**Τεκμηρίωση**

**των τεχνικών και οργανωτικών μέτρων
σύμφωνα με το άρθρο 25 ΓΚΠΔ**

*Αυτό το υπόδειγμα υποστηρίζει την τεκμηρίωση των κατάλληλων τεχνικών και οργανωτικών μέτρων σύμφωνα με το άρθρο 25 του ΓΚΠΔ, τα οποία διασφαλίζουν την προστασία των δεδομένων προσωπικού χαρακτήρα. Η τεκμηρίωση αυτή πραγματοποιείται για σύνολο του οργανισμού ή το σύνολο της εταιρείας.*

**1. Εμπιστευτικότητα (άρθρο 32 παράγραφος 1 στοιχείο β ΓΚΠΔ)**

**Έλεγχος πρόσβασης**

*Μέτρα που αποτρέπουν την πρόσβαση σε μη εξουσιοδοτημένα πρόσωπα σε συστήματα επεξεργασίας δεδομένων ,με τα οποία γίνεται επεξεργασία ή χρήση δεδομένων προσωπικού χαρακτήρα.*

*Ερωτήσεις ελέγχου*

* *Πώς διασφαλίζεται η πρόσβαση στο κτίριο ή στις εγκαταστάσεις;*
* *Εάν υπάρχει: Πώς διασφαλίζεται η πρόσβαση σε ευαίσθητες περιοχές (π.χ. αίθουσες διακομιστών ή θέσεις εργασίας του τμήματος ανθρώπινου δυναμικού);*
* *Υπάρχει σύστημα συναγερμού ή/και υπηρεσία ασφαλείας;*
* *Υπάρχουν κανόνες για τους επισκέπτες;*
* *Πώς διασφαλίζονται οι προσβάσεις από μη εξουσιοδοτημένη πρόσβαση; Υπάρχει σύστημα ελέγχου ταυτότητας πρόσβασης (π.χ. σύστημα κλειδιών, σύστημα καρτών με τσιπ κ.λπ.);*

**Έλεγχος πρόσβασης**

*Μέτρα που εμποδίζουν την χρήση συστημάτων επεξεργασίας δεδομένων από μη εξουσιοδοτημένα άτομα.*

*Ερωτήσεις ελέγχου*

* *Πώς αποτρέπεται η μη εξουσιοδοτημένη χρήση του συστήματος;*
* *Υπάρχουν κατευθυντήριες γραμμές για τον κωδικό πρόσβασης;*
* *Πώς πιστοποιούνται οι χρήστες στα πληροφοριακά συστήματα;*
* *Υπάρχει απαίτηση για έλεγχο ταυτότητας πολλαπλών παραγόντων;*
* *Είναι κρυπτογραφημένοι οι φορείς δεδομένων;*
* *Χρησιμοποιείται λογισμικό προστασίας από ιούς;*
* *Χρησιμοποιούνται τείχη προστασίας;*

**Έλεγχος πρόσβασης**

*Μέτρα που διασφαλίζουν ότι οι χρήστες ενός συστήματος επεξεργασίας δεδομένων μπορούν να έχουν πρόσβαση μόνο στα δεδομένα για τα οποία έχουν εξουσιοδοτηθεί. Μέτρα που διασφαλίζουν ότι τα δεδομένα προσωπικού χαρακτήρα δεν μπορούν να διαβαστούν, να αντιγραφούν, να τροποποιηθούν ή να αφαιρεθούν χωρίς εξουσιοδότηση κατά τη διάρκεια της επεξεργασίας ή της χρήσης.*

*Ερωτήσεις ελέγχου*

* *Υπάρχουν έννοιες για εξουσιοδοτήσεις πρόσβασης για μεμονωμένα συστήματα (π.χ. ERP, CRM κ.λπ.);*
* *Ποιοι κανονισμοί υπάρχουν για τη διαχείριση των προφίλ εξουσιοδότησης;*
* *Υπάρχουν διαδικασίες που ρυθμίζουν τον τρόπο με τον οποίο ζητούνται, εγκρίνονται, χορηγούνται και ανακαλούνται οι εξουσιοδοτήσεις πρόσβασης;*
* *Καταγράφονται οι προσβάσεις στο σύστημα; Εάν ναι, πώς;*
* *Πώς ρυθμίζεται η πρόσβαση στο εσωτερικό δίκτυο;*

