ΚΥΠΡΙΑΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΓΡΑΦΕΙΟ ΕΠΙΤΡΟΠΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Οδηγός Συμμόρφωσης με τον Γενικό Κανονισμό για την Προστασία Δεδομένων, (ΕΕ) 2016/679 (ΓΚΠΔ)

Οι ερωτήσεις που περιλαμβάνονται στον Οδηγό δεν αποτελούν εξαντλητικό κατάλογο. Επίσης, συγκεκριμένες ενότητες και/ή ερωτήσεις, ενδεχομένως, να μην πρέπει να εφαρμόζονται σε όλες τις περιπτώσεις. Σε κάθε περίπτωση, οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία θα πρέπει να χρησιμοποιήσουν τον Οδηγό, λαμβάνοντας υπόψιν τις κατηγορίες των δεδομένων που επεξεργάζονται, τις επεξεργασίες που εκτελούν, καθώς και τον τομέα δραστηριότητάς τους.

1. ΥΠΕΥΘΥΝΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
Έχει οριστεί Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ) δυνάμει των Άρθρων 37-39 του ΓΚΠΔ;
Έχουν αναρτηθεί τα στοιχεία του ΥΠΔ στην ιστοσελίδα;
Έγινε επίσημη ανακοίνωση του ορισμού του ΥΠΔ σε όλο το προσωπικό;
Ο ΥΠΔ συμμετέχει σε όλα τα ζητήματα που σχετίζονται με την προστασία δεδομένων;
Ο ΥΠΔ εκτελεί και άλλα καθήκοντα ή έχει άλλες υποχρεώσεις που ενδεχομένως να δημιουργούν σύγκρουση συμφερόντων;
Έχει επιβεβαιωθεί ότι ο ΥΠΔ δεν κατέχει θέση διευθυντή ή μέλους της διοίκησης της ελεγχόμενης;
2. ΑΡΧΕΙΟ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ - ΕΚΤΙΜΗΣΗ ΑΝΤΙΚΤΥΠΟΥ - ΠΡΟΗΓΟΥΜΕΝΗ ΔΙΑΒΟΥΛΕΥΣΗ
Έχει καταρτιστεί αρχείο καταγραφής δραστηριοτήτων δυνάμει του Άρθρου 30 του ΓΚΠΔ;
Έχουν διενεργηθεί εκτιμήσεις αντικτύπου σχετικά με την προστασία δεδομένων σε είδη επεξεργασίας που απαιτούνται από τον ΓΚΠΔ;
Έχει πραγματοποιηθεί προηγούμενη διαβούλευση με το Γραφείο της Επιτρόπου για τις επεξεργασίες που απαιτείται δυνάμει του Άρθρου 36 του ΓΚΠΔ;
3. ΠΟΛΙΤΙΚΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
Έχει καταρτιστεί πολιτική προστασίας προσωπικών δεδομένων (privacy policy);
Είναι διαθέσιμη τουλάχιστο και στην ελληνική γλώσσα;
Οι πληροφορίες που περιλαμβάνονται είναι επικαιροποιημένες;
Περιλαμβάνονται πληροφορίες σχετικά με τη δυνατότητα και τον τρόπο άσκησης των δικαιωμάτων των υποκειμένων των δεδομένων;

4. ΕΝΗΜΕΡΩΣΗ ΥΠΟΚΕΙΜΕΝΩΝ ΤΩΝ ΔΕΔΟΜΕΝΩΝ
Πραγματοποιείται ενημέρωση των υποκειμένων των δεδομένων (πελατών, εργαζομένων κ.λπ.) με βάση τα Άρθρα 12,13 και 14 του ΓΚΠΔ;
Έχουν επικαιροποιηθεί τα σχετικά έντυπα για να συνάδουν με τον ΓΚΠΔ;
Έχουν επικαιροποιηθεί όλα τα συμβόλαια (με εργαζομένους, συνεργάτες ή/και πελάτες (όπου ισχύει)) για να συνάδουν με τον ΓΚΠΔ;

