ΔΗ.Κ.Ε.
ΔΗΠΕΘΕ ΣΕΡΡΩΝ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΔΗΜΟΣ ΣΕΡΡΩΝ
ΔΗΜΟΤΙΚΟ ΠΕΡΙΦΕΡΕΙΑΚΟ ΘΕΑΤΡΟ ΣΕΡΡΩΝ
(ΔΗ.Κ.Ε. ΔΗ.ΠΕ.ΘΕ.)

ΤΙΤΛΟΣ: «Υπηρεσίες Υποστήριξης του ΔΗ.ΠΕ.ΘΕ Σερρών για την προσαρμογή στο νέο κανονισμό προστασίας δεδομένων (ΕΕ 679/2016)**»**

ΚΑ. 02.15.6116

Σέρρες 23 Απριλίου 2020
Αριθμ. Πρωτ.: 464

ΜΕΛΕΤΗ 4/2020

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

Ενδεικτικός προϋπολογισμός 3.000,00 ευρώ πλέον του ΦΠΑ 24%.

ΑΠΡΙΛΙΟΣ 2020

ΤΕΧΝΙΚΗ ΕΚΘΕΣΗ

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

Ο «Γενικός Κανονισμός Προστασίας Δεδομένων» (ΓΚΠΔ-GDPR), ΕΕ 2016/679, είναι ένα νομοθέτημα άμεσης εφαρμογής, κατισχύει των εθνικών νομοθεσιών των κρατών μελών για την προστασία προσωπικών δεδομένων, χωρίς να χρειάζεται να εισαχθεί με νόμο στην εσωτερική έννομη τάξη. Ο Κανονισμός απέκτησε τυπική ισχύ 20 ημέρες μετά τη δημοσίευσή του στην Επίσημη Εφημερίδα της ΕΕ και τέθηκε σε ισχύ στα κράτη μέλη, στις 25 Μαΐου του 2018. Καταργεί επίσης την Οδηγία 95/46 που ήταν εδώ και 20 χρόνια το βασικό νομοθέτημα για την προστασία προσωπικών δεδομένων σε επίπεδο Ευρωπαϊκών Κοινοτήτων. Ο Κανονισμός έχει σχεδιαστεί κατά τέτοιο τρόπο ώστε να δώσει στους πολίτες μεγαλύτερο έλεγχο των προσωπικών τους στοιχείων.

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

- **Δικαίωμα στη λήθη**: Όταν εκλείπει ο λόγος της επεξεργασίας των δεδομένων ή το υποκείμενο αίρει τη συγκατάθεσή του (σε περίπτωση που αυτή είναι αναγκαία) ή όταν τα δεδομένα υποβλήθηκαν σε παράνομη επεξεργασία κ.τ.λ., το υποκείμενο έχει δικαίωμα να ζητήσει τη διαγραφή των δεδομένων και ο υπεύθυνος επεξεργασίας έχει υποχρέωση άμεσα να τα διαγράψει και αν τα έχει δημοσιοποιήσει να ενημερώσει και όλους όσους τα έχουν αναδημοσιεύσει ότι το υποκείμενο ζήτησε τη διαγραφή τους.
- **Σαφής συγκατάθεση**: Το κάθε άτομο (ενδιαφερόμενο πρόσωπο) πρέπει να δώσει τη συγκατάθεσή του για την επεξεργασία των προσωπικών του δεδομένων.
- **Δικαίωμα φορητότητας των δεδομένων**: Το υποκείμενο (ενδιαφερόμενο πρόσωπο) έχει δικαίωμα να ζητά από τον υπεύθυνο επεξεργασίας να λαμβάνει τα δεδομένα σε κοινώς αναγνωρίσιμο μορφότυπο, καθώς και την απευθείας διαβίβαση των δεδομένων του σε άλλον υπεύθυνο επεξεργασίας.
- **Υποχρέωση γνωστοποίησης παραβιάσεων ασφάλειας**: Όταν ο υπεύθυνος λάβει γνώση για την παραβίαση της ασφάλειας του συστήματος οφείλει να ειδοποιήσει την ανεξάρτητη Αρχή υπεύθυνη για την προστασία προσωπικών δεδομένων. Η γνωστοποίηση πρέπει να γίνεται και στο ίδιο το υποκείμενο των δεδομένων.
- **Διασυνοριακή διαβίβαση δεδομένων**: Η οδηγία περιλαμβάνει ξεκάθαρους κανόνες για τη διαβίβαση των προσωπικών δεδομένων από τις Αρχές επιβολής του νόμου σε Αρχές εκτός της ΕΕ, έτσι ώστε να μην υπονομεύεται το επίπεδο προστασίας των φυσικών προσώπων που είναι κατοχυρωμένο στην ΕΕ.

- **Ενημέρωση για Δεδομένα Προσωπικού Χαρακτήρα**: Ο υπεύθυνος επεξεργασίας πρέπει να παρέχει όλες τις εξηγήσεις για τις πολιτικές απορρήτου σε σαφή και κατανοητή γλώσσα.
- **Πρόστιμα από μη συμμόρφωση**: Η μη συμμόρφωση με τους κανόνες προστασίας προσωπικών δεδομένων επιφέρει και πρόστιμα στις επιχειρήσεις που τον παραβιάζουν -έως 20 εκατομ. € ή 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών ("τζίρος") του προηγούμενου οικονομικού έτους (*παρ. 4, 5 & 6 του άρθρου 83 του κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016*).