**Έλεγχος διαχωρισμού**

*Μέτρα που διασφαλίζουν ότι τα δεδομένα που συλλέγονται για διαφορετικούς σκοπούς μπορούν να τύχουν χωριστής επεξεργασίας.*

*Ερωτήσεις ελέγχου*

* *Πώς διασφαλίζεται ότι τα δεδομένα που συλλέγονται για διαφορετικούς σκοπούς υποβάλλονται σε χωριστή επεξεργασία;*
* *Υπάρχουν κανόνες για το διαχωρισμό των ιδιωτικών και των επαγγελματικών δεδομένων, π.χ. σε ιδιωτικές συσκευές;*
* *Υπάρχουν δεδομένα από διαφορετικούς πελάτες ή παραγγελιοδότες; Υπάρχουν κανόνες για το διαχωρισμό των αντίστοιχων δεδομένων;*
* *IΣτο πλαίσιο της ανάπτυξης λογισμικού: Διαχωρίζονται τα περιβάλλοντα δοκιμών και παραγωγής;*

**Ψευδωνυμοποίηση (άρθρο 32 παράγραφος 1 στοιχείο α ΓΚΠΔ- άρθρο 25 παράγραφος 1 ΓΚΠΔ)**

*Ψευδωνυμοποίηση σημαίνει ότι ονόματα ή άλλα χαρακτηριστικά που μπορούν να οδηγήσουν στην ταυτοποίηση ενός προσώπου αντικαθίστανται από ψευδώνυμο. Αυτό είναι συχνά ένας κωδικός που αποτελείται από συνδυασμό γραμμάτων ή αριθμών.*

*Ερωτήσεις ελέγχου*

* *Υπάρχουν κανονισμοί για την ψευδωνυμοποίηση, ώστε να χρησιμοποιείται ένα αναγνωριστικό αντί του πλήρους ονόματος (π.χ. για τους συμμετέχοντες/ουσες σε μελέτες);*

**2. Ακεραιότητα (άρθρο 32 παράγραφος 1 στοιχείο β ΓΚΠΔ)**

**Έλεγχος μεταφοράς**

*Μέτρα που διασφαλίζουν ότι τα δεδομένα προσωπικού χαρακτήρα δεν διαβάζονται, αντιγράφονται, τροποποιούνται ή αφαιρούνται χωρίς άδεια κατά την ηλεκτρονική διαβίβαση ή μεταφορά. Επιπλέον, μέτρα που μπορούν να χρησιμοποιηθούν για να προσδιοριστεί σε ποιους φορείς προορίζεται μια διαβίβαση δεδομένων προσωπικού χαρακτήρα.*

*Ερωτήσεις ελέγχου*

* *Υπάρχουν κανονισμοί για τον χειρισμό των φορέων δεδομένων και την ανταλλαγή δεδομένων (π.χ. χρήση εξωτερικών δίσκων, στικ USB, αποθήκευση στο νέφος);*
* *Υπάρχουν κανονισμοί για την αποτροπή μη εξουσιοδοτημένης ανάγνωσης, αντιγραφής, τροποποίησης ή αφαίρεσης κατά την ηλεκτρονική διαβίβαση ή μεταφορά;*
* *Πραγματοποιείται καταγραφή;*
* *Υπάρχουν κανονισμοί για την καταστροφή των φορέων δεδομένων σύμφωνα με την προστασία των δεδομένων;*

**Έλεγχος εισαγωγής δεδομένων**

*Μέτρα που μπορούν να χρησιμοποιηθούν για να διαπιστωθεί εάν, πότε και από ποιον έχουν εισαχθεί, τροποποιηθεί ή αφαιρεθεί προσωπικά δεδομένα από συστήματα επεξεργασίας δεδομένων.*

*Ερωτήσεις ελέγχου*

* *Μπορούν να παρακολουθούνται οι καταχωρίσεις, οι αλλαγές και οι διαγραφές δεδομένων με βάση μεμονωμένα ονόματα χρηστών (καταγραφή);*

**3. διαθεσιμότητα και ανθεκτικότητα (άρθρο 32 παράγραφος 1 στοιχείο β ΓΚΠΔ)**

*Μέτρα που διασφαλίζουν ότι τα δεδομένα προσωπικού χαρακτήρα προστατεύονται από τυχαία καταστροφή ή απώλεια και ότι η πρόσβαση στα δεδομένα αποκαθίσταται το συντομότερο δυνατό μετά από διακοπή. (Αποκατάσταση σύμφωνα με το άρθρο 32 παρ. 1 στοιχ. γ ΓΚΠΔ)*

