομηνία έναρξης.
- Κατά την σύσκεψη αυτή θα μελετηθεί το Οργανόγραμμα του δήμου και θα παραληφθεί κατάλογος εργαζομένων ανά τμήμα προκειμένου να σχεδιασθεί αναλυτικά και εξαντλητικά ο σχεδιασμός της υλοποίησης του έργου.
- Ορισμός Υπεύθυνου Έργου εντός του δήμου. Για την εύρυθμη συνεργασία των δύο μερών θα ορισθεί ένας Υπεύθυνος έργου ο οποίος θα είναι ενημερωμένος για όλη την εξέλιξη του έργου.

Πριν την έναρξη των επόμενων Σταδίων θα αποσταλεί προς την Διοίκηση του δήμου και τον Υπεύθυνο του έργου **Πίνακας Προγράμματος Δράσης** βασισμένος σε συγκεκριμένες ώρες και ημέρες προκειμένου να καλυφθούν οι ανάγκες του δήμου σε σχέση και με τις διαφορετικές ώρες εργασίας.

Στάδιο 3ο : Αποτύπωση Υφιστάμενης Κατάστασης σε Διευθυντικό Επίπεδο

Η μέθοδος Αποτύπωσης Υφιστάμενης Κατάστασης σε Διευθυντικό Επίπεδο αποτελείται από τις εξής ενέργειες:

- Συνέντευξη με κάθε Εργαζόμενο Κομβικής Σημασίας (Προϊστάμενοι, Γραμματείς κλπ.) και με χρήση ειδικού ερωτηματολογίου για κάθε κατηγορία θέσεις εργασίας, πχ Μηχανογράφηση, Λογιστήριο, κλπ.
- Παραλαβή προτύπων εντύπων και συμβάσεων βάση των οποίων ο δήμος ορίζει τις σχέσεις συνεργασίας και συναλλαγής με Εργαζόμενους, Πολίτες, Προμηθευτές και Εξωτερικούς Συνεργάτες.

- Απογραφή Σημείων Επεξεργασίας Πληροφοριών για κάθε θέση Εργασίας και εφαρμογή μοναδικού κωδικού για την αναγνώριση του Σημείου. (Η/Υ, Φωριαμός, Χώρος, Είσοδος κλπ.)
- Δειγματολογική Αξιολόγηση των Πληροφοριακών Συστημάτων προκειμένου να συνταχθεί σχέδιο δράσης για την διασφάλιση της πληροφορίας η οποία παράγεται από τα συστήματα.
- Αποστολή Πρότυπων εντύπων στο Νομικό Τμήμα του Ανάδοχου για την αξιολόγηση και συμμόρφωση προς των Κανονισμό
- Αποτύπωση των παραπάνω σε ηλεκτρονική μορφή και αποστολή προς έγκριση στους αρμόδιους.

Στάδιο 4ο: Ενημέρωση εργαζομένων

Η ενημέρωση όλων των εργαζομένων, ανεξαρτήτων ειδικοτήτων, αποτελεί σημαντική προτεραιότητα τόσο κατά τον Ευρωπαϊκό Κανονισμό όσο και ως πρόβλεψη στο Ελληνικό Νομοσχέδιο. Η ενημέρωση γίνεται με προβαλλόμενες διαφάνειες σε κατάλληλη αίθουσα του δήμου και σε μέγιστο αριθμό 30 ατόμων. Η συμμετοχή των εργαζομένων βεβαιώνεται με την υπογραφή τους στο κατάλληλο έντυπο παρόντων το οποίο προσκομίζει ο Ανάδοχος.
Η διάρκεια ενημέρωσης είναι 2 ώρες και το ωράριο ορίζεται αποκλειστικά και μόνο από την διοίκηση του δήμου με γνώμονα την εύρυθμη λειτουργία του και την διευκόλυνση των βαρδιών. Το υλικό της ενημέρωσης θα συμπεριληφθεί στο Εγχειρίδιο σε έντυπη μορφή έτσι ώστε να βρίσκεται στην διάθεση του δήμου αλλά και στο υλικό εκπαίδευσης νέων εργαζομένων.
Για τους εργαζόμενους οι οποίοι απουσιάζουν λόγω άδειας ή άλλων ανειλημμένων υποχρεώσεων προβλέπεται εκπαίδευση με ηλεκτρονικό τρόπο έτσι ώστε να επιβεβαιώνεται η συμμετοχή τους και να εκπληρώνεται η υποχρέωση του δήμου.

Στάδιο 5ο: Διενέργεια Ελέγχων Αντοχής Πληροφοριακών Συστημάτων σε Κακόβουλες Επιθέσεις

Ο έλεγχος υλοποιείται σε συνεργασία με εξειδικευμένη εταιρεία κυβερνοασφάλειας και σε συνεργασία με τους υπεύθυνους του δήμου. Τα αποτελέσματα αποτελούν ένα κατάλογο πιθανόν αδυναμιών του συστήματος και οδηγούν στην σύνταξη ενός σχεδίου δράσης για την αντιμετώπιση και επίλυση τους.