5. ΝΟΜΙΚΗ ΒΑΣΗ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ
Υπάρχει νομική βάση για κάθε επεξεργασία που διενεργείται δυνάμει του Άρθρου 6 του ΓΚΠΔ;
Υπάρχει νομική βάση για κάθε επεξεργασία ευαίσθητων δεδομένων που διενεργείται δυνάμει του Άρθρου 9 του ΓΚΠΔ;
Στις περιπτώσεις όπου λαμβάνεται συγκατάθεση των υποκειμένων των δεδομένων, μπορεί να αποδειχθεί ανά πάσα στιγμή;
Παρέχεται η δυνατότητα ανάκλησης της συγκατάθεσης των υποκειμένων των δεδομένων;

6. ΑΣΚΗΣΗ ΚΑΙ ΙΚΑΝΟΠΟΙΗΣΗ ΤΩΝ ΔΙΚΑΙΩΜΑΤΩΝ ΤΩΝ ΥΠΟΚΕΙΜΕΝΩΝ ΤΩΝ ΔΕΔΟΜΕΝΩΝ
Υπάρχουν εν ισχύ καταγραμμένοι και δημοσιευμένοι μηχανισμοί και διαδικασίες άσκησης και ικανοποίησης των δικαιωμάτων των υποκειμένων των δεδομένων;
Η ενημέρωση των υποκειμένων των δεδομένων για τα δικαιώματα τους διενεργείται σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση;
Παρέχονται στα υποκείμενα των δεδομένων εύκολοι τρόποι άσκησης των δικαιωμάτων τους;
Καταγράφονται όλα τα αιτήματα τα οποία υποβάλλονται ή/και ικανοποιούνται;

7. ΠΑΡΑΒΙΑΣΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ
Υπάρχει κατάλογος παραβιάσεων προσωπικών δεδομένων (data breaches);
Έχει καταρτιστεί διαδικασία διαχείρισης περιστατικών παραβίασης προσωπικών δεδομένων;

8. ΠΟΛΙΤΙΚΗ ΑΠΕΥΘΕΙΑΣ ΕΜΠΟΡΙΚΗΣ ΠΡΟΩΘΗΣΗΣ
Σε περίπτωση που ο οργανισμός προβαίνει σε απευθείας εμπορική προώθηση (direct marketing), έχει καταρτιστεί σχετική πολιτική;
Η δυνατότητα διακοπής λήψης των προωθητικών μηνυμάτων παρέχεται ατελώς και με εύκολο τρόπο;
Σε περίπτωση που υπάρχει πρόγραμμα ανταμοιβής/επιβράβευσης πελατών, συλλέγονται μόνο τα απολύτως απαραίτητα δεδομένα που απαιτούνται για συμμετοχή στο πρόγραμμα;

9. ΣΥΜΒΑΣΕΙΣ ΑΝΑΘΕΣΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ
Στις περιπτώσεις όπου πραγματοποιείται ανάθεση εργασίας σε τρίτους, η οποία να περιλαμβάνει επεξεργασία προσωπικών δεδομένων, έχουν καταρτιστεί ή αναθεωρηθεί οι συμβάσεις ανάθεσης επεξεργασίας σύμφωνα με το άρθρο 28 του ΓΚΠΔ ;
Οι συμβάσεις ανάθεσης επεξεργασίας περιλαμβάνουν όλα τα στοιχεία που προνοούνται στο Άρθρο 28(3) του ΓΚΠΔ;

