Περιφερειακό Ταμείο Ανάπτυξης Κρήτης

ΠΡΟΣΚΛΗΣΗ ΕΚΔΗΛΩΣΗΣ ΕΝΔΙΑΦΕΡΟΝΤΟΣ

Αρ.Πρωτ.7471

Ηράκλειο 18-12-2018

Για την ανάθεση υπηρεσιών **Υπευθύνου Προσωπικών Δεδομένων (DATA PROTECTION OFFICER - D.P.O.) και υπηρεσιών συμμόρφωσης** στα πλαίσια του Κανονισμού 2016/679 (ΕΕ) - GDPR για το Περιφερειακό Ταμείο Ανάπτυξης Κρήτης συνολικού προϋπολογισμού **11.000,00€ συμπεριλαμβανομένου του Φ.Π.Α**., με κριτήριο κατακύρωσης την πλέον συμφέρουσα από οικονομική άποψης προσφορά βάσει τιμής .

Ο ΠΡΟΕΔΡΟΣ Δ.Σ ΤΟΥ ΠΤΑ ΚΡΗΤΗΣ

Έχοντας υπόψη:

1. Τις διατάξεις:

α. του Ν.3852/2010 «Νέα Αρχιτεκτονική της Αυτοδιοίκησης και της Αποκεντρωμένης Διοίκησης - Πρόγραμμα Καλλικράτης» (ΦΕΚ 87/Α΄/7-6-2010).

β. του Ν.2218/94 (Κεφ. Β' περί Περιφερειακών Ταμείων Ανάπτυξης) όπως τροποποιήθηκε με το Ν. 2307/95 άρθρο 12 παρ. 10 και με το Ν. 2503/97 άρθρο 4 παρ. 3. και ισχύει σήμερα.

γ. της υπ' αριθ. 4683/98 απόφασης του Υπουργού ΕΣΔΔΑ «Κανονισμός Προσωπικού των ΠΤΑ» (ΦΕΚ 140/Β/18-2-98).

2. Τον Ν. 4412/2016 (ΦΕΚ 147Α) «Δημόσιες συμβάσεις έργων, προμηθειών και υπηρεσιών».

3.Την υποχρέωση ορισμού Υπευθύνου Προσωπικών Δεδομένων έναντι της αρχής (ΑΠΔΠΧ) και των υποκειμένων και για την καθοδήγηση της ΠΤΑ Κρήτης κατά την συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Δεδομένων 2016/679 (ΕΕ) - GDPR.

4.Τις υπηρεσιακές ανάγκες.

ΚΑΛΕΙ

Όλους τους ενδιαφερόμενους που επιθυμούν και δραστηριοποιούνται στο αντικείμενο της παρούσης, να υποβάλλουν έγγραφες σφραγισμένες προσφορές για την **παροχή υπηρεσιών Υπευθύνου Προσωπικών Δεδομένων και υπηρεσιών συμμόρφωσης** (σύμφωνα με την ισχύουσα νομοθεσία) του ΠΤΑ Κρήτης **στα πλαίσια του Κανονισμού** 2016/679 **(ΕΕ)** - **GDPR.**

Η επαγγελματική δραστηριότητα υποδεικνύεται με εγγραφή στο οικείο επαγγελματικό μητρώο.

Ο συνολικός προϋπολογισμός ανέρχεται στο ποσό των **11.000,00 € συμπεριλαμβανομένου του Φ.Π.Α.** και κριτήριο κατακύρωσης ορίζεται η πλέον συμφέρουσα από οικονομική άποψη προσφοράς βάσει τιμής.

Η αξιολόγηση των προσφορών θα γίνει από το ΠΤΑ Κρήτης

ΤΟΠΟΣ ΥΠΟΒΟΛΗΣ ΠΡΟΣΦΟΡΩΝ	**ΚΑΤΑΛΗΚΤΙΚΗ ΗΜΕΡΟΜΗΝΙΑ ΥΠΟΒΟΛΗΣ ΠΡΟΣΦΟΡΩΝ**	**ΗΜΕΡΑ**	**ΩΡΑ**
ΠΤΑ Κρήτης **Μάχης Κρήτης και Εφόδου 3** **Μέγαρο Χάνδαξ Κτήριο Γ** **2ος Όροφος** **71 201, Ηράκλειο**	**30 Ιανουαρίου 2019**	**Τετάρτη**	**14.30 μ.μ.**

Α. Αντικείμενο της πρόσκλησης

Αντικείμενο της παρούσας πρόσκλησης είναι η **παροχή υπηρεσιών Υπευθύνου Προσωπικών Δεδομένων και υπηρεσιών συμμόρφωσης** (σύμφωνα με την ισχύουσα νομοθεσία) του ΠΤΑ Κρήτης **στα πλαίσια του Κανονισμού** 2016/679 **(ΕΕ)** - **GDPR** για **πέντε (5) μήνες**, με τη διαδικασία της απευθείας ανάθεσης. Οι τεχνικές προδιαγραφές περιγράφονται αναλυτικά στο **ΠΑΡΑΡΤΗΜΑ Α'.**
Για οποιαδήποτε πληροφορία ως προς το αντικείμενο της παρούσας: **ΠΤΑ ΚΡΗΤΗΣ τηλ. επικοινωνίας 2810-302469 ,pta@pta.gr.**
Η υποβολή προσφοράς αποτελεί τεκμήριο ότι ο προσφέρων έχει λάβει πλήρη γνώση και αποδέχεται τους όρους καθώς και τις τεχνικές προδιαγραφές της παρούσας πρόσκλησης.