Στάδιο 6ο: Αποτύπωση Υφιστάμενης Κατάστασης σε Επίπεδο Θέσης εργασίας βάσης

Η μέθοδος Αποτύπωσης Υφιστάμενης Κατάστασης σε Επίπεδο θέσης εργασίας βάσης αποτελείται από τις εξής ενέργειες:

- Συνέντευξη με κάθε Εργαζόμενο σχετικά με τις ημερήσιες διαδικασίες και καθήκοντα εργασίας στα οποία εμπεριέχεται άμεση ή έμμεση Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα
- Παραλαβή προτύπων εντύπων και συμβάσεων βάση των οποίων ο δήμος ορίζει τις σχέσεις συνεργασίας και συναλλαγής με Εργαζόμενους Δημότες, Προμηθευτές και Εξωτερικούς Συνεργάτες.
- Απογραφή Σημείων Επεξεργασίας Πληροφοριών για κάθε θέση Εργασίας και εφαρμογή μοναδικού κωδικού για την αναγνώριση του Σημείου. (Η/Υ, Φωριαμός, Χώρος, Είσοδος κλπ.)
- Αποστολή Πρότυπων εντύπων στο Νομικό Τμήμα του Ανάδοχου για την αξιολόγηση και συμμόρφωση προς των Κανονισμό.
- Αποτύπωση των παραπάνω σε ηλεκτρονική μορφή και αποστολή προς έγκριση στους αρμόδιους.

Τα παραπάνω Στάδια 2 έως 6 υλοποιούνται στην έδρα του δήμου από πολυμελή ομάδα εργασίας και για αριθμό ημερών ανάλογο των απαιτούμενων ωρών εργασίας.

Στάδιο 7ο: Υλοποίηση και Παρουσίαση Παραδοτέων

1. ***Κανονισμός Δεοντολογίας και Πολιτική Προστασίας ΔΠΧ (άρθρο 41 GDPR)***
   - ✓ Σύνταξη Κανονισμού Δεοντολογίας για τα δικαιώματα των Εργαζομένων στην σχέση τους με το δήμο και την διασφάλιση των Προσωπικών τους Δεδομένων
   - ✓ Σύνταξη Κανονισμού Δεοντολογίας ο οποίος θα καθορίζει τις ευθύνες και τις Υποχρεώσεις των Εργαζομένων απέναντι στους άλλους εργαζομένους, στο δήμο, τους Δημότες, τους προμηθευτές και τους Εξωτερικούς Συνεργάτες σε θέματα επικοινωνίας και διασφάλισης πληροφοριών και πόρων του δήμου
   - ✓ Σύνταξη κειμένου με τους Όρους τους οποίους ακολουθεί ο δήμος για την Επεξεργασία των Δεδομένων ΠΧ απέναντι σε Φυσικά Πρόσωπα εκτός του δήμου.

2. ***Ενημέρωση Προσωπικού με υποχρεωτική συμμετοχή σε ομάδες εργασίας***

Η ενημέρωση του Προσωπικού είναι ύψιστη προτεραιότητα και έχει υλοποιηθεί στο 3ο Στάδιο. Για όσους εργαζόμενους δεν συμμετείχαν στην παρουσίαση η οποία διεξάχθηκε στις εγκαταστάσεις του δήμου θα αποσταλεί προσωποποιημένη πρόσκληση συμμετοχής σε εκπαίδευση με ηλεκτρονικό τρόπο (e-learning) .

Σε περίπτωση κατά την οποία ένας εργαζόμενος αρνηθεί να συμμετάσχει το θέμα παραπέμπεται στην νομική υπηρεσία του Ανάδοχου η οποία στελεχώνεται από Εξειδικευμένη Εργατολόγο για περαιτέρω ενέργειες.

3. *Εγχειρίδιο Διαδικασιών*

Οι διαδικασίες οι οποίες έχουν χαρτογραφηθεί, καταγραφεί και εγκριθεί στα παραπάνω Στάδια περιλαμβάνονται σε πίνακα με την μορφή : Θέση Εργασίας, Χειριστές, Υποκείμενα, Νομική βάση, Αποδέκτης, Χρονική Διάρκεια, Σημείο Επεξεργασίας.

Με τον τρόπο αυτό η διοίκηση έχει μια αναλυτική και πλήρη εικόνα της Επεξεργασίας (Συλλογή, Κοινολόγηση, Μεταβίβαση, Αρχειοθέτηση κλπ.) η οποία διεξάγεται στην καθημερινότητα του δήμου.

Η ανάλυση του πίνακα αυτού παράγει τους παρακάτω πίνακες:

i. Κατάλογος διαδικασιών και νομικής βάσης τους
ii. Ροή διαδικασιών και εμπλεκόμενες θέσεις εργασίας
iii. Κατάλογος Σημείων Επεξεργασίας Πληροφορίας

4. Μητρώο Σημείων Επεξεργασίας

Κάθε χώρος, φυσικό ή ηλεκτρονικό αρχείο και τα μέσα στα οποία αυτά βρίσκονται καταγράφονται και κωδικοποιούνται όπως έχει περιγράφει στο Στάδιο 3 και 6. Η κωδικοποίησή τους είναι απαραίτητη για την υποστήριξη του έργου των συστηματικών επιθεωρήσεων από τον Υπεύθυνο Προστασίας Δεδομένων και της Διοίκησης για την υλοποίηση του Σχεδίου Δράσης περί της Προστασίας των Δεδομένων.

5. Μητρώο Πρότυπων Εντύπων για κάθε χρήση σχετικά με την εφαρμογή του Γενικού Κανονισμού

Τα έντυπα τα οποία χρησιμοποιεί ήδη ο δήμος στην σχέση του με τα Υποκείμενα αλλά και όσα θα δημιουργηθούν για την Νομική Εναρμόνιση του, να κωδικοποιούνται με βάση την πρακτική των Προτύπων Διαδικασιών τύπου ISO έτσι ώστε να μένουν αναλλοίωτα στην αντιγραφή και επεξεργασία τους από τους εργαζόμενους του δήμου.

