

9 ΙΟΥΛΙΟΥ 2018

ΜΕΛΕΤΗ 155/2018

ΥΠΗΡΕΣΙΕΣ ΥΠΟΣΤΗΡΙΞΗΣ ΤΟΥ ΔΗΜΟΥ ΚΟΖΑΝΗΣ ΓΙΑ ΤΗΝ
ΠΡΟΕΤΟΙΜΑΣΙΑ ΚΑΙ ΠΡΟΣΑΡΜΟΓΗ ΣΤΟ ΝΕΟ ΕΥΡΩΠΑΪΚΟ ΓΕΝΙΚΟ
ΚΑΝΟΝΙΣΜΟ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (GDPR) 2016/679 ΕΕ

CPV 79411000-8 ΥΠΗΡΕΣΙΕΣ ΠΑΡΟΧΗΣ ΣΥΜΒΟΥΛΩΝ ΣΕ ΘΕΜΑΤΑ ΓΕΝΙΚΗΣ ΔΙΑΧΕΙΡΙΣΗΣ

ΔΗΜΟΣ ΚΟΖΑΝΗΣ
Πλ. Νίκης 1, 50100 Κοζάνη

Περιεχόμενα

Περιεχόμενα.....	1
1 Εισαγωγή	2
2 Περιγραφή Αντικειμένου	3
2.1 Αποτύπωση υφιστάμενης κατάστασης & κατάρτιση Σχεδίου Συμμόρφωσης	3
2.1.1 Δέσμευση της Διοίκησης.....	3
2.1.2 Σύνταξη Μητρώου Επεξεργασιών Δεδομένων Προσωπικού Χαρακτήρα	3
2.1.3 Σύσταση Ομάδας Εργασίας Δήμου & Καθορισμός Αρμοδιοτήτων	4
2.1.4 Έλεγχος και αξιολόγηση πολιτικών και διαδικασιών	5
2.1.5 Έλεγχος συμβάσεων & συναλλαγών.....	5
2.1.6 Αποτίμηση Κινδύνων & Έλεγχος Ασφάλειας Συστημάτων.....	5
2.1.7 Κατάρτιση Σχεδίου Συμμόρφωσης.....	6
2.2 Υλοποίηση Σχεδίου Συμμόρφωσης - Εφαρμογή προτεινόμενων μέτρων	6
2.2.1 Ορισμός Υπεύθυνου Προστασίας Δεδομένων (DPO).....	6
2.2.2 Συγγραφή Πολιτικής Ασφάλειας	7
2.2.3 Συγγραφή Πολιτικών Συλλογής, Χρήσης και Επεξεργασίας Δεδομένων	8
2.2.4 Σύνταξη Σχεδίου Ασφάλειας.....	8
2.2.5 Σύνταξη Σχεδίου Ανάκαμψης από Καταστροφές.....	8
2.2.6 Σύνταξη Σχεδίου Διαχείρισης Συμβάντων	8
2.2.7 Προσαρμογή Συμβάσεων	8
2.2.8 Εκπαίδευση Προσωπικού & Συνεργατών.....	9
2.2.9 Σχέδιο GDPR Stress Test	9
2.3 Έλεγχος & Αξιολόγηση Συμμόρφωσης - Λήψη Διορθωτικών Μέτρων.....	9
2.3.1 Πιλοτική εφαρμογή GDPR Stress Test.....	9
2.3.2 Διορθωτικές Ενέργειες & Αναθεώρηση Πολιτικών & Εγγράφων	9
2.3.3 Αρχείο Καταγραφής Ενεργειών Συμμόρφωσης.....	10
2.4 Πίνακας Παραδοτέων	10
3 Ομάδα Έργου	12
4 Διάρκεια - Χρονοδιάγραμμα.....	13
5 Προϋπολογισμός	15
6 Τρόπος Πληρωμής	16
7 Προϋποθέσεις Συμμετοχής	17
8 Κριτήριο Ανάθεσης	19
9 Εμπιστευτικότητα Πληροφοριών.....	20
ΠΑΡΑΡΤΗΜΑ	1
Έντυπο Τεχνικής Προσφοράς	1

1 Εισαγωγή

Η παρούσα μελέτη αφορά στην ανάθεση υπηρεσιών υποστήριξης προς τον Δήμο Κοζάνης για την προετοιμασία και συμμόρφωσή του στον νέο Ευρωπαϊκό Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) 2016/679 ΕΕ, ο οποίος δημοσιεύθηκε στις 4 Μαΐου 2016 και έχει τεθεί σε εφαρμογή από τις 25 Μαΐου 2018 και ο οποίος για λόγους συντομίας θα αναφέρεται εφεξής ως **“Κανονισμός”** ή **“GDPR”**

Με τον νέο Κανονισμό, καθιερώνεται ενιαίο νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων στους φορείς του δημοσίου και ιδιωτικού τομέα σε όλα τα κράτη μέλη της ΕΕ.

Ο Δήμος Κοζάνης, ο οποίος διατηρεί και επεξεργάζεται πληθώρα δεδομένων προσωπικού χαρακτήρα καθώς και πληροφορίες είτε δικές του είτε των συναλλασσόμενων με αυτόν, είναι προφανές ότι υποχρεούται, σύμφωνα με τον εν λόγω κανονισμό, να συμμορφωθεί με τις νέες νομοθετικές επιταγές. Ειδικότερα η οργανωτική του δομή θα πρέπει να διασφαλίζει την ελεύθερη και ασφαλή ροή των δεδομένων προσωπικού χαρακτήρα και τυποποίηση των σχετικών διαδικασιών επεξεργασίας τους.

Η μη συμμόρφωση του Δήμου στις νέες συνθήκες που επιβάλλονται από τον κανονισμό μπορεί να οδηγήσει σε επιβολή προστίμων που φτάνουν έως και το 4% του ετήσιου προϋπολογισμού του.

Με βάση τα ανωτέρω, θα πρέπει να γίνει ανάθεση υπηρεσιών σε εξειδικευμένο εξωτερικό συνεργάτη – σύμβουλο, ο οποίος θα αναλάβει την υλοποίηση των απαιτούμενων ενεργειών, όπως αναλύονται παρακάτω.

2 Περιγραφή Αντικειμένου

2.1 Αποτύπωση υφιστάμενης κατάστασης & κατάρτιση Σχεδίου Συμμόρφωσης

Θα γίνει αποτύπωση της υπάρχουσας κατάστασης ως προς την επεξεργασία δεδομένων που λαμβάνει χώρα στο σύνολο των υπηρεσιών του Δήμου, τα είδη των δεδομένων και των υποκειμένων τους, τις ροές των δεδομένων, τις υφιστάμενες πρακτικές, διαδικασίες και πολιτικές του Δήμου και τα εφαρμοζόμενα μέτρα προστασίας.

2.1.1 Δέσμευση της Διοίκησης

Παρουσίαση στη Διοίκηση και τα στελέχη του Δήμου, των απαιτήσεων του Κανονισμού, ώστε να έχουν πλήρη γνώση της αναγκαιότητας του έργου, να ενημερωθούν για τα περιεχόμενα και το χρονοδιάγραμμά του και να προσδιοριστούν οι πόροι και οι προσβάσεις που θα παρασχεθούν στην ομάδα υλοποίησης του έργου.

Εν προκειμένω, ο Ανάδοχος προετοιμάζει και συντάσσει σε συνεργασία με την Διοίκηση, τις απαιτούμενες δηλώσεις που θα κοινοποιηθούν στο προσωπικό του Δήμου.