Β. Κατάρτιση και υποβολή προσφορών

Οι προσφορές υποβάλλονται ή αποστέλλονται με οποιονδήποτε τρόπο από τους υποψηφίους Αναδόχους, σε σφραγισμένο φάκελο, στον οποίο τοποθετούνται:

1. Έγγραφη οικονομική προσφορά σύμφωνα με το υπόδειγμα του **ΠΑΡΑΡΤΗΜΑΤΟΣ Β'**. Οι τιμές των προσφορών θα εκφράζονται σε ευρώ.
2. Πιστοποιητικό εγγραφής στο οικείο επιμελητήριο, σε ισχύ, στο οποίο θα αναφέρεται το ειδικό επάγγελμα.
3. Υπεύθυνη δήλωση στην οποία θα δηλώνεται ότι:

- Δεν τελούν σε πτώχευση ή σε διαδικασία πτώχευσης ή πτωχευτικού συμβιβασμού.
- Δεν έχουν καταδικασθεί για αδίκημα σχετικά με την άσκηση της επαγγελματικής τους δραστηριότητας.
- Μέχρι και την ημέρα υποβολής της προσφοράς είναι φορολογικά και ασφαλιστικά ενήμεροι ως προς τις υποχρεώσεις τους.
- Δε συντρέχουν οι λόγοι αποκλεισμού του οικονομικού φορέα από τη συμμετοχή σε διαδικασία σύναψης σύμβασης των παραγράφων 1 και 2 του άρθρου 73 του Ν.4412/2016 (147 Α)
- Δεν έχουν τιμωρηθεί με αποκλεισμό από διαγωνισμούς προμηθειών ή υπηρεσιών του δημόσιου τομέα.
- Ότι έλαβαν γνώση των όρων της παρούσας πρόσκλησης και τους αποδέχονται πλήρως και ανεπιφυλάκτως.

Στο φάκελο κάθε προσφοράς πρέπει να αναγράφονται ευκρινώς:

1) Η λέξη «ΠΡΟΣΦΟΡΑ» με κεφαλαία γράμματα.
2) Ο πλήρης τίτλος της αρμόδιας Υπηρεσίας.
3) Ο αριθμός πρωτοκόλλου της Πρόσκλησης.
4) Τα στοιχεία του αποστολέα (επωνυμία και διεύθυνση του υποψήφιου Αναδόχου, οδός, αριθμός, πόλη, ΤΚ, τηλέφωνα, fax, email).

Περιπτώσεις προσφορών που παρουσιάζουν επιφυλάξεις ή αποκλίσεις από οποιοδήποτε όρο της παρούσας **απορρίπτονται.** Αν υπάρχει στην προσφορά οποιαδήποτε διόρθωση, αυτή πρέπει να είναι καθαρογραμμένη και υπογεγραμμένη από τον υποψήφιο ή το νόμιμο εκπρόσωπό του. Για την σύγκριση των προσφορών θα λαμβάνεται υπόψη η τιμή χωρίς φ.Π.Α. Σε περίπτωση που κατατεθούν προσφορές με την ίδια ακριβώς τιμή, αυτές θεωρούνται ισότιμες και η αναθέτουσα αρχή θα επιλέξει τον ανάδοχο με κλήρωση.

Γ. Διάρκεια Σύμβασης

Η διάρκεια της σύμβασης θα είναι **για πέντε (5) μήνες** από την ημερομηνίας υπογραφής.

Επισημαίνεται ότι, το φυσικό και οικονομικό αντικείμενο της σύμβασης δεν πρέπει να μεταβάλλεται ουσιωδώς κατά τη διάρκεια εκτέλεσής της, κατά τα οριζόμενα στην παρ. 4 του άρθρο 132 του Ν.4412/2016. Δυνατότητα μεταβολής υφίσταται, μόνο υπό τις προϋποθέσεις του άρθρου 132 του Ν.4412/2016.

Δ. Υποχρεώσεις Αναδόχου

Ο Ανάδοχος υποχρεούται να συνεργαστεί με οποιαδήποτε τμήμα του ΠΤΑ Κρήτης ή και κάθε τρίτο, με τον τρόπο που θα του υποδείξει η αρμόδια Διεύθυνση.

Ο Ανάδοχος υποχρεούται να εξασφαλίσει την έγκαιρη και άριστης ποιότητας υπηρεσία, που συνιστά το αντικείμενο της παρούσας Πρόσκλησης.

Στο κόστος υπηρεσίας περιλαμβάνονται όλα τα παράπλευρα έξοδα μετακίνησης, αμοιβής προσωπικού, που κρίνονται κάθε φορά απαραίτητα.