Στο Μητρώο Πρότυπων Εντύπων περιλαμβάνονται το σύνολο των κειμένων τα οποία σχετίζονται με την Προστασία των Προσωπικών Δεδομένων συμπεριλαμβανομένων των όρων Πολιτικής Απορρήτου, Πολιτική cookies κλπ.

Το Μητρώο Πρότυπων Εντύπων αποτελείται από τα εξής:

- Πίνακα της μορφής : Τίτλος Εντύπου, Περιγραφή Περιεχομένου, Κωδικός, Τελευταία Ενημέρωση
- Φυσικό αρχείο το οποίο συμπεριλαμβάνεται στο Εγχειρίδιο Επεξεργασίας Προσωπικών Δεδομένων και περιλαμβάνει τα έντυπα σε φυσική μορφή με την φόρμα τυποποίηση τους στην πρώτη σελίδα

- Ηλεκτρονικό αρχείο το οποίο τοποθετείται από τους υπεύθυνους του δήμου σε κοινόχρηστο ηλεκτρονικό φάκελο προκειμένου να έχουν πρόσβαση σε αυτό οι αρμόδιοι εργαζόμενοι. Τα αρχεία είναι σε μορφή πρότυπο MS Word (.dotx) προκειμένου να παραμένουν αναλλοίωτα κατά την αναπαραγωγή τους.

6. Μελέτη Κινδύνων Παραβίασης Δεδομένων και Αντίκτυπος αυτών

Σύμφωνα με το άρθρο 35 του Γενικού Κανονισμού η εκτίμηση κινδύνου περιλαμβάνει τουλάχιστον τα εξής:

i. Συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών επεξεργασίας περιλαμβανομένων κατά περίπτωση του έννομου συμφέροντος που επιδιώκει ο δήμος.

ii. Εκτίμηση της Αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς.

Τα άρθρα (i) και (ii) καλύπτονται από τις εργασίες των Σταδίων **4, 6** και σε συνέπεια με τη σύνταξη του Εγχειριδίου Διαδικασιών στο Στάδιο **7.3**.

iii. Εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων.

Η εκπλήρωση του άρθρου αυτού πραγματοποιείται με την ευθύνη του Υπεύθυνου Προστασίας Δεδομένων ο οποίος και συντάσσει το έντυπο Παραγγελία Εναρμόνισης για κάθε διαδικασία η οποία έχει καταγραφεί στο Εγχειρίδιο των Διαδικασιών. (*Παραδοτέο 3, εργασία του Σταδίου 7.3*)

iv. Προβλεπόμενα μέτρα αντιμετώπισης κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφαλείας, ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα και να αποδεικνύεται η συμμόρφωση προς τον Γενικό Κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των Υποκειμένων και άλλων ενδιαφερόμενων προσώπων.

Το άρθρο αυτό εκπληρώνεται με την συνεργασία του Υπεύθυνου Προστασίας Δεδομένων, την συνεργασία της Εξειδικευμένης στην Κυβερνοασφάλεια Εταιρείας (Στάδιο 5ο) και τη Διοικητική Ομάδα του δήμου. Ακολουθώντας τον κατάλογο Διαδικασιών του Εγχειριδίου (Παραδοτέο 3) καταγράφεται για κάθε μία διαδικασία η εκτίμηση για τον τύπο κινδύνου και την κλίμακα πιθανότητας να συμβεί. Οι προτάσεις παρουσιάζονται στο Σχέδιο Δράσης.

7. Σχέδιο Δράσης για την Λειτουργική Εναρμόνιση στα πρότυπα του ISO 27001

Η σύνταξη του Σχεδίου Δράσης αποτελεί συνέχεια της εργασίας Εκτίμησης κινδύνου.

Οι λύσεις και οι βελτιώσεις οι οποίες θα σχεδιαστούν για την αντιμετώπιση των εκτιμώμενων κινδύνων, λαμβάνουν υπόψη της τα εξής :

- Ακολουθούν το πρότυπο διαδικασιών ISO 27001
- Αναγνωρίζουν και λαμβάνουν υπόψη τις δυνατότητες και ικανότητες του δήμου
- Συμφωνούνται ως προς τα χαρακτηριστικά τους και το χρονικό πλαίσιο υλοποίησης τους με την Διοίκηση του δήμου

8. Εκπαιδευτικό Υλικό για νεοεισερχόμενους εργαζομένους

Το εκπαιδευτικό υλικό το οποίο έχει παρουσιαστεί προς τους εργαζόμενους στο Στάδιο 3, το κείμενο του Γενικού Κανονισμού καθώς και το κείμενο του νομοσχεδίου θα βρίσκονται σε έντυπη και ηλεκτρονική μορφή στο **Εγχειρίδιο Επεξεργασίας Προσωπικών Δεδομένων.**
Εντούτοις για τους εργαζόμενους οι οποίοι κατά την διαδικασία ενημέρωσης του Σταδίου 3 ή για τους εποχικούς εργαζόμενους των μεταγενέστερων περιόδου από την σύνταξη του Εγχειριδίου και ως την διάθεση του Προσωρινού Υπεύθυνου Προστασίας Δεδομένων, θα υπάρχει ηλεκτρονική πλατφόρμα εκμάθησης (e-learning). Η συμμετοχή του κάθε εργαζόμενου σε αυτή θα μπορεί να γίνει κατόπιν προσωπικής πρόσκλησής του μέσω ηλεκτρονικού ταχυδρομείου. Το εκπαιδευτικό υλικό θα είναι έτσι κατασκευασμένο ώστε να αποδεικνύεται από τον αλγόριθμο λειτουργίας του ότι ο συμμετέχων έχει παρακολουθήσει όλη την ενημέρωση.

