ΠΡΟΣΚΛΗΣΗ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΕΠΙΜΕΛΗΤΗΡΙΟ ΛΑΣΙΘΙΟΥ

Αρ πρωτ: 322β/21-2-2020
ΠΡΟΣ
Επιχειρήσεις ενδιαφέροντος

Πληροφορίες Γκερεδάκη Ειρήνη

ΠΡΟΣΚΛΗΣΗ ΕΚΔΗΛΩΣΗΣ ΕΝΔΙΑΦΕΡΟΝΤΟΣ
Παροχή υπηρεσιών συμμόρφωσης, προσαρμογής και υποστήριξης ως προς τον Νέο Κανονισμό Προστασίας Προσωπικών Δεδομένων με αριθμ. 679/2016 (General Data Protection Regulation – GDPR)

Το Επιμελητήριο Λασιθίου διατηρεί και επεξεργάζεται πληθώρα δεδομένων προσωπικού χαρακτήρα, καθώς και πληροφορίες δικές του αλλά και των συναλλασσόμενων με αυτόν (πολιτών, προμηθευτών κ.α.) και υποχρεούται βάσει του Κανονισμού 679/2016, να συμμορφωθεί με τις νέες νομοθετικές επιταγές, να ορίσει υπεύθυνο προστασίας προσωπικών δεδομένων, ενώ η οργανωτική του δομή και το πλήθος των τμημάτων απαιτεί ελεύθερη και ασφαλή ροή των δεδομένων και τυποποίηση των σχετικών διαδικασιών. Μετά τη σχετική απόφαση της Δ.Ε. 49/21-2-2020, στο πλαίσιο της υποχρέωσης εφαρμογής του νέου Ευρωπαϊκού Κανονισμού για την Προστασία των Προσωπικών Δεδομένων 2016/679(GDPR) που έχει τεθεί σε σε ισχύ την 25/5/2018, σας προσκαλεί σε εκδήλωση ενδιαφέροντος για την παροχή υπηρεσιών συμμόρφωσης προς τον ανωτέρω κανονισμό.

Εκτιμώμενη αξία ΣΥΝΟΛΙΚΗ ΑΞΙΑ: 5.000,00€ συμπεριλαμβανομένου ΦΠΑ (24%).

Ημερομηνία υποβολής προσφορών έως 20/3/20.

Ειδικότερα η πρόσκληση αφορά την εύρεση εξωτερικού συνεργάτη ο οποίος θα αναλάβει :

Αναλυτικότερα οι υπηρεσίες που απαιτούνται είναι οι κάτωθι:

1) Αξιολόγηση όλων των τομέων δραστηριότητας του φορέα και όλων των τμημάτων και διευθύνσεών του, ως προς την ετοιμότητά τους έναντι του GDPR.
2) Εντοπισμό των κενών και των ελλείψεων που πρέπει να καλυφθούν.
3) Πρόταση και σχεδιασμό των αναγκαίων τεχνικών και οργανωτικών μέτρων.
4) Υλοποίηση των προτεινόμενων οργανωτικών μέτρων.
5) Υπηρεσίες Υπεύθυνου Προστασίας Δεδομένων (DPO)

Συνοπτικά :

- Την προετοιμασία του φακέλου συμμόρφωσης του Επιμελητηρίου (data mapping, gap analysis,καταγραφή δράσεων που απαιτούνται για συμμόρφωση)
- Τον έλεγχο υλοποίησης των σχετικών δράσεων και την τελική συμμόρφωση
- Την κατάρτιση προσωπικού – στελεχών
- Την ανάληψη καθηκόντων Υπεύθυνου Επεξεργασίας Δεδομένων (DPO)

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.

Δείτε παρακάτω παράρτημα των τεχνικών προδιαγραφών της πρόσκλησης μας.