Αρχές ως προς την ποιότητα των δεδομένων: Ο υπεύθυνος επεξεργασίας πρέπει να επιβεβαιώνει ότι ακόλουθες Αρχές προστασίας δεδομένων τηρούνται:

- **Πρώτη Αρχή: Νόμιμη Επεξεργασία (Lawful Processing)**: Τα προσωπικά δεδομένα θα πρέπει να επεξεργάζονται με θεμιτό και νόμιμο τρόπο.

- **Δεύτερη Αρχή: Προσδιορισμός του Σκοπού (Purpose Specification):** Τα προσωπικά δεδομένα θα πρέπει να λαμβάνονται μόνο για έναν ή περισσότερους συγκεκριμένους και νόμιμους σκοπούς, και δεν πρέπει να υποβάλλονται σε περαιτέρω επεξεργασία με οποιονδήποτε τρόπο ασυμβίβαστο με το σκοπό ή τους σκοπούς αυτούς
- **Τρίτη Αρχή: Σχετικότητα Δεδομένων (Data Relevancy):** Τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι κατάλληλα, συναφή και όχι υπερβολικά σε σχέση με το σκοπό ή τους σκοπούς για τους οποίους υφίστανται επεξεργασία.
- **Τετάρτη Αρχή: Ακρίβεια Δεδομένων (Data Accuracy):** Τα προσωπικά δεδομένα πρέπει να είναι ακριβή και, εφόσον χρειάζεται, να ενημερώνονται.
- **Πέμπτη Αρχή: Περιορισμένη Διατήρηση Δεδομένων (Limited Data Retention):** Τα προσωπικά δεδομένα που έχουν επεξεργασθεί για οποιονδήποτε σκοπό ή σκοπούς δεν θα πρέπει να διατηρούνται για μεγαλύτερο χρονικό διάστημα από ό, τι είναι απαραίτητο για το σκοπό αυτό ή τους σκοπούς αυτούς.
- **Έκτη Αρχή: Θεμιτή Επεξεργασία (Fair Processing):** Τα προσωπικά δεδομένα θα πρέπει να υποβάλλονται σε επεξεργασία σύμφωνα με τα δικαιώματα των υποκειμένων των δεδομένων δυνάμει του παρόντος νόμου.
- **Έβδομη Αρχή: Λογοδοσία (Accountability):** Θα πρέπει να ληφθούν τα κατάλληλα διοικητικά, τεχνικά και οργανωτικά μέτρα έναντι μη εξουσιοδοτημένης ή παράνομης επεξεργασίας δεδομένων προσωπικού χαρακτήρα και έναντι τυχαίας απώλειας ή καταστροφής ή βλάβης ή άλλης ζημίας στα προσωπικά δεδομένα που τηρούνται από την επιχείρηση.

- **Υπεύθυνος Προστασίας Δεδομένων:** Σε κάθε δημόσιο φορέα (εκτός από τα δικαστήρια στο πλαίσιο των δικαιοδοτικών τους αρμοδιοτήτων, εάν τα κράτη επιλέξουν να τα εξαιρέσουν) και σε κάθε ιδιωτικό φορέα που λόγω της φύσης των δραστηριοτήτων τους παρακολουθούν υποκείμενα δεδομένων σε μεγάλη κλίμακα ή επεξεργάζονται ευαίσθητα δεδομένα, ορίζεται ένα πρόσωπο ως ΥΠΔ. Ο ΥΠΔ λειτουργεί ως μια εσωτερική Αρχή Προστασίας Δεδομένων που διασφαλίζει ότι η δημόσια υπηρεσία ή ο ιδιωτικός φορέας τηρεί τις διατάξεις του Κανονισμού και συνεργάζεται με την Εθνική Αρχή Προστασίας για την τήρηση των διατάξεων.

- **Εκτίμηση Επιπτώσεων Προστασίας Δεδομένων**: Ο υπεύθυνος επεξεργασίας πρέπει να επιβεβαιώνει ότι εφαρμόζεται μία διαδικασία για τη διεξαγωγή μίας αξιολόγησης του κινδύνων προστασίας των δεδομένων (Data Protection Impact Assessment) σε όλες τις επιχειρησιακές μονάδες.

Για τη διαδικασία συμμόρφωσης του ΔΗ.ΠΕ.ΘΕυ στο «Γενικό Κανονισμό Προστασία Δεδομένων» (ΓΚΠΔ-GDPR), (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, απαιτούνται να γίνουν οι παρακάτω ενέργειες:

Σέρρες 23/04/2020 **23/04/2020**

Ο ΣΥΝΤΑΞΑΣ **Θεωρήθηκε**

Ο Πρόεδρος του Δ.Σ.

ΠΛΑΝΟ ΥΛΟΠΟΙΗΣΗΣ

Φάση 1η

- Θα παρουσιαστεί Πλάνο Υλοποίησης του έργου, στο οποίο θα αποτυπώνεται λεπτομερώς η ομάδα εργασίας του Αναδόχου, η μεθοδολογία που θα ακολουθηθεί, οι επιμέρους φάσεις, το χρονοδιάγραμμα υλοποίησης και τα παραδοτέα που θα προκύψουν από κάθε φάση. Θα δοθούν οδηγίες σχετικά με τις πρώτες ενέργειες που θα πρέπει να γίνουν, τη σύνταξη δεσμευτικής δήλωσης της Διοίκησης, τη λήψη απόφασης για την εφαρμογή της συμμόρφωσης κλπ.