2.1.2 Σύνταξη Μητρώου Επεξεργασιών Δεδομένων Προσωπικού Χαρακτήρα

Θα γίνει από τον Ανάδοχο ακριβής και λεπτομερής αποτύπωση των τμημάτων επεξεργασίας δεδομένων προσωπικού χαρακτήρα, των τηρούμενων αρχείων (έντυπων ή ηλεκτρονικών), του είδους των δεδομένων, του χρόνου διατήρησής τους, των πηγών προέλευσης, των νομικών δεσμεύσεων, της πιθανής διάθεσης δεδομένων σε τρίτους, του χρησιμοποιούμενου εξοπλισμού και των τεχνολογικών μέσων, των υποκειμένων και των ροών τους. Επίσης καθορίζονται όλες οι σχετιζόμενες με τα ανωτέρω, δεσμεύσεις από τον Κανονισμό GDPR.

Ενδεικτικά και όχι περιοριστικά, η καταγραφή αφορά στα παρακάτω επιμέρους στοιχεία.

- I. **Καταγραφή υπευθύνων ανά τμήμα & διαθέσιμων πόρων:** Πραγματοποιείται καταγραφή των υπευθύνων και των διαθέσιμων πόρων (ανθρώπινου δυναμικού και υλικών μέσων) ανά τμήμα και ανά αρχείο δεδομένων που θα εμπλακεί και θα συμβάλλει στην επίτευξη συμμόρφωσης κατά GDPR. Η καταγραφή αυτή θα χρησιμοποιηθεί κυρίως για την οργάνωση της ομάδας εργασίας (§2.1.3)
- II. **Προσδιορισμός θεσμικού πλαισίου:** Προσδιορίζεται η νομική βάση της επεξεργασίας δεδομένων και εξετάζεται η ορθότητα ή/και εγκυρότητά της. Με βάση την καταγραφή αυτή θα δημιουργηθεί το **αρχείο θεσμικού πλαισίου** που αφορά στην κάθε μορφή επεξεργασίας, καταγραφής, τεκμηρίωσης και γνωστοποίησης με σαφείς οδηγίες ενσωμάτωσης.
- III. **Χαρτογράφηση εγκατεστημένου πληροφοριακού συστήματος & λοιπών μέσων τήρησης προσωπικών δεδομένων:** Ελέγχονται, αξιολογούνται και καταγράφονται τα πληροφοριακά συστήματα του Δήμου, οι δικτυακές του υποδομές και κάθε πολιτική ή διαδικασία που άπτεται της λειτουργίας αυτών. Πέραν των πληροφοριακών συστημάτων θα καταγραφούν και οποιαδήποτε άλλα φυσικά μέσα τα οποία χρησιμοποιούνται για την

τήρηση και φύλαξη δεδομένων προσωπικού χαρακτήρα. Στα πλαίσια αυτής της καταγραφής θα συνταχθούν:

- Διάγραμμα υφιστάμενου πληροφοριακού συστήματος, με τις επιμέρους λειτουργίες
- Τοπολογικό διάγραμμα μέσων και χώρων τήρησης και φύλαξης προσωπικών δεδομένων

Με βάση τις ανωτέρω καταγραφές θα συνταχθεί το υφιστάμενο **Μητρώο Επεξεργασιών Δεδομένων Προσωπικού Χαρακτήρα**, όπου θα αποτυπώνεται ένα εύρος πληροφοριών για κάθε αρχείο και είδος επεξεργασίας, όπως:

- Κατηγορίες των επεξεργαζόμενων δεδομένων
- Μορφή δεδομένων (ηλεκτρονική, έντυπη ή μεικτή)
- Ονοματεπώνυμο υπευθύνου επεξεργασίας
- Προσδιορισμό σκοπού επεξεργασίας
- Διεύθυνση εγκατάστασης αρχείου
- Τεχνολογία που χρησιμοποιείται
- Στοιχεία εκτελούντων την επεξεργασία
- Χρονικό διάστημα που απαιτείται για την επεξεργασία
- Χρήση διαδικτύου για την επεξεργασία
- Θεσμικό πλαίσιο - νομική βάση της επεξεργασίας
- Ενημέρωση υποκείμενου για τα δικαιώματά του
- Πηγή δεδομένων
- Αποδέκτες δεδομένων
- Περίοδος τήρησης
- Ζεύξη δεδομένων
- Εάν έχει διενεργηθεί εκτίμηση αντικτύπου κινδύνου και αν ναι ποια είναι τα αποτελέσματά της
- Οποιαδήποτε άλλη πληροφορία που αφορά στην τήρηση, προέλευση και ροή των δεδομένων προσωπικού χαρακτήρα.

2.1.3 Σύσταση Ομάδας Εργασίας Δήμου & Καθορισμός Αρμοδιοτήτων

Θα συνταχθεί από τον Ανάδοχο, σε συνεργασία με τα αρμόδια όργανα του Δήμου, σχέδιο Ομάδας Εργασίας της οποίας το αντικείμενο θα είναι, η διεκπεραίωση των απαιτούμενων ενεργειών από την πλευρά του Δήμου για την συμμόρφωση κατά GDPR.

Στο σχέδιο θα περιγράφονται αναλυτικά και με σαφήνεια οι ρόλοι, αρμοδιότητες και τα τυπικά και ουσιαστικά προσόντα των μελών της ομάδας. Η σύνθεση της ομάδας εργασίας θα πρέπει να είναι αντιπροσωπευτική και να καλύπτει όλα τα τμήματα του Δήμου και τις μορφές της επεξεργασίας προσωπικών δεδομένων.

Με βάση το συνταχθέν σχέδιο ομάδας εργασίας, που θα υποβάλλει ο Ανάδοχος, ο Δήμος θα ορίσει ονομαστικά τα μέλη της.

2.1.4 Έλεγχος και αξιολόγηση πολιτικών και διαδικασιών

Ελέγχονται οι πολιτικές, τα τεχνικά και τα οργανωτικά μέτρα του οργανισμού, ως προς την επάρκειά τους για τον Κανονισμό.

Ελέγχεται και αξιολογείται αν υπάρχει πολιτική ασφαλείας που προβλέπει διαδικασίες και δυνατότητα ικανοποίησης των δικαιωμάτων των υποκειμένων, διαδικασίες για την άμεση και εντός των προβλεπόμενων χρονοδιαγραμμάτων ανταπόκριση σε αιτήματα των υποκειμένων, λήψης συγκατάθεσης των υποκειμένων, εκπαίδευση και δημιουργία κουλτούρας στο ανθρώπινο δυναμικό.

Ελέγχεται αν υπάρχει επαρκές σχέδιο επιχειρησιακής συνέχειας και ανταπόκρισης σε περιστατικά παραβίασης καθώς και αν προβλέπονται μηχανισμοί ανίχνευσης περιστατικών παραβίασης.

Ελέγχεται αν υπάρχουν διαδικασίες, και αν ναι, γίνεται αξιολόγηση της τήρησής τους, της εμπέδωσής τους από το προσωπικό σε σχέση με την πολιτική προστασίας προσωπικών δεδομένων.

Ιδιαίτερη μέριμνα θα πρέπει να δοθεί στα εφαρμοζόμενα από το Δήμο συστήματα ποιότητας (ISO 9001, Διαχειριστική Επάρκεια, κλπ) έτσι να εντοπιστούν τα σημεία που χρήζουν αναθεώρησης λόγω των νέων απαιτήσεων που θέτει ο Κανονισμός.