ΤΕΧΝΙΚΗ ΠΕΡΙΓΡΑΦΗ

Με την παρούσα πρόσκληση προβλέπεται:

Η παροχή υπηρεσιών συμμόρφωσης, προσαρμογής και υποστήριξης ως προς τον Νέο Κανονισμό Προστασίας Προσωπικών Δεδομένων με αριθμ. 679/2016 (General Data Protection Regulation – GDPR)

Αναλυτικά, το έργο θα περιλαμβάνει:

- Αποτύπωση της υπάρχουσας 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.
- 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.
- 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.
- Υλοποίηση των οργανωτικών μέτρων που θα προταθούν.
- Υπηρεσίες του Υπευθύνου Προστασίας Δεδομένων (DPO) μέχρι την ολοκλήρωση του έργου.

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.

Διαδικασία υλοποίησης υπηρεσιών

1.1 Στάδιο προετοιμασίας – Αποτύπωση υφιστάμενης κατάστασης – Προτεινόμενα μέτρα - Κατάρτιση σχεδίου συμμόρφωσης

1.1.1 Δέσμευση της Διοίκησης:

Στο στάδιο αυτό παρουσιάζονται στη Διοίκηση και τα στελέχη οι απαιτήσεις του Κανονισμού και οι ενέργειες προς τη συμμόρφωση, ώστε τα κέντρα λήψης των αποφάσεων να έχουν πλήρη γνώση και επίγνωση, να προσδιοριστεί η αναγκαιότητα του έργου και να παρασχεθεί πλήρης ενημέρωση για το προσφερόμενο έργο, τα στάδια αυτού, τα χρονοδιαγράμματα και να προσδιοριστούν 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 του φορέα.

Παραδοτέο Π1:

- **Δήλωση δέσμευσης της διοίκησης και ενημέρωσης του προσωπικού – εξουσιοδοτήσεις πρόσβασης.**

1.1.2 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.

1.1.3 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.

Παραδοτέο Π2:

- **Έγγραφη αναφορά με τα μέλη της ομάδας εργασίας και προσδιορισμός αρμοδιοτήτων και υποχρεώσεων.**

1.1.4 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.

Παραδοτέο Π3:

- **Μητρώο Επεξεργασιών Δεδομένων, το οποίο περιλαμβάνει, κατ' ελάχιστο, για κάθε αρχείο και είδος επεξεργασίας τα ακόλουθα:**
    i. Τις κατηγορίες των δεδομένων που επεξεργάζονται
    ii. Αν τα δεδομένα είναι σε ηλεκτρονική, έντυπη ή μεικτή μορφή
    iii. Ονοματεπώνυμο υπευθύνου επεξεργασίας
    iv. Προσδιορισμό του σκοπού
    v. Διεύθυνση εγκατάστασης αρχείου
    vi. Τεχνολογία που χρησιμοποιείται
    vii. Στοιχεία Εκτελούντος την Επεξεργασία
    viii. Χρονικό διάστημα που απαιτείται για την επεξεργασία
    ix. Εάν γίνεται επεξεργασία μέσω διαδικτύου
    x. Νομική Βάση της Επεξεργασίας
    xi. Εάν το Υποκείμενο έχει ενημερωθεί για τα δικαιώματά του.
    xii. Πηγή Δεδομένων
    xiii. Αποδέκτες Δεδομένων
    xiv. Περίοδο τήρησης
    xv. Ζεύξη Δεδομένων
    xvi. Εάν έχει διενεργηθεί Εκτίμηση Αντικτύπου Κινδύνου (DPIA) και αν ναι τα αποτελέσματά της

1.1.5 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.

Παραδοτέο Π4:

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

1.1.6 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.

Παραδοτέο Π5:

- **Σχηματικό διάγραμμα του πληροφοριακού συστήματος του Οργανισμού, με τις επιμέρους λειτουργίες αυτού.**

1.1.7 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.

1.1.8 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.

1.1.9 Καταγραφή Τεκμηρίωσης

Γίνεται χαρτογράφηση της υπάρχουσας τεκμηρίωσης, που αφορά στην ασφάλεια των προσωπικών δεδομένων και εξετάζεται η πληρότητα και η επάρκειά της.

1.1.10 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.).
- Ασφάλεια δικτύων επικοινωνιών (network security): Προστασία των πληροφοριών κατά τη μετάδοσή τους μέσω τοπικών, τηλεφωνικών ή άλλων δικτύων (π.χ. Internet).