Παραδοτέα:

- ✓ **Π1**. Πλάνο Υλοποίησης του έργου

Φάση 2η

- Ανάλυση της τρέχουσας κατάστασης όσον αφορά τα προσωπικά δεδομένα.

Θα γίνει καταγραφή και κατηγοριοποίηση των προσωπικών δεδομένων (απλά, ευαίσθητα, ειδικού σκοπού κλπ) που κατέχει και επεξεργάζεται το ΔΗ.ΠΕ.ΘΕ, ανά οργανική μονάδα (Διεύθυνση και Τμήμα) - (Personal Data Register). Η συλλογή των στοιχείων θα γίνει μέσω της διεξαγωγής συνεντεύξεων από στελέχη του Αναδόχου, σε στελέχη του ΔΗ.ΠΕ.ΘΕ και συμπλήρωσης κατάλληλων ερωτηματολογίων κλπ.

Θα αναλυθεί η τρέχουσα κατάσταση ως προς την προστασία των προσωπικών δεδομένων, θα αξιολογηθούν οι υφιστάμενες πρακτικές, των γραπτών πολιτικών και διαδικασιών, των πληροφοριακών συστημάτων και δικτυακών υποδομών και κάθε στοιχείου που επηρεάζει την προστασία προσωπικών δεδομένων ανά οργανική μονάδα (Διεύθυνση και Τμήμα). Θα αξιολογηθεί η υφιστάμενη κατάσταση ως προς την ασφάλεια των πληροφοριών και την επιχειρησιακή συνέχεια που αποτελούν συστατικά της προστασίας των δεδομένων.

Η ανωτέρω αξιολόγηση θα περιλαμβάνει κατ’ ελάχιστο τα ακόλουθα:

- ➢ Αξιολόγηση της νομικής βάσης, στην οποία στηρίζεται η συλλογή του συνόλου των συλλεγόμενων προσωπικών δεδομένων, της παρεχόμενης συναίνεσης από τον εκάστοτε συμβαλλόμενο, των παρεχόμενων πληροφοριών κ.λπ.

- Αξιολόγηση δυνατότητας ικανοποίησης των δικαιωμάτων των φυσικών προσώπων
- Αξιολόγηση του επιπέδου ασφαλείας και επιχειρησιακής συνέχειας
- Αξιολόγηση της οργανωτικής δομής
- Αξιολόγηση της κουλτούρας και ευαισθητοποίησης στα θέματα προστασίας προσωπικών δεδομένων
- Αξιολόγηση πληροφορικών συστημάτων και πολιτικών που επιβάλλονται από την πληροφορική
- Αξιολόγηση μηχανισμών ελέγχου και διασφάλισης της συμμόρφωσης
- Αξιολόγηση σχετικών γραπτών πολιτικών και διαδικασιών

Παραδοτέα:

- ✓ **Π2**. Κατάλογος κατηγοριοποιημένων προσωπικών δεδομένων που κατέχει και επεξεργάζεται το ΔΗ.ΠΕ.ΘΕ, ανά οργανική μονάδα (Διεύθυνση και Τμήμα) (Personal Data Register)

Φάση 3η

- Δημιουργία Λεπτομερών Χαρτογραφημένων Αρχείων (Data Flow Maps)
- Εύρεση κενών (Gap Analysis) ως προς την ικανοποίηση των απαιτήσεων του Κανονισμού
- Δημιουργία Σχεδίου Συμμόρφωσης (Compliance Plan)

Θα δημιουργηθούν Λεπτομερή Χαρτογραφημένα Αρχεία (Data Flow Maps), ανά οργανική μονάδα (Διεύθυνση και Τμήμα), ανά κατηγορία προσωπικών δεδομένων, όπου θα απεικονίζονται όλες οι πληροφορίες σχετικά με τη διαχείριση των προσωπικών δεδομένων του ΔΗ.ΠΕ.ΘΕ Σερρών. Τα λεπτομερή αρχεία θα καλύπτουν την απαίτηση του Κανονισμού για το Αρχείο Δραστηριοτήτων Επεξεργασίας Δεδομένων και θα περιέχουν όλες τις επιπλέον απαραίτητες πληροφορίες, ώστε να απεικονίζεται πλήρως η τρέχουσα κατάσταση ως προς τη διαχείριση προσωπικών δεδομένων και να εντοπίζονται κενά ως προς τις απαιτήσεις του θεσμικού πλαισίου.

Θα γίνει ανάλυση των κενών (Gap Analysis) ως προς την ικανοποίηση των απαιτήσεων του Κανονισμού, κατηγοριοποιημένα ανά θεματική περιοχή και κρισιμότητα.

Για κάθε κενό που εντοπίζεται, θα καθορίζονται οι απαραίτητες ενέργειες αντιμετώπισης και θα δημιουργηθεί ένα λεπτομερές, προτεραιοποιημένο και ολοκληρωμένο Σχέδιο Συμμόρφωσης (Compliance Plan and Road Map).

