Baker Tilly South East Europe

Σχέδιο Συμμόρφωσης με τον Γενικό Κανονισμό Προστασίας Δεδομένων του Χαροκοπείου Πανεπιστημίου

bakertilly

Περιεχόμενα

Συντομογραφίες

- **ΓΚΠΔ** – Γενικός Κανονισμός Προστασίας Δεδομένων
- **ΥΠΔ** – Υπεύθυνος Προστασίας Δεδομένων
- **ΟΠΔ** – Ομάδα Προστασίας Δεδομένων
- **ΠΣ** – Πρακτικά Συναντήσεων
- **ΕΟΜΑ / ΕΤΜΑ** – Ελάχιστα Οργανωτικά Μέτρα Ασφαλείας – Ελάχιστα Τεχνικά Μέτρα Ασφαλείας
- **ΣΕΣ** – Σχέδιο Επιχειρησιακής Συνέχειας
- **ΤΣΡ** – Τυπικές Συμβατικές Ρήτρες
- **ΣΠΔ** – Συμφωνία Προστασίας Δεδομένων
- **ΠΑΔ** – Πρόληψη Απώλειας Δεδομένων
- **ΔΠΧ –** Δεδομένα Προσωπικού Χαρακτήρα
- **ΕΑΠΔ –** Εκτίμηση Αντικτύπου Προστασίας Δεδομένων

1. Εισαγωγή

Η Baker Tilly στο πλαίσιο της σύμβασης δεσμεύτηκε να παρέχει συμβουλευτικές υπηρεσίες για την εφαρμογή του Γενικού Κανονισμού για την Προστασία των Προσωπικών στο Χαροκόπειο Πανεπιστήμιο , καθώς και την παροχή υπηρεσιών υποστήριξης Υπευθύνου/ης Προστασίας Δεδομένων (Data Protection Officer - DPO) κατά τη διάρκεια του έργου

Σε αυτό το σημείο θα θέλαμε να σας ευχαριστήσουμε για την συμβολή και τη συνεργασία σας καθ' όλη τη διάρκεια αυτού του έργου.

2. Πεδίο Εφαρμογής

Σκοπός του παρόντος είναι η δημιουργία ενός αναλυτικού και σαφές σχεδίου συμμόρφωσης του Χαροκοπείου στις απαιτήσεις του ΓΚΠΔ (GDPR) περιλαμβάνοντας νέα μέτρα ασφάλειας ή την αναβάθμιση των υπαρχόντων, καθώς επίσης και τον προγραμματισμό μέτρων έκτακτης ανάγκης που πρέπει να εφαρμοστούν σε περίπτωση παραβίασης δεδομένων. Επίσης προβλέπει συγκεκριμένες εργασίες ώστε να βελτιωθεί κατά το δυνατόν συντομότερα το επίπεδο συμμόρφωσης του Πανεπιστημίου.

3. Προσέγγιση

Για την σύνταξη του Σχεδίου Συμμορφώσεως λάβαμε υπ οψιν τα αποτελέσματα:

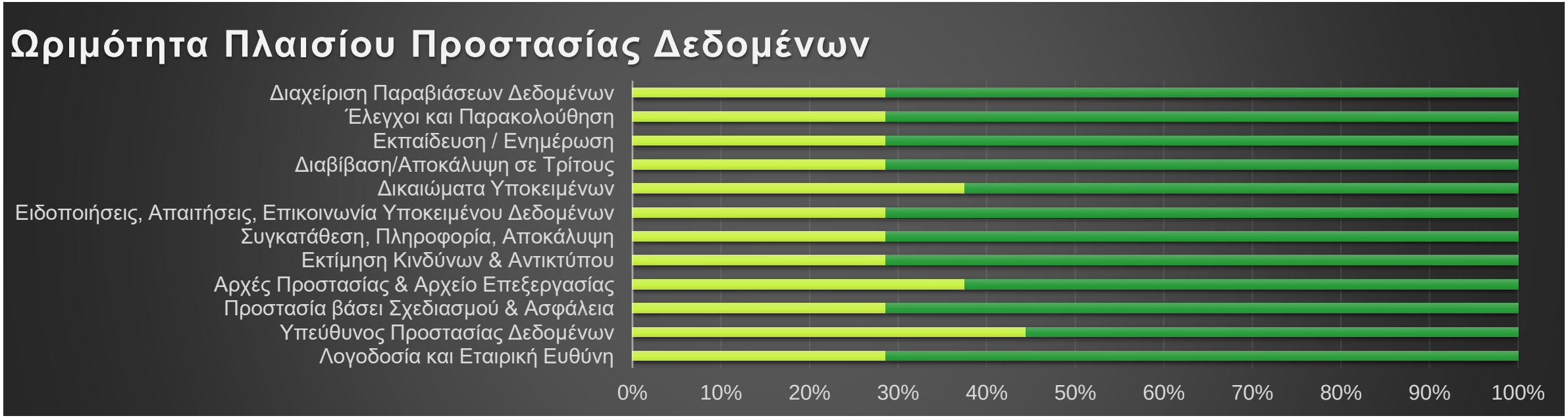
- της μελέτης ανάλυσης αποκλίσεων
- του ελέγχου IT audit
- της εκτίμησης αντικτύπου και της ανάλυσης επικινδυνότητας ασφάλειας πληροφοριών