2.1.5 Έλεγχος συμβάσεων & συναλλαγών

Ελέγχονται οι συμβάσεις και οι συναλλαγές του Δήμου με τρίτους των οποίων προσωπικά δεδομένα επεξεργάζεται ο Δήμος (προσωπικό, πελάτες, προμηθευτές, κλπ) ή οι οποίοι επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του Δήμου, όσο και με τρίτους στους οποίους διαβιβάζονται δεδομένα προσωπικού χαρακτήρα.

2.1.6 Αποτίμηση Κινδύνων & Έλεγχος Ασφάλειας Συστημάτων

Θα μελετηθούν οι εκθέσεις σε κίνδυνο των συστημάτων του Δήμου, προσδιορίζοντας τις ευπάθειες και τις απειλές του με βάση τον υφιστάμενο έλεγχο.

Τα αποτελέσματα της ανάλυσης επικινδυνότητας της υπολογιστικής και επικοινωνιακής υποδομής του Δήμου θα προσδιορίσουν τις απαιτήσεις ασφαλείας του πληροφοριακού συστήματος, καλύπτοντας τις παρακάτω συνιστώσες:

- **Φυσική ασφάλεια του συστήματος:** Προστασία ολόκληρου του σχετικού εξοπλισμού από φυσικές καταστροφές.
- **Ασφάλεια υπολογιστικού συστήματος:** Προστασία των πληροφοριών που διαχειρίζεται το λειτουργικό σύστημα (εφαρμογές, αρχεία δεδομένων, κ.ά.).
- **Ασφάλεια δικτύων επικοινωνιών:** Προστασία των πληροφοριών κατά τη μετάδοσή τους μέσω τοπικών, τηλεφωνικών ή άλλων δικτύων (π.χ. Internet)

Στα πλαίσια της ανάλυσης επικινδυνότητας, θα γίνουν απαραίτητα εκτεταμένες **δοκιμές διείσδυσης (penetration tests)** έτσι ώστε να εξακριβωθεί στο μέγιστο δυνατό βαθμό το πόσο εύαλωτο και τρωτό είναι το πληροφοριακό σύστημα του Δήμου, σε πιθανές επιθέσεις ή λανθασμένους χειρισμούς.

Επιπλέον των ανωτέρω, η αποτίμηση κινδύνων θα περιλαμβάνει ανάλυση επικινδυνότητας και για τα μη ψηφιακά δεδομένα που τηρούνται σε έντυπη μορφή. Ειδικότερα θα διερευνηθούν η προσβασιμότητα, οι κίνδυνοι δολιοφθοράς, οι μέθοδοι φύλαξης, η επάρκεια των μέσων και χώρων φύλαξης και η έκθεση σε φυσικές καταστροφές.

ΠΡΟΣΟΧΗ: Τα αποτελέσματα της αποτίμησης κινδύνων και ιδιαίτερα όσων άπτονται των πληροφοριακών συστημάτων χαρακτηρίζονται άκρως εμπιστευτικά και ως εκ τούτου, θα πρέπει να κοινοποιηθούν αυστηρά και μόνο στα οριζόμενα για το σκοπό αυτό, άτομα.

2.1.7 Κατάρτιση Σχεδίου Συμμόρφωσης

Σύνταξη αναλυτικού σχεδίου συμμόρφωσης, στο οποίο θα περιλαμβάνονται όλα τα οργανωτικά και τεχνικά μέτρα που θα πρέπει να λάβει ο δήμος, για να συμμορφωθεί με τις απαιτήσεις του Κανονισμού, καθώς και πιθανές συστάσεις για μέτρα, τα οποία ναι μεν δεν είναι απαραίτητα για την συμμόρφωση προς τον Κανονισμό, αλλά θα μπορούσαν να συμβάλλουν στην εύρυθμη λειτουργία του.

Σε κάθε περίπτωση, το τελικό Σχέδιο Συμμόρφωσης θα πρέπει να είναι της απόλυτης αποδοχής του Δήμου και θα πρέπει να εναρμονίζεται με τις οικονομικές και οργανωτικές ικανότητες του Δήμου έτσι ώστε οι προτάσεις του να μπορούν να υλοποιηθούν σε εύλογο χρονικό διάστημα.

2.2 Υλοποίηση Σχεδίου Συμμόρφωσης - Εφαρμογή προτεινόμενων μέτρων

2.2.1 Ορισμός Υπεύθυνου Προστασίας Δεδομένων (DPO)

Αμέσως μετά την ολοκλήρωση του Σχεδίου Συμμόρφωσης και την λήψη των πρώτων ελάχιστων απαιτούμενων μέτρων συμμόρφωσης σύμφωνα με το σχέδιο συμμόρφωσης, θα οριστεί ένα μέλος της Ομάδας Έργου ή άλλο άτομο επιλογής του αναδόχου ως προσωρινός Υπεύθυνος Προστασίας Δεδομένων (DPO) του Δήμου, μέχρι την λήξη των συμβατικών υποχρεώσεων του Αναδόχου, το οποίο θα πρέπει να διαθέτει κατά τον χρόνο ορισμού του, έγκυρη και σε ισχύ, πιστοποίηση DPO αναγνωρισμένη από το ΕΣΥΔ (Εθνικό Σύστημα Διαπίστευσης).

Στο διάστημα που θα επιτελεί τα καθήκοντά του ο οριζόμενος, από τον Ανάδοχο, DPO, ο Ανάδοχος σε συνεργασία με τον Δήμο Κοζάνης, θα προετοιμάσει την διάδοχη κατάσταση, με έναν από τους παρακάτω δύο τρόπους που θα επιλέξει ο Δήμος.

Σε κάθε περίπτωση ο Ανάδοχος, θα συντάξει το απαιτούμενο για τη θέση του DPO, προφίλ, στο οποίο θα περιλαμβάνονται τα τυπικά και ουσιαστικά προσόντα που θα πρέπει να έχει καθώς και τους ενδεχόμενους περιορισμούς και κωλύματα της θέσης.

i. Περίπτωση Α: Ορισμός ενός υπαλλήλου του Δήμου ως Υπεύθυνου Προστασίας Δεδομένων

Ο Δήμος ορίζει δύο υπαλλήλους του, οι οποίοι θα εκπαιδευτούν κατάλληλα από τον Ανάδοχο έτσι ώστε ο ένας εξ' αυτών να οριστεί ως ο κύριος Υπεύθυνος Προστασίας Δεδομένων και ο άλλος ως αναπληρωτής του.

Οι εν λόγω υπάλληλοι, από τον ορισμό τους και μέχρι την λήξη των συμβατικών υποχρεώσεων του Αναδόχου, θα παρακολουθούν και θα υποβοηθούν στο έργο του, τον ορισμένο από τον Ανάδοχο DPO. Παράλληλα, οι εν λόγω υπάλληλοι, θα προετοιμαστούν κατάλληλα από τον Ανάδοχο, ο οποίος θα τους παρέχει είτε ο ίδιος είτε μέσω τρίτου ειδικευμένου φορέα την απαιτούμενη εκπαίδευση προκειμένου να αποκτήσουν πιστοποίηση DPO αναγνωρισμένη από το ΕΣΥΔ.

Επίσης, μέχρι την λήξη της σύμβασης, ο Ανάδοχος θα πρέπει να διεκπεραιώσει όλες τις απαιτούμενες διαδικασίες προκειμένου οι ανωτέρω υπάλληλοι του Δήμου να αποκτήσουν πιστοποίηση DPO.