Παραδοτέο 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**

1.2 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.

Παραδοτέο 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.

1.3 **Στάδιο εφαρμογής – Υλοποίηση προτεινόμενων μέτρων – Επίτευξη συμμόρφωσης**

Λήψη Οργανωτικών Μέτρων

1.3.1 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.**

Παραδοτέο Π8:

- **Εγχειρίδιο πολιτικών – διαδικασιών συλλογής και επεξεργασίας δεδομένων. Μπορεί να αποτελέσει και στοιχείο της Πολιτικής Ασφαλείας.**

1.3.2 Συγγραφή πολιτικής ασφαλείας:

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. Ενδεικτικά μπορεί να περιλαμβάνει διαδικασίες για τη συλλογή και αποθήκευση των δεδομένων, για τη διαγραφή ή καταστροφή τους, για την τήρηση αρχείου, για την ενσωμάτωση της προστασίας των δεδομένων, σε προϊόντα και υπηρεσίες.

Παραδοτέο Π9:

- **Πλήρες κείμενο Πολιτικής Ασφαλείας**

1.3.3 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.

Παραδοτέο Π10:

- **Πλήρες κείμενο Σχεδίου Ασφαλείας**

1.3.4 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 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.

Παραδοτέο Π11:

- **Πλήρες κείμενο Σχεδίου Ανάκαμψης από Καταστροφές**

1.3.5 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.

1.3.6 Μηχανισμοί Ασφάλειας

Καθορισμός των απαιτούμενων μέτρων που θα ικανοποιήσουν τις απαιτήσεις ασφαλείας του συστήματος. Τα προτεινόμενα μέτρα θα καλύπτουν τις παρακάτω βασικές κατηγορίες:

- Οργάνωση και διαχείριση της ασφάλειας του πληροφοριακού συστήματος
- Ασφάλεια ανάπτυξης και συντήρησης του πληροφοριακού συστήματος
- Φυσική ασφάλεια
- Ασφάλεια της υπολογιστικής και τηλεπικοινωνιακής υποδομής

Η αποτελεσματικότητα των μέτρων προστασίας ή αντιμέτρων εξαρτάται από:

- Την επίγνωση του μεγέθους του προβλήματος ασφάλειας από τους εμπλεκόμενους χρήστες.
- Το σχεδιασμό περιοδικών επισκοπήσεων και αναθεωρήσεων των μέτρων. Ο προσδιορισμός διαδικασιών τακτικής επιθεώρησης και ανασκόπησης των μέτρων ασφαλείας αποτελεί μια από τις σημαντικότερες συνιστώσες επιτυχίας.
- Την αλληλοεπικάλυψη των μέτρων. Ένας συνδυασμός μέτρων ελαχιστοποιεί τις απειλές και αυξάνει την αξιοπιστία του συστήματος προστασίας.

Παραδοτέο Π12:

Μελέτη επικαιροποίησης των υφιστάμενων μηχανισμών και επέκτασή τους

1.3.7 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.

Το σχέδιο διαχείρισης συμβάντων θα περιλαμβάνει:

- Προσδιορισμό πιθανών κινδύνων και κριτηρίων για ενεργοποίηση του σχεδίου,
- Προσδιορισμό των σημαντικών λειτουργιών και των αντίστοιχων συστημάτων (critical functions and systems) του οργανισμού,
- Καθορισμό της στρατηγικής προστασίας (protection strategy),
- Ιεράρχηση των δραστηριοτήτων και καθορισμός προτεραιοτήτων για την ενεργοποίησή τους στο εναλλακτικό σύστημα,
- Πλάνο Υλοποίησης με αρμοδιότητες προσωπικού και χρονοπρογραμματισμό ενεργειών αποκατάστασης.

Παραδοτέο Π13:

- **Πλήρες κείμενο Σχεδίου Διαχείρισης Συμβάντων**

1.3.8 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.

1.3.9 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.

Παραδοτέο Π14:

- **Συλλογή αρχείων καταγραφής ενεργειών, αυτοματοποιημένων και μη.**

1.3.10 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.