9. Παρουσίαση Έργου στα διευθυντικά στελέχη του δήμου

Η ολοκλήρωση σύνταξης του Εγχειριδίου Επεξεργασίας Προσωπικών Δεδομένων παρουσιάζεται κατά την διαδικασία παράδοσης του έργου ολόκληρο σε φυσική και ηλεκτρονική μορφή προς την διοίκηση.

Η παράδοση θα πραγματοποιηθεί σε αίθουσα του δήμου, θα προσφερθούν ροφήματα και θα παρουσιασθεί το εξής πρόγραμμα :

1. *Παρουσίαση σε διαφάνειες των κύριων σημείων της υπηρεσίας*
2. *Αναλυτική παρουσίαση του Σχεδίου Δράσης*
3. *Παράδοση Φακέλων Συμμόρφωσης προς την διοίκηση του δήμου*
4. *Παράδοση ενός καταστροφέα εγγράφων*
5. *Παράδοση του ηλεκτρονικού αρχείου σε USB*
6. *Υπογραφή πρωτόκολλου παραλαβής*

Παραδοτέα και ανάλυση κόστους

Α/Α σταδίου	ΣΤΑΔΙΑ - ΠΑΡΑΔΟΤΕΑ	Ανθρωποώρες	Κόστος Ανθρωποώρας χωρίς ΦΠΑ	ΣΥΝΟΛΟ *(χωρίς ΦΠΑ)*
1	Ενημέρωση Α.Π.Δ.Π.Χ	1	25,00 €	25,00 €
2	Συντονισμός και Προγραματισμός έργου	25	35,00 €	875,00 €
3	Αποτύπωση υφιστάμενης κατάστασης σε Διευθυντικό επίπεδο.	30	50,00 €	1.500,00 €
4	Ενημέρωση εργαζομένων	30	50,00 €	1.500,00 €
5	Διενέργεια ελέγχων αντοχής ΠΣ σε κακόβουλες επιθέσεις	35	50,00 €	1.750,00 €
6	Αποτύπωση υφιστάμενης κατάστασης σε επίπεδο θέσης εργασίας βάσης	55	50,00 €	2.750,00 €
7	Οδηγός συμμόρφωσης - Έκθεση αξιολόγησης επιπτώσεων αξιοπιστίας Δεδομένων (DPIA) - Παρουσίαση παραδοτέων	80	50,00 €	4.000,00 €
17	DPO	100	50,00 €	5.000,00 €
	ΣΥΝΟΛΑ	400		**17.400,00 €**
	ΦΠΑ 24%			**4.176,00 €**
	ΓΕΝΙΚΟ ΣΥΝΟΛΟ			**21.576,00 €**

Υπηρεσίες Υπεύθυνου Προστασίας Δεδομένων (DPO)

Περιγραφή Υπηρεσιών Υπευθύνου Προστασίας Προσωπικών Δεδομένων, σύμφωνα με τα αναφερόμενα στο άρθρο 39 του Κανονισμού, ***μέχρι την ολοκλήρωση του έργου:***

- Ο Υπεύθυνος Ασφαλείας Προσωπικών Δεδομένων ενημερώνει και συμβουλεύει τον Υπεύθυνο Επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους Εργαζόμενους που επεξεργάζονται προσωπικά δεδομένα, για τις υποχρεώσεις τους που απορρέουν από τον παρόντα Κανονισμό και από άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία προσωπικών δεδομένων.

- Ο Υπεύθυνος Ασφαλείας Προσωπικών Δεδομένων παρακολουθεί τη συμμόρφωση με τον παρόντα Κανονισμό (Ε.Ε.) 2016/679, με άλλες διατάξεις της Ε.Ε. ή του κράτους μέλους σχετικά με την προστασία δεδομένων και με τις πολιτικές του Υπευθύνου Επεξεργασίας ή του Εκτελούντος την Επεξεργασία σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της ανάθεσης αρμοδιοτήτων, της ευαισθητοποίησης και της κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας και των σχετικών ελέγχων.

- Ο Υπεύθυνος Ασφαλείας Προσωπικών Δεδομένων παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων- εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα- και παρακολουθεί την υλοποίηση της (Άρθρο 35).

- Ο Υπεύθυνος Ασφαλείας Προσωπικών Δεδομένων συνεργάζεται με την Εποπτική Αρχή.

- Ο Υπεύθυνος Ασφαλείας Προσωπικών Δεδομένων ενεργεί ως σημείο επικοινωνίας για την εποχική αρχή για ζητήματα που σχετίζονται με την επεξεργασία, περιλαμβανομένης της προηγούμενης διαβούλευσης (που αναφέρεται στο Άρθρο 36), και πραγματοποιεί διαβουλεύσεις, ανάλογα με την περίπτωση, για οποιοδήποτε άλλο θέμα.