10. ΕΙΔΙΚΕΣ ΕΠΕΞΕΡΓΑΣΙΕΣ
Υπάρχει νομική βάση στις περιπτώσεις όπου τηρούνται αντίγραφα δελτίων ταυτότητας ή διαβατηρίων;
Τα αντίγραφα διατηρούνται μόνο για όσο διάστημα χρειάζεται;
Υπάρχει νομική βάση στις περιπτώσεις όπου τα αντίγραφα κοινοποιούνται σε αποδέκτες;
Στις περιπτώσεις ελέγχου πρόσβασης, προσέλευσης/αποχώρησης του προσωπικού, ο έλεγχος διενεργείται με τον λιγότερο παρεμβατικό τρόπο;
Στις περιπτώσεις όπου γίνεται χρήση/επεξεργασία βιομετρικών δεδομένων, διενεργήθηκε εκτίμηση αντικτύπου και προηγούμενη διαβούλευση με την Επίτροπο (όπου απαιτείται);
Στις περιπτώσεις όπου πραγματοποιείται καταγραφή κλήσεων, ενημερώνεται το υποκείμενο των δεδομένων πριν την καταγραφή;
Σε περίπτωση εναντίωσης του υποκειμένου των δεδομένων στην καταγραφή της κλήσης, παρέχεται εναλλακτικός τρόπος επικοινωνίας/παροχής υπηρεσίας;
Όταν δεν εφαρμόζεται η παράγραφος 2 του Άρθρου 22 του ΓΚΠΔ, δίνεται στα υποκείμενα των δεδομένων η δυνατότητα εναντίωσης σε ενδεχόμενη κατάρτιση προφίλ;
Στις περιπτώσεις όπου υπάρχει εγκατεστημένο κλειστό κύκλωμα βίντεο-παρακολούθησης (CCTV), διενεργήθηκε εκτίμηση αντικτύπου;
Λήφθηκαν υπόψιν οι σχετικές οδηγίες της Επιτρόπου και οι Κατευθυντήριες Γραμμές του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων;

11. ΔΙΑΒΙΒΑΣΕΙΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΕ ΤΡΙΤΕΣ ΧΩΡΕΣ Ή ΔΙΕΘΝΕΙΣ ΟΡΓΑΝΙΣΜΟΥΣ
Στις περιπτώσεις όπου διαβιβάζονται προσωπικά δεδομένα σε χώρες εκτός Ε.Ε. και Ε.Ο.Χ. ή σε διεθνείς οργανισμούς, τηρούνται οι πρόνοιες του Κεφαλαίου V του ΓΚΠΔ και λαμβάνονται συμπληρωματικά μέτρα εάν απαιτείται;
Υπάρχουν σε ισχύ διαδικασίες για εντοπισμό περιπτώσεων διαβιβάσεων προσωπικών δεδομένων σε τρίτες χώρες;

12. ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ
Υπάρχει καταγραμμένη Πολιτική Ασφάλειας Πληροφοριών σε ενιαίο κείμενο που είναι κατάλληλη, παρέχει ένα πλαίσιο για τον καθορισμό στόχων και αποδεικνύει τη δέσμευση για ικανοποίηση των απαιτήσεων και για συνεχή βελτίωση;
Η Πολιτική αυτή κοινοποιείται στους εργαζομένους και τα σχετικά ενδιαφερόμενα μέρη;
Υπάρχει πρόνοια για επικαιροποίηση της Πολιτικής;
Η Πολιτική Ασφάλειας Πληροφοριών περιλαμβάνει τις πιο κάτω γενικές πληροφορίες:
Βασικές αρχές ασφαλείας που πρέπει να τηρούνται, όπως η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των δεδομένων.
Αγαθά (αρχεία σε οποιαδήποτε μορφή ή εξοπλισμός) τα οποία πρέπει να προστατεύονται
Σκοπός και πεδίο εφαρμογής της Πολιτικής ως προς τη διαφύλαξη των αγαθών και των βασικών αρχών ασφαλείας.
Οργανωτικό πλαίσιο ρόλων, αρμοδιοτήτων και καθηκόντων που αφορούν στην ασφάλεια.
Ενημέρωση του προσωπικού σχετικά με την υποχρέωση για συμμόρφωση καθώς και για ενδεχόμενες συνέπειες σε περιπτώσεις μη συμμόρφωσης ή παραβίασης της.
Διαδικασία εσωτερικών ή εξωτερικών ελέγχων για την επισκόπηση της ορθής εφαρμογής της Πολιτικής και την αποτίμηση της αποτελεσματικότητας των μέτρων ασφαλείας.
Είδος και χρονική διάρκεια της επεξεργασίας, στις περιπτώσεις όπου η επεξεργασία προσωπικών δεδομένων γίνεται από εκτελούντες.