4. Επίπεδο Ωριμότητας Πλαισίου Προστασίας Δεδομένων

Η αξιολόγηση του επιπέδου ωριμότητας του Πανεπιστημίου χρησιμοποιείται για να αποκαλύψει την τρέχουσα κατάσταση σχεδιασμού, εφαρμογής και συμμόρφωσης με τον GDPR έναντι της επιθυμητής κατάστασης και πώς να γνωρίζει το Πανεπιστήμιο πότε έχει φτάσει στο σημείο των κατάλληλων και αναλογικών ελέγχων με βάση τον κίνδυνο.

α/α	Κατηγορίες Προστασίας ΔΠΧ	Βαθμός Ετοιμότητας	Βέλτιστο Επίπεδο
1	Λογοδοσία και Εταιρική Ευθύνη	2	5
2	Υπεύθυνος Προστασίας Δεδομένων	4	5
3	Προστασία βάσει Σχεδιασμού & Ασφάλειας	2	5
4	Αρχές Προστασίας & Αρχείο Επεξεργασίας	3	5
5	Εκτίμηση Κινδύνων & Αντικτύπου	2	5
6	Συγκατάθεση, Πληροφορία, Αποκάλυψη	2	5
7	Ειδοποιήσεις, Απαιτήσεις, Επικοινωνία Υποκειμένου Δεδομένων	2	5
8	Δικαιώματα Υποκειμένων	3	5
9	Διαβίβαση/Αποκάλυψη σε Τρίτους	2	5
10	Εκπαίδευση / Ενημέρωση	2	5
11	Έλεγχοι και Παρακολούθηση	2	5
12	Διαχείριση Παραβιάσεων Δεδομένων	2	5

4. Επίπεδο Ωριμότητας Πλαισίου Προστασίας Δεδομένων



Α.Α.	Ωριμότητα Μηχανισμών Προστασίας
0	**Δεν υπάρχει:** καμία ένδειξη / απόδειξη καταχωρημένου μηχανισμού προστασίας
1	**Αρχική:** Τα στοιχεία ελέγχου θεωρούνται απρόβλεπτα και αντιδραστικά.
2	**Διαχείριση:** Οι έλεγχοι «σχεδιάζονται, εκτελούνται, μετρούνται και ελέγχονται» σε αυτό το επίπεδο, αλλά υπάρχουν ακόμη πολλά ζητήματα που πρέπει να αντιμετωπιστούν.
3	**Καθορισμός:** Το Πανεπιστήμιο είναι πιο ενεργό παρά αντιδραστικό. Υπάρχει ένα σύνολο «προτύπων σε όλο το Πανεπιστήμιο» για «παροχή καθοδήγησης στο απόρρητο». Το Πανεπιστήμιο κατανοεί τις ελλείψεις του, πώς να τις αντιμετωπίσει και ποιος είναι ο στόχος για βελτίωση.
4	**Ποσοτική διαχείριση:** Αυτό το στάδιο είναι πιο μετρήσιμο και ελεγχόμενο. Το Πανεπιστήμιο επεξεργάζεται ελέγχους για να καθορίσει προβλέψιμες διαδικασίες που ευθυγραμμίζονται με τις ανάγκες Προστασίας Προσωπικών Δεδομένων. Το Πανεπιστήμιο προηγείται των κινδύνων, με περισσότερες γνώσεις σχετικά με τις ελλείψεις της διαδικασίας βάσει δεδομένων.
5	**Βελτιστοποίηση:** Εδώ, οι διαδικασίες του Πανεπιστημίου είναι σταθερές και ευέλικτες. Σε αυτό το τελικό στάδιο, το Πανεπιστήμιο θα βρίσκεται σε συνεχή κατάσταση βελτίωσης και ανταπόκρισης σε αλλαγές ή άλλες ευκαιρίες. Το Πανεπιστήμιο είναι σταθερό, γεγονός που επιτρέπει περισσότερη «ευελιξία και καινοτομία», σε ένα προβλέψιμο περιβάλλον.