Οι δαπάνες για τις πιστοποιήσεις DPO καθώς και οι προαναφερθείσες δαπάνες εκπαίδευσης βαρύνουν εξ' ολοκλήρου τον Ανάδοχο και εμπεριέχονται στο συμβατικό τίμημα.

ii. Περίπτωση Β: Ανάθεση σε εξωτερικό συνεργάτη των υπηρεσιών Υπεύθυνου Προστασίας Δεδομένων

Ο Δήμος ορίζει δύο υπαλλήλους του, οι οποίοι θα εκπαιδευτούν από τον Ανάδοχο έτσι ώστε, αφενός μεν να είναι γνώστες των απαιτήσεων της συμμόρφωσης του Δήμου κατά GDPR και αφετέρου δε, των μέτρων που πρέπει να ληφθούν στα πλαίσια της εφαρμογής του Σχεδίου Συμμόρφωσης (§2.1.7)

Οι εν λόγω υπάλληλοι, από τον ορισμό τους και μέχρι την λήξη των συμβατικών υποχρεώσεων του Αναδόχου, θα παρακολουθούν και θα υποβοηθούν στο έργο του, τον ορισμένο από τον Ανάδοχο DPO. Παράλληλα, θα προετοιμαστούν κατάλληλα από τον Ανάδοχο, ο οποίος θα τους παρέχει είτε ο ίδιος είτε μέσω τρίτου ειδικευμένου φορέα την απαιτούμενη εκπαίδευση προκειμένου να αποκτήσουν πιστοποίηση DPO αναγνωρισμένη από το ΕΣΥΔ.

Οι δαπάνες εκπαίδευσης βαρύνουν τον Ανάδοχο και εμπεριέχονται στο συμβατικό τίμημα, ενώ η δαπάνη των πιστοποιήσεων DPO, όταν αυτή γίνει, θα βαρύνει τον Δήμο.

Επιπρόσθετα, ο Ανάδοχος θα σχεδιάσει και θα υποδείξει την κατάλληλη διαγωνιστική διαδικασία, συντάσσοντας όλα τα απαιτούμενα τεύχη, έτσι ώστε ο Δήμος να μπορέσει να αναθέτει σε εξωτερικό συνεργάτη (φυσικό ή νομικό πρόσωπο) την παροχή υπηρεσιών DPO.

2.2.2 Συγγραφή Πολιτικής Ασφάλειας

Η Πολιτική Ασφάλειας είναι ένα έγγραφο, στο οποίο περιγράφονται οι στόχοι της ασφάλειας και οι αντίστοιχες διαδικασίες που πρέπει να ακολουθούνται για την επίτευξή τους. Καθορίζει τη δέσμευση της Διοίκησης και την προσέγγιση του Δήμου, αναφορικά με την ασφάλεια των πληροφοριακών συστημάτων και δικτύων και την προστασία προσωπικών δεδομένων, στις ακόλουθες περιπτώσεις:

- **Οργανωτικά Μέτρα Ασφάλειας**
Μέτρα σχετικά με τους ρόλους και τις αρμοδιότητες του προσωπικού και των εξωτερικών συνεργατών – που εμπλέκονται με την επεξεργασία των δεδομένων. Καθορισμός και αρμοδιότητες του υπευθύνου ασφαλείας, εκπαίδευση του προσωπικού, διαχείριση περιστατικών ασφαλείας καθώς και την καταστροφή των προσωπικών δεδομένων.
- **Τεχνικά Μέτρα Ασφάλειας**
Αφορούν στη διαχείριση των χρηστών, την αναγνώριση και ταυτοποίησή τους, την ασφάλεια των επικοινωνιών, τη λειτουργία των αρχείων καταγραφής του πληροφοριακού συστήματος, την εξαγωγή αντιγράφων ασφαλείας,
- **Μέτρα Φυσικής Ασφάλειας.**
Προσδιορίζει επακριβώς τον ρόλο κάθε εμπλεκόμενου εντός του Δήμου, τις αρμοδιότητες, τις ευθύνες και τα καθήκοντά του ως προς τις διαδικασίες που αφορούν στην ασφάλεια.

Τέλος, στην Πολιτική Ασφάλειας περιγράφονται και οι κατάλληλες διαδικασίες για την αναθεώρησή της.

2.2.3 Συγγραφή Πολιτικών Συλλογής, Χρήσης και Επεξεργασίας Δεδομένων

Αφορά στον καθορισμό των πολιτικών συλλογής, χρήσης και επεξεργασίας δεδομένων που θα πρέπει να εφαρμόζονται και ειδικότερα:

- Επανεξέταση του τρόπου λήψης και καταγραφής της συγκατάθεσης
- Έλεγχος ή/και εφαρμογή συστημάτων για την διαπίστωση της ηλικίας ή την εξακρίβωση ταυτότητας των εκάστοτε κηδεμόνων, σε περίπτωση ανηλίκων, και τη λήψη σχετικής συγκατάθεσης
- Διασφάλιση τρόπων άσκησης των δικαιωμάτων των υποκειμένων. Σχεδιασμός τρόπου διαχείρισης των αιτημάτων εντός των προβλεπόμενων χρονικών ορίων.

2.2.4 Σύνταξη Σχεδίου Ασφάλειας

Το Σχέδιο Ασφάλειας είναι το έγγραφο όπου περιγράφονται τα οργανωτικά, τεχνικά και τα μέτρα φυσικής ασφάλειας, που εφαρμόζονται για την κάλυψη των βασικών αρχών και κανόνων ασφάλειας, που αναφέρονται στην Πολιτική Ασφαλείας.

Το Σχέδιο αυτό υπόκειται σε τακτικές επισκοπήσεις και αναθεωρήσεις, δεδομένης της ραγδαίας ανάπτυξης τεχνολογικών λύσεων και της εφαρμογής τους στα πληροφοριακά συστήματα και τις τεχνολογικές υποδομές.

2.2.5 Σύνταξη Σχεδίου Ανάκαμψης από Καταστροφές

Το Σχέδιο Ανάκαμψης από Καταστροφές είναι το έγγραφο, που αναφέρεται στα μέτρα προστασίας, ανάκαμψης και αποκατάστασης πληροφοριακών συστημάτων και τεχνολογικών υποδομών σε περιπτώσεις έκτακτης ανάγκης, όπως φυσικές καταστροφές (π.χ. σεισμός, πυρκαγιά, πλημμύρα, εξωτερικές επιθέσεις/εισβολές κλπ).

Ελέγχεται περιοδικά, προκειμένου να διαπιστώνεται το επίπεδο της αποτελεσματικότητας των μεθόδων ανάκαμψης.

2.2.6 Σύνταξη Σχεδίου Διαχείρισης Συμβάντων

Αφορά στον έλεγχο του υφισταμένου και στην εφαρμογή νέου μηχανισμού εντοπισμού παραβιάσεων ή και απλών περιστατικών ασφαλείας με αυτόματη καταγραφή.

Συγκεκριμένα το σχέδιο διαχείρισης συμβάντων είναι το έγγραφο, που αναφέρεται στις διαδικασίες, που θα εφαρμοσθούν σε περίπτωση παραβίασης ασφαλείας. Προσδιορίζει επακριβώς τον ρόλο κάθε εμπλεκόμενου εντός και εκτός του Δήμου, τις αρμοδιότητες, τις ευθύνες και τα καθήκοντά του, ως προς τις διαδικασίες, που αφορούν στην αντίδραση του Δήμου, σε περίπτωση παραβίασης και απώλειας δεδομένων.