13. ΟΡΓΑΝΩΤΙΚΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ
Υπάρχουν καταγραμμένα στην Πολιτική ή σε άλλο επίσημο έγγραφο τα **οργανωτικά μέτρα** που εφαρμόζονται ή/και πρόκειται να εφαρμοστούν για την κάλυψη των βασικών αρχών και κανόνων ασφαλείας που αναφέρονται στην Πολιτική Ασφαλείας, καθώς και οι απαραίτητες ενέργειες για την υλοποίησή τους;
Περιγράφονται και υλοποιούνται τα πιο κάτω **οργανωτικά μέτρα**:
Ορισμός Υπεύθυνου Ασφαλείας (Information Security Officer).
Καταμερισμός/ανάθεση ρόλων και εξουσιοδοτήσεων στη βάση της Αρχής ανάγκης γνώσης.
Περιοδική επανεξέταση και αναθεώρηση των εξουσιοδοτήσεων και δικαιωμάτων πρόσβασης για όλα τα στάδια της εργασιακής πορείας του προσωπικού.
Δέσμευση εμπιστευτικότητας προσωπικού.
Δήλωση εμπιστευτικότητας.
Κώδικας δεοντολογίας προσωπικού.
Επαγγελματικό απόρρητο.
Διαδικασία προσανατολισμένη στην ασφάλεια κατά την αποχώρηση προσωπικού.
Καταγραφή πληροφοριακών αγαθών (υποδομών, συστημάτων, λογισμικού κ.λπ.).
Διαδικασίες για την ορθή οργάνωση/αρχειοθέτηση/ταξινόμηση του φυσικού αρχείου (δηλ. του αρχείου με τους φυσικούς φακέλους).
Διαβάθμιση πληροφοριών βάσει του είδους και της κρισιμότητάς τους.
Διαδικασίες για τη διακίνηση πληροφοριακών αγαθών (π.χ. μεταφορά υπολογιστών ή USB stick εντός ή εκτός των εγκαταστάσεων).
Διαδικασίες και πολιτική καταστροφής δεδομένων.