Ε. Εμπιστευτικότητα - Εχεμύθεια

Τα συμβαλλόμενα μέρη δεσμεύονται πλήρως ότι δεν θα κοινοποιήσουν σε τρίτους, παρά μόνο για σκοπούς που σχετίζονται με την παρούσα σύμβαση, οποιαδήποτε πληροφορία που από τη φύση της ή κατόπιν συμφωνίας θεωρείται εμπιστευτική, ενδεικτικά αναφερομένων εγγράφων, αναφορών, λογισμικού, οργανωτικών πληροφοριών, σχεδίων, εικόνων, κινούμενων εικόνων, βίντεο, φωτογραφιών, ηχητικών σημάτων, γραφικών κλπ., ή πληροφοριών που μπορεί να σχετίζονται με την εσωτερική οργάνωση του ΠΤΑ Κρήτης , τον τρόπο λειτουργίας των συστημάτων, καθώς και πληροφορίες που αφορούν σε προσωπικά δεδομένα πολιτών, επιχειρήσεων, επαγγελματιών και γενικά οικονομικών και επαγγελματικών φορέων.

- Δεν επιτρέπεται χρήση των πληροφοριών αυτών, πέραν του σκοπού των εργασιών που ανατίθενται.
- Τα συμβαλλόμενα μέρη αποκαλύπτουν εμπιστευτικές πληροφορίες μόνο σε όσους υπαλλήλους ασχολούνται άμεσα με το περιεχόμενο της παρούσας και διασφαλίζουν ότι οι υπάλληλοι αυτοί γνωρίζουν και αποδέχονται τις υποχρεώσεις εχεμύθειας.
- Θα λαμβάνονται από τον ανάδοχο όλα τα απαραίτητα μέτρα για την προστασία των πληροφοριών καθ' όλη τη διάρκεια των εργασιών του. Εάν οποιαδήποτε στιγμή, υπάρξουν ενδείξεις ότι έχουν διαρρεύσει ή πρόκειται να διαρρεύσουν πληροφορίες, θα ενημερωθεί άμεσα το ΠΤΑ Κρήτης.
- Δύναται να ελεγχθεί οποιοσδήποτε προσωπικός υπολογιστής ή φορητό αποθηκευτικό μέσο του αναδόχου, βρεθεί στην υπηρεσία.
- Ο ανάδοχος, με κανένα τρόπο, δεν επιτρέπεται να προβαίνει σε δημόσιες δηλώσεις σχετιζόμενες με την εν γένει κατάσταση του ΠΤΑ Κρήτης , χωρίς την προηγούμενη άδεια της Διοίκησης του ΠΤΑ Κρήτης.
- Οι όροι της σύμβασης δεσμεύουν τον Ανάδοχο ακόμα και μετά τη λήξη των εργασιών του.

Αθέτηση του καθήκοντος εχεμύθειας εκ μέρους ενός των συμβαλλομένων μερών θα συνεπάγεται έναντι του αντισυμβαλλομένου υποχρέωση αποζημίωσης και αποκατάστασης της τυχόν ζημίας, παύσης κοινοποίησης των εμπιστευτικών πληροφοριών και παράλειψης κοινοποίησής τους στο μέλλον.

ΣΤ. Κρατήσεις - Πληρωμή

Η πληρωμή θα γίνεται τμηματικά μετά την οριστική παραλαβή των παρεχόμενων υπηρεσιών που θα παραδίδονται κάθε φορά από τον ανάδοχο με την εξόφληση του 100% της αξίας του τιμολογίου που θα εκδίδει.

Τα δικαιολογητικά που απαιτούνται είναι τα παρακάτω:

1. Πρωτόκολλο παράδοσης-παραλαβής το οποίο συντάσσεται από την αρμόδια επιτροπή παραλαβής.
2. Τιμολόγιο του αναδόχου.
3. Φορολογική και Ασφαλιστική ενημερότητα.
4. Εξοφλητική απόδειξη του αναδόχου, εάν το τιμολόγιο δεν φέρει την ένδειξη «Εξοφλήθηκε».
5. Οποιοδήποτε άλλο δικαιολογητικό μπορεί να ζητηθεί από την Υπηρεσία.

Τον Ανάδοχο θα βαρύνουν οι νόμιμες κρατήσεις επί της καθαρής συμβατικής αξίας.

Η δαπάνη θα βαρύνει τον προϋπολογισμό του ΠΤΑ Κρήτης

Η παρούσα Πρόσκληση θα δημοσιευθεί στην ιστοσελίδα του ΠΤΑ Κρήτης (www.pta.gr) και αντίγραφο της θα τοιχοκολληθεί στον πίνακα ανακοινώσεων του κτιρίου του ΠΤΑ Κρήτης .

Ο ΠΡΟΕΔΡΟΣ Δ.Σ ΠΤΑ ΚΡΗΤΗΣ

ΣΤΑΥΡΟΣ ΑΡΝΑΟΥΤΑΚΗΣ

ΠΑΡΑΡΤΗΜΑ Α'
ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ

Αντικείμενο της παρούσας πρόσκλησης είναι η **παροχή υπηρεσιών Υπευθύνου Προσωπικών Δεδομένων (DATA PROTECTION OFFICER - D.P.O.) και υπηρεσιών συμμόρφωσης** στα πλαίσια του Κανονισμού 2016/679 **{ΕΕ) - GDPR** του ΠΤΑ Κρήτης για **πέντε (5) μήνες** από την ημερομηνία υπογραφής της σχετικής σύμβασης, ο οποίος:

* θα ορισθεί ως υπεύθυνος έναντι της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) και των υποκειμένων και
* θα καθοδηγήσει το ΠΤΑ Κρήτης για την πλήρη συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Δεδομένων 2016/679 (ΕΕ) – GDPR , σε όλες τις απαιτούμενες ενέργειες γενικότερα.