*Ερωτήσεις ελέγχου*

* *Υπάρχει έννοια δημιουργίας αντιγράφων ασφαλείας; Δημιουργείται τακτικά αντίγραφο ασφαλείας των δεδομένων της εταιρείας;*
* *Υπάρχει αδιάλειπτη παροχή ρεύματος (UPS);*
* *Χρησιμοποιούνται συστήματα ασφαλείας, όπως προστασία από ιούς και τείχη προστασίας;*
* *Υπάρχει σχέδιο έκτακτης ανάγκης που ρυθμίζει τη συμπεριφορά σε περίπτωση συμβάντος προστασίας δεδομένων;*
* *Τα δεδομένα της εταιρείας αποθηκεύονται σε ασφαλή τοποθεσία και προστατεύονται από μη εξουσιοδοτημένη πρόσβαση;*
* *Είναι εγγυημένη η δυνατότητα αποκατάστασης των δεδομένων της εταιρείας σε περίπτωση αμφιβολιών;*

**4. Διαδικασίες για την τακτική δοκιμή, εκτίμηση και αξιολόγηση (άρθρο 32 παράγραφος 1 στοιχείο δ) ΓΚΠΔ- άρθρο 25 παράγραφος 1 ΓΚΠΔ)**

**Διαχείριση προστασίας δεδομένων**

*Μέτρα που διασφαλίζουν ότι οι απαιτήσεις του ΓΚΠΔ έχουν εφαρμοστεί με επαληθεύσιμο τρόπο.*

*Ερωτήσεις ελέγχου*

* *Πώς εφαρμόζεται η προστασία των δεδομένων στην εταιρεία;*
* Ποιες διαδικασίες και μέτρα εφαρμόζονται; (Παράδειγμα: τακτική καθοδήγηση των εργαζομένων στην προστασία των δεδομένων, δοκιμή και επικαιροποίηση της τεκμηρίωσης για την προστασία των δεδομένων κ.λπ.

**Διαχείριση αντιμετώπισης περιστατικών (Incident Response)**

*Μέτρα που διασφαλίζουν ότι μετά από ένα συμβάν, τα άτομα ή οι οργανισμοί λαμβάνουν πληροφορίες σχετικά με το συμβάν, σε περίπτωση που τα δεδομένα τους έχουν επηρεαστεί.*

*Ερωτήσεις ελέγχου*

* *Υπάρχει οργανωτική και τεχνική διαδικασία σε περίπτωση συμβάντος ασφάλειας ή διαταραχής στον τομέα των πληροφοριακών συστημάτων;*

**Προεπιλεγμένες ρυθμίσεις φιλικές προς την προστασία των δεδομένων (άρθρο 25 παράγραφος 2 ΓΚΠΔ)**

*Μέτρα που διασφαλίζουν ότι οι προεπιλεγμένες ρυθμίσεις στα συστήματα λαμβάνουν ήδη υπόψη την προστασία των δεδομένων(«προστασία δεδομένων και της ιδιωτικής ζωής ήδη από τον σχεδιασμό»).*

*Ερωτήσεις ελέγχου*

* *Ποιες προεπιλεγμένες ρυθμίσεις χρησιμοποιούνται για να διασφαλιστεί ότι υποβάλλονται σε επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που απαιτούνται για τον αντίστοιχο σκοπό επεξεργασίας;*

**Έλεγχος παραγγελιών**

*Μέτρα που διασφαλίζουν ότι τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία για λογαριασμό του πελάτη υποβάλλονται σε επεξεργασία μόνο σύμφωνα με τις οδηγίες του πελάτη.*

*Ερωτήσεις ελέγχου*

* *Κατά περίπτωση: Υπάρχει επίσημο σύστημα διαχείρισης παραγγελιών;*
* *Έχουν δοκιμαστεί και αξιολογηθεί οι υφιστάμενοι πάροχοι υπηρεσιών όσον αφορά τη νομοθεσία περί προστασίας δεδομένων;*
* *Έχουν συναφθεί αντίστοιχες συμφωνίες επεξεργασίας δεδομένων με τους εκτελούντες την επεξεργασία δεδομένων;*
* *Παρέχουν οι εκτελούντες επεξεργασίας δεδομένων επαρκείς πληροφορίες σχετικά με τα δικά τους τεχνικά και οργανωτικά μέτρα στις συμβάσεις τους;*