ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

###### ΝΟΜΟΣ ΕΒΡΟΥ

#### ΚΕΝΤΡΟ ΚΟΙΝΩΝΙΚΗΣ ΠΡΟΣΤΑΣΙΑΣ

#### ΑΛΛΗΛΕΓΓΥΗΣ ΠΑΙΔΕΙΑΣ ΚΑΙ ΠΕΡΙΒΑΛΛΟΝΤΟΣ

#### ΔΗΜΟΥ ΑΛΕΞΑΝΔΡΟΥΠΟΛΗΣ

Τηλέφωνο: 25510 83012 - 53225

Φαξ: 2551038713

Πληροφορίες: ΓΚΑΜΠΙΤΣΑΚΗΣ ΖΑΧΑΡΙΑΣ

Email: ps@alexpolis.gr

|  |  |
| --- | --- |
|  | **ΑΡΙΘΜ. ΠΡΩΤ.: 2135** ΗΜΕΡΟΜΗΝΙΑ: 10 Ιουνίου 2019 |
|  |  |

ΠΡΟΣΚΛΗΣΗ

**ΘΕΜΑ:** **Απευθείας** α**νάθεση για** **παροχή υπηρεσιών συμμόρφωσης, προσαρμογής και υποστήριξης ως προς τον Νέο Κανονισμό Προστασίας Προσωπικών Δεδομένων με αριθμ. 679/2016 (General Data Protection Regulation – GDPR)**.

Σας ανακοινώνουμε ότι το Κέντρο Κοινωνικής Προστασίας Αλληλεγγύης Παιδείας και Περιβάλλοντος Δήμου Αλεξανδρούπολης θα προχωρήσει στην **παροχή υπηρεσιών συμμόρφωσης, προσαρμογής και υποστήριξης ως προς τον Νέο Κανονισμό Προστασίας Προσωπικών Δεδομένων με αριθμ. 679/2016 (General Data Protection Regulation – GDPR)** με τη διαδικασία της απευθείας ανάθεσης, συνολικού προϋπολογισμού **18.500,00 €** χωρίς το ΦΠΑ, σύμφωνα με την υπ’ αριθ. **12/2019** μελέτη.

Ημερομηνία έναρξης υποβολής προσφορών: 10/06/2019.

Καλείστε μέχρι και την **18/06/2019**, ημέρα **Τρίτη** και ώρα **03.00 μ.μ.,** να καταθέσετε την προσφορά σας στο Κέντρο Κοινωνικής Προστασίας Αλληλεγγύης Παιδείας και Περιβάλλοντος Δήμου Αλεξ/πολης , Καρτάλη 2, σύμφωνα με τις διατάξεις του Ν. 4412/2016.

Ο φάκελος της προσφοράς πρέπει να περιλαμβάνει:

* Τα παρακάτω αναφερόμενα δικαιολογητικά
* Οικονομική Προσφορά (σε ξεχωριστό σφραγισμένο φάκελο).

Προς απόδειξη της μη συνδρομής των λόγων αποκλεισμού από διαδικασίες σύναψης δημοσίων συμβάσεων των παρ.1 και 2 του άρθρου 73 του Ν.4412/2016, παρακαλούμε, μαζί με την προσφορά σας, να μας αποστείλετε τα παρακάτω δικαιολογητικά:

α. Υπεύθυνη Δήλωση του Ν. 1599/1986 (τ. Α) ως προκαταρτική απόδειξη ότι δεν υπάρχει εις βάρος του συμμετέχοντος τελεσίδικη καταδικαστική απόφαση για έναν από τους παρακάτω λόγους: α) συμμετοχή σε εγκληματική οργάνωση, β) δωροδοκία, γ) απάτη, δ) τρομοκρατικά εγκλήματα ή εγκλήματα συνδεόμενα με τρομοκρατικές δραστηριότητες, ε) νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή χρηματοδότηση της τρομοκρατίας, στ) παιδική εργασία και άλλες μορφές εμπορίας ανθρώπων (άρθρο 73 του ν. 4412/2016).

Η υποχρέωση αποκλεισμού οικονομικού φορέα εφαρμόζεται επίσης όταν το πρόσωπο εις βάρος του οποίου εκδόθηκε τελεσίδικη δικαστική απόφαση είναι μέλος του διοικητικού, διευθυντικού ή εποπτικού οργάνου του εν λόγω οικονομικού φορέα ή έχει εξουσία εκπροσώπησης, λήψης αποφάσεων ή ελέγχου σε αυτό. Η υποχρέωση αφορά ιδίως: αα) στις περιπτώσεις εταιρειών περιορισμένης ευθύνης (Ε.Π.Ε.) και προσωπικών εταιρειών (Ο.Ε. και Ε.Ε.), τους διαχειριστές, ββ) στις περιπτώσεις ανωνύμων εταιρειών (Α.Ε.), τον Διευθύνοντα Σύμβουλο, καθώς και όλα τα μέλη του Διοικητικού Συμβουλίου.

β. Υπεύθυνη Δήλωση του Ν. 1599/1986 (τ. Α) στην οποία θα αναφέρει ότι: α) η επιχείρηση είναι εγγεγραμμένη στο οικείο Επιμελητήριο ή σε οικείο επαγγελματικό σύλλογο και ασκώ επάγγελμα συναφές με το αντικείμενο της σύμβασης, β) ότι μελέτησα και αποδέχομαι πλήρως και ανεπιφύλακτα τους όρους της παρούσας πρόσκλησης και την **12/2019** μελέτη και ότι τα είδη που προσφέρω τηρούν τις ζητούμενες προδιαγραφές, γ) δεν έχει αποκλειστεί η συμμετοχή μου σε διαγωνισμού του δημοσίου ή των Οργανισμών Τοπικής Αυτοδιοίκησης (ΟΤΑ).

γ. Φορολογική ενημερότητα.

δ. Ασφαλιστική ενημερότητα (άρθρο 80 παρ.2 του Ν.4412/2016).

ε. Εφόσον πρόκειται για νομικό πρόσωπο, αποδεικτικά έγγραφα νομιμοποίησης του νομικού προσώπου (άρθρο 93 του Ν.4412/2016).

Από τον ανάδοχο θα ζητηθεί Απόσπασμα ποινικού μητρώου προς απόδειξη των ανωτέρω και Πιστοποιητικό Οικείου Επιμελητηρίου προ της υπογραφής της σύμβασης.

**Ο ΠΡΟΕΔΡΟΣ ΤΟΥ Δ.Σ.**

**ΓΕΡΑΚΟΠΟΥΛΟΣ ΧΡΗΣΤΟΣ**



**ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ**

**ΝΟΜΟΣ ΕΒΡΟΥ  
ΚΕΝΤΡΟ ΚΟΙΝΩΝΙΚΗΣ ΠΡΟΣΤΑΣΙΑΣ, ΑΛΛΗΛΕΓΓΥΗΣ,  
ΠΑΙΔΕΙΑΣ ΚΑΙ ΠΕΡΙΒΑΛΛΟΝΤΟΣ  
ΔΗΜΟΥ ΑΛΕΞΑΝΔΡΟΥΠΟΛΗΣ**

**«ΠΟΛΥΚΟΙΝΩΝΙΚΟ»  
Αρ. Μελέτης : 12/2019**

**ΤΕΧΝΙΚΗ ΕΚΘΕΣΗ**

**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)**

CPV: 79417000-0 - [Υπηρεσίες παροχής συμβουλών σε θέματα ασφάλειας](https://www.contracts.gr/cpv/458bba11-b9b7-4a44-b4b2-f2dfc44f89ae)

