ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΝΟΜΟΣ ΘΕΣΣΑΛΟΝΙΚΗΣ
ΣΥΝΔΕΣΜΟΣ ΔΗΜΩΝ
ΔΥΤΙΚΗΣ ΘΕΣΣΑΛΟΝΙΚΗΣ
ΤΕΧΝΙΚΗ ΥΠΗΡΕΣΙΑ
Τ.Θ. 30505
56210 ΕΥΟΣΜΟΣ
Πληροφορίες: Κοντολέων Μηνάς
Τηλέφωνο: 2310778664
Email: minas@sddt.org.gr
Fax: 2310778662

ΜΕΛΕΤΗ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΣΥΜΜΟΡΦΩΣΗΣ, ΠΡΟΣΑΡΜΟΓΗΣ ΚΑΙ ΥΠΟΣΤΗΡΙΞΗΣ ΩΣ ΠΡΟΣ ΤΟΝ ΝΕΟ ΚΑΝΟΝΙΣΜΟ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΤΗΣ Ε.Ε. 679/2016

Θεσσαλονίκη 07.05.2018
Αρ. Πρωτ.: **1557**

ΤΕΧΝΙΚΗ ΕΚΘΕΣΗ

Ο Σύνδεσμος Δήμων Δυτικής Θεσσαλονίκης (Σ.Δ.Δ.Θ), προτίθεται να προχωρήσει σε ανάθεση υπηρεσιών συμμόρφωσης, προσαρμογής και υποστήριξης ως προς τον Νέο Κανονισμό Προστασίας Προσωπικών Δεδομένων της Ε.Ε. με αριθ. 679/2016 (General Data Protection Regulation – GDPR), ενδεικτικού προϋπολογισμού **15.000,00€** μη συμπεριλαμβανομένου του Φ.Π.Α. 24%.

Η χρηματοδότηση της δαπάνης θα γίνει από ίδιους πόρους.

ΔΙΑΡΘΡΩΣΗ

1. ΕΝΔΕΙΚΤΙΚΟΣ ΠΡΟΫΠΟΛΟΓΙΣΜΟΣ……2
2. ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ……3
3. ΠΑΡΑΡΤΗΜΑ ……17

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΝΟΜΟΣ ΘΕΣΣΑΛΟΝΙΚΗΣ
ΣΥΝΔΕΣΜΟΣ ΔΗΜΩΝ
ΔΥΤΙΚΗΣ ΘΕΣΣΑΛΟΝΙΚΗΣ

ΜΕΛΕΤΗ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΣΥΜΜΟΡΦΩΣΗΣ, ΠΡΟΣΑΡΜΟΓΗΣ ΚΑΙ ΥΠΟΣΤΗΡΙΞΗΣ ΩΣ ΠΡΟΣ ΤΟΝ ΝΕΟ ΚΑΝΟΝΙΣΜΟ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΤΗΣ Ε.Ε 679/2016

1. ΕΝΔΕΙΚΤΙΚΟΣ ΠΡΟΫΠΟΛΟΓΙΣΜΟΣ

Α/Α	CPV	ΠΕΡΙΓΡΑΦΗ	ΠΟΣΟΤΗΤΑ	ΜΟΝ. ΜΕΤΡ.	ΕΝΔΕΙΚΤΙΚΗ ΤΙΜΗ ΜΟΝΑΔΟΣ	ΔΑΠΑΝΗ
1	79417000-0	Υπηρεσίες συμμόρφωσης, προσαρμογής και υποστήριξης ως προς τον Νέο Κανονισμό Προστασίας Προσωπικών Δεδομένων της Ε.Ε. με αριθ. 679/2016	1	ΥΠΗΡΕΣΙΑ	15.000,00	15.000,00
					ΑΘΡΟΙΣΜΑ	15.000,00
					ΦΠΑ 24%	3.600,00
					ΓΕΝΙΚΟ ΣΥΝΟΛΟ	18.600,00

Συνολικός ενδεικτικός προϋπολογισμός: **Δεκαοχτώ χιλιάδες εξακόσια ευρώ.**

Θεσσαλονίκη 07/05/2018
Ο συντάξας

ΚΟΝΤΟΛΕΩΝ ΜΗΝΑΣ
ΠΕ Πολιτικός Μηχανικός

ΘΕΩΡΗΘΗΚΕ
Θεσσαλονίκη 07/05/2018
Ο Διευθυντής

ΠΑΠΑΔΟΠΟΥΛΟΣ ΘΕΟΔΩΡΟΣ
ΠΕ Γεωπόνος

2. ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ

ΤΕΧΝΙΚΗ ΠΕΡΙΓΡΑΦΗ ΠΑΡΕΧΟΜΕΝΩΝ ΥΠΗΡΕΣΙΩΝ

Η εταιρεία που θα αναλάβει να διεκπεραιώσει τις υπηρεσίες συμμόρφωσης, προσαρμογής και υποστήριξης ως προς τον Νέο Κανονισμό Προστασίας Προσωπικών Δεδομένων της Ε.Ε. με αριθ. 679/2016 (General Data Protection Regulation – GDPR) θα πρέπει να παράσχει τις ακόλουθες υπηρεσίες:

1. **Αποτύπωση της υφιστάμενης κατάστασης**, ως προς την επεξεργασία δεδομένων που λαμβάνει χώρα στο φορέα, τα είδη των δεδομένων και των υποκειμένων τους, τις ροές των δεδομένων, τις υφιστάμενες πρακτικές, διαδικασίες και πολιτικές του φορέα, τη δυναμική των φυσικών πόρων του φορέα, τη δυναμική των τεχνικών πόρων του φορέα και τα εφαρμοζόμενα μέτρα προστασίας.
2. **Διεξαγωγή αξιολόγησης – αποτίμησης της ασφάλειας του πληροφοριακού συστήματος του οργανισμού** σε όλο το εύρος της δικτυακής υποδομής, που περιλαμβάνει συστήματα, δικτυακό εξοπλισμό, εφαρμογές, δεδομένα και υπηρεσίες. Η αξιολόγηση – αποτίμηση θα αφορά το σύνολο των υποδομών και των υπηρεσιών που παρέχει ο οργανισμός.
3. **Σύνταξη έκθεσης**, η οποία - λαμβάνοντας υπόψη τα αποτελέσματα της αποτύπωσης της κατάστασης - θα προτείνει εξατομικευμένο σχέδιο συμμόρφωσης, όπου θα περιγράφονται τα προτεινόμενα μέτρα προς συμμόρφωση με τον Κανονισμό, οι διορθωτικές κινήσεις που πρέπει να γίνουν, τα σημεία αναπροσαρμογής, οι νέες εφαρμοστέες διαδικασίες, η ενίσχυση με περαιτέρω τεχνικά ή οργανωτικά μέτρα, οι τρόποι υλοποίησης, τα χρονοδιαγράμματα και πιθανές εναλλακτικές.
4. **Υλοποίηση των οργανωτικών μέτρων** που θα προταθούν.

5. **Υπηρεσίες του Υπευθύνου Προστασίας Δεδομένων** (DPO)

Η παροχή των παραπάνω υπηρεσιών, θα πραγματοποιηθεί βασισμένη σε δοκιμασμένες διαδικασίες και τεχνικές, και με τον ακριβή καθορισμό παραδοτέων και χρονοδιαγραμμάτων που θα διασφαλίσουν το άρτιο αποτέλεσμα. Οι μελέτες που θα διενεργηθούν στο πλαίσιο του έργου θα καταγράψουν τις απαιτήσεις ασφάλειας που αρμόζουν στον οργανισμό, θα αναδείξουν τις παρούσες παθογένειες των υφιστάμενων υπηρεσιών - υποδομών και θα προσδιορίσουν τις ευρέως καταξιωμένες βέλτιστες πρακτικές για την πρόληψη, αποτροπή και αντιμετώπιση παραβιάσεων ασφάλειας.

2.1 ΑΝΑΛΥΤΙΚΗ ΠΕΡΙΓΡΑΦΗ ΔΙΑΔΙΚΑΣΙΑΣ ΥΛΟΠΟΙΗΣΗΣ ΥΠΗΡΕΣΙΩΝ

Η διαδικασία υλοποίησης των υπηρεσιών συμμόρφωσης, προσαρμογής και υποστήριξης ως προς τον Νέο Κανονισμό Προστασίας Προσωπικών Δεδομένων με αριθ. 679/2016 επιμερίζεται σε τέσσερα (4) διακριτά βήματα:

Βήμα 1ο: Αποτύπωση υφιστάμενης κατάστασης

ΠΑΡΑ-ΔΟΤΕΟ	ΠΕΡΙΓΡΑΦΗ
	Δέσμευση της Διοίκησης: Στο στάδιο αυτό παρουσιάζονται στη Διοίκηση και τα στελέχη οι απαιτήσεις του Κανονισμού και οι ενέργειες προς τη συμμόρφωση, τα χρονοδιαγράμματα και προσδιορίζονται οι πόροι και οι προσβάσεις που θα παρασχεθούν στην ομάδα έργου. Εν συνεχεία πραγματοποιείται η δέσμευση της διοίκησης με τη δρομολόγηση και την προετοιμασία των δηλώσεων που θα κοινοποιηθούν στο προσωπικό.
Π1	**Δήλωση δέσμευσης της διοίκησης και ενημέρωσης του προσωπικού – εξουσιοδοτήσεις πρόσβασης.**
	Καταγραφή υπευθύνων ανά τμήμα: Προσδιορίζονται οι διευθύνσεις και τα τμήματα του φορέα. Γίνεται καταγραφή των ανά τμήμα και ανά αρχείο δεδομένων υπευθύνων. Η καταγραφή αυτή αποτυπώνεται στο Μητρώο Επεξεργασιών Δεδομένων.
	Καταγραφή διαθέσιμων φυσικών πόρων: Καταγραφή των διαθέσιμων πόρων (ανθρώπων ανά τμήμα), που τίθενται στην διάθεση του Υπεύθυνου Προστασίας Δεδομένων για την περάτωση των εργασιών, προς την επίτευξη συμμόρφωσης και δημιουργία ομάδας εργασίας, με ανάθεση ρόλων και αρμοδιοτήτων,