Θα πραγματοποιηθεί έλεγχος σε όλες τις εμπλεκόμενες εφαρμογές λογισμικού, σε όλα τα αποθηκευτικά μέσα (ψηφιακά, έντυπα, ηχητικά κλπ), τις ιστοσελίδες του ΔΗ.ΠΕ.ΘΕυ κλπ και θα προταθούν με σαφήνεια

οι απαιτούμενες αλλαγές και τροποποιήσεις βάσει του νέου Κανονισμού. Η αξιολόγηση θα περιλαμβάνει το σύνολο των συλλεγόμενων προσωπικών δεδομένων, της νομικής βάσης πάνω στην οποία στηρίζεται η συλλογή, της παρεχόμενης συναίνεσης από τον εκάστοτε συμβαλλόμενο, των παρεχόμενων πληροφοριών κ.λπ. Θα πραγματοποιηθεί αξιολόγηση όλων των πρακτικών που σχετίζονται με την επεξεργασία των προσωπικών δεδομένων και θα δοθούν συγκεκριμένες και λεπτομερείς προτάσεις για δράσεις συμμόρφωσης με τον νέο Κανονισμό. Όλες οι προτεινόμενες ενέργειες συμμόρφωσης θα καλύπτουν ολόκληρο τον κύκλο ζωής των προσωπικών δεδομένων (δηλ. συλλογή, καταγραφή, τροποποίηση/ενημέρωση, αποθήκευση, μεταφορά, διαγραφή/καταστροφή κ.λπ.) και θα έχουν συμφωνηθεί με την ομάδα έργου και τους επιχειρησιακούς ιδιοκτήτες των δεδομένων του ΔΗ.ΠΕ.ΘΕ πριν την παράδοση του πλάνου συμμόρφωσης.

Παραδοτέα:

- ✓ **Π3**. Λεπτομερή Χαρτογραφημένα Αρχεία (Data Flow Maps)
- ✓ **Π4**. Αρχείο Δραστηριοτήτων Επεξεργασίας Δεδομένων
- ✓ **Π5**. Λίστα κενών ως προς την ικανοποίηση των απαιτήσεων του Κανονισμού
- ✓ **Π6**. Σχέδιο Συμμόρφωσης (Compliance Plan and Road Map)

Φάση 4η

- Εκτίμηση Αντικτύπου Προστασίας Δεδομένων (Data Protection Impact Assessment)
- Ανάλυση Επικινδυνότητας Ασφάλειας Πληροφοριών (Information Security Risk Assessment)
- Δημιουργία Εγχειριδίου Προστασίας Προσωπικών Δεδομένων
- Συγγραφή πολιτικής ασφαλείας
- Έλεγχος και εφαρμογή μηχανισμού παραβιάσεων
- Έλεγχος των συμβάσεων του οργανισμού εσωτερικά και με τρίτους
- Κατάρτιση σχεδίου διαχείρισης συμβάντων
- Κατάρτιση Σχεδίου Αναγγελίας Διαρροής στην Αρχή Προστασίας Προσωπικών Δεδομένων

Θα συνταχθεί Μελέτη Ανάλυσης Επικινδυνότητας Ασφάλειας Πληροφοριών (Information Security Risk Assessment). Οι ανωτέρω αναλύσεις επικινδυνότητας και εκτίμησης επιπτώσεων θα είναι συμβατές μεταξύ τους και δεν θα περιέχουν αλληλεπικαλύψεις, κενά ή αλληλοσυγκρουόμενες πληροφορίες.
Θα συνταχθεί Εγχειρίδιο Προστασίας Προσωπικών Δεδομένων, το οποίο θα περιλαμβάνει όλες τις απαραίτητες Πολιτικές και Διαδικασίες Προστασίας Προσωπικών Δεδομένων, Ασφάλειας Πληροφοριών και Επιχειρησιακής Συνέχειας, έντυπα και ότι άλλο είναι απαραίτητο. Το Εγχειρίδιο Προστασίας

Προσωπικών Δεδομένων θα καλύπτει το σύνολο των απαιτήσεων του Κανονισμού και θα λαμβάνει υπόψη τα προτεινόμενα μέτρα του πλάνου συμμόρφωσης.

Η πολιτική Ασφαλείας (Security policy) που θα συνταχθεί θα αποτελεί έγγραφο του υπεύθυνου επεξεργασίας στο οποίο θα περιγράφονται οι στόχοι της ασφάλειας και οι αντίστοιχες διαδικασίες που πρέπει να ακολουθούνται.

Θα γίνει έλεγχος υφιστάμενου ή εφαρμογή νέου μηχανισμού εντοπισμού παραβιάσεων (security Breaches) ή απλών περιστατικών ασφαλείας (security incident) με αυτόματη καταγραφή (Security log).

Θα γίνει έλεγχος των υπαρχουσών συμβάσεων του ΔΗ.ΠΕ.ΘΕ.

Το σχέδιο διαχείρισης συμβάντων είναι το έγγραφο που αναφέρεται στις διαδικασίες που θα ακολουθηθούν σε περίπτωση παραβίασης ασφαλείας.

Τέλος, θα γίνει κατάρτιση σχεδίου ώστε να είναι δυνατή η αναγγελία της διαρροής εντός 72 ωρών, όπως προβλέπεται από τον κανονισμό.