5. Σχέδιο Συμμορφώσεως

Το Σχέδιο Συμμορφώσεως παρέχει ένα σχέδιο δράσης που προσδιορίζει και θέτει προτεραιότητες στα βασικά ζητήματα που πρέπει να αντιμετωπίσει το Πανεπιστήμιο για να συμμορφώνεται με τις ρυθμιστικές απαιτήσεις του ΓΚΠΔ.

1. ΛΟΓΟΔΟΣΙΑ & ΕΤΑΙΡΙΚΗ ΕΥΘΥΝΗ	Υψηλό	Μεσαίο	Χαμηλό	Ελάχιστο

Εύρημα	Επίπτωση Κινδύνου
• Έλλειψη επίσημων πολιτικών και διαδικασιών προστασίας δεδομένων προσωπικού χαρακτήρα (π.χ. Πολιτική αντιμετώπισης περιστατικών ασφαλείας, Πολιτική Διατήρησης Δεδομένων, Διαδικασία και πρωτόκολλο ενημέρωσης της Αρχής) • Έλλειψη πλαισίου διαχείρισης και παρακολούθησης προστασίας και ασφάλειας δεδομένων • Έλλειψη μητρώου ρίσκων απορρήτου και της σχετικής πολιτικής	Αδυναμία τεκμηρίωσης απτών αποδείξεων συμμόρφωσης και καθιέρωσης επαρκούς λογοδοσίας και υπευθυνότητας δημιουργούν ένα σημαντικό λειτουργικό κίνδυνο που επαγωγικά μπορεί να οδηγήσει σε: • λειτουργικές αποτυχίες και ζητήματα απορρήτου, υποτίμηση ή άγνοια σοβαρών κινδύνων απορρήτου • επιβολή δυσανάλογων κυρώσεων ή προστίμων από την αρμόδια Ρυθμιστική Αρχή

Ενέργειες Αντιμετώπισης
1. Δημιουργία Ομάδας Έργου / Επιτροπής Προστασίας Δεδομένων (ΟΠΔ): Βασιζόμενοι στις δυνατότητες και ανάγκες του Ιδρύματος για προστασία ΔΠΧ θα πρέπει να καθοριστεί μια ομάδα προστασίας δεδομένων με συγκεκριμένους ρόλους και αρμοδιότητες αποφάσεων και συντονισμού στο πλαίσιο των καθημερινών λειτουργιών. 2. Αξιολόγηση Κινδύνων Επεξεργασίας ΔΠΧ: ανάπτυξη εργαλείου και τεκμηρίωση βασικής αναφοράς εκτίμησης κινδύνων και αποτύπωσης των πιθανών κενών συμμόρφωσης με τις απαιτήσεις του ΓΚΠΔ με στόχο την ανάπτυξη του πλάνου δράσεων, προϋπολογισμού και γενικότερων πόρων για την εφαρμογή του πλάνου υλοποίησης. 3. Πολιτικές / Διαδικασίες: Ανάπτυξη και εφαρμογή των πολίτικων ασφάλειας και προστασίας ΔΠΧ (π.χ. Πολιτική αντιμετώπισης περιστατικών ασφαλείας, Πολιτική Διατήρησης Δεδομένων, Διαδικασία και πρωτόκολλο ενημέρωσης της Αρχής). 4. Μητρώο / Αρχείο Δραστηριοτήτων Επεξεργασίας: Περιοδική επικύρωση και τήρηση μητρώου των δραστηριοτήτων επεξεργασίας με τους προϊστάμενους / υπεύθυνους κάθε τμήματος