Επίσης περιγράφεται και η κατάλληλη διαδικασία για την αναθεώρηση του σχεδίου .

2.2.7 Προσαρμογή Συμβάσεων

Αφορά στην προσαρμογή των ισχυουσών συμβάσεων του Δήμου α) με το προσωπικό και τους εξωτερικούς συνεργάτες οι οποίο εμπλέκονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα και β) με τρίτους στους οποίους διαβιβάζονται δεδομένα προσωπικού χαρακτήρα.

Όπου απαιτείται θα γίνεται προσαρμογή των συμβάσεων αυτών σύμφωνα με τις ειδικότερες απαιτήσεις του GDPR. Στις περιπτώσεις που δεν υπάρχουν συμβάσεις θα συνταχθούν νέες.

Επίσης θα συνταχθούν και αντίστοιχα πρότυπα συμβάσεων για μελλοντική χρήση.

2.2.8 Εκπαίδευση Προσωπικού & Συνεργατών

Θα υλοποιηθεί πρόγραμμα εκπαίδευσης του εμπλεκόμενου προσωπικού του Δήμου και των εξωτερικών συνεργατών, το οποίο θα αφορά, ειδικότερα στην Πολιτική Ασφάλειας του Δήμου και γενικότερα σε θέματα προσωπικών δεδομένων και της ασφάλειάς τους.

Στόχος της εκπαίδευσης είναι η κατανόηση από το ανθρώπινο δυναμικό του Δήμου, των απαιτήσεων του GDPR και των θεμάτων που άπτονται με την ασφάλεια των δεδομένων προσωπικού χαρακτήρα τα οποία θα πρέπει να εκλαμβάνονται εφεξής ως περιουσιακό στοιχείο του Δήμου.

Να σημειωθεί ότι, η εν λόγω εκπαίδευση αποτελεί βασικό τεκμήριο συμμόρφωσης με τον GDPR.

2.2.9 Σχέδιο GDPR Stress Test

Αφορά στη σύνταξη της μεθοδολογίας για τον έλεγχο (stress test) όλων των εφαρμοζόμενων διαδικασιών και συστημάτων ασφαλείας για να διαπιστωθεί ο βαθμός ανταπόκρισής τους στις απαιτήσεις του Σχεδίου Ασφάλειας Προσωπικών Δεδομένων αλλά και του κανονισμού GDPR γενικότερα.

Καθορίζεται επίσης η συχνότητα διενέργειας των stress tests, το επίπεδο ελέγχου, ο βαθμός έντασης, όπως επίσης και από ποιους θα γίνονται και με ποια διαδικασία θα επιλέγονται αυτοί που θα διενεργούν τους ελέγχους.

2.3 Έλεγχος & Αξιολόγηση Συμμόρφωσης – Λήψη Διορθωτικών Μέτρων

2.3.1 Πιλοτική εφαρμογή GDPR Stress Test

Σύμφωνα με το σχέδιο GDPR Stress Test (§2.2.9) που έχει συντάξει ο Ανάδοχος, θα προχωρήσει ο ίδιος στην πρώτη πιλοτική εφαρμογή του. Με βάση τα ευρήματα του stress test, ο Ανάδοχος θα συντάξει σχετική έκθεση όπου θα προτείνονται τα απαιτούμενα διορθωτικά μέτρα.

Η έκθεση χαρακτηρίζεται ως εμπιστευτική και θα διαβιβαστεί αποκλειστικά και μόνο στα αρμόδια όργανα του Δήμου.

2.3.2 Διορθωτικές Ενέργειες & Αναθεώρηση Πολιτικών & Εγγράφων

Από το σύνολο των απαιτούμενων διορθωτικών μέτρων που θα προταθούν από τον Ανάδοχο, για την αντιμετώπιση των δυσλειτουργιών και των προβλημάτων που θα προκύψουν από τη διενέργεια του stress test, ο Δήμος θα εφαρμόσει εκείνα που κατά την κρίση του είναι απολύτως αναγκαία και εφικτό να υλοποιηθούν στα πλαίσια των τρεχουσών οργανωτικών και οικονομικών του δυνατοτήτων.

Με βάση τις επιλογές του Δήμου, στην εφαρμογή των διορθωτικών μέτρων που θα τελικά θα υλοποιηθούν, ο Ανάδοχος θα προχωρήσει στην αναθεώρηση όσων από τα παραδοτέα της Β' φάσης (§2.3.3) απαιτηθεί, υποβάλλοντας στον Δήμου τις αντίστοιχες αναθεωρημένες εκδόσεις. Πέραν

αυτού, ο Ανάδοχος, δεν έχει καμία άλλη συμβατική υποχρέωση στην εφαρμογή των διορθωτικών μέτρων.

2.3.3 Αρχείο Καταγραφής Ενεργειών Συμμόρφωσης

Αφορά στην τεκμηρίωση της συμμόρφωσης ή των βημάτων που έχουν γίνει προς την κατεύθυνση της συμμόρφωσης προς τις απαιτήσεις του GDPR και περιλαμβάνει κατ' ελάχιστον:

- καταγραφή των διαδικασιών συλλογής και επεξεργασίας των δεδομένων,
- ποσοστό ολοκλήρωσης (με αναλυτικά βήματα) των διαφόρων σχεδίων,
- αναλυτικά στοιχεία για την εκπαίδευση του προσωπικού
- την καταγραφή των περιστατικών ασφάλειας

2.4 Πίνακας Παραδοτέων

ΠΑΡΑΔΟΤΕΑ Α' ΦΑΣΗΣ		
A	Δήλωση Δέσμευσης της Διοίκησης	§2.1.1
B	Αρχείο θεσμικού πλαισίου με οδηγίες ενσωμάτωσης στην κάθε μορφή επεξεργασίας, καταγραφής, τεκμηρίωσης και γνωστοποίησης δεδομένων προσωπικού χαρακτήρα	§2.1.2
C	Διάγραμμα υφιστάμενου πληροφοριακού συστήματος, με τις επιμέρους λειτουργίες	§2.1.2
D	Τοπολογικό διάγραμμα μέσων και χώρων τήρησης και φύλαξης προσωπικών δεδομένων	§2.1.2
E	Μητρώο Επεξεργασιών Δεδομένων Προσωπικού Χαρακτήρα	§2.1.2
F	Σχέδιο Οργάνωσης & Αρμοδιότητες Ομάδας Εργασίας Συμμόρφωσης	§2.1.3
G	Έκθεση αξιολόγησης πολιτικών & διαδικασιών	§2.1.4
H	Έκθεση ελέγχου συμβάσεων & συναλλαγών	§2.1.5
I	Έκθεση Αποτίμησης Κινδύνων & Αποτελέσματα Ελέγχου Δοκιμών Ασφάλειας	§2.1.6
J	Σχέδιο Συμμόρφωσης κατά GDPR	§2.1.7

ΠΑΡΑΔΟΤΕΑ Β' ΦΑΣΗΣ		
K	Προφίλ θέσης DPO Πιστοποιήσεις DPO ή Μεθοδολογία Ανάθεσης Υπηρεσιών DPO	§2.2.1
L	Πολιτική Ασφαλείας	§2.2.2
M	Εγχειρίδιο Πολιτικών & Διαδικασιών Συλλογής και Επεξεργασίας Δεδομένων	§2.2.3
N	Σχέδιο Ασφάλειας	§2.2.4