Παραδοτέα:

- ✓ **Π7**. Μελέτη Ανάλυσης Επικινδυνότητας Ασφάλειας Πληροφοριών (Information Security Risk Assessment)
- ✓ **Π8**. Εγχειρίδιο Προστασίας Προσωπικών Δεδομένων (Personal Data Protection Policies and Procedures)
- ✓ **Π9**. Κείμενο πολιτικής ασφάλειας
- ✓ **Π10**. Αναφορά ελέγχου εντοπισμού παραβιάσεων ή απλών περιστατικών ασφαλείας
- ✓ **Π11**. Πλήρες κείμενο διαχείρισης συμβάντων
- ✓ **Π12**. Σχέδιο Αναγγελίας Διαρροής

Φάση 5η

- Εκπαίδευση εργαζομένων, σε θέματα που αφορούν την τήρηση των προϋποθέσεων του κανονισμού. Δημιουργία κουλτούρας προστασίας προσωπικών δεδομένων.
- Επαναξιολόγηση (Compliance Audit)
- Παρουσίαση του έργου στην Διοίκηση και τα ανώτερα στελέχη του Φορέα

Με την ολοκλήρωση του συνόλου των ενεργειών γίνεται επαναξιολόγηση του επιπέδου συμμόρφωσης του ΔΗ.ΠΕ.ΘΕ Σερρών και των νομικών του προσώπων μέσω των επιθεωρήσεων ετοιμότητας.

Θα γίνει εκπαίδευση των εργαζομένων και θα πραγματοποιηθεί τελική συνάντηση του Αναδόχου με τη Διοίκηση και τα ανώτερα στελέχη του ΔΗ.ΠΕ.ΘΕ Σερρών κατά την οποία θα γίνει αναλυτική παρουσίαση των εργασιών που έγιναν. Θα παρουσιαστούν τα παραδοτέα και θα δοθούν τελικές οδηγίες.

Παραδοτέα:

- ✓ **Π13**. Πρόγραμμα εκπαίδευσης ανά οργανωτική μονάδα με ορισμένο εκπαιδευτικό πρόγραμμα υλικό και παρουσιολόγιο. Αποτελεί τμήμα της απαραίτητης για την συμμόρφωση τεκμηρίωσης

<u>Σύνολο Παραδοτέων</u>

- ✓ **Π1**. Πλάνο Υλοποίησης του έργου.
- ✓ **Π2.** Κατάλογος κατηγοριοποιημένων προσωπικών δεδομένων που κατέχει και επεξεργάζεται το ΔΗ.ΠΕ.ΘΕ, ανά οργανική μονάδα (Διεύθυνση και Τμήμα) (Personal Data Register).
- ✓ **Π3**. Λεπτομερή Χαρτογραφημένα Αρχεία (Data Flow Maps).
- ✓ **Π4**. Αρχείο Δραστηριοτήτων Επεξεργασίας Δεδομένων.
- ✓ **Π5**. Λίστα κενών ως προς την ικανοποίηση των απαιτήσεων του Κανονισμού.
- ✓ **Π6**. Σχέδιο Συμμόρφωσης (Compliance Plan and Road Map).
- ✓ **Π7**. Μελέτη Ανάλυσης Επικινδυνότητας Ασφάλειας Πληροφοριών (Information Security Risk Assessment).
- ✓ **Π8**. Εγχειρίδιο Προστασίας Προσωπικών Δεδομένων (Personal Data Protection Policies and Procedures).
- ✓ **Π9.** Κείμενο πολιτικής ασφάλειας.
- ✓ **Π10**. Αναφορά ελέγχου εντοπισμού παραβιάσεων ή απλών περιστατικών ασφαλείας.
- ✓ **Π11**. Πλήρες κείμενο διαχείρισης συμβάντων.
- ✓ **Π12**. Σχέδιο Αναγγελίας Διαρροής.
- ✓ **Π13**. Πρόγραμμα εκπαίδευσης ανά οργανωτική μονάδα με ορισμένο εκπαιδευτικό πρόγραμμα υλικό και παρουσιολόγιο. Αποτελεί τμήμα της απαραίτητης για την συμμόρφωση τεκμηρίωσης.

Ενδεικτικό Χρονοδιάγραμμα Υλοποίησης (συνολικά 4 μήνες από την υπογραφή της σύμβασης)

		1				2				3				4			
		12	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Φάση 1η	Παρουσίαση του Κανονισμού στη Διοίκηση και τα ανώτερα στελέχη του Φορέα															
Φάση 2η	Ανάλυση της τρέχουσας κατάστασης όσον αφορά στα προσωπικά δεδομένα															
Φάση 3η	Δημιουργία Λεπτομερών Χαρτογραφημένων Αρχείων (Data Flow Maps)															
	Εύρεση κενών (Gap Analysis)															
	Δημιουργία Σχεδίου Συμμόρφωσης (Compliance Plan)															
Φάση 4η	Ανάλυση Επικινδυνότητας ασφάλειας πληροφοριών (Information Security Risk Assessment)															
	Δημιουργία εγχειριδίου Προστασίας Προσωπικών Δεδομένων															
	Συγγραφή πολιτικής ασφαλείας															
	Έλεγχος και εφαρμογή μηχανισμού παραβιάσεων															
	Κατάρτιση σχεδίου διαχείρισης συμβάντων															
	Κατάρτιση Σχεδίου Αναγγελίας Διαρροής στην Αρχή Προστασίας Προσωπικών Δεδομένων															
Φάση 5η	Εκπαίδευση εργαζομένων, σε θέματα που αφορούν την τήρηση των προϋποθέσεων του κανονισμού. Δημιουργία κουλτούρας προστασίας προσωπικών δεδομένων.															
	Παρουσίαση του έργου στην Διοίκηση και τα ανώτερα στελέχη του Φορέα															

Σέρρες 23/04/2020

Ο ΣΥΝΤΑΞΑΣ

23/04/2020

Θεωρήθηκε

Ο Πρόεδρος του Δ.Σ.