Η συνολική προϋπολογιζόμενη δαπάνη είναι **11.000,00 € ως τελική αξία των υπηρεσιών,** συμπεριλαμβανομένων όλων των επιβαρύνσεων.

1.ΕΙΣΑΓΩΓΗ

Λαμβάνοντας υπόψη τις επιταγές του Γενικού Κανονισμού Προστασίας Δεδομένων 2016/679 (ΕΕ) – GDPR το ΠΤΑ Κρήτης στο πλαίσιο των υποχρεώσεών της, ο ανάδοχος θα πρέπει να υλοποιήσει και να παραδώσει τα παρακάτω:

1. Στάδιο προετοιμασίας -αποτύπωση υφιστάμενης κατάστασης

1.1 Δέσμευση Διοίκησης

Παρουσίαση στην Διοίκηση του ΠΤΑ Κρήτης και στα στελέχη του, των απαιτήσεων που θέτει Κανονισμός, προσδιορισμός όλων των απαραιτήτων ενεργειών που απαιτούνται για την εφαρμογή του, δέσμευση της διοίκησης, προσδιορισμός πόρων και προσβάσεων που θα παρασχεθούν και ενημέρωση του προσωπικού του ΠΤΑ Κρήτης .

Παραδοτέο:

Ενέργειες πρώτης ενημέρωσης Διοίκησης - προσωπικού συνοδευόμενο από Δήλωση Δέσμευσης της Διοίκησης.

1.2 Καταγραφή υπευθύνων ανά οργανωτική μονάδα.

Προσδιορίζονται τα τμήματα του ΠΤΑ Κρήτης , γίνεται καταγραφή των ανά τμήμα και ανά αρχείο, δεδομένων και των υπευθύνων. Η καταγραφή αποτυπώνεται στο μητρώο επεξεργασίας δεδομένων.

1.3 Καταγραφή διαθεσίμων φυσικών πόρων

Καταγραφή των διαθεσίμων ανθρώπινων πόρων ανά τμήμα που τίθενται στην διάθεση του Υπεύθυνου Προστασίας. Δημιουργία αντιπροσωπευτικής ομάδας εργασίας σε σχέση με τα υφιστάμενα δεδομένα και τις οργανωτικές μονάδες που τα επεξεργάζονται.

Παραδοτέο:

Έγγραφη αναφορά σε συνεργασία με τα μέλη της ομάδας εργασίας και προσδιορισμός αρμοδιοτήτων και υποχρεώσεων.

1.4 Αναλυτική καταγραφή και χαρτογράφηση των δεδομένων προσωπικού χαρακτήρα που τηρούνται του ΠΤΑ Κρήτης, της επεξεργασίας και της κυκλοφορίας τους.

Καταγραφή ανά επεξεργασία, αρχείο και είδος δεδομένων που τηρούνται και διακινούνται. Αποτύπωση ροής των προσωπικών δεδομένων (DATA FLOW MAP) ανά κατηγορία, ώστε να δημιουργηθούν τα Αρχεία των Δραστηριοτήτων Επεξεργασίας, κατ' απαίτηση του Κανονισμού (ΕΕ) \ 679/2016 (άρθρο 30) ώστε να υπάρχει πλήρης αποτύπωση της διαχείρισης των προσωπικών δεδομένων. Καθορισμός είδους επεξεργασίας, πηγές προέλευσης δεδομένων, χρόνος τήρησής τους.

Παραδοτέο:

«Αρχείο Δραστηριοτήτων Επεξεργασίας» σύμφωνα με το άρθρο 30 του Κανονισμού αν απαιτείται .

1.5 Προσδιορισμός Νομικής Βάσης - έλεγχος ορθότητας.

Προσδιορίζεται η Νομική Βάση που στηρίζεται η επεξεργασία των δεδομένων, εξετάζεται, η ορθότητα, η πληρότητα και εγκυρότητα, η καταγραφή και τεκμηρίωση και ο τρόπος γνωστοποίησης στα \ υποκείμενα.

Παραδοτέο:

Πρότυπα κείμενα θεμελίωσης νομιμοποιητικής βάσης - οδηγίες ενσωμάτωσης στην κάθε μορφή επεξεργασίας, καταγραφής τεκμηρίωσης και γνωστοποίησης.

1.6 Χαρτογράφηση του εγκατεστημένου πληροφοριακού συστήματος

Έλεγχος, αξιολόγηση, καταγραφή πληροφοριακού συστήματος και δικτυακών υποδομών και διαδικασιών λειτουργίας.

Παραδοτέο:

Σχηματικό διάγραμμα του πληροφοριακού συστήματος με τις επί μέρους λειτουργίες αυτού.

1.7 Έλεγχος και αξιολόγηση πολιτικών και διαδικασιών.

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

1.8 Καταγραφή τεκμηρίωσης

Χαρτογράφηση της υπάρχουσας τεκμηρίωσης, που αφορά την ασφάλεια των προσωπικών δεδομένων, εξέταση πληρότητας και ασφάλειάς της.