ΕΝΔΕΙΚΤΙΚΟΣ ΠΡΟΫΠΟΛΟΓΙΣΜΟΣ : **22.940,00** € με ΦΠΑ 24%

|  |  |
| --- | --- |
| **ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ**  **ΝΟΜΟΣ ΕΒΡΟΥ**  **ΚΕΝΤΡΟ ΚΟΙΝΩΝΙΚΗΣ ΠΡΟΣΤΑΣΙΑΣ, ΑΛΛΗΛΕΓΓΥΗΣ, ΠΑΙΔΕΙΑΣ ΚΑΙ ΠΕΡΙΒΑΛΛΟΝΤΟΣ –ΔΗΜΟΥ ΑΛΕΞΑΝΔΡΟΥΠΟΛΗΣ**  **«ΠΟΛΥΚΟΙΝΩΝΙΚΟ»**  **ΑΡ.ΜΕΛΕΤΗΣ 12/2019** | **Παροχή υπηρεσιών συμμόρφωσης, προσαρμογής και υποστήριξης ως προς τον Νέο Κανονισμό Προστασίας Προσωπικών Δεδομένων με αριθμ. 679/2016 (General Data Protection Regulation - GDPR)**  **Προϋπολογισμός: 22.940,00€ με ΦΠΑ 24%** |

##### ΤΕΚΜΗΡΙΩΣΗ ΣΚΟΠΙΜΟΤΗΤΑΣ ΤΩΝ ΥΠΗΡΕΣΙΩΝ

Ο νέος Κανονισμός Προστασίας Προσωπικών Δεδομένων (General Data Protection Regulation – GDPR 2016/679, εφεξής Κανονισμός) της ΕΕ αναφέρεται στην προστασία των φυσικών προσώπων από τη μη νόμιμη – μη εξουσιοδοτημένη χρήση δεδομένων προσωπικού χαρακτήρα και ισχύει για όλους τους οργανισμούς και τις επιχειρήσεις που έχουν έδρα ή/και δραστηριοποιούνται στην ΕΕ.

Η ημερομηνία έναρξης ισχύος του Κανονισμού είναι η 25η Μαΐου 2018. Έως τότε, κάθε Οργανισμός πρέπει να προβεί σε μια σειρά ενεργειών-σταδίων προετοιμασίας, προκειμένου να αποφευχθούν διενέξεις με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και παραβάσεις που μπορεί να οδηγήσουν σε ιδιαίτερα υψηλά πρόστιμα, τα οποία, σύμφωνα με το άρθρο 83 - Γενικοί όροι επιβολής διοικητικών προστίμων, φτάνουν έως 20.000.000 €. Οι έλεγχοι, από την Αρχή Προστασίας για τη συμμόρφωση στον κανονισμό, μπορεί να διενεργηθούν είτε κατόπιν ερωτημάτων–καταγγελιών είτε/και προληπτικά-δειγματοληπτικά. Είναι σημαντικό εξάλλου να τονιστεί ότι οι προθεσμίες για τις απαντήσεις-συμμόρφωση του φορέα προβλέπεται και πρέπει να είναι άμεσες και εντός λίγων ημερών (γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή, εντός 72 ωρών, άρθρο 33).

Ο Κανονισμός πρέπει να εφαρμοστεί σε όλο τον Οργανισμό του Κέντρου Κοινωνικής Προστασίας, Αλληλεγγύης, Παιδείας και Περιβάλλοντος – Πολυκοινωνικό Δήμου Αλεξανδρούπολης και αφορά όλο το προσωπικό που χειρίζεται προσωπικά δεδομένα τα οποία βρίσκονται όχι μόνο στο πληροφοριακό σύστημα και στα συστήματα μηχανογράφησης του Ν.Π.Δ.Δ. αλλά και σε φυσική / έντυπη μορφή και σε πολλές περιπτώσεις αποτελούν συναλλακτικό αγαθό. Με δεδομένο ότι η συμμόρφωση με το Κανονισμό αποτελεί μια πολύπλοκη και πολυεπίπεδη διαδικασία, ο ανάδοχος καλείται να παρέχει υπηρεσίες συμβουλευτικής, συντονισμού, σχεδιασμού και ανάπτυξης / υλοποίησης για ένα αριθμό σημαντικών και κρίσιμων ενεργειών (πολλές από τις οποίες απαιτούν νομικές και τεχνικές γνώσεις και εμπειρία) όπως, ενδεικτικά αλλά όχι περιοριστικά:

* ο ορισμός Ομάδας Εργασίας με συγκεκριμένους ρόλους από πλευράς του φορέα υπό τον συντονισμό της διοίκησης,
* η ενεργητική εμπλοκή στη διαδικασία προετοιμασίας, όλων των υπηρεσιών για την αποτελεσματική και έγκαιρη συμμόρφωση του φορέα με τον Κανονισμό (καταγραφή στοιχείων και χαρτογράφηση «περιοχών δεδομένων», καταγραφή διαδικασιών σχετικών με προσωπικά δεδομένα ανά υπηρεσία κλπ.),
* η κατάρτιση πλάνου δράσης εναρμόνισης των πολιτικών / διεργασιών επεξεργασίας προσωπικών δεδομένων με τον Κανονισμό και στη συνέχεια ο χρονοπρογραμματισμός και υλοποίηση των ενεργειών του και
* η προετοιμασία επιλογής Υπευθύνου Προστασίας Δεδομένων - ΥΠΔ (Data Protection Officer ή DPO) από τον φορέα, τα καθήκοντα του οποίου καθορίζονται στο άρθρο 39 του κανονισμού και ο οποίος είναι το άτομο-συντονιστής της απαιτούμενης συνεργασίας για θέματα προστασίας προσωπικών δεδομένων με διοίκηση, υπηρεσίες, πολίτες και αρχή ελέγχου.

Η εναρμόνιση του Ν.Π.Δ.Δ. με τον Κανονισμό αναμένεται ότι, μεταξύ των άλλων,

* θα προσδώσει προστιθέμενη αξία στην παροχή υπηρεσιών μέσω της δημιουργίας στρατηγικής διαχείρισης των προσωπικών δεδομένων,
* θα ενισχύσει την αξιοπιστία και τη φήμη του Οργανισμού ως υπεύθυνου φορέα διατήρησης και επεξεργασίας προσωπικών δεδομένων,
* θα ενισχύσει τη διαφάνεια ως προς τη διαχείριση των προσωπικών δεδομένων απέναντι στα υποκείμενα και
* θα θωρακίσει τον οργανισμό έναντι των αυστηρών προστίμων και αποζημιώσεων που προβλέπονται από τυχόν παραβάσεις του.

**ΠΡΟΫΠΟΛΟΓΙΣΜΟΣ**

**Συνοπτικός ενδεικτικός προϋπολογισμός**

|  |  |  |  |
| --- | --- | --- | --- |
| **Ομάδα** | **Συνοπτική περιγραφή υπηρεσίας** | **CPV** | **Ποσό** |
| Α | Παροχή υπηρεσιών συμμόρφωσης, προσαρμογής και υποστήριξης ως προς τον Νέο Κανονισμό Προστασίας Προσωπικών Δεδομένων με αριθμ. 679/2016 (General Data Protection Regulation - GDPR) | 79417000-0 | **18.500,00** € |
| ΦΠΑ 24% : | | | **4.440,00** € |
| Γενικό Σύνολο : | | | **22.940,00€**  63.547,47 |

**Αναλυτικός ενδεικτικός προϋπολογισμός**

| **Α/Α Ομάδας** | **ΣΥΝΟΠΤΙΚΗ ΠΕΡΙΓΡΑΦΗ ΥΠΗΡΕΣΙΩΝ** | **Ποσό (χωρίς ΦΠΑ)** | **ΦΠΑ 24%** | **Σύνολο με ΦΠΑ 24%** |
| --- | --- | --- | --- | --- |
| Α1 | |  | | --- | | Υπηρεσίες διάγνωσης και αποτύπωσης του επιπέδου συμμόρφωσης με τον Κανονισμό | | **7.500,00 €** | **1.800,00 €** | **9.300,00 €** |
| Α2 | Υπηρεσίες συμμόρφωσης με τον Κανονισμό | **11.000,00 €** | **2.640,00 €** | **13.640, 00 €** |
| ΓΕΝΙΚΟ ΣΥΝΟΛΟ | | | | **22.940,00 €** |

Κάθε υποψήφιος ανάδοχος οφείλει να υποβάλει προσφορά για **ΟΛΕΣ** τις υπηρεσίες που περιγράφονται στην παρούσα. Οι τιμές του ενδεικτικού προϋπολογισμού ανά υπηρεσία είναι οι μέγιστες που γίνονται αποδεκτές στον διαγωνισμό.

