



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΥΠΟΥΡΓΕΙΟ ΠΟΛΙΤΙΣΜΟΥ
ΚΑΙ ΑΘΛΗΤΙΣΜΟΥΤΑΜΕΙΟ ΑΡΧΑΙΟΛΟΓΙΚΩΝ ΠΟΡΩΝ
ΚΑΙ ΑΠΑΛΛΟΤΡΙΩΣΕΩΝΑθήνα, 28 /03/2019
Αρ. Πρωτ.: ΔΙΟΙΚ/Β/5359

ΔΙΕΥΘΥΝΣΗ : ΔΙΟΙΚΗΤΙΚΟΥ
ΤΜΗΜΑ : ΛΟΓΙΣΤΗΡΙΟΥ
Ταχ. Δ/ση : Ελ. Βενιζέλου 57
Ταχ. Κώδικας : 105 64 ΑΘΗΝΑ
Πληροφορίες : Γρ. Προμηθειών
Τηλ. : 2103722500

ΠΡΟΣΚΛΗΣΗ ΕΚΔΗΛΩΣΗΣ ΕΝΔΙΑΦΕΡΟΝΤΟΣ

Προμήθεια υπηρεσίας υλοποίησης συμμόρφωσης του ΤΑΠ με τις απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) 2016/679 της Ευρωπαϊκής Ένωσης (General Date Protection Regulation)- GDPR για τις υπηρεσιακές ανάγκες της κεντρικής Υπηρεσίας του ΤΑΠ ποσού 20.000,00€ μη συμπεριλαμβανομένου ΦΠΑ.

Το Ταμείο Αρχαιολογικών Πόρων και Απαλλοτριώσεων (αναθέτουσα αρχή) πρόκειται να προβεί στην προμήθεια υπηρεσίας υλοποίησης συμμόρφωσης του ΤΑΠ με τις απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) 2016/679 της Ευρωπαϊκής Ένωσης (General Date Protection Regulation)- GDPR για τις υπηρεσιακές ανάγκες της κεντρικής Υπηρεσίας του ΤΑΠ ποσού 20.000,00€ συμπεριλαμβανομένου ΦΠΑ.

Για το σκοπό αυτό, με απόφαση Διοικητικού Συμβουλίου 1/15.01.2019 (θέμα 15°).

ΑΠΕΥΘΥΝΕΙ ανοικτή πρόσκληση

προς όλους τους ενδιαφερόμενους για την υποβολή προσφοράς για την ανωτέρω προμήθεια μέχρι ποσού 20.000,00€ μη συμπεριλαμβανομένου ΦΠΑ.

Παρακάτω παρουσιάζονται τα χαρακτηριστικά Τεχνικής και επαγγελματικής ικανότητας, Χρόνος υλοποίησης καθώς και πίνακας Παραδοτέων που ζητούνται.

Τεχνική και επαγγελματική ικανότητα

Όσον αφορά στην τεχνική και επαγγελματική ικανότητα για την παρούσα διαδικασία σύναψης σύμβασης, οι υποψήφιοι ανάδοχοι οφείλουν ν' αποδείξουν ότι διαθέτουν:

α) Εμπειρία στην παροχή συμβουλευτικών υπηρεσιών ως προς τη συμμόρφωση των επιχειρήσεων με τις απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων 2016/679 (GDPR). Για την τεκμηρίωση της ως άνω εμπειρίας, οι υποψήφιοι θα πρέπει να έχουν

αναλάβει, κατά την τελευταία διετία, τρία (3) τουλάχιστον αντίστοιχα έργα παροχής υπηρεσιών για τη συμμόρφωση με τον ως άνω Κανονισμό (GDPR).

Για την τεκμηρίωση της ως άνω εμπειρίας οι υποψήφιοι ανάδοχοι θα πρέπει να προσκομίσουν αναλυτικό κατάλογο με τα εξής πεδία συμπληρωμένα για κάθε έργο : Επωνυμία πελάτη, τίτλος έργου, περιεχόμενο έργου, προϋπολογισμός, χρονική διάρκεια (Από.... Έως...), στοιχεία επικοινωνίας υπεύθυνου πελάτη.