1.9 Εκτίμηση κινδύνων για τις δραστηριότητες επεξεργασίας

Παραδοτέο:

Αναφορά εκτίμησης κινδύνου για κάθε δραστηριότητα επεξεργασίας

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

Παραδοτέο: Έκθεση αξιολόγησης για απαίτηση ή μη διεξαγωγής DPIA

Εφόσον προκύψει ότι απαιτείται Μελέτη Εκτίμησης Αντίκτυπου DPIA) ,

Παραδοτέο:

Μελέτη εκτίμησης αντίκτυπου σχετικά με την προστασία δεδομένων (Data Privacy Impact Assessment-DPIA)

• Διενέργεια εκτίμησης αντίκτυπου σύμφωνα με τις πρόνοιες του DPIA, στην περίπτωση που ένα είδος από τις χρησιμοποιούμενες τεχνολογίες του ΠΤΑ Κρήτης εκτιμηθεί ότι ενδέχεται να θέσει σε διακινδύνευση τα δικαιώματα και τις ελευθερίες των υποκειμένων της επεξεργασίας προσωπικών δεδομένων.

• Κατάρτιση κατάλληλων μέτρων και μηχανισμών ασφαλείας που θα πρέπει να υιοθετηθούν ώστε το ΠΤΑ Κρήτης να μπορεί να διαχειριστεί / απομειώσει τον πιθανό αντίκτυπο μιας παραβίασης των προσωπικών δεδομένων.

1.11. Έκθεση αποκλίσεων από τον κανονισμό (Gap Analysis)

Παραδοτέο: Έκθεση αποκλίσεων (Gap Analysis)

2. Στάδιο ολοκλήρωσης διαδικασίας συμμόρφωσης

2.1 Προτεινόμενα μέτρα - Κατάρτιση σχεδίου συμμόρφωσης

Με βάση τις διαπιστώσεις, θα υπάρξει σχεδιασμός και πλήρη περιγραφή λεπτομερούς και ολοκληρωμένου σχεδίου

συμμόρφωσης με τις επιταγές του κανονισμού, που θα καλύπτει όλο το φάσμα των επεξεργασιών που γίνονται σε όλο τον κύκλο της ζωής των δεδομένων και αποτελούν αντικείμενο επεξεργασίας.

Παραδοτέο :

Αναλυτικό σχέδιο συμμόρφωσης με τον κανονισμό, που θα περιλαμβάνει όλα τα οργανωτικά , τεχνικά μέτρα και μέτρα πληροφορικής υποδομής που θα πρέπει να λάβει το ΠΤΑ Κρήτης, αλλά και πιθανές συστάσεις που θα συντείνουν στην εν γένει εύρυθμη λειτουργία της.

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

Παραδοτέο:

Εγχειρίδιο πολιτικών διαδικασιών συλλογής και επεξεργασίας δεδομένων που μπορεί να αποτελεί και στοιχείο της πολιτικής ασφαλείας του ΠΤΑ Κρήτης .

2.3 Συγγραφή πολιτικής ασφαλείας

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

Παραδοτέο:
Πλήρες κείμενο πολιτικής ασφάλειας

2.4 Συγγραφή σχεδίου ανάκαμψης από καταστροφές.

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

Παραδοτέο:
Πλήρες κείμενο σχεδίου ανάκαμψης από καταστροφές.

2.5 Έλεγχος και εφαρμογή μηχανισμού παραβιάσεων.

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

2.6. Κατάρτιση σχεδίου διαχείρισης συμβάντων

Το σχέδιο διαχείρισης συμβάντων είναι το έγγραφο που αναφέρεται στις διαδικασίες που θα ακολουθηθούν σε περίπτωση παραβίασης ασφαλείας. Περιγράφει δε και την κατάλληλη διαδικασία αναθεώρησής της.

Παραδοτέο:
Πλήρες κείμενο διαχείρισης συμβάντων

2.7 Κατάρτιση Σχεδίου Αναγγελίας Διαρροής στην Αρχή Προστασίας Προσωπικών Δεδομένων

Κατάρτιση σχεδίου ώστε να είναι δυνατή η αναγγελία της διαρροής εντός 72 ωρών, όπως προβλέπεται από τον κανονισμό.

Παραδοτέο:
Σχέδιο Αναγγελίας Διαρροής.

2.8 Δημιουργία αρχείου καταγραφής ενεργειών (Audit Log)

Αποτελεί σημαντικό αρχείο της τεκμηρίωσης της συμμόρφωσης ή της προόδου που έχει γίνει στην κατεύθυνση της συμμόρφωσης προς τις απαιτήσεις του κανονισμού. Περιλαμβάνει την καταγραφή των διαδικασιών συλλογής και επεξεργασίας των δεδομένων, το ποσοστό ολοκλήρωσης των διαφόρων σχεδίων.

Παραδοτέο:
Συλλογή αρχείων καταγραφής, αυτοματοποιημένων και μη.

2.9 Έλεγχος και προσαρμογή των συμβάσεων του οργανισμού εσωτερικά και με τρίτους:

Γίνεται έλεγχος των υπαρχουσών συμβάσεων του ΠΤΑ, τόσο με το προσωπικό όσον και με εξωτερικούς συνεργάτες. Όπου χρειάζεται γίνεται αναμόρφωσή τους. Όπου δεν υπάρχουν, συγγράφονται νέες.

Παραδοτέο:
Αναμορφωμένες συμβάσεις και πρότυπα συμβάσεων προσαρμοσμένα στον κανονισμό.