**ΠΗΓΗ ΧΡΗΜΑΤΟΔΟΤΗΣΗΣ**

Το ποσό για την παροχή των περιγραφόμενων στην παρούσα τεχνική έκθεση υπηρεσιών θα βαρύνει τον ακόλουθο ΚΑ του προϋπολογισμού του οικονομικού έτους 2019: **Κ.Α..00.6117.05** «Παροχή υπηρεσιών συμμόρφωσης, προσαρμογής και υποστήριξης ως προς τον Νέο Κανονισμό Προστασίας Προσωπικών Δεδομένων με αριθμ. 679/2016 (General Data Protection Regulation - GDPR)»

**ΣΥΓΓΡΑΦΗ ΥΠΟΧΡΕΩΣΕΩΝ**

**ΆΡΘΡΟ 1 Αντικείμενο των υπηρεσιών**

Η συγγραφή αυτή αφορά την παροχή υπηρεσιών εναρμόνισης / συμμόρφωσης του Οργανισμού του Κέντρου Κοινωνικής Προστασίας, Αλληλεγγύης, Παιδείας και Περιβάλλοντος – Πολυκοινωνικό Δήμου Αλεξανδρούπολης με τον νέο Ευρωπαϊκό Γενικό Κανονισμό Προστασίας Δεδομένων (General Data Protection Regulation – GDPR).

Ο ανάδοχος θα παρέχει υπηρεσίες για την ανάπτυξη, σύμφωνα με τον Κανονισμό, της Πολιτικής Προστασίας Προσωπικών Δεδομένων του Οργανισμού, που θα επικεντρώνεται στον τρόπο με τον οποίο θα γίνεται η συλλογή, αποθήκευση, επεξεργασία και διαχείριση των προσωπικών δεδομένων, καθώς και η συναίνεση του υποκειμένου, το δικαίωμα να διαγραφεί, η καταγραφή και γνωστοποίηση παραβιάσεων (διαδικασία γνωστοποίησης της παραβίασης δεδομένων & σχέδιο απόκρισης σε περίπτωση συμβάντων) και των πολιτικών και διαδικασιών για ενημερώσεις, επιθεωρήσεις και συνεχή βελτίωση.

Ενδεικτικά ο Ανάδοχος καλείται να αναπτύξει:

* Πολιτική Προστασίας Προσωπικών Δεδομένων που πληροί τις νομικές απαιτήσεις και αντιμετωπίζει το λειτουργικό κίνδυνο και τον κίνδυνο βλάβης των ατόμων,
* Πολιτική προστασίας προσωπικών δεδομένων των εργαζομένων,
* Κώδικα Δεοντολογίας που περιλαμβάνει άρθρα για την Προστασία Προσωπικών Δεδομένων,
* Πολιτική/διαδικασίες για τη συλλογή και τη χρήση ειδικών προσωπικών δεδομένων,
* Πολιτική/διαδικασίες για τη διατήρηση της ποιότητας των δεδομένων,
* Πολιτική/διαδικασίες για τη διαγραφή των προσωπικών δεδομένων,
* Πολιτική/διαδικασίες για δευτερεύουσες χρήσεις προσωπικών δεδομένων,
* Πολιτική/διαδικασίες για την απόκτηση έγκυρης συναίνεσης,
* Πολιτική/διαδικασίες για ασφαλή καταστροφή προσωπικών δεδομένων
* Πολιτική/διαδικασίες για τη χρήση των cookies και των μηχανισμών παρακολούθησης,
* Πολιτική/διαδικασίες για τη διατήρηση αρχείων,
* Οδηγίες για ενσωμάτωση της προστασίας των προσωπικών δεδομένων στη χρήση των κοινωνικών μέσων δικτύωσης από τον οργανισμό,
* Οδηγίες για ενσωμάτωση της προστασίας των προσωπικών δεδομένων στις πολιτικές / διαδικασίες του Bring Your Own Device (BYOD),
* Οδηγίες για ενσωμάτωση της προστασίας των προσωπικών δεδομένων σε πρακτικές υγείας και ασφάλειας,
* Οδηγίες για ενσωμάτωση της προστασίας των προσωπικών δεδομένων στη χρήση ΙP καμερών (ζωντανές βιντεοδιαλέξεις) και κάμερες ασφαλείας,
* Οδηγίες για ενσωμάτωση της προστασίας των προσωπικών δεδομένων σε πολιτικές / διαδικασίες σχετικά με την πρόσβαση σε λογαριασμούς υπηρεσιακού ηλεκτρονικού ταχυδρομείου των υπαλλήλων,
* Διαδικασίες ανταπόκρισης σε αιτήματα πρόσβασης σε προσωπικά δεδομένα,
* Διαδικασίες ανταπόκρισης σε αιτήματα διόρθωσης προσωπικών δεδομένων,
* Διαδικασίες ανταπόκρισης σε αιτήματα για εξαίρεση, περιορισμό της επεξεργασίας ή αντιρρήσεις στην επεξεργασία,
* Διαδικασίες ανταπόκρισης στα αιτήματα για πληροφορίες,
* Διαδικασίες ανταπόκρισης στα αιτήματα φορητότητας δεδομένων,
* Διαδικασίες (οργανωτικές και τεχνικές) ανταπόκρισης σε αιτήματα για διαγραφή δεδομένων,
* Διαδικασίες καταγραφής παραπόνων σχετικά με την προστασία των προσωπικών δεδομένων,
* Πολιτική/Διαδικασίες διαχείρισης των παραβιάσεων της ασφάλειας των προσωπικών δεδομένων ή της διαρροής αυτών,
* Σχέδιο αντιμετώπισης περιστατικών παραβίασης, διατήρηση αρχείου καταγραφής με στοιχεία όπως η φύση της παραβίασης, ο κίνδυνος, η προέλευση,
* Διαδικασίες κοινοποίησης της παραβίασης (στα ενδιαφερόμενα άτομα) και υποβολή αναφορών (σε ρυθμιστικές αρχές, πιστωτικές υπηρεσίες, κ.λπ.),
* Διαδικασία συνεχούς παρακολούθησης και ενημέρωσης για νέες απαιτήσεις συμμόρφωσης, προσδοκίες και βέλτιστες πρακτικές.