ΔΗ.Κ.Ε.
ΔΗΠΕΘΕ ΣΕΡΡΩΝ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΔΗΜΟΣ ΣΕΡΡΩΝ
ΔΗΜΟΤΙΚΟ ΠΕΡΙΦΕΡΕΙΑΚΟ ΘΕΑΤΡΟ ΣΕΡΡΩΝ
(ΔΗ.Κ.Ε. ΔΗ.ΠΕ.ΘΕ.)

ΣΥΓΓΡΑΦΗ ΥΠΟΧΡΕΩΣΕΩΝ

Άρθρο 1ο: Αντικείμενο εργασίας

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

Άρθρο 2ο: Ισχύουσες διατάξεις

Η εκτέλεση της υπηρεσίας διέπεται από:

1. Τον Ν.3463/2006 «Κύρωση του Κώδικα Δήμων και Κοινοτήτων», όπως ισχύει.
2. Τον Ν.3852/2010 «Νέα Αρχιτεκτονική της Αυτοδιοίκησης και της Αποκεντρωμένης Διοίκησης – Πρόγραμμα Καλλικράτης».
3. Τον Ν. 3886/2010 «Δικαστική προστασία κατά τη σύναψη δημοσίων συμβάσεων-Εναρμόνιση της ελληνικής νομοθεσίας με την Οδηγία 89/665/εοκ του Συμβουλίου της 21ης Ιουνίου 1989(L 395) και την Οδηγία 92/13/ΕΟΚ του Συμβουλίου της 25ης Φεβρουαρίου 1992 (L76), όπως τροποποιήθηκαν».
4. Τον Κανονισμό ΕΕ 1251/2011 της Ευρωπαϊκής Επιτροπής της 30/11/2011.6. Την Π1/358/27-01-1999 Υπ. Απόφαση ως ισχύει περί εξαιρέσεως από το Ε.Π.Π προμηθειών που πραγματοποιούνται με τη ανάδειξη προμηθευτών χορηγητών.
5. Το ν.4281/2014 (ΦΕΚ 160’Α)«Μέτρα στήριξης και ανάπτυξης της ελληνικής οικονομίας, οργανωτικά θέματα Υπουργείου Οικονομικών και άλλες διατάξεις.».
6. Το ν.4250/2014(ΦΕΚ 74Α’) «Διοικητικές Απλουστεύσεις – Καταργήσεις, Συγχωνεύσεις Νομικών Προσώπων και Υπηρεσιών Του Δημοσίου Τομέα – Τροποποίηση Διατάξεων Του Π.Δ. 318/1992 (Α’161) και λοιπές ρυθμίσεις.
7. Το άρθρο 32 παρ. 6 του Ν.4412/2016 περί προσφυγής στη διαδικασία με διαπραγμάτευση χωρίς προηγούμενη δημοσίευση.

8. Τον ν. 2741/99 (φεκ199/α/28-9-99) άρθρο 8 «Ενιαίος Φορέας ελέγχου Τροφίμων άλλες ρυθμίσεις θεμάτων αρμοδιότητας του Υπουργείου Ανάπτυξης και λοιπές διατάξεις», όπως τροποποιήθηκε με τα άρθρα 2 ν.3060/02, παρ3 Ν.3090/02, 9 ΠΑΡ.3 3090/02,12 ΠΑΡ 27 Ν. 3310 και 3414/05 περί ελέγχου νομιμότητας των σχεδίων συμβάσεων από το Ελεγκτικό Συνέδριο.

9.Τις διατάξεις του άρθρου 58 του Ν. 3852/2010.

10. Τις διατάξεις του άρθρου 118 του Ν. 4412/2016.

11. Την παρ. 4 του άρθρου 209 του Ν. 3463/2006, όπως αναδιατυπώθηκε με την παρ. 3 του άρθρου 22 του Ν. 3536/2007.

12. Τις διατάξεις της παρ. 9 του άρθρου 209 του Ν. 3463/2006, όπως προστέθηκε με την παρ. 13 του άρθρου 20 του Ν. 3731/2008 και διατηρήθηκε σε ισχύ με την περίπτωση 38 της παρ. 1 του άρθρου 377 του Ν. 4412/2016.

Άρθρο 3ο: Συμβατικά στοιχεία

Τα συμβατικά στοιχεία κατά σειρά ισχύος είναι:

i) Η Τεχνική έκθεση
ii) Η Συγγραφή των Υποχρεώσεων
iii) Η Οικονομική Προσφορά

Άρθρο 4ο : Χρόνος εκτέλεσης υπηρεσίας

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

Άρθρο 5ο : Δικαιολογητικά συμμετοχής

1) Υπεύθυνη Δήλωση του Ν.1599/86 στην οποία οι υποψήφιοι Ανάδοχοι θα δηλώνουν:
   - ότι αποδέχονται τους όρους της μελέτης και ότι η προσφορά τους είναι σύμφωνη με την Τεχνική έκθεση
   - ότι τηρούν τις υποχρεώσεις που απορρέουν από τις διατάξεις του άρθρου 18 του ν. 4412/2016 (περί περιβαλλοντικής, κοινωνικοασφαλιστικής και εργατικής νομοθεσίας)
   - την έδρα της επιχείρησης, και τη νομική μορφή της επιχείρησης
2) Οικονομική Προσφορά των υποψηφίων Αναδόχων. Η Οικονομική προσφορά θα συνταχθεί σύμφωνα με το ΠΑΡΑΡΤΗΜΑ Ι της παρούσας μελέτης.
3) Κατάλογο των μελών της ομάδας έργου των υποψηφίων Αναδόχων και συνοπτικά βιογραφικά σημειώματα όλων των μελών της. Η ομάδα έργου θα πρέπει να απαρτίζεται από τουλάχιστον τρία (3) μέλη, εκ των οποίων:
   - τα 2 μέλη (το ένα θα οριστεί υπεύθυνος έργου) θα πρέπει
     - να έχουν αποδεδειγμένη εμπειρία τουλάχιστον 15 ετών σε θέματα Ασφάλειας