2.10 Εκπαίδευση εργαζομένων

Εκπαίδευση εργαζομένων, σε θέματα που αφορούν την τήρηση των προϋποθέσεων του κανονισμού. Δημιουργία κουλτούρας προστασίας προσωπικών δεδομένων.

Παραδοτέο:

Πρόγραμμα εκπαίδευσης ανά οργανωτική μονάδα με ορισμένο εκπαιδευτικό πρόγραμμα υλικό και παρουσιολόγιο. Αποτελεί τμήμα της απαραίτητης για την συμμόρφωση τεκμηρίωσης.

2.11 Επαναξιολόγηση.

Με την ολοκλήρωση του συνόλου των ενεργειών γίνεται επαναξιολόγηση του επιπέδου συμμόρφωσης του ΠΤΑ Κρήτης.

Για την υλοποίηση των παραπάνω, τόσο ο Κανονισμός (GDPR), όσο και οι ιδιαίτερες απαιτήσεις των επί μέρους εργασιών, απαιτούν:

1. Συγκεκριμένα επαγγελματικά προσόντα, ικανότητες, δεξιότητες και εκπαίδευση –επιμόρφωση του DPO,
2. Πλαισίωση του DPO με ομάδα ανθρώπων διαφόρων ειδικοτήτων ή ικανοτήτων (νομικών, πληροφορικής, ειδικών ασφάλειας, συμβούλων τήρησης διαδικασιών κλπ.) για να είναι σε θέση να εκπληρώσει τα καθήκοντά του.
3. Εξειδικευμένους συμβούλους για την εξειδίκευση και την περιγραφή τόσο του συστήματος διαχείρισης διαδικασιών, όσο και των υπηρεσιών που θα υλοποιηθούν σε όλες τις φάσεις υλοποίησης, ανάλογα με τις εκάστοτε δυνατότητες της υπηρεσίας.

Το ΠΤΑ Κρήτης, ως είναι υποχρεωμένο σύμφωνα με το άρθρο 38 του Γενικού Κανονισμού Προστασίας Δεδομένων 2016/679 (ΕΕ) - GDPR, θα διασφαλίσει την ενεργή συμμετοχή του DPO και τους απαραίτητους πόρους, ώστε να ανταποκριθεί στις υποχρεώσεις του.

2.ΕΛΑΧΙΣΤΕΣ ΠΡΟΫΠΟΘΕΣΕΙΣ ΣΥΜΜΕΤΟΧΗΣ

Εξαιτίας της ιδιαίτερης σχέσης των υπό προμήθεια υπηρεσιών με θέματα ποιότητας, ασφάλειας, εχεμύθειας και τεχνολογιών πληροφορικής, απαιτούνται τα παρακάτω:

Α) Υποψήφιος ανάδοχος

Ο υποψήφιος ανάδοχος θα πρέπει:

1. Να διαθέτει πιστοποίηση ποιότητας ως προς το πρότυπο 9001 στην εν ισχύ έκδοση του, για την παροχή συμβουλευτικών υπηρεσιών **ή / και**

Να διαθέτει πιστοποίηση ασφάλειας πληροφοριών ως προς το πρότυπο IS0 27001 στην εν ισχύ έκδοση του, για την παροχή συμβουλευτικών υπηρεσιών.

2. Να έχει προβεί ο ίδιος σε όλες τις απαραίτητες ενέργειες συμμόρφωσης κατά GDPR.
3. Να έχει αποδεδειγμένη εμπειρία στην παροχή συμβουλευτικών υπηρεσιών σε φορείς ΟΤΑ ή του Ευρύτερου Δημοσίου ή Ν.Π.Ι.Δ για τουλάχιστον τρία (3) έτη. Προς απόδειξη να καταθέσει σχετικό κατάλογο με τον πίνακα των έργων και τα αποδεικτικά υλοποίησης (πρωτόκολλα παραλαβής / καλής εκτέλεσης).
4. Να έχει αποδεδειγμένη εμπειρία σε τουλάγιστον πέντε (5) έργα (υλοποιημένα ή σε εξέλιξη) συμμόρφωσης κατά GDPR. Προς απόδειξη να καταθέσει σχετικό κατάλογο με τον πίνακα των έργων και τα αποδεικτικά ανάληψης ή υλοποίησης (συμβάσεις ή πρωτόκολλα παραλαβής /

καλής εκτέλεσης).

Β) Ομάδα έργου

Η ζητούμενη ομάδα έργου να είναι τουλάχιστον **τετραμελής** και να αποτελείται από:

1. Ένα έμπειρο στέλεχος - νομικό με αποδεδειγμένη γνώση στην προστασία προσωπικών δεδομένων (που θα διαθέτει πιστοποιητικό DPO).
2. Ένα έμπειρο στέλεχος πληροφορικής με αποδεδειγμένη γνώση στην προστασία προσωπικών δεδομένων (που θα διαθέτει πιστοποιητικό DPO).
3. Ένα έμπειρο στέλεχος πληροφορικής με αποδεδειγμένη γνώση στην ασφάλεια των πληροφοριών και των πληροφοριακών συστημάτων.
4. Ένα έμπειρο στέλεχος 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). Προς απόδειξη να διαθέτει και να καταθέσει αναγνωρισμένα πιστοποιητικά.