	κατόπιν συναξιολόγησης με τους υπευθύνους των τμημάτων. Η ομάδα εργασίας πρέπει να είναι αντιπροσωπευτική και να καλύπτει όλα τα τμήματα του φορέα και τις μορφές της επεξεργασίας προσωπικών δεδομένων.
Π2	**Έγγραφη αναφορά με τα μέλη της ομάδας εργασίας και προσδιορισμός αρμοδιοτήτων και υποχρεώσεων.**
	Καταγραφή και χαρτογράφηση των Δεδομένων Προσωπικού Χαρακτήρα, που τηρούνται από τον Οργανισμό/Φορέα, της επεξεργασίας και της κυκλοφορίας τους. Στο στάδιο αυτό, γίνεται καταγραφή, ανά επεξεργασία και ανά αρχείο δεδομένων, του είδους των δεδομένων που τηρούνται, των υποκειμένων, των ροών και περιλαμβάνονται όλες οι απαραίτητες πληροφορίες που απαιτεί ο Κανονισμός στα πλαίσια της υποχρέωσης για τήρηση αρχείου επεξεργασίας, ώστε να αποτυπώνεται πλήρως η κατάσταση επί της διαχείρισης των προσωπικών δεδομένων. Στο πλαίσιο αυτό καθορίζονται τα είδη της επεξεργασίας που πραγματοποιεί ο φορέας, τα δεδομένα που αφορούν κάθε είδος επεξεργασίας, τα υποκείμενα που αφορούν κάθε είδος επεξεργασίας, ο σκοπός και η νομική βάση της επεξεργασίας, οι πηγές προέλευσης των δεδομένων, ο χρόνος τήρησης των δεδομένων, ο τόπος (φυσικός ή ηλεκτρονικός) τήρησης των δεδομένων, τα τεχνικά μέτρα και οι τεχνολογία που χρησιμοποιείται, οι πιθανές διαβιβάσεις ή αναθέσεις σε τρίτους μέρους της επεξεργασίας.
Π3	**Μητρώο Επεξεργασιών Δεδομένων**
	Προσδιορισμός Νομικής Βάσης – Έλεγχος ορθότητας: Προσδιορίζεται η Νομική Βάση στην οποία στηρίζεται η επεξεργασία των δεδομένων και εξετάζεται η ορθότητα, η πληρότητα και η εγκυρότητά της. Επιπλέον, ελέγχεται η σωστή καταγραφή και τεκμηρίωση αυτής, καθώς και ο τρόπος γνωστοποίησής της προς τα υποκείμενα.
Π4	**Πρότυπα κείμενα θεμελίωσης νομιμοποιητικής βάσης – οδηγίες ενσωμάτωσης στην κάθε μορφή επεξεργασίας, καταγραφής, τεκμηρίωσης και γνωστοποίησης**
	Χαρτογράφηση του εγκατεστημένου πληροφοριακού συστήματος. Στο στάδιο αυτό ελέγχονται, αξιολογούνται και καταγράφονται τα πληροφοριακά συστήματα του οργανισμού, οι δικτυακές του υποδομές και κάθε πολιτική ή διαδικασία που άπτεται της λειτουργίας αυτών και του τομέα της πληροφορικής.
Π5	**Σχηματικό διάγραμμα του πληροφοριακού συστήματος του Οργανισμού, με τις επιμέρους λειτουργίες αυτού.**

Βήμα 2ο: Διεξαγωγή αξιολόγησης – Αποτίμησης της ασφάλειας του πληροφοριακού συστήματος του οργανισμού

	Έλεγχος και αξιολόγηση πολιτικών και διαδικασιών. Στο στάδιο αυτό ελέγχονται οι πολιτικές, τα τεχνικά και τα οργανωτικά μέτρα του οργανισμού, ως προς την επάρκειά τους για τον Κανονισμό. Ελέγχεται και αξιολογείται αν υπάρχει πολιτική ασφαλείας που προβλέπει διαδικασίες και δυνατότητα ικανοποίησης των δικαιωμάτων των υποκειμένων, διαδικασίες για την άμεση και εντός των προβλεπόμενων χρονοδιαγραμμάτων ανταπόκριση σε αιτήματα των υποκειμένων, λήψης συγκατάθεσης των υποκειμένων, εκπαίδευση και δημιουργία κουλτούρας στο ανθρώπινο δυναμικό. Ελέγχεται αν υπάρχει επαρκές σχέδιο επιχειρησιακής συνέχειας και ανταπόκρισης σε περιστατικά παραβίασης καθώς και αν προβλέπονται μηχανισμοί ανίχνευσης περιστατικών παραβίασης. Ελέγχεται αν υπάρχουν διαδικασίες, γίνεται αξιολόγηση των διαδικασιών, της τήρησής τους, της εμπέδωσής τους από το προσωπικό σε σχέση με την πολιτική προστασίας προσωπικών δεδομένων.
	Έλεγχος Συμβάσεων. Ελέγχονται οι συμβάσεις του οργανισμού με τρίτους των οποίων προσωπικά δεδομένα επεξεργάζεται (π.χ. προσωπικό, πελάτες) ή οι οποίοι επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του, όσο και με τρίτους στους οποίους διαβιβάζονται δεδομένα προσωπικού χαρακτήρα.
	Καταγραφή Τεκμηρίωσης Γίνεται χαρτογράφηση της υπάρχουσας τεκμηρίωσης, που αφορά στην ασφάλεια των προσωπικών δεδομένων και εξετάζεται η πληρότητα και η επάρκειά της.
	Διεξαγωγή αξιολόγησης – αποτίμησης της ασφάλειας του πληροφοριακού συστήματος **Αποτίμηση Κινδύνου (Risk Assessment)** Θα μελετηθούν οι εκθέσεις σε κίνδυνο (exposures) των συστημάτων του οργανισμού, προσδιορίζοντας τις ευπάθειες (vulnerabilities) και τις απειλές (threats) του με βάση τον υφιστάμενο έλεγχο (control). Τα αποτελέσματα της ανάλυσης επικινδυνότητας (risk analysis review) της υπολογιστικής και επικοινωνιακής υποδομής του οργανισμού θα προσδιορίσουν τις απαιτήσεις ασφαλείας του πληροφοριακού συστήματος, καλύπτοντας τις παρακάτω συνιστώσες: • Φυσική ασφάλεια του συστήματος (physical security): Προστασία ολόκληρου του σχετικού εξοπλισμού από φυσικές καταστροφές. • Ασφάλεια υπολογιστικού συστήματος (computer security): Προστασία των πληροφοριών του συστήματος που διαχειρίζεται το λειτουργικό σύστημα (εφαρμογές, αρχεία δεδομένων, κ.ά.).