Παραδοτέο Π15:

- **Πρόγραμμα εκπαιδεύσεων κατά τμήμα με αναλυτικό, εκπαιδευτικό πρόγραμμα, υλικό και παρουσιολόγιο. Αποτελεί τμήμα της απαραίτητης για την συμμόρφωση τεκμηρίωσης.**

1.3.11 Επαναξιολόγηση:

Αφού ολοκληρωθεί η λήψη των Οργανωτικών και Τεχνικών Μέτρων, γίνεται επαναξιολόγηση του επιπέδου συμμόρφωσης του Οργανισμού.

Υπηρεσίες Υπευθύνου Προστασίας Δεδομένων (DPO)

Εξωτερικός Υπεύθυνος Προστασίας Δεδομένων:
Ορίζεται άτομο του παρόχου, ως Υπεύθυνος Προστασίας Δεδομένων του Οργανισμού, ο οποίος και εκτελεί όλα τα χρέη του DPO, τόσο με επιτόπου επισκέψεις, όσο και εξ αποστάσεως, μέχρι και την ημερομηνία ολοκλήρωσης της υλοποίησης των προτεινόμενων οργανωτικών μέτρων σύμφωνα με τα παραπάνω. Είναι δε προσβάσιμος από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, τον Οργανισμό αλλά και τα Υποκείμενα των Δεδομένων, 24/365.

Ελάχιστες Προϋποθέσεις Συμμετοχής

Ο υποψήφιος ανάδοχος θα πρέπει να διαθέτει τα παρακάτω χαρακτηριστικά:

- Εμπειρία στην υλοποίηση ή παροχή συμβουλευτικών υπηρεσιών οργάνωσης, ιδιαίτερα, στον τομέα της ασφάλειας πληροφοριών, της επιχειρησιακής συνέχειας και της βελτιστοποίησης επιχειρησιακών διαδικασιών.
- Να διαθέτει αποδεδειγμένη γνώση των νομικών και τεχνικών θεμάτων των προσωπικών δεδομένων και σχετική προϋπηρεσία περιλαμβανομένης τυχόν έργων συμμόρφωσης έναντι του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) (5 συναφή έργα).
- Η ομάδα έργου να περιλαμβάνει:
    - Εξειδικευμένους νομικούς στην προστασία δεδομένων
    - Ειδικούς στην ασφάλεια πληροφοριών
    - Ειδικούς στις τεχνολογικές υποδομές πληροφορικής
    - Συμβούλους οργάνωσης
    - Πιστοποιημένους Υπευθύνους Προστασίας Δεδομένων (DPO)

  οι οποίοι να έχουν εμπλακεί σε έργα GDPR.
- Θα πρέπει να έχει ολοκληρώσει ή να βρίσκεται σε στάδιο υλοποίησης σε 5 (πέντε) τουλάχιστον έργα με το ρόλο του συμβούλου σε έργα παρόμοια με τη συγκεκριμένη τεχνική προδιαγραφή, με στόχο την παροχή υπηρεσιών αναγνώρισης υφιστάμενης κατάστασης, τον προσδιορισμό σχετικών ενεργειών και την εκπόνηση σχετικού προγραμματισμού κάλυψης των απαιτήσεων του Κανονισμού GDPR και δη ως ανάδοχος ή μέλος αναδόχου κοινοπραξίας.

  Προς απόδειξη της εμπειρίας θα πρέπει να προσκομίσει υπεύθυνη δήλωση του Ν. 1599/86 συμπληρωμένη από τον ανάδοχο 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 υπεύθυνης δήλωσης να υποβάλλει σχετική δήλωση του φορέα υλοποίησης στην οποία να ενημερώνει για την ομαλή και εντός του συμβατικού χρονοδιαγράμματος εξέλιξη του έργου. Η δήλωση αυτή βρίσκεται στο Παράρτημα Α της παρούσας. Κάθε έργο του Πίνακα της υπεύθυνης δήλωσης Ν. 1599/86 το οποίο δε θα συνοδεύεται από την αντίστοιχη δήλωση του φορέα υλοποίησης, δε θα προσμετράται στα προαναφερόμενα κριτήρια εμπειρίας.