   Ως Υπεύθυνος Ομάδας Έργου, να ορισθεί ένα εκ των μελών της ομάδας έργου, το οποίο θα διαθέτει επιστημονική κατάρτιση και αποδεδειγμένη γνώση στη διοίκηση και διαχείριση έργων (project management).

3. ΤΕΧΝΙΚΗ ΠΕΡΙΓΡΑΦΗ

3.1 Αντικείμενο

Παροχή συμβουλευτικών υπηρεσιών προκειμένου το ΠΤΑ Κρήτης να συμμορφωθεί στις υποχρεώσεις του, όπως αυτές απορρέουν από τον Γενικό Κανονισμό Προστασίας Δεδομένων 2016/679 (ΕΕ) — GDPR, **ορίζοντας Υπεύθυνο Προστασίας Προσωπικών Δεδομένων** – DATA PROTECTION OFFICER **(D.P.O.),** ο οποίος θα μεριμνήσει για όλες τις απαιτούμενες ενέργειες πλήρους συμμόρφωσης με τις απαιτήσεις του Κανονισμού (GDPR).

Ο DATA PROTECTION OFFICER θα πρέπει να έχει τις κατάλληλες γνώσεις και δεξιότητες για να ανταποκριθεί στον ρόλο του, με αποδεδειγμένη γνώση και εμπειρία στη νομοθεσία και πρακτική εφαρμογή των διαδικασιών διαχείρισης προσωπικών δεδομένων, σύμφωνα με το άρθρο 39 του GDPR.

Χαρακτηριστικά θέσης DPO

- Είναι λειτουργικά «ανεξάρτητο» στέλεχος, με την έννοια ότι διαθέτει αυτονομία στην άσκηση των καθηκόντων του και αναφέρεται απευθείας στη Διοίκηση, ώστε να μην υπάρχει ενδιάμεσο στάδιο ελέγχου δυνάμενο να επηρεάσει την ανεξαρτησία του.
- Δεσμεύεται από εμπιστευτικότητα.
- Δεν μπορεί να έχει σύγκρουση συμφερόντων λόγω πρόσθετων αρμοδιοτήτων ή καθηκόντων.
- Αποτελεί τον κύριο συνομιλητή της Διοίκησης για τα θέματα προστασίας δεδομένων και εξασφαλίζει την υποστήριξή της και τον απαιτούμενο προϋπολογισμό για την εφαρμογή του Προγράμματος Προστασίας Δεδομένων. Έχει λόγο για όλα τα θέματα που αφορούν την προστασία προσωπικών δεδομένων στον φορέα.
- Παρέχει ξεκάθαρη πρόσβαση στο Υποκείμενο των Δεδομένων.
- Συμμετέχει σε όλα τα ζητήματα σχετικά με την προστασία προσωπικών δεδομένων.
- Καταρτίζει το Πρόγραμμα και την Πολιτική Προστασίας Δεδομένων και εποπτεύει την εφαρμογή του, αξιολογεί τον βαθμό συμμετοχής και την επιτυχία του και προβαίνει στις αναγκαίες

διορθώσεις, όπου απαιτείται.

- Εκτιμά και συμβουλεύει για την κατά περίπτωση αναγκαιότητα κατάρτισης μιας Εκτίμησης Αντίκτυπου κατά το Άρθρο 35 του Κανονισμού και καταρτίζει πρότυπο υπόδειγμα DPIA.
- Συντονίζει την διατμηματική συνεργασία με τα τμήματα Ανθρώπινου Δυναμικού, Ασφάλειας Πληροφορικής, Πληροφοριακών Συστημάτων (ΙΤ), Νομικής και Κανονιστικής Συμμόρφωσης κλπ. για τη δημιουργία μιας διαρκούς εταιρικής <u>κουλτούρας</u> *προστασίας δεδομένων* <u>ως πολύτιμου περιουσιακού στοιχείου</u>.
- Σχεδιάζει εσωτερικά εκπαιδευτικά προγράμματα και τηρεί τα απαιτούμενα Αρχεία Ολοκλήρωσης των εκπαιδεύσεων ανά ομάδα εργαζομένων.
- Δεν φέρει προσωπική ευθύνη για μη συμμόρφωση με τις απαιτήσεις του ΓΚΠΔ στην προστασία των δεδομένων. Η ευθύνη για παραβίαση της νομοθεσίας σχετικά με τα Δεδομένα Προσωπικού Χαρακτήρα παραμένει στη Διοίκηση του φορέα.

3.2 Υποχρεώσεις Υπευθύνου Προστασίας Προσωπικών Δεδομένων (Υ.Π.Δ. - D.P.O.)

Ένα εκ των μελών της ζητούμενης ομάδας έργου, θα ορισθεί ως Υπεύθυνος Προστασίας Δεδομένων (DPO), υπεύθυνος έναντι της Αρχής Προστασίας Προσωπικών Δεδομένων και *έναντι* των υποκειμένων, ενώ θα επιβλέπει παράλληλα, όλη τη διαδικασία προσαρμογής του ΠΤΑ Κρήτης κατά GDPR.

Η διάρκεια παροχής των υπηρεσιών ορίζεται σε πέντε (5) μήνες από την υπογραφή της σχετικής σύμβασης.