Πληροφοριακών Συστημάτων και Πληροφοριών
- ο να έχουν συμμετάσχει στην υλοποίηση τουλάχιστον 3 αντίστοιχων έργων και να δοθούν οι σχετικές βεβαιώσεις.
- ο να συμμετέχουν στην υλοποίηση τουλάχιστον ενός αντίστοιχου έργου, σε φορέα άνω των 500 ατόμων και να κατατεθεί η σχετική σύμβαση.

- το 1 μέλος θα είναι νομικός με μεταπτυχιακό τίτλο σπουδών με εξειδίκευση σε θέματα Προστασίας Προσωπικών Δεδομένων καθώς και αποδεδειγμένη νομική εμπειρία τουλάχιστον 15 ετών σε θέματα Προστασίας Προσωπικών Δεδομένων. Για την απόδειξη της απαίτησης να κατατεθούν οι τίτλοι σπουδών και οι βεβαιώσεις έργων Προστασίας Προσωπικών Δεδομένων.
- τουλάχιστον 1 μέλος της ομάδας θα πρέπει να διαθέτει τις ακόλουθες πιστοποιήσεις και οι οποίες θα πρέπει να κατατεθούν **ISO 27001 Auditor** και **ITIL Expert**.

ο Κατάθεση εν ισχύ πιστοποιητικού **IS0-27001:2013**, ή ισοδύναμου αυτού.

4) Αντίγραφο ποινικού μητρώου (πρωτότυπο). Η υποχρέωση αφορά ιδίως: α) στις περιπτώσεις εταιρειών περιορισμένης ευθύνης (Ε.Π.Ε.) και προσωπικών εταιρειών (Ο.Ε. και Ε.Ε.), τους διαχειριστές, β) στις περιπτώσεις ανωνύμων εταιρειών (Α.Ε.), τον Διευθύνοντα Σύμβουλο, καθώς και όλα τα μέλη του Διοικητικού Συμβουλίου
5) Ο αναδοχος να διαθέτει ISO 9001 ISO 27001 ISO 20000
6) Φορολογική ενημερότητα
7) Ασφαλιστική ενημερότητα
8) Εφόσον πρόκειται για νομικό πρόσωπο, αποδεικτικά έγγραφα νομιμοποίησης του νόμιμου εκπροσώπου (άρθρο 93 του Ν.4412/2016)

Άρθρο 6ο : Επιλογή Αναδόχου

Η σύμβαση θα συναφθεί με τον Ανάδοχο που θα προσφέρει τη συμφερότερη από οικονομικής άποψης προσφορά μόνο βάσει της τιμής.

Άρθρο 7ο : Συμφωνητικό Εχεμύθειας – Εμπιστευτικότητας του Αναδόχου

Με την έναρξη της υπηρεσίας ο Ανάδοχος υποχρεούται να υπογράψει Συμφωνητικό Εχεμύθειας – Εμπιστευτικότητας, σύμφωνα με το οποίο θα εγγυάται την εχεμύθεια των αποτελεσμάτων και όσων δεδομένων συλλεχθούν κατά την υλοποίηση της εργασίας. Το Συμφωνητικό θα καλύπτει όλα τα αποτελέσματα, καθώς και όλες τις πληροφορίες που θα πρέπει να ανακτηθούν κατά τη διάρκεια του έργου. Σύμφωνα με αυτό ο Ανάδοχος θα αναλαμβάνει την ευθύνη για τη διασφάλιση της εμπιστευτικότητας των εμπλεκόμενων συμβούλων, μηχανικών και τεχνικών,

όσον αφορά τη μη διαρροή πληροφοριών του είδους, του βαθμού διεκπεραίωσης του έργου καθώς και τις λεπτομέρειες αυτού.

Άρθρο 8ο : Υποχρεώσεις του Αναδόχου

Ο Ανάδοχος υποχρεούται να παρέχει:

1. Άρτια εργασία σύμφωνα με τους κανόνες της επιστήμης, της τεχνικής, και του επαγγέλματος
2. Αναπροσαρμογή των περιεχομένων της εργασίας ανάλογα με τις παρατηρήσεις της επιβλέπουσας υπηρεσίας
3. Αναλυτικές προτάσεις με τεκμηρίωση

4. Παράδοση της υπηρεσίας εμπρόθεσμα
5. Οι υπηρεσίες θα υλοποιούνται εξ ολοκλήρου από τον Ανάδοχο και το εξειδικευμένο του προσωπικό ή εξωτερικούς συνεργάτες. Την πληρωμή του προσωπικού (αποδοχές, εισφορές, κλπ.) αναλαμβάνει εξ ολοκλήρου ο Ανάδοχος

Άρθρο 9ο : Υποχρεώσεις της Αναθέτουσας αρχής

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

Άρθρο 10ο : Ανωτέρα βία

Ως ανωτέρα βία θεωρείται κάθε απρόβλεπτο και τυχαίο γεγονός που είναι αδύνατο να προβλεφθεί έστω και εάν για την πρόβλεψη και αποτροπή της επέλευσης του καταβλήθηκε υπερβολική επιμέλεια και επιδείχθηκε η ανάλογη σύνεση. Ο όρος περί ανωτέρας βίας εφαρμόζεται ανάλογα και για τον εντολέα προσαρμοζόμενος ανάλογα.