Διαδικασίες διαχείρισης περιστατικών παραβίασης προσωπικών δεδομένων.
Διαδικασίες για τη διενέργεια προγραμματισμένων ελέγχων (εσωτερικών ή εξωτερικών).
Πληροφορίες για εκπαίδευση του προσωπικού σε θέματα ασφάλειας/εμπιστευτικότητας/προστασίας προσωπικών δεδομένων.
Οργανωτικά μέτρα που αφορούν στους εκτελούντες την επεξεργασία:
Διαδικασία για καταγραφή και τήρηση αρχείου με όλους τους εκτελούντες την επεξεργασία.
Διαδικασία για τη διενέργεια σύμβασης ανάθεσης δυνάμει του Άρθρου 28 του ΓΚΠΔ.
Μέτρα ασφαλείας που αφορούν στους εκτελούντες την επεξεργασία.
Έλεγχος τήρησης όρων πολιτικής ασφαλείας που αφορούν στους εκτελούντες την επεξεργασία.
Έλεγχος τήρησης των μέτρων ασφάλειας που προβλέπονται στη σύμβαση ανάθεσης.
Τόπος επεξεργασίας των δεδομένων από τον εκτελούντα την επεξεργασία.
Δέσμευση εμπιστευτικότητας προσωπικού.
Κώδικας δεοντολογίας προσωπικού.
Επαγγελματικό απόρρητο.
14. ΤΕΧΝΙΚΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ
Υπάρχουν καταγραμμένα στην Πολιτική ή σε άλλο επίσημο έγγραφο τα **τεχνικά μέτρα** που εφαρμόζονται ή/και πρόκειται να εφαρμοστούν για την κάλυψη των βασικών αρχών και κανόνων ασφαλείας που αναφέρονται στην Πολιτική Ασφαλείας, καθώς και οι απαραίτητες ενέργειες για την υλοποίησή τους;
Περιγράφονται και υλοποιούνται τα πιο κάτω **τεχνικά μέτρα**:
Χρήση λογισμικού για διαχείριση λογαριασμών χρηστών (π.χ. Active Directory).
Μηχανισμοί ελέγχου πρόσβασης στα συστήματα από εξουσιοδοτημένους ή μη χρήστες.
Ενιαία πολιτική κωδικών πρόσβασης με προκαθορισμένα ελάχιστα χαρακτηριστικά.
Πολιτική για τη λήψη και διαχείριση των αντιγράφων ασφαλείας.
Τήρηση αντιγράφων ασφαλείας σε διαφορετικό χώρο/φυσική τοποθεσία από τα πρωτογενή δεδομένα.
Χρήση antivirus σε όλους τους υπολογιστές και εξυπηρετητές.
Περιορισμός των ενεργειών απλών χρηστών στους υπολογιστές οι οποίες επηρεάζουν τη συνολική τους διαμόρφωση (π.χ. εγκατάσταση προγραμμάτων).
Ελεγχόμενη χρήση αποσπώμενων μέσων αποθήκευσης (π.χ. USB, CD/DVD).
Μη ύπαρξη ανοιχτών θυρών (ports) στους υπολογιστές, ώστε να μη μπορούν οι χρήστες να συνδέουν αποσπώμενα μέσα αποθήκευσης.
Ελεγχόμενη πρόσβαση στο διαδίκτυο από το εσωτερικό δίκτυο.
Διαδικασίες για τήρηση, έλεγχο και διαγραφή αρχείων καταγραφής ενεργειών χρηστών και συμβάντων ασφαλείας (log files).
Διαδικασίες για τον έλεγχο και τη διαχείριση δικτυακών συσκευών και πρωτοκόλλων δικτύου.
Διαδικασίες για τη διαχείριση απομακρυσμένης πρόσβασης σε συστήματα.
Διαδικασίες για την εγκατάσταση και χρήση περιμετρικής ασφάλειας (π.χ. firewalls, IDS).
Διαδικασίες για την προστασία αρχείων λειτουργικών συστημάτων.
Πολιτική διαχείρισης αλλαγών που πραγματοποιούνται στα πληροφοριακά συστήματα.
Διαδικασία για μη επιτυχημένες απόπειρες πρόσβασης.
Διαδικασία για ασφάλεια αδρανοποιημένου υπολογιστή.