5. Σχέδιο Συμμορφώσεως

2. ΠΡΟΣΤΑΣΙΑ ΒΑΣΕΙ ΣΧΕΔΙΑΣΜΟΥ & ΑΣΦΑΛΕΙΑΣ ΕΠΕΞΕΡΓΑΣΙΑΣ:	Υψηλό	Μεσαίο	Χαμηλό	Ελάχιστο

Εύρημα	Επίπτωση Κινδύνου
• Ύπαρξη τοπικών διαχειριστών σε υπολογιστές του Ιδρύματος • Πολλαπλές μέθοδοι αυθεντικοποίησης στην υποδομή • Έλλειψη πλαισίου διαχείρισης προσβάσεων συνεργατών στα συστήματα του Ιδρύματος • Ελλιπής διαχείριση πληροφοριακών αγαθών • Ύπαρξη συστημάτων και εφαρμογών μη υποστηριζόμενης έκδοσης • Ελλιπής διαχωρισμός δικτύου • Έλλειψη διαχείρισης και αξιολόγησης ευπαθειών • Έλλειψη διαχείρισης ενημερώσεων συστημάτων και συσκευών δικτύου • Δεν έχει πραγματοποιηθεί έλεγχος διείσδυσης στην υποδομή του Ιδρύματος • Δεν υπάρχει σχέδιο ανάκτησης δεδομένων μετά από καταστροφή • Δεν υπάρχει σχέδιο επιχειρησιακής συνέχειας • Ύπαρξη κοινών λογαριασμών χρηστών • Ύπαρξη διπλών λογαριασμών χρηστών • Έλλειψη κρυπτογράφησης σε συστήματα και βάσεις δεδομένων • Ελλιπείς πολιτικές και διαδικασίες • Έλλειψη πολιτικής ιδίων συσκευών • Δεν υπάρχει κεντρική διαχείριση του συστήματος προστασίας από ιούς • Αδυναμία πλήρους καταγραφής και επίβλεψης συστημάτων και διαδικασιών	Αδυναμία παροχής επαρκούς πλαισίου ασφάλειας και προστασίας δεδομένων μέσω εργαλείων σχεδιασμού μπορεί να έχει σαν αποτέλεσμα την δημιουργία πολλαπλών κίνδυνων όπως : - μη εξουσιοδοτημένη πρόσβαση των δεδομένων - μη εξουσιοδοτημένη μεταβολή των δεδομένων - μη διαθεσιμότητα συστημάτων και δεδομένων - διαρροή προσωπικών δεδομένων - σημαντικές λειτουργικές αποτυχίες και βλάβες - νομικές ενέργειες κατά του Πανεπιστημίου από τα υποκείμενα δεδομένων - κυρώσεις (περιορισμοί/πρόστιμα) από την Ρυθμιστική Αρχή και οικονομικές ζημίες -ζημιά στο κυρός του σήματος του Πανεπιστημίου.

5. Σχέδιο Συμμορφώσεως

2. ΠΡΟΣΤΑΣΙΑ ΒΑΣΕΙ ΣΧΕΔΙΑΣΜΟΥ & ΑΣΦΑΛΕΙΑΣ ΕΠΕΞΕΡΓΑΣΙΑΣ:	Υψηλό	Μεσαίο	Χαμηλό	Ελάχιστο