Άρθρο 11ο : Αναθεώρηση τιμών

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

Άρθρο 12ο : Παραλαβή παραδοτέων

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

Άρθρο 13ο : Τρόπος πληρωμής

Η πληρωμή των 3.720,00 € συμπεριλαμβανομένου Φ.Π.Α., θα γίνεται τμηματικά με την πρόοδο των εργασιών, μετά την ολοκλήρωση της κάθε φάσης και την παράδοση και παραλαβή του συνόλου των παραδοτέων της.

Το ποσό πληρωμής θα αναπροσαρμοστεί ανάλογα, σύμφωνα με την έκπτωση που θα δώσει ο Ανάδοχος στον ενδεικτικό προϋπολογισμό της μελέτης.

Η καταβολή θα γίνει κατόπιν εκδόσεως βεβαίωσης καλής εκτέλεσης από την αρμόδια υπηρεσία, εκδόσεως του σχετικού δελτίου παροχής υπηρεσιών του Αναδόχου και πρακτικού παραλαβής από την αρμόδια επιτροπή.
Τον Ανάδοχο βαρύνουν όλες οι νόμιμες κρατήσεις εκτός του ΦΠΑ, ο οποίος βαρύνει την Αναθέτουσα Αρχή. Η αμοιβή δεν υπόκειται σε καμία αναθεώρηση για οποιοδήποτε λόγο και αιτία και παραμένει σταθερή και αμετάβλητη καθ' όλη την διάρκεια ισχύος της σύμβασης. Η αμοιβή καταβάλλεται όπως αναφέρεται παραπάνω, με πιστοποιήσεις της επιβλέπουσας υπηρεσίας και εξοφλείται μετά την παράδοση.

Χορήγηση προκαταβολής δεν προβλέπεται.

Άρθρο 14ο : Φόροι, τέλη, κρατήσεις

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

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

Άρθρο 15ο : Τόπος

Ο Ανάδοχος θα παρέχει τις υπηρεσίες από την έδρα του. Οι συναντήσεις, οι συνεντεύξεις και η συμπλήρωση ερωτηματολογίων θα γίνεται σε χώρους που θα υποδεικνύει το ΔΗ.ΠΕ.ΘΕ Σερρών.

Άρθρο 16ο : Επίλυση διαφορών

Κάθε διαφορά που θα προκύπτει από την εφαρμογή της σύμβασης αυτής και στις περιπτώσεις που δεν θα μπορεί να διευθετηθεί μεταξύ του ΑΝΑΔΟΧΟΥ και του ΣΥΜΒΑΛΛΟΜΕΝΟΥ θα υπάγεται στην αρμοδιότητα των Δικαστηρίων Σερρών.

Άρθρο 17ο : Έκπτωση Αναδόχου

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

Σέρρες 23/04/2020

Ο ΣΥΝΤΑΞΑΣ

23/04/2020

Θεωρήθηκε

Ο Πρόεδρος του Δ.Σ.

ΔΗ.Κ.Ε.
ΔΗΠΕΘΕ ΣΕΡΡΩΝ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΔΗΜΟΣ ΣΕΡΡΩΝ
ΔΗΜΟΤΙΚΟ ΠΕΡΙΦΕΡΕΙΑΚΟ ΘΕΑΤΡΟ ΣΕΡΡΩΝ
(ΔΗ.ΚΕ.ΔΗ.ΠΕ.ΘΕ)

ΤΙΤΛΟΣ: «Υπηρεσίες Υποστήριξης του ΔΗ.ΠΕ.ΘΕ Σερρών για την προετοιμασία και προσαρμογή στο νέο κανονισμό προστασίας δεδομένων (ΕΕ679/2016)»

ΕΝΤΥΠΟ ΟΙΚΟΝΟΜΙΚΗΣ ΠΡΟΣΦΟΡΑΣ

ΠΡΟΣ «Δημοτικό Περιφερειακό Θέατρο Σερρών »

Του/ης……με

έδρα……οδός……Αριθμ……Τ.Κ……

τηλ. ……Fax……e-mail:……

Υποβάλλω την παρούσα προσφορά και δηλώνω ότι αποδέχομαι πλήρως και χωρίς επιφύλαξη όλες τις υποχρεώσεις που απορρέουν από την Τεχνική Έκθεση και αναλαμβάνω την εκτέλεση της υπηρεσίας με τις ακόλουθες τιμές επί των τιμών του προαναφερόμενου Προϋπολογισμού.

Η οικονομική προσφορά του ΔΗ.ΠΕ.ΘΕ Σερρών για το σύνολο έργου ανέρχεται στο ποσό των …… Ευρώ πλέον αναλογούντος ΦΠΑ. Ο Αναλογούν ΦΠΑ ανέρχεται στο ποσό των ……. Ευρώ.

Η τελική συνολική τιμή είναι …….. (ολογράφως) και αριθμητικώς ……. €

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

……, ……/……/……

Ο ΠΡΟΣΦΕΡΩΝ

(Ονοματεπώνυμο – Σφραγίδα – Υπογραφή)