- Ο Υπεύθυνος Ασφαλείας Προσωπικών Δεδομένων συνεργάζεται με την Εποπτική Αρχή και έχει δικαίωμα στον έλεγχο των προσωπικών δεδομένων των υπηρεσιών σας για την διερεύνηση περιπτώσεων που άπτονται της προστασίας δεδομένων.

- Ο Υπεύθυνος Ασφαλείας Προσωπικών Δεδομένων επιθεωρεί την τήρηση των συμφωνηθέντων διαδικασιών, προκειμένου να εκπληρώνεται η συμμόρφωση του δήμου, στο νομικό και λειτουργικό πλαίσιο, το οποίο έχει οριστεί κατά τη διαδικασία της εναρμόνισης.

- Ο Υπεύθυνος Ασφαλείας Προσωπικών Δεδομένων εγγυάται με προσωπική και αστική ευθύνη την εργασία του ,καθώς αναλαμβάνει την ευθύνη αποκατάστασης κάθε ζημίας, απώλειας, κόστους και δαπάνης που μπορεί να υποστεί ο Εργοδότης στην περίπτωση που υπάρξει αποτυχία στην επισήμανση κινδύνου και στις πρακτικές οι οποίες μπορεί να οδηγήσουν σε παραβίαση των διατάξεων του Γ.Κ.Π.Π.Χ. (Σύμβαση DPO Άρθρο 18)

Χρονοδιάγραμμα Υλοποίησης

Αριθμός Σταδίου	Περιγραφή Εργασίας	Χρόνος Παράδοσης
Στάδιο 1°	Ενημέρωση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα	Εντός 2 ημερών από την υπογραφή της σύμβασης
Στάδιο 2°	Συντονισμός και προγραμματισμός έργου	Εντός 2 εβδομάδων από την υπογραφή της σύμβασης
Στάδιο 3°	Αποτύπωση Υφιστάμενης Κατάστασης σε Διευθυντικό Επίπεδο	Εντός 40 ημερών από την υπογραφή της σύμβασης
Στάδιο 4°	Ενημέρωση εργαζομένων	Εντός 40 ημερών από την υπογραφή της σύμβασης
Στάδιο 5°	Διενέργεια Ελέγχων Αντοχής Πληροφοριακών Συστημάτων σε Εξωτερικές Κακόβουλες Επιθέσεις	Εντός 70 ημερών από την υπογραφή της σύμβασης
Στάδιο 6°	Αποτύπωση Υφιστάμενης Κατάστασης σε Επίπεδο θέσης εργασίας βάσης	Εντός 40 ημερών από την υπογραφή της σύμβασης
Στάδιο 7°	Οδηγός συμμόρφωσης- Έκθεση Αξιολόγησης Επιπτώσεων Αξιοπιστίας Δεδομένων (DPIA)- Παρουσίαση Παραδοτέων	Εντός 120 ημερών από την υπογραφή της σύμβασης

Αγ. Βαρβάρα ... /... / 2019

Παράρτημα Ι – Συγγραφή υποχρεώσεων

ΣΥΓΓΡΑΦΗ ΥΠΟΧΡΕΩΣΕΩΝ

Άρθρο 1ο: Αντικείμενο εργασίας

Η παρούσα μελέτη αφορά την ανάθεση σε Ανάδοχο της διαδικασίας συμμόρφωσης του δήμου στο «Γενικό Κανονισμό Προστασίας Δεδομένων» (ΓΚΠΔ-GDPR), (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

Άρθρο 2ο: Ισχύουσες διατάξεις

Η εκτέλεση της υπηρεσίας διέπεται από:

1. Τις διατάξεις του Ν. 3463/2006 «Κύρωση του Κώδικα Δήμων και Κοινοτήτων», όπως τροποποιήθηκε και ισχύει
2. Τις διατάξεις του Ν. 3731/2008, άρθρο 20 παρ. 13, που συμπληρώνει τον Κώδικα Δήμων και Κοινοτήτων
3. Τις διατάξεις του Ν. 3852/2010 (ΦΕΚ 87Α/7-6-2010) «Πρόγραμμα Καλλικράτης», όπως τροποποιήθηκε και ισχύει
4. Το Ν. 3861/2010 Φ.Ε.Κ. 112Α/13-7-2010: Ενίσχυση της διαφάνειας με την υποχρεωτική ανάρτηση νόμων και πράξεων των κυβερνητικών, διοικητικών και αυτοδιοικητικών οργάνων στο διαδίκτυο «Πρόγραμμα Διαύγεια» και άλλες διατάξεις
5. Τις διατάξεις του Ν. 4013/2011: «Σύσταση ενιαίας Ανεξάρτητης Αρχής Δημοσίων Συμβάσεων και Κεντρικού Ηλεκτρονικού Μητρώου Δημοσίων Συμβάσεων» όπως τροποποιήθηκε και ισχύει
6. Τις διατάξεις του Ν. 4250/2014, άρθρο 1 παρ. 2 «Διοικητικές Απλουστεύσεις – Καταργήσεις, Συγχωνεύσεις Νομικών Προσώπων και Υπηρεσιών του Δημοσίου Τομέα – Τροποποίηση Διατάξεων του Π. . 318/1992 (Α΄ 161) και λοιπές ρυθμίσεις»
7. Τις διατάξεις του Ν. 3536/2007 - ΦΕΚ 42/Α'/23.2.2007
8. Το Π. . 80/2016 «Ανάληψη υποχρεώσεων από τους Διατάκτες» (ΦΕΚ 145/Α'/5-8-2016)
9. Το Ν. 4412/2016 (ΦΕΚ 147/Α'/8-8-2016) «Δημόσιες Συμβάσεις Έργων, Προμηθειών και Υπηρεσιών (προσαρμογή στις Οδηγίες 2014/24/ΕΕ και 2014/25/ΕΕ)»
10. Η δαπάνη θα βαρύνει τον κωδικό 10-6142.003 προϋπολογισμού 2019 του Δήμου.