β) Οργάνωση, δομή και μέσα, με τα οποία είναι ικανοί ν' αντεπεξέλθουν πλήρως, άρτια και ολοκληρωμένα στις απαιτήσεις του αντικειμένου της παρούσας Πρόσκλησης, όπως λ.χ. Οργανωτική δομή ή Ομάδα Έργου, η οποία να περιλαμβάνει συμβούλους οργάνωσης, ειδικούς στην ασφάλεια των πληροφοριών, νομικούς, ειδικούς στις τεχνολογικές υποδομές πληροφορικής, κλπ, και οι οποίοι έχουν εμπλακεί σε έργα, όπως αναφέρονται ανωτέρω υπό στοιχείο (α)

Για την τεκμηρίωση της ως άνω απαίτησης οι υποψήφιοι ανάδοχοι θα πρέπει να προσκομίσουν αναλυτικά βιογραφικά σημειώματα της ομάδας υλοποίησης έργου.

Χρόνος υλοποίησης

Για τα δεδομένα του νέου συστήματος E-Ticket & ERP του ΤΑΠ εντός ενός (1) μήνα από την υπογραφή της σύμβασης

Για τα υπόλοιπα δεδομένα του ΤΑΠ εντός τριών (3) μηνών από την υπογραφή της σύμβασης

Ακολουθεί ο αναλυτικός πίνακας παραδοτέων :

Πίνακας Παραδοτέων

ΑΑ	Παραδοτέο
1	Data mapping / Καταγραφή πράξεων επεξεργασίας Κατάλογος των σημείων όπου υπάρχουν προσωπικά δεδομένα, όλων των πράξεων επεξεργασίας που πραγματοποιούνται από το ΤΑΠ, καθώς και το είδος των δεδομένων, την χρήση αυτών, τους εκτελούντες την επεξεργασία, τους αποδέκτες των δεδομένων, τους σκοπούς επεξεργασίας κλπ
2	Διάγραμμα/μελέτη ροής δεδομένων και διαδικασιών Διαδικασία διαχείρισης δεδομένων, με τις κύριες πηγές δεδομένων, τη συλλογή δεδομένων και τα μέσα αποθήκευσης δεδομένων του ΤΑΠ
3	GAP Analysis Summary Report & Detailed GAP analysis Report Κατάλογος συνολικών απαιτήσεων Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR), τεκμηρίωση βαθμού κάλυψης του ΤΑΠ, Μελέτη Ανάλυσης Αποκλίσεων, Προγραμματισμός ενεργειών κάλυψης κενών και προτεινόμενες διαδικασίες

ΑΑ	Παραδοτέο
	συμμόρφωσης με αναλυτικό σχέδιο ενεργειών συμμόρφωσης
4	Risk Assessment - Αξιολόγηση των κινδύνων για το ΤΑΠ
5	<p>Data Privacy Impact Assessment (DPIA) - Μελέτη του αντίκτυπου για τα υποκείμενα των προσωπικών δεδομένων</p> <p>Διενέργεια DPIA κατά τα κάτωθι ενδεικτικώς αναφερόμενα:</p> <ul style="list-style-type: none"> - Προσδιορισμός της ανάγκης για DPIA - Καθορισμός εγγενών κινδύνων της επεξεργασίας που επιβάλλουν την DPIA. - Προσδιορισμός των συναφών της ιδιωτικότητας κινδύνων και του αντίκτυπου τους για το ΤΑΠ και ιεράρχηση προτεραιοτήτων βάσει των επιπτώσεων τους. - Εύρεση και αξιολόγηση των λύσεων για κάθε διαπιστωμένο κίνδυνο, λήψη απόφασης απόρριψης ή αποδοχής του. Λήψη κατάλληλων μέτρων περιορισμού του κινδύνου - Εξαγωγή και καταγραφή των αποτελεσμάτων της DPIA σε έκθεση που υποβάλλεται από τον ανάδοχο στο ΤΑΠ με εισήγηση για την ανάγκη ή όχι διαβίβασης της στη ρυθμιστική αρχή για διαβούλευση. - Ενσωμάτωση των αποτελεσμάτων της DPIA στο σχέδιο του έργου της συμμόρφωσης στον GDPR
6	Αρχείο της επεξεργασίας της πληροφορίας κατά τις προδιαγραφές του άρθρου 30 του Κανονισμού
7	<p>Εκπαίδευση προσωπικού σε θέματα GDPR</p> <p>Διεξαγωγή επιμορφωτικών σεμιναρίων για το προσωπικό του ΤΑΠ σχετικά με την προστασία προσωπικών δεδομένων, προσαρμοσμένων στη χρήση, διαχείριση και επεξεργασία τους από έκαστο τμήμα/διεύθυνση του.</p>
8	<p>Νόμιμη βάση επεξεργασίας</p> <p>Αξιολόγηση της νόμιμης βάσης έκαστης επεξεργασίας και πρόταση αναζήτησης εναλλακτικής βάσης επεξεργασίας σε περίπτωση διαπίστωσης ελλείψεων</p>
9	<p>Συναίνεση</p> <p>Επικαιροποίηση ή/και παροχή πρόσθετης συναίνεσης σύμφωνα με τις επιταγές του GDPR. Σύνταξη προτύπων δηλώσεων συναίνεσης, σε αντιστοιχία με τις χρήσεις/επεξεργασίες</p>
10	<p>Ενημέρωση Υποκειμένων (Privacy Notices)</p> <p>Σύνταξη ενημερώσεων (Privacy Notices) για έκαστη επεξεργασία προς τα αντίστοιχα υποκείμενα, όπως ενδεικτικά: οφειλέτες, εργαζόμενους, αντισυμβαλλόμενους</p> <p>Διαμόρφωση προτύπων των απαιτούμενων όρων ανά κατηγορία συμβάσεως (εργασίας, ανεξαρτήτων υπηρεσιών, έργου κλπ.)</p>