Π6	**Μελέτη ανάλυσης επικινδυνότητας και αξιολόγησης κινδύνων των Πληροφοριακών Συστημάτων, που σκοπό έχει να:** • *Αποτιμήσει την αξία των αγαθών (assets) των Ολοκληρωμένων Πληροφοριακών Συστημάτων (ΟΠΣ) και των εγκαταστάσεων* • *Εντοπίσει τις αδυναμίες (vulnerabilities)* • *Περιγράψει τις επιπτώσεις και τις συνέπειες που θα επιφέρει στον Φορέα κάποια ενδεχόμενη απειλή* • *Αποτιμήσει την επικινδυνότητα των ΟΠΣ και των εγκαταστάσεων* • *Εντοπίσει μεθοδικά και να περιγράψει με σαφήνεια όλα τα μέτρα ασφαλείας που πρέπει να ληφθούν για την επαρκή προστασία των ΟΠΣ και των εγκαταστάσεων.*

Βήμα 3ο : Σύνταξη Έκθεσης - Κατάρτιση Σχεδίου Συμμόρφωσης

ΠΑΡΑ-ΔΟΤΕΟ	**ΠΕΡΙΓΡΑΦΗ**
	Προτεινόμενα μέτρα - Κατάρτιση σχεδίου συμμόρφωσης Σε αυτό το στάδιο θα σχεδιαστεί λεπτομερές και ολοκληρωμένο πλάνο συμμόρφωσης του οργανισμού με τις επιταγές του Κανονισμού. Αφού αποτυπωθούν τα αποτελέσματα των προηγούμενων σταδίων, όπως αυτά θα προκύψουν από τους ελέγχους και τις αξιολογήσεις, θα προταθούν πιθανές συμπληρώσεις, αλλαγές ή νέα μέτρα. Οι προτεινόμενες ενέργειες θα καλύπτουν όλο το φάσμα των επεξεργασιών που γίνονται και όλο τον κύκλο ζωής των προσωπικών δεδομένων που αποτελούν αντικείμενο επεξεργασίας. Ο σχεδιασμός θα γίνει από την ομάδα έργου, σύμφωνα με τα ευρήματα του σταδίου της αποτύπωσης και πάντα σύμφωνα με τη φιλοσοφία του οργανισμού και των ανθρώπων του.
Π7	**Αναλυτικό σχέδιο συμμόρφωσης, το οποίο περιλαμβάνει όλα τα Οργανωτικά και Τεχνικά μέτρα, που θα πρέπει να λάβει ο Οργανισμός για να συμμορφωθεί με τις απαιτήσεις του Κανονισμού, όλες τις συμπληρώσεις ή προσαρμογές που πρέπει να κάνει σε σχέση με τα υπάρχοντα μέτρα, όπου χρειάζεται, γίνεται αναμόρφωση των συμβάσεων με τρίτους, με βάση τις απαιτήσεις του Κανονισμού, όπου δεν υπάρχουν συμβάσεις συγγράφονται νέες και δημιουργούνται πρότυπα συμβάσεων για μελλοντική χρήση**.

Βήμα 4ο: Στάδιο Εφαρμογής – Υλοποίηση προτεινόμενων μέτρων – Επίτευξη συμμόρφωσης - Λήψη Οργανωτικών Μέτρων

	Συγγραφή πολιτικών συλλογής, χρήσης και επεξεργασίας

	δεδομένων • Επανεξέταση του τρόπου λήψης και καταγραφής της συγκατάθεσης. • Έλεγχος ή/και εφαρμογή συστημάτων για την διαπίστωση της ηλικίας ή την εξακρίβωση ταυτότητας των εκάστοτε κηδεμόνων, σε περίπτωση ανηλίκων, και τη λήψη σχετικής συγκατάθεσης. • Διασφάλιση τρόπων άσκησης των δικαιωμάτων των υποκειμένων. Σχεδιασμός τρόπου διαχείρισης των αιτημάτων εντός των προβλεπόμενων χρονικών ορίων.
Π8	**Εγχειρίδιο πολιτικών – διαδικασιών συλλογής και επεξεργασίας δεδομένων. Μπορεί να αποτελέσει και στοιχείο της Πολιτικής Ασφαλείας.**
	Συγγραφή πολιτικής ασφάλειας: Η Πολιτική Ασφάλειας (Security Policy) αποτελεί έγγραφο του Υπευθύνου Επεξεργασίας ή του Εκτελούντος την Επεξεργασία, στο οποίο περιγράφονται οι στόχοι της ασφάλειας και οι αντίστοιχες διαδικασίες που πρέπει να ακολουθούνται, ώστε να επιτευχθούν αυτοί οι στόχοι. Καθορίζει τη δέσμευση της Διοίκησης και την προσέγγιση του Οργανισμού, αναφορικά με την ασφάλεια των πληροφοριακών συστημάτων και δικτύων και την προστασία προσωπικών δεδομένων, που τηρεί ο Υπεύθυνος Επεξεργασίας. Κατ' ελάχιστο, περιγράφονται οι βασικές αρχές προστασίας προσωπικών δεδομένων και ασφάλειας που εφαρμόζονται. Ειδικότερα, θέτει τις βασικές αρχές για α) οργανωτικά μέτρα ασφάλειας αναφορικά με τους ρόλους και τις αρμοδιότητες του προσωπικού και των εξωτερικών συνεργατών-εκτελούντων την επεξεργασία, τον καθορισμό και τις αρμοδιότητες του υπευθύνου ασφαλείας, την εκπαίδευση του προσωπικού, τη διαχείριση περιστατικών ασφαλείας, καθώς και την καταστροφή των προσωπικών δεδομένων, β) τα τεχνικά μέτρα ασφάλειας αναφορικά με τη διαχείριση των χρηστών, την αναγνώριση και αυθεντικοποίησή τους, την ασφάλεια των επικοινωνιών, τη λειτουργία των αρχείων καταγραφής του πληροφοριακού συστήματος, την εξαγωγή αντιγράφων ασφαλείας, γ) τα μέτρα φυσικής ασφάλειας. Προσδιορίζει επακριβώς τον ρόλο κάθε εμπλεκομένου εντός του Οργανισμού, τις αρμοδιότητες, τις ευθύνες και τα καθήκοντά του ως προς τις διαδικασίες που αφορούν στην ασφάλεια. Περιγράφει ακόμη κατάλληλη διαδικασία για την αναθεώρησή της.
Π9	**Πλήρες κείμενο Πολιτικής Ασφαλείας**
	Συγγραφή Σχεδίου Ασφάλειας • Το Σχέδιο Ασφάλειας (Security Plan) είναι το έγγραφο, στο οποίο περιγράφονται τα οργανωτικά και τεχνικά μέτρα, καθώς και τα μέτρα φυσικής ασφάλειας, που εφαρμόζονται για την κάλυψη των βασικών αρχών και κανόνων ασφάλειας, που αναφέρονται στην Πολιτική Ασφαλείας. Το Σχέδιο αυτό υπόκειται σε τακτικές επισκοπήσεις και αναθεωρήσεις, δεδομένης της ραγδαίας