Άρθρο 3ο: Συμβατικά στοιχεία

Τα συμβατικά στοιχεία κατά σειρά ισχύος είναι:

i) Η Τεχνική έκθεση

ii) Η Συγγραφή των Υποχρεώσεων

iii) Ο Ενδεικτικός Προϋπολογισμός

iv) Η Οικονομική Προσφορά

v) Η Σύμβαση

Άρθρο 4ο : Χρόνος εκτέλεσης υπηρεσίας

Η συνολική διάρκεια υλοποίησης της υπηρεσίας ορίζεται σε τέσσερεις (4) μήνες από την ημερομηνία υπογραφής της σχετικής σύμβασης. Ο Ανάδοχος μπορεί να υποβάλει τα επιμέρους παραδοτέα, σύμφωνα με το ενδεικτικό χρονοδιάγραμμα της τεχνικής έκθεσης ή στο τέλος της σύμβασης. Σε περίπτωση ανάγκης περαιτέρω παράτασης, αυτή δύναται να χορηγηθεί με απόφαση του Δημοτικού Συμβουλίου με αιτιολόγηση και χωρίς τροποποίηση του οικονομικού αντικειμένου (σχετ. άρθρο 217 του 4412/2016).

Άρθρο 5ο : Δικαιολογητικά συμμετοχής

1) Υπεύθυνη Δήλωση του Ν.1599/86 στην οποία οι υποψήφιοι Ανάδοχοι θα δηλώνουν:
   - ότι αποδέχονται τους όρους της μελέτης και ότι η προσφορά τους είναι σύμφωνη με την Τεχνική έκθεση
   - ότι τηρούν τις υποχρεώσεις που απορρέουν από τις διατάξεις του άρθρου 18 του ν. 4412/2016 (περί περιβαλλοντικής, κοινωνικοασφαλιστικής και εργατικής νομοθεσίας)
   - την έδρα της επιχείρησης, και τη νομική μορφή της επιχείρησης

2) Οικονομική Προσφορά των υποψηφίων Αναδόχων. Η Οικονομική προσφορά θα συνταχθεί σύμφωνα με το ΠΑΡΑΡΤΗΜΑ ΙΙ της παρούσας μελέτης.

3) Κατάλογο των μελών της ομάδας έργου των υποψηφίων Αναδόχων και συνοπτικά βιογραφικά σημειώματα όλων των μελών της. Η ομάδα έργου θα πρέπει να απαρτίζεται από τουλάχιστον πέντε (5) μέλη, εκ των οποίων:
   - ✓ Το προτεινόμενο μέλος της Ομάδας Έργου που θα αναλάβει τη θέση DPO να είναι πιστοποιημένο κατά **ISO–IEC 17024.**

- ✓ Μέλος της Ομάδας Έργου είναι πιστοποιημένος ως **OSCP** (*Offensive Security Certified Professional*) και κατά **ISO 27001** και οι σχετικές αναγνωρισμένες πιστοποιήσεις να συμπεριληφθούν στην προσφορά καθώς και αναλυτικό βιογραφικό σημείωμα.
- ✓ Μέλος της Ομάδας Έργου είναι πιστοποιημένος ως **OSCP** και **CEH** (*Certified Ethical Hacker*) και οι σχετικές αναγνωρισμένες πιστοποιήσεις να συμπεριληφθούν στην προσφορά καθώς και αναλυτικό βιογραφικό σημείωμα.
- ✓ Μέλος της Ομάδας Έργου είναι πιστοποιημένος ως **OSCP** και **CCNA** (*Cisco Certified Network Administrator*) και οι σχετικές αναγνωρισμένες πιστοποιήσεις να συμπεριληφθούν στην προσφορά καθώς και αναλυτικό βιογραφικό σημείωμα.
- ✓ το ένα (1) μέλος θα είναι νομικός με αποδεδειγμένη νομική εμπειρία τουλάχιστον 15 ετών σε θέματα Προστασίας Προσωπικών Δεδομένων και πιστοποιημένο κατά **ISO–IEC 17024.** Για την τεκμηρίωση της εμπειρίας να δοθεί αναλυτικό βιογραφικό σημείωμα. Η σχετική αναγνωρισμένη πιστοποίηση να συμπεριληφθεί στην προσφορά.

4) Αντίγραφο ποινικού μητρώου (πρωτότυπο). Η υποχρέωση αφορά ιδίως: αα) στις περιπτώσεις εταιρειών περιορισμένης ευθύνης (Ε.Π.Ε.) και προσωπικών εταιρειών (Ο.Ε. και Ε.Ε.), τους διαχειριστές, β) στις περιπτώσεις ανωνύμων εταιρειών (Α.Ε.), τον Διευθύνοντα Σύμβουλο, καθώς και όλα τα μέλη του Διοικητικού Συμβουλίου

5) Κατάθεση εν ισχύ πιστοποιητικού **ISO-9001:2008** (ή νεότερου) και πιστοποιητικού **ISO-27001:2013, ISO 20000** ή ισοδύναμων αυτών από τον οικονομικό φορέα.