ΑΑ	Παραδοτέο
	Διαμόρφωση Δηλώσεων Προστασίας Προσωπικών Δεδομένων για την ιστοσελίδα του ΤΑΠ / Etickets.tap.gr
11	<p>Αυτοματοποιημένη επεξεργασία – Profiling</p> <p>Έλεγχος πραγματοποίησης αυτοματοποιημένης επεξεργασίας από το ΤΑΠ ή/και τρίτους εκτελούντες την επεξεργασία για λογαριασμό του, συμπεριλαμβανομένης της κατάρτισης προφίλ Αξιολόγηση των επιπτώσεων τους στο υποκείμενο των δεδομένων. Αξιολόγηση αναγκαιότητας συγκατάθεσης. Διαμόρφωση ειδικών δηλώσεων συναίνεσης</p>
12	<p>Privacy by design & Privacy by default</p> <p>Έλεγχος εν γένει της εφαρμογής κατάλληλων τεχνικών και οργανωτικών μέτρων σχεδιασμένων για την εφαρμογή αρχών προστασίας των δεδομένων και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία και για να διασφαλιστεί ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον</p> <p>εκάστοτε σκοπό της επεξεργασίας. Αξιολόγηση της αποδοτικότητας και καταλληλότητας των μέτρων αυτών. Ανάπτυξη προτάσεων/λύσεων για τη βελτίωση των μέτρων ασφαλείας κατά τρόπο ώστε να πληρούν τις απαιτήσεις του GDPR.</p>
13	<p>Εκτελούντες την επεξεργασία</p> <p>Δημιουργία πρότυπων συμβάσεων με τους εκτελούντες την επεξεργασία και τροποποίηση των υφιστάμενων των συμβάσεων με τους εκτελούντες την επεξεργασία σύμφωνα με τις επιταγές του GDPR.</p>
14	<p>Εσωτερικές Πολιτικές και Διαδικασίες</p> <p>Αναθεώρηση ή/και σύνταξη εσωτερικών πολιτικών και διαδικασιών σύμφωνων με τα προβλεπόμενα στον GDPR και προσαρμοσμένες στις ανάγκες και ιδιαιτερότητες του ΤΑΠ. (Privacy Policy, Acceptable Use Policy, Information Security Policy, κλπ.)</p> <p>Ενδεικτική Λίστα:</p> <ul style="list-style-type: none"> • Πολιτική προστασίας προσωπικών δεδομένων εργαζομένων • Πολιτική / διαδικασίες για την χρήση ευαίσθητων προσωπικών δεδομένων (εάν υπάρχουν) • Πολιτική / διαδικασίες για την διαγραφή προσωπικών δεδομένων • Πολιτική / διαδικασίες για τον έλεγχο της επεξεργασίας που διεξάγεται συνολικά ή εν μέρει με αυτοματοποιημένα μέσα (ιδιαίτερα αν γίνεται profiling) • Πολιτική / διαδικασίες για την απόκτηση έγκυρης συναίνεσης