15. ΜΕΤΡΑ ΦΥΣΙΚΗΣ ΑΣΦΑΛΕΙΑΣ
Υπάρχουν καταγραμμένα στην Πολιτική ή σε άλλο επίσημο έγγραφο τα **μέτρα φυσικής ασφάλειας** που εφαρμόζονται ή/και πρόκειται να εφαρμοστούν για την κάλυψη των βασικών αρχών και κανόνων ασφαλείας που αναφέρονται στην Πολιτική Ασφαλείας, καθώς και οι απαραίτητες ενέργειες για την υλοποίησή τους;
Περιγράφονται και υλοποιούνται τα πιο κάτω **μέτρα φυσικής ασφάλειας**:
Έλεγχος φυσικής πρόσβασης στους κρίσιμους χώρους όπου βρίσκεται ο φυσικός εξοπλισμός (συμπεριλαμβανομένης τηλεπικοινωνιακής και δικτυακής καλωδίωσης) που υποστηρίζει τα πληροφοριακά συστήματα και την επεξεργασία προσωπικών δεδομένων.
Διατήρηση επικαιροποιημένου καταλόγου με τα δικαιώματα φυσικής πρόσβασης του προσωπικού.
Φρουροί ασφαλείας στις εγκαταστάσεις.
Σύστημα συναγερμού/πυρόσβεσης σε όλες τις εγκαταστάσεις.
Μέτρα για προστασία από φυσικές καταστροφές.
Μέτρα προστασίας φορητών μέσων αποθήκευσης (φύλαξη - καταγραφή).
Τήρηση πολιτικής διακίνησης φορητών μέσων αποθήκευσης.
Οι φάκελοι που περιέχουν προσωπικά δεδομένα (φυσικό αρχείο) είναι τοποθετημένοι σε φωριαμούς που κλειδώνουν.
Καταγραφή της μεταφοράς των φυσικών φακέλων σε άλλα γραφεία ή οργανωτικές μονάδες.
Τήρηση πολιτικής καθαρού γραφείου (Clean desk policy).
16. ΣΧΕΔΙΟ ΑΝΑΚΑΜΨΗΣ ΑΠΟ ΚΑΤΑΣΤΡΟΦΕΣ
Υπάρχει Σχέδιο Ανάκαμψης από Καταστροφές (Disaster Recovery Plan);
Γίνονται περιοδικοί έλεγχοι του Σχεδίου προκειμένου να διαπιστώνεται η αποτελεσματικότητα των μεθόδων ανάκαμψης;
Έχουν προσδιοριστεί οι σημαντικές λειτουργίες και τα αντίστοιχα συστήματα;
Έχουν προσδιοριστεί οι πιθανοί κίνδυνοι για τις πιο πάνω λειτουργίες και συστήματα;
Έχει προσδιοριστεί η στρατηγική προστασίας από τους πιθανούς κινδύνους (protection strategy) και η προτεραιότητα με την οποία θα τεθούν σε εφαρμογή οι δραστηριότητες στο εναλλακτικό σύστημα;
Έχει συσταθεί κατάσταση με τα μέλη του προσωπικού που θα κληθούν στην περίπτωση καταστροφής, καθώς και τα τηλέφωνα επικοινωνίας των προμηθευτών υλικού και λογισμικού, των σημαντικών συνεργατών ή πελατών, των ατόμων που βρίσκονται σε διαφορετικές εγκαταστάσεις που θα χρησιμοποιηθούν για τη συνέχιση της λειτουργίας;
Το Σχέδιο περιέχει διαδικασίες για τον υπολογισμό της ζημιάς από την καταστροφή που συντελέστηκε;
Το Σχέδιο περιέχει ένα ρεαλιστικό χρονοπρογραμματισμό με σαφή ανάθεση καθηκόντων για την αποκατάσταση;
Γίνεται χρήση ειδικών συσκευών φιλτραρίσματος, όπως τα φίλτρα αέρος, που περιορίζουν τις ζημιές από τον καπνό και από άλλα βλαβερά αέρια, και τα φίλτρα θορύβου, που ελαττώνουν το άκουσμα εξωτερικών θορύβων;

Γίνεται χρήση συσκευών ή μεθόδων που ελέγχουν τη θερμοκρασία, την πίεση, την υγρασία και άλλους περιβαλλοντικούς παράγοντες;
Γίνεται χρήση ειδικού λογισμικού ή εξοπλισμού για την αντιμετώπιση εισβολών (IDS/IPS);
Γίνεται χρήση ειδικών γεννητριών για την αντιμετώπιση των διακοπών στην παροχή ηλεκτρικού ρεύματος;
Υπάρχουν εναλλακτικές εγκαταστάσεις που θα χρησιμοποιηθούν σε περίπτωση καταστροφής (cold/hot site);
Πραγματοποιείται εκπαίδευση, εξοικείωση και εξάσκηση του ανθρώπινου δυναμικού σε διαδικασίες έκτακτης ανάγκης;
Προβλέπεται ρεαλιστικό πλάνο αναφορικά με τον χρονικό προγραμματισμό για την ανάκαμψη και την αποκατάσταση της λειτουργίας;