6) Να έχει ολοκληρώσει τουλάχιστον δύο (2) έργα συμμόρφωσης και εφαρμογής με τον ΓΚΠΔ (GDPR) στον κλάδο της Τοπικής Αυτοδιοίκησης (Ο.Τ.Α). Να κατατεθούν τα σχετικά πρωτόκολλα οριστικής παραλαβής.

7) Φορολογική ενημερότητα

8) Ασφαλιστική ενημερότητα

9) Εφόσον πρόκειται για νομικό πρόσωπο, αποδεικτικά έγγραφα νομιμοποίησης του νομίμου εκπροσώπου (*άρθρο 93 του Ν.4412/2016*)

Άρθρο 6ο : Συμφωνητικό Εχεμύθειας – Εμπιστευτικότητας του Αναδόχου

Με την έναρξη της υπηρεσίας ο Ανάδοχος υποχρεούται να υπογράψει Συμφωνητικό Εχεμύθειας – Εμπιστευτικότητας, σύμφωνα με το οποίο θα εγγυάται την εχεμύθεια των αποτελεσμάτων και όσων δεδομένων συλλεχθούν κατά την υλοποίηση της εργασίας. Το Συμφωνητικό θα καλύπτει όλα τα αποτελέσματα, καθώς και όλες τις πληροφορίες που θα πρέπει να ανακτηθούν κατά τη διάρκεια του

έργου. Σύμφωνα με αυτό ο Ανάδοχος θα αναλαμβάνει την ευθύνη για τη διασφάλιση της εμπιστευτικότητας των εμπλεκόμενων συμβούλων, μηχανικών και τεχνικών, όσον αφορά τη μη διαρροή πληροφοριών του είδους, του βαθμού διεκπεραίωσης του έργου καθώς και τις λεπτομέρειες αυτού.

Άρθρο 7ο : Υποχρεώσεις του Αναδόχου

Ο Ανάδοχος υποχρεούται να παρέχει:

1. Άρτια εργασία σύμφωνα με τους κανόνες της επιστήμης, της τεχνικής, και του επαγγέλματος
2. Αναπροσαρμογή των περιεχομένων της εργασίας ανάλογα με τις παρατηρήσεις της επιβλέπουσας υπηρεσίας
3. Αναλυτικές προτάσεις με τεκμηρίωση
4. Παράδοση της υπηρεσίας εμπρόθεσμα
5. Οι υπηρεσίες θα υλοποιούνται εξ ολοκλήρου από τον Ανάδοχο και το εξειδικευμένο του προσωπικό ή εξωτερικούς συνεργάτες. Την πληρωμή του προσωπικού (αποδοχές, εισφορές, κλπ.) αναλαμβάνει εξ ολοκλήρου ο Ανάδοχος

Άρθρο 8ο : Υποχρεώσεις της Αναθέτουσας αρχής

Ο Δήμος υποχρεούται να διευκολύνει την εργασία του Αναδόχου παρέχοντας κάθε δυνατή διευκόλυνση όπως η συνεργασία με την διοίκηση και η συνεργασία με υπηρεσιακούς παράγοντες.

Άρθρο 9ο : 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. Ο όρος περί ανωτέρας βίας εφαρμόζεται ανάλογα και για τον εντολέα προσαρμοζόμενος ανάλογα.

Άρθρο 10ο : Αναθεώρηση τιμών

Οι τιμές δεν υπόκεινται σε καμία αναθεώρηση για οποιονδήποτε λόγο ή αιτία, αλλά παραμένουν σταθερές και αμετάβλητες.

Άρθρο 11ο : Παραλαβή παραδοτέων

Η παραλαβή των παρεχόμενων υπηρεσιών – παραδοτέων θα γίνει σύμφωνα με το άρθρο 219 του Ν. 4412/2016 από την αρμόδια επιτροπή παραλαβής όπως αυτά αναφέρονται στην τεχνική έκθεση. Λόγω της ιδιαιτερότητας του θέματος, όποια διευκρίνηση ενδεχομένως δεν αναφέρεται στην παρούσα μελέτη, και αφορά τα παραδοτέα, θα εγγραφεί στους όρους της σύμβασης

Άρθρο 12ο : Τρόπος πληρωμής

Α. Παροχή υπηρεσιών υποστήριξης, συμμόρφωσης και προσαρμογής στο νέο Κανονισμό προστασίας Προσωπικών Δεδομένων.

Η πληρωμή θα γίνεται τμηματικά με την πρόοδο των εργασιών, μετά την ολοκλήρωση του κάθε σταδίου και την παράδοση και παραλαβή του συνόλου των παραδοτέων της. Το ποσό πληρωμής θα αναπροσαρμοστεί ανάλογα, σύμφωνα με την έκπτωση που θα δώσει ο Ανάδοχος στον ενδεικτικό προϋπολογισμό της μελέτης. Η καταβολή θα γίνει κατόπιν εκδόσεως βεβαίωσης καλής εκτέλεσης από την αρμόδια υπηρεσία, εκδόσεως του σχετικού δελτίου παροχής υπηρεσιών του Αναδόχου και πρακτικού παραλαβής από την αρμόδια επιτροπή.

Ειδικότερα:

- Πρώτη ($1^{η}$) πληρωμή θα πραγματοποιηθεί με την ολοκλήρωση των τεσσάρων (4) πρώτων φάσεων.
- Δεύτερη ($2^{η}$) πληρωμή θα πραγματοποιηθεί με την ολοκλήρωση των υπολοίπων τριών (3) σταδίων και την οριστική παραλαβή του έργου

Β. Παροχή υπηρεσιών προστασίας προσωπικών δεδομένων (DPO).