Σε αυτό το πλαίσιο, ο ανάδοχος καλείται να παρέχει υπηρεσίες συμβουλευτικής, συντονισμού, σχεδιασμού και ανάπτυξης / υλοποίησης για ένα αριθμό σημαντικών και κρίσιμων ενεργειών, οι οποίες απαιτούνται για την προσαρμογή του Ν.Π.Δ.Δ. στον GDPR, όπως

* ο ορισμός Ομάδας Εργασίας με συγκεκριμένους ρόλους από πλευράς του φορέα υπό τον συντονισμό της Διοίκησης,
* η κατάρτιση ηλεκτρονικών **Αρχείων Δραστηριοτήτων Επεξεργασίας** (ΑΔΕ), με τη συμμετοχή όλων των Υπηρεσιών καθώς και συνεργατών που επεξεργάζονται προσωπικά δεδομένα,
* η διενέργεια επιθεωρήσεων συμμόρφωσης (**compliance audits**) του Οργανισμού στο νέο Κανονισμό, προσομοίωσης ακραίων καταστάσεων και ελέγχων τρωτότητας (GDPR stress testing) του πληροφοριακού του συστήματος,
* καταγραφή των αποκλίσεων (με αναφορά στα σχετικά άρθρα του Κανονισμού) και αξιολόγηση αντικτύπου των κινδύνων παραβίασης προσωπικών δεδομένων (**Data Protection Impact Assessment - DPIA**) που απορρέουν από τις αποκλίσεις,
* Αποτίμηση Επικινδυνότητας (**Risk Assessment**) και Διαχείριση Κινδύνων (**Risk Treatment/Management**),
* η κατάρτιση πλάνου δράσης εναρμόνισης (**compliance plan**) των πολιτικών / διεργασιών επεξεργασίας προσωπικών δεδομένων με τον Κανονισμό και στη συνέχεια ο χρονοπρογραμματισμός και υλοποίηση των ενεργειών του,
* η ανάπτυξη **ενοποιημένου πληροφοριακού συστήματος** διαχείρισης προσωπικών δεδομένων,
* η προετοιμασία για πιστοποίηση και επαλήθευση της συμμόρφωσης με τον Κανονισμό,
* η προετοιμασία για την επιλογή Υπευθύνου Προστασίας Δεδομένων - ΥΠΔ (**Data Protection Officer - DPO**) στον φορέα,
* η διενέργεια εκπαιδευτικών σεμιναρίων ΥΠΔ για τα ενδιαφερόμενα στελέχη του Οργανισμού,
* η παροχή υπηρεσιών νομικής συμμόρφωσης,
* η εκπαίδευση των Υπεύθυνων Επεξεργασίας και όλου του προσωπικού στο νέο Κανονισμό.

**Αναλυτική Περιγραφή Παρεχόμενων Υπηρεσιών**

**A1. Διάγνωση και αποτύπωση του επιπέδου συμμόρφωσης με τον Κανονισμό**

Αρχικά ο Ανάδοχος θα προβεί σε αποτύπωση της μέχρι σήμερα κατάστασης με τη διαδικασία συνεντεύξεων με τη Διοίκηση, τους Διευθυντές και τους Προϊσταμένους του Οργανισμού. Τα τρέχοντα μέτρα ασφαλείας και οι έλεγχοι για την προστασία των Προσωπικών Δεδομένων θα τεκμηριωθούν και θα ληφθούν υπόψη.

**A1.1 Ενημέρωση για τον Κανονισμό και καθορισμός Ομάδας Εργασίας του Οργανισμού**

Για τη συμμόρφωση των Διευθύνσεων-Τμημάτων με το νέο Κανονισμό, κρίνεται απαραίτητη η ενημέρωση και συμμετοχή των Διευθυντών-Προϊσταμένων και του εμπλεκόμενου προσωπικού σε όλη τη διαδικασία εναρμόνισης του Ν.Π.Δ.Δ. με τον Κανονισμό με στόχο να γίνει σαφές ποιες είναι οι απαιτήσεις του και πώς η εφαρμογή του επηρεάζει τη λειτουργία των Διευθύνσεων-Τμημάτων και εντέλει όλο τον Οργανισμό. Για την επίτευξη του παραπάνω στόχου κρίνονται απαραίτητες οι παρακάτω ενέργειες/δράσεις:

* Διεξαγωγή τουλάχιστον μίας (1) εναρκτήριας συνάντησης με τον Οργανισμό με στόχο την παρουσίαση του Κανονισμού, την ευαισθητοποίηση των στελεχών του και την εξασφάλιση της δέσμευσης της διοίκησης.
* Διεξαγωγή τουλάχιστον δύο (2) συναντήσεων με στελέχη του οργανισμού που επεξεργάζονται προσωπικά δεδομένα με στόχο τον προγραμματισμό και τον καθορισμό του εύρους της παρέμβασης μέσω της συμπλήρωσης ερωτηματολογίων και της συλλογής των υφιστάμενων εγγράφων προκειμένου:
  + να αναγνωριστούν οι βασικές επιχειρησιακές περιοχές (υπηρεσίες και τμήματα) και οι επί μέρους επιχειρησιακοί υπεύθυνοι του Οργανισμού (οργανόγραμμα με αρμοδιότητες) και
  + να εντοπιστούν/επιλεγούν οι εμπλεκόμενοι με την επεξεργασία προσωπικών δεδομένων που θα αποτελέσουν την Ομάδα Εργασίας του Οργανισμού.
* Σχεδιασμός υλοποίησης της διαδικασίας, ο οποίος περιλαμβάνει:
  + τον ορισμό σημαντικών οροσήμων και των βασικών προ απαιτούμενων, ώστε να ξεκινήσουν τα επόμενα στάδια και
  + τον καθορισμό της μεθοδολογίας και των μέσων αλληλεπίδρασης και επικοινωνίας των μελών της ομάδας έργου του Αναδόχου με τα μέλη της Ομάδας Εργασίας από τη μεριά του Οργανισμού και των λοιπών ενδιαφερόμενων μερών.

**A1.2 Δημιουργία Αρχείων Δραστηριοτήτων Επεξεργασίας (ΑΔΕ) και Ροών Προσωπικών Δεδομένων**

Ο ανάδοχος σε συνεργασία με το προσωπικό του Ν.Π.Δ.Δ. θα δημιουργήσει τα απαραίτητα αρχεία που θα πρέπει να έχει στην κατοχή του και να μπορεί να επιδεικνύει ο Οργανισμός. Απαιτείται η διερεύνηση σε βάθος της οργανωτικής δομής του οργανισμού. Μέσω συνεντεύξεων και επιθεωρήσεων συμμόρφωσης (compliance audits) θα αναλυθούν σε βάθος οι διαδικασίες που αφορούν την επεξεργασία προσωπικών δεδομένων. Στα πλαίσια αυτά, απαιτείται:

* η διενέργεια συναντήσεων/συσκέψεων για την επισκόπηση των διαθέσιμων επιχειρησιακών, τεχνικών και λειτουργικών διαδικασιών προκειμένου να γίνει κατανοητή η υφιστάμενη επεξεργασία προσωπικών δεδομένων και η σχετική τεχνολογική υποδομή. Η επισκόπηση περιλαμβάνει τις ακόλουθες εργασίες:
  + αναγνώριση των συστημάτων στα οποία γίνεται επεξεργασία προσωπικών δεδομένων,
  + εντοπισμός (αναγνώριση) των προσωπικών δεδομένων (σε έντυπη ή ηλεκτρονική μορφή),
  + προσδιορισμός (αναγνώριση) των υποκειμένων των δεδομένων (υπάλληλοι, πολίτες, ανήλικοι, συνεργάτες, προμηθευτές κλπ.),
  + αποτύπωση των συστημάτων και των εφαρμογών επεξεργασίας προσωπικών δεδομένων σε σχέση με τρίτα μέρη,
  + αναγνώριση και αποτύπωση των διοικητικών ρόλων του Οργανισμού (υπεύθυνοι επιχειρησιακών διαδικασιών ή συστημάτων),
* η επιθεώρηση των σημείων αποθήκευσης των προσωπικών δεδομένων, έγγραφων και ηλεκτρονικών, η πρόσβαση σε αυτά, καθώς επίσης και οι συμφωνίες εμπιστευτικότητας που έχουν υπογραφεί, ώστε να επιβεβαιωθεί η διαφύλαξη της ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας των προσωπικών δεδομένων και των απαιτήσεων του GDPR,
* η επιθεώρηση του τρόπου επικοινωνίας με λοιπά εμπλεκόμενα τρίτα μέρη, το είδος της πληροφορίας που ανταλλάσσεται (στην περίπτωση που ανταλλάσσονται προσωπικά δεδομένα) και η αποθήκευσή της,
* η επεξεργασία των δεδομένων που καταγράφηκαν στις συναντήσεις και τις επιθεωρήσεις για τη δημιουργία ενδεικτικά:
  + καταλόγου δεδομένων προσωπικού χαρακτήρα (ποια προσωπικά δεδομένα συλλέγονται, ο σκοπός επεξεργασίας, η διαδικασία λήψης συγκατάθεσης, η πρόσβαση στα δεδομένα -εντός και εκτός του οργανισμού- η έγγραφη και / ή ηλεκτρονική αποθήκευσή τους, ο χρόνος διατήρησης)
  + ταξινόμησης των προσωπικών δεδομένων που έχει στην κατοχή του ο οργανισμός ανά τύπο (π.χ. ειδικά, εμπιστευτικά, δημόσια),
  + διαγραμμάτων ροής για τυχόν ροές δεδομένων (π.χ. μεταξύ συστημάτων, μεταξύ διαδικασιών, μεταξύ χωρών),
* η δημιουργία των Αρχείων Δραστηριοτήτων (και μέσων) Επεξεργασίας (ΑΔΕ) προσωπικών δεδομένων που επεξεργάζεται ο Οργανισμός ή συνεργαζόμενα τρίτα μέρη, κατά τα ειδικότερα οριζόμενα στο άρθρο 30 του Κανονισμού (Records of Processing Activities).

Ο ανάδοχος θα σχεδιάσει τις φόρμες βάσει των οποίων θα γίνει η καταγραφή και θα δημιουργήσει τα σχετικά αρχεία.

**A1.3 Εντοπισμός και διαπίστωση αποκλίσεων από τον Κανονισμό**

Συνίσταται στην ενδελεχή ανάλυση των αποκλίσεων των δραστηριοτήτων του Οργανισμού σε σχέση με τις απαιτήσεις του Κανονισμού και τον εντοπισμό των σημείων εκείνων που χρήζουν βελτίωσης ώστε με τις απαραίτητες συμβουλευτικές, νομικές και τεχνικές ενέργειες να επέλθει η τελική συμμόρφωση με τον Κανονισμό. Επιπλέον, θα πρέπει να καθορισθεί ποια τεχνικά και διαδικαστικά μέτρα και πολιτικές υπάρχουν και ποια πρέπει να σχεδιαστούν και να υλοποιηθούν για την προστασία των προσωπικών δεδομένων που επεξεργάζεται ο Οργανισμός (π.χ. κρυπτογράφηση δεδομένων, ασφαλής αποθήκευση και κατάλληλοι μηχανισμοί ελέγχου). Αναλυτικότερα, θα πρέπει να πραγματοποιηθούν τα παρακάτω:

* Καταγραφή των αποκλίσεων (με αναφορά στα σχετικά άρθρα του Κανονισμού) και της σημαντικότητάς τους και αξιολόγηση των επιπτώσεων παραβίασης προσωπικών δεδομένων (Data Protection Impact Assessment – DPIA).
* Αναγνώριση των απαιτούμενων προσαρμογών στα υφιστάμενα μέτρα προστασίας μέσω προσομοίωσης ακραίων καταστάσεων και ελέγχων τρωτότητας του δικτύου και του πληροφοριακού συστήματος του Οργανισμού (GDPR stress testing – ΙΤ Security Audits).
* Ενημέρωση/Επικαιροποίηση των ΑΔΕ και λοιπών ηλεκτρονικών αρχείων προσωπικών δεδομένων, εφόσον απαιτηθεί.

Η εκτίμηση αντικτύπου (DPIA) σχετικά με την προστασία προσωπικών δεδομένων θα περιλαμβάνει τουλάχιστον τα παρακάτω:

* συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, περιλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει o Οργανισμός,
* εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς και
* εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων (υποκειμένων των δεδομένων).

Ο ανάδοχος θα πρέπει να διενεργήσει τη διαδικασία προσομοίωσης ακραίων καταστάσεων (GDPR stress testing) με χρήση εξειδικευμένου λογισμικού και με πιστοποιημένο σε αυτό μηχανικό. Το εν λόγω λογισμικό, το οποίο θα πρέπει να αναφέρεται στην προσφορά του, θα πρέπει να είναι προσαρμοσμένο σε διαδικασίες ασφαλείας συμβατές με τον Κανονισμό.

**A1.4 Αποτίμηση Επικινδυνότητας και Διαχείριση Κινδύνων**

Κατά τη φάση αυτή και λαμβάνοντας υπόψιν τους κινδύνους που εντοπίστηκαν κατά την επιθεώρηση συμμόρφωσης και την εκτίμηση αντικτύπου, ο ανάδοχος θα διεξάγει τις διαδικασίες Αποτίμησης Επικινδυνότητας (Risk Assessment) και Διαχείρισης Κινδύνων (Risk Treatment/Management).

Η διαδικασία Αποτίμησης Επικινδυνότητας θα περιλαμβάνει την αποτίμηση της τρέχουσας κατάστασης και την εκτίμηση των κινδύνων για τα προσωπικά δεδομένα, των απειλών και των ευπαθειών των εξεταζόμενων πληροφοριακών συστημάτων (στα οποία είναι αποθηκευμένα τα προσωπικά δεδομένα), με την ταυτόχρονη ανάθεση υπευθυνότητας (risk owner) για κάθε ένα από τους κινδύνους. Η εκτίμηση θα γίνει με βάση την επίδραση που θα έχει η διαρροή, αποκάλυψη ή η μη εξουσιοδοτημένη τροποποίηση ή καταστροφή τους, στα φυσικά πρόσωπα που αφορούν και στην ομαλή λειτουργία του οργανισμού.

Κατά τη διαδικασία Διαχείρισης Κινδύνων, ο Οργανισμός, με τη συμβουλευτική υποστήριξη του αναδόχου, θα αποφασίσει για τη διαχείριση των κινδύνων εξετάζοντας λύσεις όπως, Αποδοχή του Επιπέδου Επικινδυνότητας (Risk Acceptance), Μεταβίβαση του Επιπέδου Επικινδυνότητας (Risk Transfer), Αποφυγή του Επιπέδου Επικινδυνότητας (Risk Avoidance) και Αντιμετώπιση του Επιπέδου Επικινδυνότητας (Risk Mitigation). Στην Αντιμετώπιση του Επιπέδου Επικινδυνότητας (Risk Mitigation) ο ανάδοχος θα προσδιορίσει τους μηχανισμούς ασφάλειας που θα χρειαστεί να υιοθετηθούν λαμβάνοντας υπόψη τους ήδη εγκατεστημένους μηχανισμούς.