	ανάπτυξης τεχνολογικών λύσεων και της εφαρμογής τους στα πληροφοριακά συστήματα και τις τεχνολογικές υποδομές.
Π10	**Πλήρες κείμενο Σχεδίου Ασφαλείας**
	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 περιπτώσεις έκτακτης ανάγκης, όπως φυσικές καταστροφές (πχ σεισμός, πυρκαγιά, πλημμύρα), εξωτερικές επιθέσεις/εισβολές κλπ. Συμπληρώνει ή αποτελεί μέρος του Σχεδίου Ασφαλείας. Ελέγχεται δε, περιοδικά, προκειμένου να διαπιστώνεται η αποτελεσματικότητα των μεθόδων ανάκαμψης.
Π11	**Πλήρες κείμενο Σχεδίου Ανάκαμψης από Καταστροφές**
	Έλεγχος ή/και εφαρμογή Μηχανισμού Εντοπισμού Παραβιάσεων: Έλεγχος υφισταμένου ή εφαρμογή νέου Μηχανισμού Εντοπισμού Παραβιάσεων (Security Breaches)ή και 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.
	Κατάρτιση Σχεδίου Διαχείρισης Συμβάντων: Το Σχέδιο Διαχείρισης Συμβάντων είναι το έγγραφο που αναφέρεται στις διαδικασίες, οι οποίες θα εφαρμοσθούν σε περίπτωση Παραβίασης Ασφαλείας. Προσδιορίζει επακριβώς τον ρόλο κάθε εμπλεκομένου εντός και εκτός του Οργανισμού, τις αρμοδιότητες, τις ευθύνες και τα καθήκοντά του (ως προς τις διαδικασίες) που αφορούν στην αντίδραση του Οργανισμού, σε περίπτωση παραβίασης και απώλειας δεδομένων. Περιγράφει ακόμη την κατάλληλη διαδικασία για την αναθεώρησή της.
Π12	**Πλήρες κείμενο Σχεδίου Διαχείρισης Συμβάντων**
	Διενέργεια Εκτίμησης Αντικτύπου για προστασία των Προσωπικών Δεδομένων (DPIA) Θα προδιαγραφεί και θα εφαρμοστεί μία διαδικασία εκτίμησης αντικτύπου (Data Protection - ή Privacy – Impact Assessment) σε όποιες επεξεργασίες δεδομένων αυτό χρειάζεται και τα αποτελέσματα θα αποτυπωθούν στο Μητρώο Επεξεργασιών.
	Δημιουργία αρχείου καταγραφής ενεργειών (Audit log): Αποτελεί την κορωνίδα της τεκμηρίωσης της συμμόρφωσης ή των βημάτων, που έχουν γίνει προς την κατεύθυνση της συμμόρφωσης, προς τις απαιτήσεις του Κανονισμού. Περιλαμβάνει, κατ' ελάχιστο, την καταγραφή των διαδικασιών συλλογής και επεξεργασίας των δεδομένων,

	το ποσοστό ολοκλήρωσης (με αναλυτικά βήματα) των διαφόρων σχεδίων, το παρουσιολόγιο της κατά τμήματα εκπαίδευσης, το Security log.
Π13	**Συλλογή αρχείων καταγραφής, αυτοματοποιημένων και μη.**
	Δημιουργία κουλτούρας προστασίας προσωπικών δεδομένων στον Οργανισμό - Εκπαίδευση εργαζομένων κατά τμήμα: Εκτεταμένη, κατά τμήματα, εκπαίδευση του προσωπικού πάνω στην Πολιτική Ασφαλείας του Οργανισμού, αλλά και γενικότερα, σε θέματα προσωπικών δεδομένων και της ασφάλειάς τους, με σκοπό να δημιουργηθεί στον οργανισμό κουλτούρα ασφάλειας προσωπικών δεδομένων. Να αναγνωρίζονται αυτά από τους εργαζομένους, ως πολύτιμο περιουσιακό στοιχείο του οργανισμού, το οποίο χρήζει προστασίας.
Π14	**Πρόγραμμα εκπαιδεύσεων κατά τμήμα με αναλυτικό, εκπαιδευτικό πρόγραμμα, υλικό και παρουσιολόγιο. Αποτελεί τμήμα της απαραίτητης για την συμμόρφωση τεκμηρίωσης.**
	Επαναξιολόγηση: Αφού ολοκληρωθεί η λήψη των Οργανωτικών και Τεχνικών Μέτρων, γίνεται επαναξιολόγηση του επιπέδου συμμόρφωσης του Οργανισμού.