Το ποσό πληρωμής θα αναπροσαρμοστεί ανάλογα, σύμφωνα με την έκπτωση που θα δώσει ο Ανάδοχος στον ενδεικτικό προϋπολογισμό της μελέτης και θα καταβάλλεται ισόποσα υπολογισμένο βάσει του συνολικού αριθμού μηνών που θα παρασχεθεί η υπηρεσία DPO.

Τέλος, τον Ανάδοχο βαρύνουν όλες οι νόμιμες κρατήσεις εκτός του ΦΠΑ, ο οποίος βαρύνει το δήμο. Η αμοιβή δεν υπόκειται σε καμία αναθεώρηση για οποιοδήποτε λόγο και αιτία και παραμένει σταθερή και αμετάβλητη καθ' όλη την διάρκεια ισχύος της σύμβασης. Η αμοιβή καταβάλλεται όπως αναφέρεται παραπάνω, με πιστοποιήσεις της επιβλέπουσας υπηρεσίας και εξοφλείται μετά την παράδοση. Να σημειωθεί ότι Χορήγηση προκαταβολής δεν προβλέπεται.

Άρθρο 13ο : Φόροι, τέλη, κρατήσεις

Ο Ανάδοχος σύμφωνα με τις ισχύουσες διατάξεις βαρύνεται με όλους ανεξαιρέτως τους φόρους, τέλη, δασμούς και εισφορές υπέρ του δημοσίου, δήμων ή τρίτων που ισχύουν σύμφωνα με την κείμενη νομοθεσία.

Η αναθέτουσα αρχή βαρύνεται με τον αναλογούντα Φ.Π.Α.

Άρθρο 14ο : Τόπος

Ο Ανάδοχος θα παρέχει τις υπηρεσίες από την έδρα του. Οι συναντήσεις, οι συνεντεύξεις και η συμπλήρωση ερωτηματολογίων θα γίνεται στους χώρους των αρμόδιων υπηρεσιών ή σε χώρους που θα υποδεικνύει ο δήμος.

Άρθρο 15ο : Επίλυση διαφορών

Οι τυχόν διαφορές που θα εμφανισθούν κατά την εφαρμογή της σύμβασης, επιλύονται σύμφωνα με τις ισχύουσες διατάξεις και σύμφωνα με την Ελληνική νομοθεσία.

Άρθρο 16ο : Έκπτωση Αναδόχου

Εάν ο Ανάδοχος δεν συμμορφώνεται προς τις υποχρεώσεις που απορρέουν από τη σύμβαση ή προς τις νόμιμες εντολές και υποδείξεις της υπηρεσίας, καλείται με ειδική πρόσκληση να συμμορφωθεί προς τις υποχρεώσεις αυτές ή τις εντολές μέσα σε εύλογη προθεσμία, όχι πάντως μικρότερη των δέκα ημερών. Εάν ο Ανάδοχος δεν ανταποκριθεί εμπρόθεσμα στην ανωτέρω ειδική πρόσκληση, κηρύσσεται έκπτωτος, ύστερα από εισήγηση της υπηρεσίας σύμφωνα με τις ισχύουσες διατάξεις.

16/05/2019

ΘΕΩΡΗΘΗΚΕ

Σιαπέρα Αθανασία

16/05/2019

Ο ΣΥΝΤΑΞΑΣ

Αντώνης Ζυματούρας

ΕΓΚΡΙΘΗΚΕ

Ο ΔΗΜΑΡΧΟΣ

ΓΕΩΡΓΙΟΣ ΚΑΠΛΑΝΗΣ

Παράρτημα ΙΙ - Σχέδιο οικονομικής προσφοράς

ΕΝΤΥΠΟ ΟΙΚΟΝΟΜΙΚΗΣ ΠΡΟΣΦΟΡΑΣ

ΠΡΟΣ: **Δήμο Αγίας Βαρβάρας**

Του/ης.....με

έδρα.....οδός.....Αριθμ.....Τ.Κ.....

τηλ. .....Fax.....e-mail:.....

Αφού έλαβα γνώση των όρων της υπ' αριθμ. **...../2019** μελέτης «Παροχή υπηρεσιών για τη διαδικασία συμμόρφωσης στον "Γενικό Κανονισμό Προστασίας Δεδομένων"», καθώς και των συνθηκών εκτέλεσης αυτής, υποβάλλω την παρούσα προσφορά και δηλώνω ότι αποδέχομαι πλήρως και χωρίς επιφύλαξη όλα αυτά και αναλαμβάνω την εκτέλεση της υπηρεσίας με τις ακόλουθες τιμές επί των τιμών Προϋπολογισμού Μελέτης.

Το κόστος της προσφερόμενης υπηρεσίας ανέρχεται στο ποσό των ..... € (αριθμητικώς) πλέον ΦΠΑ (24%) ..... € (αριθμητικώς). Η συνολική τιμής της προσφοράς, συμπεριλαμβανομένου του ΦΠΑ (24%) ανέρχεται στο ποσό των ..... € (αριθμητικώς), ... (ολογράφως).

Ο/Η .....είναι φορολογικά και ασφαλιστικά ενήμερος/η.

....., .../...../ **2019**

Ο ΠΡΟΣΦΕΡΩΝ

(Ονοματεπώνυμο – Σφραγίδα – Υπογραφή)