**A2. Υπηρεσίες συμμόρφωσης με τον Κανονισμό**

**A2.1 Υπηρεσία κατάρτισης Σχεδίου Συμμόρφωσης (Compliance Plan) με τον Κανονισμό**

Σε συνέχεια των παραπάνω και λαμβάνοντας υπόψη τους κινδύνους που εντοπίστηκαν και τις διαδικασίες Αποτίμησης Επικινδυνότητας και Διαχείρισης Κινδύνων, θα καταρτισθεί ένα συνολικό πλάνο δράσης εναρμόνισης (compliance plan) το οποίο θα περιλαμβάνει όλες τις απαιτούμενες ενέργειες προκειμένου ο Οργανισμός να υιοθετήσει τις διαδικασίες που θα του επιτρέψουν να συμμορφωθεί με τις απαιτήσεις του Κανονισμού. Το πλάνο θα περιλαμβάνει συγκεκριμένες προτάσεις ευθυγράμμισης με τον Κανονισμό και θα δώσει τα μέσα-εργαλεία συμμόρφωσης στα στελέχη του οργανισμού που εμπλέκονται στις διαδικασίες επεξεργασίας προσωπικών δεδομένων. Ειδικότερα απαιτούνται:

* Η κατάρτιση σαφούς σχεδίου στο οποίο θα συμπεριλαμβάνονται οι προτάσεις βελτίωσης, με σκοπό την αντιμετώπιση των ελλείψεων ή / και αποκλίσεων σε σχέση με τις απαιτήσεις του Κανονισμού. Το σχέδιο θα συμπεριλαμβάνει:
  + λίστα αποκλίσεων που θα πρέπει να καλυφθούν,
  + προσδιορισμό συγκεκριμένων εργασιών, ώστε να βελτιωθεί κατά το δυνατόν πιο άμεσα το επίπεδο συμμόρφωσης με αναφορά σε προτεινόμενες ενέργειες για την αντιμετώπιση των μη συμμορφώσεων και σε προτεινόμενα μέτρα ελέγχου για τον περιορισμό των κινδύνων.
* Η παροχή προτάσεων για την υλοποίηση διορθωτικών ενεργειών που άπτονται των νομικών απαιτήσεων του Κανονισμού καθώς και του περιβάλλοντος λειτουργίας των πληροφοριακών συστημάτων του Οργανισμού.

Για την κάθε ενέργεια της μεθοδολογίας που θα καταρτιστεί σε αυτό το στάδιο, εκτός από την εκτίμηση χρόνου και κόστους, ο ανάδοχος, σε συνεννόηση και συμφωνία με την Ομάδα Εργασίας του Ν.Π.Δ.Δ., θα πρέπει να καταγράψει κατά πόσον το συγκεκριμένο βήμα μπορεί να υλοποιηθεί από το προσωπικό του Οργανισμού ή με τη βοήθεια τρίτου, και σε ποιο βαθμό.

**A2.2 Υπηρεσία Ανάλυσης Πληροφοριακού Συστήματος Διαχείρισης Προσωπικών Δεδομένων**

Το επόμενο στάδιο είναι η ανάλυση του πληροφοριακού συστήματος διαχείρισης των υποχρεώσεων του Κανονισμού που θα υποστηρίζει:

* όλες τις απαιτούμενες πολιτικές και διαδικασίες προστασίας προσωπικών δεδομένων που θα αποφασιστούν και
* τις περιοδικές ή έκτακτες υποχρεώσεις του οργανισμού στην έκδοση αναφορών και τη διαχείριση των απαιτήσεων των υποκειμένων επεξεργασίας προσωπικών δεδομένων.

Επιπλέον, ο ανάδοχος θα επικαιροποιήσει τα ΑΔΕ, εφόσον απαιτηθεί, και θα προτείνει και θα αναλάβει την επίβλεψη της υλοποίησης όλων των απαραίτητων τεχνικών ενεργειών για

* την πλήρη συμβατότητα και διαλειτουργικότητα του νέου πληροφοριακού συστήματος με το ήδη εγκατεστημένο πληροφοριακό σύστημα του Ν.Π.Δ.Δ. και
* την προσαρμογή του υφιστάμενου πληροφοριακού συστήματος στις ανάγκες του Κανονισμού, σε διαρκή συνεννόηση/επικοινωνία με τους συνεργαζόμενους τρίτους, οι οποίοι παρέχουν λογισμικό και υπηρεσίες που σχετίζεται με την επεξεργασία προσωπικών δεδομένων, ως υποσυστήματα του πληροφοριακού συστήματος του Ν.Π.Δ.Δ.

**A2.3 Υπηρεσίες νομικής συμμόρφωσης**

Στο πλαίσιο της ανάπτυξης των πολιτικών / διαδικασιών σύμφωνα με τον Κανονισμό, ο ανάδοχος θα παρέχει, σε συνεργασία με το νομικό τμήμα του Οργανισμού, υπηρεσίες νομικής συμμόρφωσης για:

* την προσαρμογή στις απαιτήσεις του Κανονισμού των συμβολαίων και συμβάσεων του οργανισμού με προμηθευτές, συνεργάτες, πελάτες και εργαζομένους καθώς επίσης και των φορμών συγκατάθεσης των υποκειμένων και
* την κατάρτιση Κώδικα Δεοντολογίας, με τη μορφή που περιγράφεται στον Κανονισμό, ώστε να μπορεί ο Δήμος να τον παραδώσει στην Εποπτική Αρχή για έγκριση.

Ειδικότερα, η Πολιτική Συνεργατών θα περιλαμβάνει ενδεικτικά τα παρακάτω:

* Απαιτήσεις από τους συνεργάτες για την Προστασία των Προσωπικών Δεδομένων κατά την εκτέλεση συμβάσεων ή συμφωνιών.
* Όροι για δέουσα επιμέλεια σχετικά με την Προστασία των Προσωπικών Δεδομένων.
* Ειδικοί όροι για τους παρόχους cloud.
* Άρθρα για την αντιμετώπιση περιπτώσεων μη συμμόρφωσης με συμβάσεις και συμφωνίες ή τους όρους προστασίας προσωπικών δεδομένων που επιβάλλει ο GDPR.

Επιπλέον, ο ανάδοχος θα παρέχει σχετικά κείμενα ως προς τη συγγραφή της συναίνεσης.

Τέλος ο ανάδοχος θα συνεισφέρει στο σχεδιασμό ενός σήματος αξιοπιστίας και εφαρμογής του Γενικού Κανονισμού για την ιστοσελίδα του Κέντρου Κοινωνικής Προστασίας, Αλληλεγγύης, Παιδείας και Περιβάλλοντος – Πολυκοινωνικό Δήμου Αλεξανδρούπολης με στόχο την ενίσχυση της εμπιστοσύνης προς το Κέντρου Κοινωνικής Προστασίας, Αλληλεγγύης, Παιδείας και Περιβάλλοντος – Πολυκοινωνικό Δήμου Αλεξανδρούπολης.

**A2.4 Συμβουλευτικές υπηρεσίες επιλογής Υπεύθυνου Προστασίας Δεδομένων (ΥΠΔ)**

Στο πλαίσιο των εν λόγω υπηρεσιών ο ανάδοχος θα διενεργήσει εκπαιδευτικά σεμινάρια ΥΠΔ για τα στελέχη που θα υποδείξει ο Δήμος και θα παρέχει συμβουλευτικές υπηρεσίες για την επιλογή Data Protection Officer (DPO) και της ομάδας που θα τον/την πλαισιώνει από το προσωπικό του Ν.Π.Δ.Δ..