Εναλλακτικά, για έργα σε φορείς δημοσίου, πρωτόκολλα παραλαβής από την αρμόδια επιτροπή.

- Να διαθέτει ISO 27001 ή άλλο ανάλογο πιστοποιητικό (που να αφορά σε ασφάλεια πληροφοριών).

Πίνακας Παραδοτέων

Κωδικός	Παραδοτέο	Εκτιμώμενος Χρόνος Ολοκλήρωσης (σε μήνες)
Π1	Δήλωση δέσμευσης της διοίκησης και ενημέρωσης του προσωπικού – εξουσιοδοτήσεις πρόσβασης	2
Π2	Έγγραφη αναφορά με τα μέλη της ομάδας εργασίας και προσδιορισμός αρμοδιοτήτων και υποχρεώσεων	2
Π3	Μητρώο Επεξεργασιών Δεδομένων	
Π4	Πρότυπα κείμενα θεμελίωσης νομιμοποιητικής βάσης – οδηγίες ενσωμάτωσης στην κάθε μορφή επεξεργασίας, καταγραφής, τεκμηρίωσης και γνωστοποίησης	6
Π5	Σχηματικό διάγραμμα του πληροφοριακού συστήματος του Οργανισμού, με τις επιμέρους λειτουργίες αυτού	6
Π6	Μελέτη ανάλυσης επικινδυνότητας και αξιολόγησης κινδύνων των Πληροφοριακών Συστημάτων	6
Π7	Αναλυτικό σχέδιο συμμόρφωσης	6
Π8	Εγχειρίδιο πολιτικών – διαδικασιών συλλογής και επεξεργασίας δεδομένων.	6
Π9	Πλήρες κείμενο Πολιτικής Ασφαλείας	6
Π10	Πλήρες κείμενο Σχεδίου Ασφαλείας	6
Π11	Πλήρες κείμενο Σχεδίου Ανάκαμψης από Καταστροφές	6
Π12	Μελέτη επικαιροποίησης των υφιστάμενων μηχανισμών και επέκτασή τους	6
Π13	Πλήρες κείμενο Σχεδίου Διαχείρισης Συμβάντων	6
Π14	Συλλογή αρχείων καταγραφής, αυτοματοποιημένων και μη	6
Π15	Πρόγραμμα εκπαιδεύσεων κατά τμήμα με αναλυτικό, εκπαιδευτικό πρόγραμμα, υλικό και παρουσιολόγιο.	6

Προς απόδειξη της μη συνδρομής των λόγων αποκλεισμού από διαδικασίες σύναψης δημοσίων συμβάσεων των παρ.1 και 2 του άρθρου 73 του Ν.4412/2016,

παρακαλούμε, μαζί με την προσφορά σας, να μας αποστείλετε τα παρακάτω δικαιολογητικά :α. Απόσπασμα ποινικού μητρώου. Η υποχρέωση αφορά ιδίως: αα) στις περιπτώσεις εταιρειών περιορισμένης ευθύνης (Ε.Π.Ε.) και προσωπικών εταιρειών (Ο.Ε. και Ε.Ε.), τους διαχειριστές, ββ) στις περιπτώσεις ανωνύμων εταιρειών (Α.Ε.), τον Διευθύνοντα Σύμβουλο, καθώς και όλα τα μέλη του Διοικητικού Συμβουλίου.

β. Φορολογική ενημερότητα

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

[Τα ανωτέρω δικαιολογητικά δεν απαιτούνται σε δημόσιες συμβάσεις με εκτιμώμενη αξία ίση ή κατώτερη των δύο χιλιάδων πεντακοσίων (2.500) ευρώ χωρίς Φ.Π.Α.. (άρθρο 73 παρ.6 Ν.4412/2016, όπως προστέθηκε με την παρ.9 του άρθρου 107 του Ν.4497/2017, άρθρο 80 παρ.11 Ν.4412/2016, όπως προστέθηκε με την παρ.15 του άρθρου 107 του Ν.4497/2017)]

Ο Πρόεδρος

ΘΩΜΑΣ ΧΑΡΙΤΑΚΗΣ