O	Σχέδιο Ανάκαμψης από Καταστροφές	§2.2.5
P	Σχέδιο Διαχείρισης Συμβάντων	§2.2.6
Q	Πρότυπα Συμβάσεων εναρμονισμένα με τον Κανονισμό GDPR	§2.2.7
R	Τροποποιημένες Συμβάσεις	§2.2.7
S	Παροχή Εκπαίδευσης (Πρόγραμμα & Τεκμηρίωση)	§2.2.8
T	Σχέδιο GDPR Stress Test	§2.2.9

ΠΑΡΑΔΟΤΕΑ Γ' ΦΑΣΗΣ

U	Έκθεση GDPR Stress Test	§2.3.1
V	Αναθεωρημένες Εκδόσεις Παραδοτέων Β' Φάσης	§2.3.2
W	Αρχείο Ενεργειών Συμμόρφωσης	§2.3.3

3 Ομάδα Έργου

Η παροχή των ζητούμενων υπηρεσιών θα γίνει από Ομάδα Έργου που θα συστήσει ο Ανάδοχος και η οποία κατ' ελάχιστο θα έχει την παρακάτω σύνθεση:

- Ένα άτομο, νομικό με πιστοποίηση DPO
- Ένα άτομο, ειδικότητας πληροφορικής με πιστοποίηση DPO
- Ένα άτομο, ειδικότητας πληροφορικής με αποδεδειγμένη εμπειρία και γνώση στην ασφάλεια των πληροφοριών και των πληροφοριακών συστημάτων και ειδικότερα στις δοκιμές διείσδυσης (penetration tests).
- Ένα άτομο, ειδικό στην παροχή υπηρεσιών εφαρμογής και επιθεώρησης συστημάτων διαχείρισης ποιότητας (ISO 9001) ή/και στην παροχή υπηρεσιών εφαρμογής και επιθεώρησης συστημάτων διαχείρισης ασφάλειας πληροφοριών (ISO 27001), το οποίο θα διαθέτει και τις αντίστοιχες πιστοποιήσεις.

Πέραν των ανωτέρω μελών, στην ομάδα έργου μπορεί να προστεθεί ένα ακόμη μέλος το οποίο θα είναι ο επικεφαλής και project manager της ομάδας και θα έχει τον γενικό συντονισμό των εργασιών της. Εναλλακτικά, το ρόλο αυτό μπορεί να τον αναλάβει και κάποιος από τα προαναφερόμενα μέλη. Σε κάθε περίπτωση όμως, ο επικεφαλής της ομάδας θα πρέπει να διαθέτει αποδεδειγμένη εμπειρία στην υλοποίηση έργων συμμόρφωσης κατά GDPR.

Τα μέλη της ομάδας έργου μπορούν να είναι είτε υπάλληλοι του υποψήφιου αναδόχου είτε εξωτερικοί συνεργάτες (φυσικά ή νομικά πρόσωπα) που θα δεσμεύονται για την παροχή των ζητούμενων υπηρεσιών, με σχετική δήλωση συνεργασίας.

Για όλα τα μέλη της ομάδας έργου θα πρέπει να κατατεθούν τα αντίστοιχα αποδεικτικά στοιχεία της ζητούμενης εμπειρίας ή/και γνώσης τους (τίτλοι σπουδών, πιστοποιήσεις κλπ)

Σημείωση:

Όλες οι ζητούμενες πιστοποιήσεις των μελών της Ομάδας Έργου, θα πρέπει να είναι σε ισχύ κατά το χρόνο υποβολής της προσφοράς και να είναι αναγνωρισμένες από το Εθνικό Σύστημα Διαπίστευσης (ΕΣΥΔ)

4 Διάρκεια - Χρονοδιάγραμμα

Η συνολική διάρκεια της Υπηρεσίας καθορίζεται σε 25 εβδομάδες από την υπογραφή της σχετικής σύμβασης.

Οι επιμέρους τμηματικές προθεσμίες που αναφέρονται στο χρονοδιάγραμμα, είναι δεσμευτικές ως προς το χρόνο υποβολής των παραδοτέων κάθε φάσης και μπορούν να παραταθούν μόνο σε περίπτωση μη υπαιτιότητας του Αναδόχου, ειδικότερα, θα πρέπει να υποβληθούν σε:

- 9 εβδομάδες από την υπογραφή της σύμβασης τα παραδοτέα της Α' Φάσης
- 18 εβδομάδες από την υπογραφή της σύμβασης τα παραδοτέα της Β' Φάσης
- 24 εβδομάδες από την υπογραφή της σύμβασης τα παραδοτέα της Γ' Φάσης

Γενικότερα, για τυχόν καθυστερήσεις και υπερβάσεις στο χρονοδιάγραμμα του έργου εφαρμόζονται οι ισχύουσες διατάξεις.

Χρονοδιάγραμμα																													
ID	Task Name	W-1	W1	W2	M1 W3	W4	W5	W6	M2 W7	W8	W9	W10	M3 W11	W12	W13	W14	W15	M4 W16	W17	W18	W19	M5 W20	W21	W22	W23	M6 W24	W25	W26	
1	Αποτύπωση υφιστάμενης κατάστασης & κατάρτιση σχεδίου συμμόρφωσης																												
2	Υλοποίηση Ενεργειών Α' Φάσης																												
3	Δέσμευση Διοίκησης																												
4	Σύσταση Ομάδας Εργασίας																												
5	Υποβολή Παραδοτέων Α' Φάσης																												
6	Έγκριση Παραδοτέων Α' Φάσης																												
7	Υλοποίηση Σχεδίου Συμμόρφωσης - Εφαρμογή Προτεινόμενων Μέτρων																												
8	Υλοποίηση Ενεργειών Β' Φάσης																												
9	Ορισμός DPO																												
10	Εκπαίδευση Προσωπικού																												
11	Υποβολή Παραδοτέων Β' Φάσης																												
12	Έγκριση Παραδοτέων Β' Φάσης																												
13	Έλεγχοι & Αξιολόγηση Συμμόρφωσης																												
14	GDPR Stress Test																												
15	Έγκριση Διορθωτικών Μέτρων																												
16	Αναθεώρηση Παραδοτέων Β' Φάσης																												
17	Υποβολή Τελικών Παραδοτέων Β' & Γ' Φάσης																												
18	Έγκριση Τελικών Παραδοτέων Β' & Γ' Φάσης																												
Project: Χρονοδιάγραμμα Date: Fri 22/6/18		Task		Project Summary		Manual Task		Start-only		Deadline																			
		Split		Inactive Task		Duration-only		Finish-only		Progress																			
		Milestone		Inactive Milestone		Manual Summary Rollup		External Tasks		Manual Progress																			
		Summary		Inactive Summary		Manual Summary		External Milestone																					
Page 1																													

5 Προϋπολογισμός

Η υπηρεσία χρηματοδοτείται από τον ετήσιο προϋπολογισμό του 2018 του Δήμου Κοζάνης με ΚΑ 00.6117.0007 και έχει προϋπολογισμό 24.180€ συμπεριλαμβανομένου ΦΠΑ.