Κατά την διάρκεια της σύμβασης ο Υ.Π.Δ., αναλαμβάνει:

1. Να εκπροσωπεί το ΠΤΑ Κρήτης έναντι της εποπτικής αρχής (ΑΠΔΠΧ).
2. Να εκπροσωπεί το ΠΤΑ Κρήτης έναντι των υποκειμένων.
3. Να συμβουλεύει τη Διοίκηση το ΠΤΑ Κρήτης σε θέματα προστασίας προσωπικών δεδομένων.
4. Να εισηγείται απευθείας στην Διοίκηση του ΠΤΑ Κρήτης τις κατάλληλες πολιτικές προστασίας των δεδομένων, θεωρώντας τα ως πολύτιμο περιουσιακό στοιχείο του φορέα.
5. Ο Υ.Π.Δ. υποχρεούται να πραγματοποιεί τουλάχιστον 10 επισκέψεις μηνιαίως στο ΠΤΑ Κρήτης κατά τις εργάσιμες ημέρες και ώρες.
6. Ο Υ.Π.Δ. *θα συνεργάζεται άμεσα* με όλα τα στελέχη του ΠΤΑ Κρήτης και λογοδοτεί στον Διευθυντή.

Τα **καθήκοντα** του DPO (Υ.Π.Δ.), σύμφωνα και με το άρθρο 39 του ΓΚΠΔ, θα είναι:

1. Ενημερωτικές και συμβουλευτικές υπηρεσίες σχετικά με τις υποχρεώσεις του ΠΤΑ Κρήτης και των συνεργαζόμενών «Εκτελούντος την Επεξεργασία».
2. Διασφάλιση της εναρμόνισης (υλοποίηση και συμμόρφωση) της λειτουργίας του ΠΤΑ Κρήτης σε ό,τι αφορά τις πολιτικές, πρακτικές και μεθοδολογία επεξεργασίας, αποθήκευσης και μεταφοράς Δεδομένων Προσωπικού Χαρακτήρα σύμφωνα με τον Κανονισμό GDPR.
3. Κατάρτιση Κώδικα Δεοντολογίας για την προστασία των δικαιωμάτων των υποκειμένων.
4. Την επισκόπηση των εντύπων στα οποία συμπληρώνονται προσωπικά στοιχεία των υποκειμένων. Στα έντυπα αυτά θα πρέπει να αναφέρεται α) ότι τα δεδομένα τυγχάνουν επεξεργασίας σύμφωνα με τον ΓΚΠΔ και β) τα δικαιώματα των υποκειμένων.

5. Το έλεγχο συγκατάθεσης, δηλαδή τις μεθόδους εξασφάλισης συγκατάθεσης των υποκειμένων για κάθε επιδιωκόμενο σκοπό επεξεργασίας.
6. Δημιουργία της κατάλληλης κουλτούρας στο ανθρώπινο δυναμικό του φορέα.
7. Παρακολούθηση εσωτερικής συμμόρφωσης και σχεδιασμός αναγκαίων μελλοντικών Πολιτικών Ασφάλειας.
8. Παρακολούθηση Σχεδίου Αντιμετώπισης Περιστατικών, και αξιολόγηση και λήψη των κατάλληλων μέτρων ασφάλειας.
9. Εκτίμηση Αντικτύπου (impact Assessment, άρθρο 35 ΓΚΠΔ) - Συμβουλευτικές υπηρεσίες και παρακολούθηση υλοποίησης.
10. Συνεργασία και σημείο επικοινωνίας με την εποπτική αρχή (ΑΠΔΠΧ). Εκπροσώπηση του φορέα έναντι των Εθνικών και Ευρωπαϊκών Αρχών, συνολικά, σχετικά με το αντικείμενο του έργου.
11. Προστασία του φορέα από τους κινδύνους επιβολής των σημαντικότατων και βαρύτατων διοικητικών προστίμων που προβλέπει ο Κανονισμός.

ΠΑΡΑΡΤΗΜΑ Β
ΥΠΟΔΕΙΓΜΑ ΟΙΚΟΝΟΜΙΚΗΣ ΠΡΟΣΦΟΡΑΣ

Ο (υποψήφιος Ανάδοχος) ..... με έδρα ..... οδός ..... αριθμός ..... Τ.Κ ..... τηλ..... φαξ ....., αφού έλαβα γνώση της αρ. πρωτ..... πρόσκλησης για την προμήθεια /παροχή υπηρεσιών για τις ανάγκες του ΠΤΑ Κρήτης, υποβάλλω την παρούσα προσφορά και δηλώνω ότι αποδέχομαι πλήρως και χωρίς επιφύλαξη όλους τους όρους της πρόσκλησης και αναλαμβάνω την εκτέλεση της στην κάτωθι τιμή:

Ε1ΔΟΣ/ΠΑΡΕΧΟΜΕΝΗ ΥΠΗΡΕΣΙΑ	
ΤΙΜΗ ΠΡΟΣΦΟΡΑΣ χωρίς Φ.Π.Α.	
Φ.Π.Α.	
ΣΥΝΟΛΙΚΗ ΑΞΙΑ ΣΥΜΠΕΡΙΛΑΜΒΑΝΟΜΕΝΟΥ ΦΠΑ (αριθμητικώς και ολογράφως)	

(Ημερομηνία)
Ο Προσφέρων

(Ονοματεπώνυμο-Υπογραφή-Σφραγίδα)