Ο Data Protection Officer θα παρακολουθεί, αναθεωρεί και βελτιώνει τις πολιτικές / διαδικασίες Προσωπικών Δεδομένων που θα αναπτύξει και θα λειτουργεί το Κέντρο Κοινωνικής Προστασίας, Αλληλεγγύης, Παιδείας και Περιβάλλοντος – Πολυκοινωνικό Δήμου Αλεξανδρούπολης, με βάση τις απαιτήσεις του Κανονισμού για την προστασία των προσωπικών δεδομένων. Επιπλέον, θα παρακολουθεί την εφαρμογή των τεχνικών και οργανωτικών μέτρων που έχει δεσμευτεί να πραγματοποιήσει ο Κέντρο Κοινωνικής Προστασίας, Αλληλεγγύης, Παιδείας και Περιβάλλοντος – Πολυκοινωνικό Δήμου Αλεξανδρούπολης στο Compliance Plan, θα επικαιροποιεί το/α DPIAs που έχουν δημιουργηθεί για τις επεξεργασίες υψηλού ρίσκου, θα δημιουργεί νέα DPIAs για νέες επεξεργασίες υψηλού ρίσκου, θα αναλαμβάνει τις ενημερώσεις του προσωπικού και τις εσωτερικές επιθεωρήσεις, με στόχο την επίτευξη του βέλτιστου επιπέδου προστασίας.

**A2.5 Υπηρεσίες διαχείρισης ποιότητας και Υπηρεσίες Εκπαίδευσης**

Με το πέρας της υλοποίησης των μέτρων συμμόρφωσης και του πληροφοριακού συστήματος διαχείρισης θα διενεργηθούν εκ νέου επιθεωρήσεις ετοιμότητας (compliance audits), Data Protection Impact Assessment (DPIA), έλεγχοι τρωτότητας του πληροφοριακού συστήματος του Οργανισμού, αποτίμηση επικινδυνότητας και διαχείριση κινδύνων στα πλαίσια της προετοιμασίας και εκπόνησης διαδικασιών για πιστοποίηση και επαλήθευση της συμμόρφωσης με τον Κανονισμό.

Ο ανάδοχος θα παρουσιάσει στη Διοίκηση του Οργανισμού τα αποτελέσματα των επιθεωρήσεων συμμόρφωσης, των ελέγχων τρωτότητας, των DPIA’s και των διαδικασιών αποτίμησης επικινδυνότητας και διαχείρισης κινδύνων, τόσο κατά το πρώτο στάδιο καταγραφής των αποκλίσεων από τον Κανονισμό όσο και στο τέλος της παροχής των υπηρεσιών. Σε κάθε παρουσίαση θα αναλυθούν οι μεγαλύτεροι κίνδυνοι που αντιμετωπίζει ο Δήμος όσον αφορά τα προσωπικά δεδομένα, οι risk owners, καθώς επίσης και τα προτεινόμενα μέτρα και οι ενέργειες αποκατάστασης, με εκτίμηση χρόνου και κόστους υλοποίησης.

Επίσης, ο ανάδοχος θα πρέπει να διενεργήσει εκπαίδευση των στελεχών στον Κανονισμό αναφορικά με τις απαιτήσεις στο χειρισμό δεδομένων, υπηρεσιών και περιστατικών παραβιάσεων προσωπικών δεδομένων. Σημαντική μέριμνα θα υπάρξει για την εκπαίδευση τόσο των Υπευθύνων Επεξεργασίας του Οργανισμού στη μεθοδολογία των επιθεωρήσεων (audits) και στις βέλτιστες, διεθνώς ακολουθούμενες πρακτικές επί της επεξεργασίας και ασφάλειας των προσωπικών δεδομένων, όσο και όλου του προσωπικού και των εκπροσώπων του Νομικού Τμήματος, έτσι ώστε όλοι να:

* Είναι ενήμεροι για τον GDPR, τις απαιτήσεις του κανονισμού και την υποχρέωση του Οργανισμού να συμμορφώνεται με αυτές.
* Είναι γνώστες των πολιτικών προστασίας προσωπικών δεδομένων και των επιμέρους διαδικασιών.
* Καταλαβαίνουν πλήρως το ρόλο και τις ευθύνες που τους έχουν ανατεθεί σχετικά με τη συμμόρφωση με τον GDPR.
* Γνωρίζουν για τις διαδικασίες αντιμετώπισης συμβάντων αλλά και τις υπόλοιπες κρίσιμες διαδικασίες Προστασίας Προσωπικών Δεδομένων.
* Αποδέχονται τις Πολιτικές Προστασίας Προσωπικών Δεδομένων και τις αντίστοιχες διαδικασίες.

Ο υποψήφιος ανάδοχος, θα πρέπει να παρουσιάσει στην προσφορά του ολοκληρωμένο προτεινόμενο πρόγραμμα κατάρτισης ανά κατηγορία εκπαιδευομένων και γνωστικό αντικείμενο καθώς επίσης και αναλυτικό χρονοδιάγραμμα εκπαίδευσης ανά ομάδα εκπαιδευομένων και εκπαιδευτικό κύκλο. Ο ανάδοχος θα παρέχει τουλάχιστον 150 ώρες εκπαίδευση των στελεχών του Ν.Π.Δ.Δ. σε χώρους του Οργανισμού, σε τμήματα που θα διαμορφώσει ανάλογα με το ρόλο και τον βαθμό εμπλοκής των εκπαιδευόμενων με προσωπικά δεδομένα. Επίσης θα πρέπει να οργανώσει 3 τουλάχιστον ημερίδες σε χώρους του Ν.Π.Δ.Δ. που θα αφορούν την ευρύτερη ενημέρωση όλου του προσωπικού για τις νέες διαδικασίες. Πέραν των εκπαιδεύσεων με τη φυσική του παρουσία, ο ανάδοχος θα παρέχει / δημιουργήσει κατάλληλο εκπαιδευτικό υλικό που θα διατεθεί σε όλο το προσωπικό του Ν.Π.Δ.Δ.

**ΆΡΘΡΟ 2 Ομάδες Υπηρεσιών**

| **Α/Α** | **ΣΥΝΟΠΤΙΚΗ ΠΕΡΙΓΡΑΦΗ ΥΠΗΡΕΣΙΩΝ** |
| --- | --- |
| **Α1** | **Υπηρεσίες διάγνωσης και αποτύπωσης του επιπέδου συμμόρφωσης με τον Κανονισμό** |
| Α1.1 | |  | | --- | | Ενημέρωση για τον Κανονισμό και καθορισμός Ομάδας Εργασίας του Οργανισμού | |
| Α1.2 | Δημιουργία Αρχείων Δραστηριοτήτων Επεξεργασίας (ΑΔΕ) και Ροών Προσωπικών Δεδομένων |
| Α1.3 | Εντοπισμός και διαπίστωση αποκλίσεων από τον Κανονισμό |
| A1.4 | Αποτίμηση Επικινδυνότητας και Διαχείριση Κινδύνων |
| **Α2** | **Υπηρεσίες συμμόρφωσης με τον Κανονισμό** |
| Α2.1 | Υπηρεσίες κατάρτισης Σχεδίου Συμμόρφωσης με τον GDPR |
| Α2.2 | Υπηρεσία ανάλυσης Πληροφοριακού Συστήματος Διαχείρισης Προσωπικών Δεδομένων |
| A2.3 | Υπηρεσίες νομικής συμμόρφωσης |
| Α2.4 | Συμβουλευτικές υπηρεσίες επιλογής Υπεύθυνου Προστασίας Δεδομένων (ΥΠΔ) |
| Α2.5 | Υπηρεσίες διαχείρισης ποιότητας και Υπηρεσίες Εκπαίδευσης |

### ΆΡΘΡΟ 3 Ισχύουσα νομοθεσία

Στην παρούσα υπηρεσία ισχύουν οι παρακάτω νόμοι και διατάξεις,

1. Οι διατάξεις του Ν. 4412/2016 «Δημόσιες Συμβάσεις Έργων, Προμηθειών και

Υπηρεσιών.