ΑΑ	Παραδοτέο
	<ul style="list-style-type: none"> • Πολιτική / διαδικασίες για την χρήση των cookies και των μηχανισμών παρακολούθησης • Πολιτικές / διαδικασίες για την τήρηση αρχείων • Οδηγίες για την ενσωμάτωση της προστασίας προσωπικών δεδομένων στις πρακτικές πρόσληψης • Οδηγίες για την ενσωμάτωση της προστασίας προσωπικών δεδομένων στη χρήση CCTV/Βιντεοεπιτήρησης/Access Control • Οδηγίες για την ενσωμάτωση της προστασίας προσωπικών δεδομένων στην χρήση εταιρικών email accounts
15	<p>Διεθνείς Διαβιβάσεις</p> <p>Αξιολόγηση των εγγυήσεων υπό τις οποίες πραγματοποιούνται τυχόν διεθνείς διαβιβάσεις. Ανάπτυξη προτάσεων/λύσεων για τη νομιμότητα εν γένει διεθνών διαβιβάσεων. Σύνταξη εταιρικών κανόνων για τις διεθνείς διαβιβάσεις</p>
16	<p>Ασφάλεια δεδομένων</p> <p>Εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων για τη διασφάλιση του κατάλληλου επιπέδου ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση:</p> <p>α) της ψευδωνυμοποίησης και της κρυπτογράφησης δεδομένων προσωπικού χαρακτήρα,</p> <p>β) της δυνατότητας διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας,</p> <p>γ) της δυνατότητας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος,</p> <p>δ) διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.</p>
17	<p>Περιστατικά Ασφαλείας</p> <p>Αναθεώρηση ή/και σύνταξη πολιτικής για την καταγραφή περιστατικών ασφαλείας με στόχο την ενημέρωση των αρχών και των υποκειμένων εντός των προβλεπόμενων προθεσμιών, σύμφωνα με τον GDPR.</p>
18	<p>Διαδικασία ικανοποίησης δικαιώματος πρόσβασης, διαγραφής και εναντίωσης</p> <p>Σύνταξη πολιτικής και διαμόρφωση διαδικασίας σχετικής με το</p>

ΑΑ	Παραδοτέο
	δικαίωμα πρόσβασης του υποκειμένου στα δεδομένα του και διαγραφής αυτών κατά τα προβλεπόμενα στον GDPR.
19	Data Protection Officer Παροχή υπηρεσιών DPO για χρονικό διάστημα 1 έτους από την ημερομηνία υπογραφής της σύμβασης

Στην προσφορά θα πρέπει να αναφέρονται ρητώς τα κάτωθι:

- Η οικονομική προσφορά θα πρέπει να αναφέρει συνολικά το κόστος όλων των παραχωρημένων υπηρεσιών συν Φ.Π.Α.
- Το χρονικό διάστημα που απαιτείται για την πλήρη παράδοση της προμήθειας.

Η ελάχιστη διάρκεια ισχύος των προσφορών ορίζεται στους δύο (2) μήνες από την ημέρα δημοσίευσης του παρόντος στην ιστοσελίδα www.tap.gr.

Οι ενδιαφερόμενοι θα πρέπει να υποβάλλουν τις προσφορές τους σε σφραγισμένο φάκελο στο γραφείο πρωτοκόλλου της κεντρικής Υπηρεσίας του Ταμείου Αρχαιολογικών Πόρων, Ελ. Βενιζέλου (Πανεπιστημίου) 57, Αθήνα, 4ος όροφος, εντός **πέντε (5) εργάσιμων ημερών** από τη δημοσίευση του παρόντος στην ιστοσελίδα www.tap.gr, με την ένδειξη:

« Προσφορά για την Προμήθεια υπηρεσίας υλοποίησης συμμόρφωσης του ΤΑΠ με τις απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) 2016/679 της Ευρωπαϊκής ένωσης (General Date Protection Regulation)- GDPR για τις υπηρεσιακές ανάγκες της κεντρικής Υπηρεσίας του ΤΑΠ ποσού 20.000,00€ μη συμπεριλαμβανομένου ΦΠΑ

υπόψη της επιτροπής αξιολόγησης προσφορών

Οι ενδιαφερόμενοι μπορούν να απευθύνουν τυχόν ερωτήματα που αφορούν τις παρούσες προδιαγραφές στην ηλεκτρονική διεύθυνση gkamptris@tap.gr, atsogkas@tap.gr στο τηλ. 2103722593. ή στο τηλ. 2103722500.

Τέλος, σας γνωστοποιούμε ότι η πληρωμή από το Ταμείο μας γίνεται επί πιστώσει και η διαδικασία μέχρι την τελική πληρωμή διαρκεί περίπου ένα (1) μήνα από την οριστική παραλαβή της προμήθειας.

Η προϊσταμένη του Τμήματος Λογιστηρίου	Αναπληρώτρια προϊσταμένη της Διεύθυνσης Διοικητικού	Η πρόεδρος Δ.Σ. του ΤΑΠ
Χ. Σταυριανουδάκη	Ε. Κώτσου	Σιδηροπούλου Παρασκευή