2.2 ΥΠΗΡΕΣΙΕΣ ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (DPO)

Εξωτερικός Υπεύθυνος Προστασίας Δεδομένων:

Ένας εκ των μελών της ζητούμενης ομάδας έργου όπως ορίζεται στην παράγραφο **2.5.1** της μελέτης, θα ορισθεί ως Υπεύθυνος Προστασίας Δεδομένων (DPO), υπεύθυνος έναντι της αρχής προστασίας προσωπικών δεδομένων και έναντι των υποκειμένων, σύμφωνα με το άρθρο 37 παρ. 1.α, ενώ θα επιβλέψει παράλληλα όλη την διαδικασία προσαρμογής της Υπηρεσίας κατά GDPR.

- **Η διάρκεια παροχής των υπηρεσιών ορίζεται σε έξι (6) μήνες**.

Κατά την διάρκεια της σύμβασης ο D.P.O., αναλαμβάνει:

1. Να εκπροσωπήσει τον Υπεύθυνο Επεξεργασίας έναντι της εποπτικής αρχής (ΑΠΔΠΧ)
2. Να εκπροσωπήσει τον Υπεύθυνο Επεξεργασίας έναντι των υποκειμένων

3. Να συμβουλεύσει την Διοίκηση σε θέματα προστασίας προσωπικών δεδομένων
4. Να εισηγηθεί απευθείας στην Διοίκηση τις κατάλληλες πολιτικές προστασίας των δεδομένων θεωρώντας τα ως πολύτιμο περιουσιακό στοιχείο του Οργανισμού/Φορέα

Χαρακτηριστικά και καθήκοντα του DPO

Τα καθήκοντα του DPO (ΥΠΔ) σύμφωνα με το άρθρο 39 παρ. 1 ΓΚΠΔ, θα είναι:

1. Ενημερωτικές / συμβουλευτικές υπηρεσίες σχετικά με υποχρεώσεις Υπευθύνου Επεξεργασίας & Εκτελούντος την Επεξεργασία
2. Διασφάλιση της εναρμόνιση της λειτουργίας του Υπευθύνου ή του Εκτελούντος την Επεξεργασία (ανάλογα ποιος τον ορίζει) σε ότι αφορά τις πολιτικές, πρακτικές και μεθοδολογία επεξεργασίας, αποθήκευσης και μεταφοράς Δεδομένων Προσωπικού Χαρακτήρα με το νέο νομοθετικό πλαίσιο
3. Παρακολούθηση εσωτερικής συμμόρφωσης
4. Εκτίμηση αντικτύπου (άρθρο 35 ΓΚΠΔ) – Συμβουλευτικές υπηρεσίες κατόπιν αίτησης & παρακολούθηση υλοποίησης
5. Συνεργασία με εποπτική αρχή (ΑΠΔΠΧ)
6. Σημείο επικοινωνίας με εποπτική αρχή (ΑΠΔΠΧ)

Χαρακτηριστικά θέσης DPO

- Έχει μεγάλο βαθμό ανεξαρτησίας, άμεση πρόσβαση στη Διοίκηση (π.χ. αναφέρεται στον Περιφερειάρχη, τον Πρόεδρο του Περιφερειακού Συμβουλίου κλπ.). Έχει δε, υποχρέωση αναφοράς στην ΑΠΔΠΧ, σε περίπτωση που η διοίκηση δεν υιοθετήσει την πρότασή του ή δεν τηρεί τα μέτρα.
- Δεσμεύεται από εμπιστευτικότητα
- Δεν μπορεί να έχει σύγκρουση συμφερόντων λόγω πρόσθετων αρμοδιοτήτων στο πλαίσιο άλλου έργου ή σύμβασης με την Υπηρεσία.
- 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

- 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 Αντικτύπου κατά το Άρθρο 35 του Κανονισμού και καταρτίζει πρότυπο υπόδειγμα DPIA (Data Privacy Impact Assessment)
- Συντονίζει την διατμηματική συνεργασία με τα τμήματα Ανθρώπινου Δυναμικού, Ασφάλειας Πληροφορικής, Πληροφοριακών Συστημάτων (IT), Νομικής και Κανονιστικής Συμμόρφωσης κλπ. για τη δημιουργία μιας διαρκούς εταιρικής κουλτούρας προστασίας δεδομένων ως πολύτιμου περιουσιακού στοιχείου
- Σχεδιάζει και πραγματοποιεί εσωτερικά εκπαιδευτικά προγράμματα και τηρεί τα απαιτούμενα Αρχεία Ολοκλήρωσης των Εκπαιδεύσεων ανά τμήμα – ομάδα εργαζομένων
- Έχει λόγο για όλα τα θέματα που αφορούν την προστασία προσωπικών δεδομένων στον Οργανισμό/Φορέα και για τον λόγο αυτό πρέπει να έχει πρόσβαση σε όλες τις βάσεις δεδομένων και στα συστήματα του Οργανισμού/Φορέα
- Αναφέρεται στην ανώτατη Διοίκηση του Οργανισμού/Φορέα χωρίς να παρεμβάλλεται ενδιάμεσος αναφοράς
- Είναι λειτουργικά «ανεξάρτητος» 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
- Δεν φέρει προσωπική ευθύνη κατά την άσκηση των καθηκόντων του, αλλά η ευθύνη για παραβίαση της νομοθεσίας σχετικά με τα Δεδομένα Προσωπικού Χαρακτήρα παραμένει στη Διοίκηση
- Διασφαλίζει την επικοινωνία, την υποβολή αιτημάτων και την ικανοποίησή τους ή είναι διαθέσιμος για την υποβολή αιτημάτων και φροντίζει για την άμεση επίλυση.