1. Οι διατάξεις της παρ. 9 του άρθρου 209 του Ν. 3463/2006 «Κύρωση του Κώδικα Δήμων και Κοινοτήτων» (ΦΕΚ Α 114/8.6.2006).
2. Οι διατάξεις του Ν. 3852/2010 (ΦΕΚ 87 Α) «Νέα Αρχιτεκτονική της Αυτοδιοίκησης και της Αποκεντρωμένης Διοίκησης – Πρόγραμμα Καλλικράτης», όπως ισχύει σήμερα.
3. Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)

**ΆΡΘΡΟ 4 Οικονομική Προσφορά**

Ο κάθε υποψήφιος θα πρέπει να υποβάλει προσφορά **για το σύνολο** των υπηρεσιών που περιγράφονται στην παρούσα τεχνική έκθεση**.** Δεν γίνονται δεκτές προσφορές για ορισμένες μόνο υπηρεσίες. Οι προσφορές ισχύουν και δεσμεύουν τους οικονομικούς φορείς για **εκατό είκοσι (120)** ημέρες από την επομένη της κατάθεσης.

**ΆΡΘΡΟ 5 Πληρωμές Αναδόχου**

Η καταβολή της αμοιβής του αναδόχου θα γίνεται τμηματικά μετά την προσκόμιση των σχετικών τιμολογίων και των δικαιολογητικών που απαιτούνται για την έκδοση χρηματικών ενταλμάτων πληρωμής, ως εξής:

το 40% του ενδεικτικού προϋπολογισμού θα καταβληθεί με την ολοκλήρωση των εργασιών της ομάδας Α1 και το 60% του ενδεικτικού προϋπολογισμού θα καταβληθεί με την ολοκλήρωση των εργασιών της ομάδας Α2.

Τα εκδιδόμενα τιμολόγια θα εξοφληθούν πλήρως (100%) μετά από την οριστική παραλαβή των επιμέρους υπηρεσιών της κάθε ομάδας (άρθρο 200 παρ. 1-4 Ν. 4412/2016).

**ΆΡΘΡΟ 6 Αναθεώρηση τιμών**

Το ποσό της προσφοράς του αναδόχου είναι σταθερό και αμετάβλητο σ’ όλη τη διάρκεια της σύμβασης που θα συναφθεί και δεν αναθεωρείται για κανένα λόγο.

**ΆΡΘΡΟ 7 Προθεσμία εκτέλεσης των υπηρεσιών/ Χρονοδιάγραμμα Υλοποίησης**

Ως χρόνος ολοκλήρωσης των υπηρεσιών των Ομάδων Υπηρεσιών Α1 και Α2 ορίζονται οι δύο (2) και δύο (2) μήνες αντίστοιχα, από την υπογραφή της σύμβασης. Ο ανάδοχος θα πρέπει να υποβάλλει σχετικό χρονοδιάγραμμα υλοποίησης/παροχής των παραπάνω υπηρεσιών λαμβάνοντας υπόψη ότι οι υπηρεσίες που σχετίζονται με τη συμμόρφωση του Ν.Π.Δ.Δ. θα πρέπει να έχουν ολοκληρωθεί το αργότερο εντός πέντε (5) μηνών από την υπογραφή της σύμβασης.

**ΑΡΘΡΟ 8 Κριτήριο κατακύρωσης**

Η ανάθεση της υπηρεσίας θα γίνει µε κριτήριο κατακύρωσης την πλέον συμφέρουσα από οικονομική άποψη προσφορά αποκλειστικά βάσει τιμής (χαμηλότερη τιμή) στο σύνολο του ενδεικτικού προϋπολογισμού εφόσον η προσφορά είναι σύμφωνη με όσα προβλέπονται στην παρούσα τεχνική έκθεση.

**ΆΡΘΡΟ 9 Εμπιστευτικότητα και ασφάλεια δεδομένων**

Ο Ανάδοχος υποχρεούται να μην ανακοινώνει, διαθέτει ή δημοσιοποιεί με οποιονδήποτε τρόπο σε τρίτους, οι οποίοι δεν σχετίζονται με τους σκοπούς των εργασιών συμμόρφωσης με τον GDPR και για τους οποίους δεν υπάρχει τέτοια υποχρέωση ή δικαίωμα από το νόμο ή δικαστική απόφαση, πληροφορίες που έχουν λάβει και επεξεργάζονται στα πλαίσια της παροχής υπηρεσιών εκ μέρους τους. Ειδικότερα αναλαμβάνει να τηρεί τις υποχρεώσεις που απορρέουν από τον Ν.2472/1997 περί προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τις σχετικές πράξεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, όπως αυτές αναμένεται να προσαρμοστούν μετά την καθολική εφαρμογή του Κανονισμού σε Εθνικό Επίπεδο.

Αλεξανδρούπολη, 22-04-2019

|  |  |
| --- | --- |
| Ο ΣΥΝΤΑΞΑΣ  ΚΑΛΤΣΟΥΚΑΛΑ ΔΗΜΗΤΡΑ | ΘΕΩΡΗΘΗΚΕ  Ο ΑΝ. ΠΡΟΪΣΤΑΜΕΝΟΣ  ΟΙΚΟΝΟΜΙΚΟΥ ΤΜΗΜΑΤΟΣ  ΓΚΑΜΠΙΤΣΑΚΗΣ ΖΑΧΑΡΙΑΣ |

1. **Αποδεικτικά τεχνικής και επαγγελματικής ικανότητας** **:**

Όσον αφορά στην τεχνική και επαγγελματική ικανότητα για την παρούσα διαδικασία σύναψης σύμβασης, οι οικονομικοί φορείς απαιτείται:

* κατά τη διάρκεια της τελευταίας 2ετίας, να έχουν εκτελέσει ή να εκτελούν τουλάχιστον 3 έργα που αφορούν το σύνολο του προγράμματος συμμόρφωσης GDPR είτε σε οργανισμός τοπικής αυτοδιοίκησης (Ο.Τ.Α.), είτε σε εταιρείες ή άλλους οργανισμούς. Προς απόδειξη αυτού είναι η προσκόμιση των αντίστοιχων συμβάσεων παροχής υπηρεσιών ή βεβαιώσεις καλής εκτέλεσης τους.
* να διαθέτουν πιστοποίηση κατά ISO 9001:2015 και 27001:2013. Προς απόδειξη αυτού απαιτείται η προσκόμιση των εν λόγω πιστοποιητικών από διαπιστευμένους φορείς πιστοποίησης.
* Η προτεινόμενη ομάδα έργου θα πρέπει να περιλαμβάνει κατ’ ελάχιστο τις ακόλουθες ειδικότητες:

1. Τουλάχιστον ένα (1) νομικό, με επιθυμητή πιστοποίηση Υπευθύνου Επεξεργασίας Δεδομένων (DPO) και αποδεδειγμένη προϋπηρεσία σε έργα εναρμόνισης οργανισμών: τοπικής αυτοδιοίκησης, δημόσιών ή και ιδιωτικών.
2. Τουλάχιστον ένα (1) πτυχιούχο ανώτατης εκπαίδευσης στο αντικείμενο πληροφορικής, και να διαθέτει τουλάχιστον 3ετή επαγγελματική σχετική εμπειρία σε πληροφοριακά συστήματα και εφαρμογές ασφαλείας, σύμφωνα με τις ανάγκες και προβλέψεις του GDPR.
3. Τα ακαδημαϊκά προσόντα και η προϋπηρεσία των στελεχών του Αναδόχου θα πιστοποιούνται με την προσκόμιση (i) Βιογραφικών Σημειωμάτων, (ii) αντίγραφα ακαδημαϊκών τίτλων, και (iii) αντίγραφα ή άλλο έγγραφα, από το οποία να προκύπτει η σχετική επαγγελματική εμπειρία, ως ανωτέρω (ανάθεση, σύμβαση, πιστοποιητικά καλής εκτέλεσης, δημοσιεύσεις, πιστοποιήσεις κλπ).