Περιγραφή	Αξία
Υπηρεσίες υποστήριξης του Δήμου Κοζάνης για την προετοιμασία και προσαρμογή στο νέο Ευρωπαϊκό Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) 2016/679 ΕΕ	19.500€
	ΦΠΑ 24% 4.680€
	Σύνολο 24.180€

6 Τρόπος Πληρωμής

Η πληρωμή του Αναδόχου θα γίνεται τμηματικά, με την ολοκλήρωση και παραλαβή των παραδοτέων, ως εξής:

- 25% με την παραλαβή των παραδοτέων της Α' Φάσης (§2.3.3)
- 30% με την παραλαβή των παραδοτέων της Β' Φάσης (§2.3.3)
- 45% με παραλαβή των παραδοτέων της Γ' Φάσης και την ολοκλήρωση του συνολικού αντικειμένου της σύμβασης (§2.3.3)

7 Προϋποθέσεις Συμμετοχής

Λόγω των ειδικών δυσκολιών αλλά και της ιδιαίτερης συνδυαστικής σχέσης των ζητούμενων υπηρεσιών με θέματα ποιότητας, ασφάλειας, εχεμύθειας και τεχνολογιών πληροφορικής, ο υποψήφιος ανάδοχος για να συμμετάσχει στο διαγωνισμό θα πρέπει καλύπτει τις παρακάτω απαιτήσεις:

Απαίτηση	Τεκμηρίωση
Συμμόρφωση κατά GDPR του ιδίου	Σχετική πιστοποίηση ή υπεύθυνη δήλωση
Αποδεδειγμένη εμπειρία σε τουλάχιστον τρία (3) έργα συμμόρφωσης κατά GDPR, ιδιωτικά ή δημόσια, υλοποιημένα ή σε εξέλιξη, εξαιρουμένου του έργου της ίδιας συμμόρφωσης.	Πίνακας έργων GDPR, όπου θα υπάρχουν απαραίτητα τα παρακάτω στοιχεία: • Τίτλος Έργου, • Κύριος του Έργου/Φορέας Υλοποίησης • Περιγραφή Αντικειμένου • Διάρκεια Υλοποίησης, • Ποσό σύμβασης • Στοιχεία επικοινωνίας υπευθύνου φορέα υλοποίησης Για κάθε έργο θα υπάρχει και η αντίστοιχη τεκμηρίωση, όπως σύμβαση ή βεβαίωση καλής εκτέλεσης ή πρωτόκολλο παραλαβής
Αποδεδειγμένη εμπειρία στην παροχή συμβουλευτικών υπηρεσιών σε φορείς ΟΤΑ ή του ευρύτερου δημοσίου τα τελευταία 3 έτη.	Πίνακας συμβάσεων συμβουλευτικών υπηρεσιών, όπου θα υπάρχουν απαραίτητα τα παρακάτω στοιχεία: • Τίτλος Έργου, • Κύριος του Έργου/Φορέας Υλοποίησης • Περιγραφή Αντικειμένου • Διάρκεια Υλοποίησης, • Ποσό σύμβασης • Στοιχεία επικοινωνίας υπευθύνου φορέα υλοποίησης Για κάθε έργο θα υπάρχει και το αντίστοιχο έγγραφο τεκμηρίωσης, όπως σύμβαση ή βεβαίωση καλής εκτέλεσης ή πρωτόκολλο παραλαβής
Πιστοποίηση κατά ISO 9001 για την παροχή συμβουλευτικών υπηρεσιών	Πιστοποιητικό ISO αναγνωρισμένο από το ΕΣΥΔ σε ισχύ κατά το χρόνο υποβολής προσφοράς
Πιστοποίηση κατά ISO 27001 για την διαχείριση ασφάλειας πληροφοριών	Πιστοποιητικό ISO αναγνωρισμένο από το ΕΣΥΔ σε ισχύ κατά το χρόνο υποβολής προσφοράς

Ομάδα Έργου	Κατάλογος με την σύνθεση της ομάδας έργου με τα αντίστοιχα έγγραφα τεκμηρίωσης σύμφωνα με τα οριζόμενα στη §3
-------------	---

8 Κριτήριο Ανάθεσης

Κριτήριο ανάθεσης της σύμβασης είναι η πλέον συμφέρουσα από οικονομικής άποψης προσφορά βάσει τιμής προσφοράς.

9 Εμπιστευτικότητα Πληροφοριών

Επειδή για την υλοποίηση της παρούσας υπηρεσίας, θα περιέλθουν προς γνώση του Αναδόχου Εμπιστευτικές Πληροφορίες, θα πρέπει να δοθεί ιδιαίτερη μέριμνα στη χρήση και διακίνησή τους.

Ο όρος Εμπιστευτικές Πληροφορίες αφορά σε οποιαδήποτε σημαντική μη δημόσιου χαρακτήρα πληροφορία σχετικά με την οργάνωση, τις υπηρεσίες, τα οικονομικά στοιχεία, τον εξοπλισμό και την ασφάλεια συστημάτων τόσο του Δήμου Κοζάνης όσο και τρίτων για τους οποίους διατηρεί στοιχεία ο Δήμος Κοζάνης και ιδίως δεδομένα προσωπικού χαρακτήρα, που περιέρχεται κατά την εκτέλεση του συμβατικού αντικειμένου του Αναδόχου, στον Ανάδοχο ή στο προσωπικό του Αναδόχου ή σε τρίτους συνεργαζόμενους με τον Ανάδοχο, με οποιοδήποτε τρόπο η με οποιαδήποτε υλική ή άυλη μορφή.

Ο Ανάδοχος και ιδίως τα μέλη της Ομάδας Έργου (§3) αλλά και οποιαδήποτε λοιπά εμπλεκόμενα μέρη (νομικά ή φυσικά πρόσωπα) καθ' όλη τη διάρκεια εκτέλεσης της σύμβασης με τον Δήμο, που λειτουργούν κατ' εντολή του αναδόχου, εφόσον θα καταστούν αποδέκτες Εμπιστευτικών Πληροφοριών, θα πρέπει να υπογράψουν πριν την ανάληψη των συμβατικών τους υποχρεώσεων, σχετική δήλωση εμπιστευτικότητας. Η υπογραφή της δήλωσης και η αποδοχή των όρων της είναι απαραίτητη προϋπόθεση για την συμμετοχή τους στην υλοποίηση του συμβατικού αντικειμένου του Αναδόχου. Ειδικότερα με την δήλωση εμπιστευτικότητας θα δεσμεύονται κατ' ελάχιστον για τα παρακάτω:

- Να μη χρησιμοποιούν τις Εμπιστευτικές Πληροφορίες για οποιοδήποτε άλλο σκοπό παρά μόνο για το αντικείμενο της εργασίας του και τις δραστηριότητές του σε σχέση με την παρεχόμενη Υπηρεσία.
- Να μην ανακοινώνουν τις Εμπιστευτικές Πληροφορίες σε άλλους συνεργάτες που απασχολούνται στον Ανάδοχο ή σε τρίτους παρά μόνο όταν αυτό είναι αναγκαίο για να φέρει σε πέρας το έργο που έχουν αναλάβει και μόνο ύστερα από σχετική έγγραφη εντολή και συναίνεση του Δήμου.
- Να μην αναπαράγουν οποτεδήποτε τις Εμπιστευτικές Πληροφορίες ούτε να τις αποθηκεύουν σε ηλεκτρονική μορφή, παρά μόνο για να φέρουν σε πέρας το έργο που έχουν αναλάβει από τον Δήμο.
- Σε περίπτωση αναπαραγωγής των πληροφοριών εν συνόλω ή εν μέρει τα αντίγραφα πρέπει να φέρουν την ένδειξη «ΑΝΤΙΓΡΑΦΟ» και θα τηρείται αρχείο όλων των αντιγράφων
- Να διατηρούν υπό ασφαλείς συνθήκες το σύνολο των Εμπιστευτικών Πληροφοριών, καθώς και οποιοδήποτε αντικείμενο που περιέχει Εμπιστευτικές Πληροφορίες, μόνο για όσο διάστημα απαιτείται για τις ανάγκες εκτέλεσης των συμβατικών του υποχρεώσεων.
- Να επιστρέφουν, οποτεδήποτε, ύστερα από σχετικό αίτημα του Δήμου, το σύνολο ή μέρος των Εμπιστευτικών Πληροφοριών που βρίσκονται στην κατοχή τους
- Σε περίπτωση λήξεως ή λύσεως της σύμβασης με τον Δήμο, για οποιοδήποτε λόγο, αν διαπιστωθεί εκ μέρους Δήμου η με οποιοδήποτε τρόπο παράβαση των όρων της δήλωσης εμπιστευτικότητας εκ' μέρους του Αναδόχου, αυτός είναι υποχρεωμένος:
 - να σταματήσει αμέσως να κάνει χρήση των Εμπιστευτικών Πληροφοριών

- να παραδώσει αμέσως στον Δήμο οποιαδήποτε αντικείμενα ή έγγραφα τα οποία περιέχουν Εμπιστευτικές Πληροφορίες και βρίσκονται στην κατοχή του ή, κατά παράβαση των όρων της παρούσας, στην κατοχή τρίτων και
- να αποστέλλει εγγράφως κατάλογο των ονομάτων και διευθύνσεων των τρίτων προσώπων στους οποίους έχει ανακοινώσει Εμπιστευτικές Πληροφορίες
- Η παραβίαση ενός ή περισσότερων όρων της δήλωσης εμπιστευτικότητας από τους υπογράφοντες την δήλωση αποτελεί σημαντικό λόγω καταγγελίας της σύμβασης με τον Δήμο.

Το παραγόμενο από τον Ανάδοχο έργο, κατά το μέρος που περιέχει οποιεσδήποτε πληροφορίες σχετικές με την ασφάλεια των πληροφοριακών συστημάτων του Δήμου, την φύλαξη αρχείων και δεδομένων, στοιχεία συναλλαγών και συμβάσεων τρίτων με τον Δήμο, και το οποίο περιέχεται στη κατοχή του Δήμου ως παραδοτέο του συμβατικού του αντικειμένου και γενικότερα οτιδήποτε άλλο χαρακτηρίζεται διαβαθμισμένο από τον Δήμο, αποτελεί εμπιστευτική διαβαθμισμένη πληροφορία η οποία θα διαβιβάζεται μόνο στα υποδεικνυόμενα από τον Δήμο φυσικά πρόσωπα, σύμφωνα με τις αντίστοιχες εσωτερικές διαδικασίες του Δήμου.

Σε κάθε περίπτωση ο Ανάδοχος, όντας πιστοποιημένος κατά ISO 27001, θα πρέπει πέραν των προβλεπόμενων από το σύστημά του διαδικασιών, σχετικά με την ασφάλεια πληροφοριών, να τηρεί και τις τυχόν επιπρόσθετες απαιτήσεις ασφάλειας και εμπιστευτικότητας που πηγάζουν από τα τεύχη της διακήρυξης.

Ο ΣΥΝΤΑΚΤΗΣ

Κοζάνη 9/7/2018

ΘΕΩΡΗΘΗΚΕ

Ο Προϊστάμενος του Γραφείου
Προγραμματισμού & Ανάπτυξης

Κωνσταντίνος ΙΣΠΟΓΛΟΥ

Βασίλειος ΚΟΡΚΑΣ

ΠΑΡΑΡΤΗΜΑ

Έντυπο Τεχνικής Προσφοράς

α/α	Απαίτηση	Απαιτούμενα δικαιολογητικά	Συμμόρφωση (ΝΑΙ/ΟΧΙ)
1	Συμμόρφωση κατά GDPR του ιδίου	Σχετική πιστοποίηση ή υπεύθυνη δήλωση	
2	Αποδεδειγμένη εμπειρία σε τουλάχιστον τρία (3) έργα συμμόρφωσης κατά GDPR, ιδιωτικά ή δημόσια, υλοποιημένα ή σε εξέλιξη, εξαιρουμένου του έργου της ίδιας συμμόρφωσης.	Πίνακας έργων GDPR, όπου θα υπάρχουν απαραίτητα τα παρακάτω στοιχεία: • Τίτλος Έργου, • Κύριος του Έργου/Φορέας Υλοποίησης • Περιγραφή Αντικειμένου • Διάρκεια Υλοποίησης, • Ποσό σύμβασης • Στοιχεία επικοινωνίας υπευθύνου φορέα υλοποίησης Για κάθε έργο θα υπάρχει και η αντίστοιχη τεκμηρίωση, όπως σύμβαση ή βεβαίωση καλής εκτέλεσης ή πρωτόκολλο παραλαβής	
3	Αποδεδειγμένη εμπειρία στην παροχή συμβουλευτικών υπηρεσιών σε φορείς ΟΤΑ ή του ευρύτερου δημοσίου τα τελευταία 3 έτη.	Πίνακας συμβάσεων συμβουλευτικών υπηρεσιών, όπου θα υπάρχουν απαραίτητα τα παρακάτω στοιχεία: • Τίτλος Έργου, • Κύριος του Έργου/Φορέας Υλοποίησης • Περιγραφή Αντικειμένου • Διάρκεια Υλοποίησης, • Ποσό σύμβασης • Στοιχεία επικοινωνίας υπευθύνου φορέα υλοποίησης Για κάθε έργο θα υπάρχει και το αντίστοιχο έγγραφο τεκμηρίωσης, όπως σύμβαση ή βεβαίωση καλής εκτέλεσης ή πρωτόκολλο παραλαβής	

ΥΠΗΡΕΣΙΕΣ ΥΠΟΣΤΗΡΙΞΗΣ ΤΟΥ ΔΗΜΟΥ ΚΟΖΑΝΗΣ ΓΙΑ ΤΗΝ
ΠΡΟΕΤΟΙΜΑΣΙΑ ΚΑΙ ΠΡΟΣΑΡΜΟΓΗ ΣΤΟ ΝΕΟ ΕΥΡΩΠΑΪΚΟ ΓΕΝΙΚΟ
ΚΑΝΟΝΙΣΜΟ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (GDPR) 2016/679 ΕΕ

α/α	Απαίτηση	Απαιτούμενα δικαιολογητικά	Συμμόρφωση (ΝΑΙ/ΟΧΙ)
4	Πιστοποίηση κατά ISO 9001 για την παροχή συμβουλευτικών υπηρεσιών	Πιστοποιητικό ISO αναγνωρισμένο από το ΕΣΥΔ σε ισχύ κατά το χρόνο υποβολής προσφοράς	
5	Πιστοποίηση κατά ISO 27001 για την διαχείριση ασφάλειας πληροφοριών	Πιστοποιητικό ISO αναγνωρισμένο από το ΕΣΥΔ σε ισχύ κατά το χρόνο υποβολής προσφοράς	
6	Ομάδα Έργου	Κατάλογος με την σύνθεση της ομάδας έργου με τα αντίστοιχα έγγραφα τεκμηρίωσης σύμφωνα με τα οριζόμενα στη §3	