- Η Υπηρεσία, είναι υποχρεωμένη σύμφωνα με το άρθρο 38, να διασφαλίσει την ενεργή συμμετοχή του DPO και τους απαραίτητους πόρους, ώστε να ανταποκριθεί στις υποχρεώσεις του.

2.3 ΠΙΝΑΚΑΣ ΠΑΡΑΔΟΤΕΩΝ

Κωδικός	ΠΑΡΑΔΟΤΕΟ	Εκτιμώμενος Χρόνος Ολοκλήρωσης
Π1	Δήλωση δέσμευσης της διοίκησης και ενημέρωσης του προσωπικού – εξουσιοδοτήσεις πρόσβασης	Εντός δύο (2) μηνών
Π2	Έγγραφη αναφορά με τα μέλη της ομάδας εργασίας και προσδιορισμός αρμοδιοτήτων και υποχρεώσεων	Εντός δύο (2) μηνών
Π3	Μητρώο Επεξεργασιών Δεδομένων – Αποτελέσματα διενέργειας Εκτίμησης Αντικτύπου στην Ασφάλεια των Δεδομένων (DPIA)	Εντός έξι (6) μηνών
Π4	Πρότυπα κείμενα θεμελίωσης νομιμοποιητικής βάσης – οδηγίες ενσωμάτωσης στην κάθε μορφή επεξεργασίας, καταγραφής, τεκμηρίωσης και γνωστοποίησης	Εντός δύο (2) μηνών
Π5	Σχηματικό διάγραμμα του πληροφοριακού συστήματος του Οργανισμού, με τις επιμέρους λειτουργίες αυτού	Εντός δύο (2) μηνών
Π6	Μελέτη ανάλυσης επικινδυνότητας και αξιολόγησης κινδύνων των Πληροφοριακών Συστημάτων	Εντός έξι (6) μηνών
Π7	Αναλυτικό σχέδιο συμμόρφωσης	Εντός έξι (6) μηνών
Π8	Εγχειρίδιο πολιτικών – διαδικασιών συλλογής και επεξεργασίας δεδομένων.	Εντός έξι (6) μηνών
Π9	Πλήρες κείμενο Πολιτικής Ασφαλείας	Εντός έξι (6) μηνών
Π10	Πλήρες κείμενο Σχεδίου Ασφαλείας	Εντός έξι (6) μηνών
Π11	Πλήρες κείμενο Σχεδίου Ανάκαμψης από Καταστροφές	Εντός έξι (6) μηνών
Π12	Πλήρες κείμενο Σχεδίου Διαχείρισης Συμβάντων	Εντός έξι (6) μηνών
Π13	Συλλογή αρχείων καταγραφής, αυτοματοποιημένων και μη	Εντός έξι (6) μηνών

Π14	Πρόγραμμα εκπαιδεύσεων κατά τμήμα με αναλυτικό, εκπαιδευτικό πρόγραμμα, υλικό και παρουσιολόγιο.	Εντός δύο (2) μηνών

- ***Προσοχή****: Ο ανάδοχος πρέπει να* ***δηλώσει*** *ότι αναλαμβάνει την* ***πλήρη υλοποίηση κατά 100% όλων των παραδοτέων****. Η Υπηρεσία αναλαμβάνει να ορίσει υπεύθυνους ανά διεύθυνση ή τμήμα για να του παρέχουν τις απαραίτητες πληροφορίες. Πέραν αυτών, τα στελέχη της Υπηρεσίας, δεν οφείλουν να αναλάβουν καμία εργασία για την καταγραφή, την αποτύπωση, την επεξεργασία κ.λπ., κανενός από τα παραπάνω παραδοτέα.*

2.4 ΧΡΟΝΟΔΙΑΓΡΑΜΜΑ ΥΛΟΠΟΙΗΣΗΣ

Τα παραδοτέα Π1, Π2, Π4, Π5, Π14, εκτιμάται ότι πρέπει να παραδοθούν εντός δύο (2) μηνών από την υπογραφή της σύμβασης

Τα υπόλοιπα παραδοτέα, θα πρέπει να παραδοθούν εντός έξι (6) μηνών από την υπογραφή της σύμβασης.

2.5 ΕΛΑΧΙΣΤΕΣ ΠΡΟΫΠΟΘΕΣΕΙΣ ΣΥΜΜΕΤΟΧΗΣ

Λόγω των ειδικών δυσκολιών αλλά και της ιδιαίτερης σχέσης των υπό προμήθεια υπηρεσιών με θέματα ποιότητας, ασφάλειας, εχεμύθειας και τεχνολογιών πληροφορικής, απαιτείται ότι:

<u>Ο υποψήφιος ανάδοχος θα πρέπει:</u>

1. Να έχει προβεί ο ίδιος σε όλες τις απαραίτητες ενέργειες συμμόρφωσης κατά GDPR.
2. Να διαθέτει πιστοποίηση ποιότητας ως προς το **πρότυπο ISO 9001** στην εν ισχύ έκδοση του, για την παροχή **συμβουλευτικών υπηρεσιών**.
3. Να έχει **αποδεδειγμένη εμπειρία** στην παροχή **συμβουλευτικών υπηρεσιών** σε φορείς ΟΤΑ ή του Ευρύτερου Δημοσίου **τουλάχιστον για 3 έτη**. Προς απόδειξη να καταθέσει σχετικό κατάλογο με τον πίνακα των έργων και τα αποδεικτικά υλοποίησης: Συμβάσεις / πρωτόκολλα παραλαβής ή καλής εκτέλεσης.
4. Να έχει αποδεδειγμένη εμπειρία σε **τουλάχιστον πέντε (5) έργα συμμόρφωσης κατά GDPR** (υλοποιημένα ή σε εξέλιξη).
   Προς απόδειξη της εμπειρίας θα πρέπει να προσκομίσει υπεύθυνη δήλωση στην οποία θα περιλαμβάνεται ένας Πίνακας με τα εξής πεδία συμπληρωμένα για κάθε σχετικό έργο: επωνυμία φορέα υλοποίησης, τίτλος έργου,

περιεχόμενο έργου, χρονική διάρκεια (από- έως), υπεύθυνος φορέα και στοιχεία επικοινωνίας υπευθύνου. Ο υποψήφιος ανάδοχος είναι υποχρεωμένος για την κάθε εγγραφή του πίνακα της δήλωσης να υποβάλλει και τα σχετικά τεκμήρια (Σύμβαση ή βεβαίωση καλής εκτέλεσης ή πρωτόκολλο παραλαβής / καλής εκτέλεσης).

5. Να έχει **αποδεδειγμένη εμπειρία** σε θέματα **εκπαίδευσης**, στο **σχεδιασμό** και στην **οργάνωση εκπαιδευτικών προγραμμάτων ή εκδηλώσεων** και να διαθέτει σχετική **πιστοποίηση για την παροχή υπηρεσιών εκπαίδευσης**.

2.5.1 ΟΜΑΔΑ ΕΡΓΟΥ

Ο Ανάδοχος θα πρέπει να διαθέτει το απαιτούμενο προσωπικό για την στελέχωση της ζητούμενης ομάδας έργου η οποία να αποτελείται από:

1. Ένα έμπειρο **στέλεχος-νομικό** με αποδεδειγμένη γνώση στην **προστασία προσωπικών δεδομένων**, που θα διαθέτει **πιστοποιητικό DPO** (με σφραγίδα του ΕΣΥΔ).
2. Ένα έμπειρο **στέλεχος πληροφορικής** με αποδεδειγμένη γνώση στην **προστασία προσωπικών δεδομένων**, που θα διαθέτει πιστοποιητικό DPO (με σφραγίδα του ΕΣΥΔ).
3. Ένα έμπειρο **στέλεχος πληροφορικής** με αποδεδειγμένη γνώση στην **ασφάλεια των πληροφοριών** και των **πληροφοριακών συστημάτων**, **ειδικό Δοκιμών Παρείσδυσης** (Penetration Tester). Προς απόδειξη να διαθέτει και να καταθέσει αναγνωρισμένο πιστοποιητικό (OSCP).
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.

Της παραπάνω ομάδας θα πρέπει να ηγείται έμπειρο στέλεχος με αποδεδειγμένη πτυχιακή ή μεταπτυχιακή ή και διδακτορική γνώση στο αντικείμενο της ασφάλειας πληροφοριών, με εμπειρία στην ανάπτυξη πολιτικών ασφαλείας.

- Ως Υπεύθυνος Ομάδας Έργου, μπορεί να ορισθεί και ένα στέλεχος εκ των μελών της, αρκεί να διαθέτει θα διαθέτει τα απαιτούμενα προσόντα.

Για όλα τα μέλη της Ομάδας Έργου, θα πρέπει να **κατατεθούν βιογραφικά σημειώματα** συμπληρωμένα σύμφωνα με τους πρότυπους πίνακες που δίνονται στο Παράρτημα.

Στον πίνακα της ομάδας έργου που θα κατατεθεί, να αναφέρονται τα στελέχη αποκλειστικής απασχόλησης στον προσφέροντα. ***Τουλάχιστον το 60% της Ομάδας έργου, υποχρεωτικά, θα πρέπει να αποτελείται από στελέχη του προσφέροντος, με αποκλειστική σχέση απασχόλησης***.

Θεσσαλονίκη 07/05/2018
Ο συντάξας

ΚΟΝΤΟΛΕΩΝ ΜΗΝΑΣ
ΠΕ Πολιτικός Μηχανικός

ΘΕΩΡΗΘΗΚΕ
Θεσσαλονίκη 07/05/2018
Ο Διευθυντής

ΠΑΠΑΔΟΠΟΥΛΟΣ ΘΕΟΔΩΡΟΣ
ΠΕ Γεωπόνος

3. ΠΑΡΑΡΤΗΜΑ

3.1 ΠΡΟΤΥΠΟ ΒΙΟΓΡΑΦΙΚΟ ΣΗΜΕΙΩΜΑ

ΠΡΟΣΩΠΙΚΑ ΣΤΟΙΧΕΙΑ			
Επώνυμο		Όνομα	
Πατρώνυμο		Μητρώνυμο	
Ημερομηνία Γέννησης		Τόπος Γέννησης	

Τηλέφωνο		E-mail	
Fax:			
Διεύθυνση Κατοικίας:			

ΕΚΠΑΙΔΕΥΣΗ

Όνομα Ιδρύματος	**Τίτλος Πτυχίου**	**Ειδικότητα**	**Ημ/νία Απόκτησης Πτυχίου**
			../../....
			../../....
			../../....
			../../....

ΚΑΤΗΓΟΡΙΑ ΣΤΕΛΕΧΟΥΣ

(στο προτεινόμενο, από τον υποψήφιο Ανάδοχο, σχήμα διοίκησης Έργου)	

ΕΠΑΓΓΕΛΜΑΤΙΚΗ ΕΜΠΕΙΡΙΑ

Έργο	**Εργοδότης**	**Θέση και Καθήκοντα στο Έργο**	**Απασχόληση στο έργο**	
			Περίοδος (από-έως)	**α/μ**
			../../.... - ../../....	
			../../.... - ../../....	
			../../.... - ../../....	
			../../.... - ../../....	

ΠΡΟΣΘΕΤΑ ΣΤΟΙΧΕΙΑ