Ενέργειες Αντιμετώπισης

5. Συμμετοχή του αρμοδίου ΥΠΔ στην Διακυβέρνηση της Ασφάλειας, συμμετοχή στις αποφάσεις προστασίας πληροφοριών και υποδομών της εταιρίας
6. Συμμετοχή του ΥΠΔ σε νέα έργα: Διασφάλιση της συμμέτοχης του ΥΠΔ/DPO στην αρχική φάση σκοπιμότητας και σχεδιασμού ενός νέου έργου, ανάπτυξης/απόκτησης συστήματος, συμβόλαιο/σύμβαση με εξωτερικό συνεργάτη για επεξεργασία ΔΠΧ.
7. Προστασία δεδομένων βάσει Σχεδιασμού σε νέα έργα: εφαρμογή ελέγχων της προστασίας ΔΠΧ βάσει σχεδιασμού:
   - σχεδιασμός και υιοθέτηση των αναγκαίων και απαραίτητων μηχανισμών προστασίας και ασφάλειας κατά την ανάπτυξη ή/και απόκτηση νέων συστημάτων
   - εκτέλεση ανάλυσης DPIA πριν από μεγάλη και σημαντική επεξεργασία προσωπικών δεδομένων (μεταφορά, πρόσβαση, ανταλλαγή κλπ.) που ενδεχομένως θέτει σε κίνδυνο τα δικαιώματα και τα δεδομένα των υποκειμένων
   - εκτέλεση τεχνικών ελέγχων ασφάλειας πριν την εισαγωγή νέων συστημάτων και λογισμικού σε περιβάλλον παραγωγής
   - Υιοθέτηση μηχανισμών κρυπτογράφησης και ελαχιστοποίησης δεδομένων
8. ΕΟΜΑ / ΕΤΜΑ : σχεδιασμός, ανάπτυξη και υλοποίηση ελάχιστων τεχνικών και οργανωτικών μηχανισμών ασφάλειας με σκοπό την βελτίωση του πλαισίου ελέγχου της ασφάλειας πληροφοριών και δεδομένων ώστε να μετριάζεται / ελαχιστοποιείται η πιθανή έκθεση του Πανεπιστημίου στους σχετικούς κινδύνους. Κατ' ελάχιστο θα πρέπει:
   - να υπάρχει αυστηρός έλεγχος και διαχείριση προσβάσεων βάσει ρόλων και αρμοδιοτήτων
   - ελαχιστοποίηση ή κατάργηση λογαριασμών με δικαιώματα διαχειριστή με ταυτόχρονη εφαρμογή ισχυρών προγραμμάτων antivirus για κάθε συσκευή (microsoft + mac) μέσω κεντρικού ελέγχου και διαχείρισης
   - να υλοποιηθεί μια κεντρική διαχείριση χρηστών (active directory) και δικτυακών υποδομών από κεντρικές κονσόλες (firewalling, IDS/IPS, network central monitoring)
   - εκτέλεση ειδικών τεχνικών προγραμμάτων / ελέγχων patch management, hardening
   - υιοθέτηση περιοδικών τεχνικών ελέγχων penetration test / Vulnerability Assessment (internal, external, network, application, phising/social engineering) από εξειδικευμένους εξωτερικούς παρόχους, ειδικά σε νέα συστήματα και εφαρμογές πριν το περιβάλλον παραγωγής
   - να υπάρχει έλεγχος και παρακολούθηση εξωτερικών απομακρυσμένων συνδέσεων (RAS).
   - διαβάθμιση πληροφοριών και επεξεργασία των ΔΠΧ με βάσει αυστηρών κανόνων ασφάλειας κατά την πρόσβαση, διαβίβαση, αποθήκευση
   - κρυπτογράφηση βάσεων και αρχείων
   - θέσπιση αυστηρών διαδικασιών παράδοσης παραλαβής και ελέγχου εξοπλισμού χρηστών (laptop, mobile phone, access cards etc.)
   - θέσπιση ρόλων και αρμοδιοτήτων διαχείρισης και διακυβέρνησης ασφάλειας συστημάτων και πληροφοριών
9. Υιοθέτηση μηχανισμών κρυπτογράφησης ειδικά για όσα ΔΠΧ διαβιβάζονται σε βάσεις, πλατφόρμες και υποδομές τρίτων παρόχων
10. Πρέπει το Ίδρυμα να δημιουργήσει πολίτικες και διαδικασίες αναφορικά με το σχέδιο επιχειρησιακής συνεχείας έτσι ώστε να είναι σε θέση να επαναλειτουργήσει ορθά είτε υστέρα από κάποια καταστροφή, πανδημία η και κάποια κυβερνοεπιθεση όπου θα προκαλέσει διακοπή της λειτουργίας των συστημάτων. Έτσι κρίνεται απαραίτητη η δημιουργία Disaster Recovery και Business Continuity Plan.

5. Σχέδιο Συμμορφώσεως

3. ΑΡΧΕΣ ΠΡΟΣΤΑΣΙΑΣ & ΜΗΤΡΩΟ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ ΕΠΕΞΕΡΓΑΣΙΑΣ:	Υψηλό	Μεσαίο	Χαμηλό	Ελάχιστο

Εύρημα	Επίπτωση Κινδύνου
• Έλλειψη επίσημης διαδικασίας αναφορικά με την περιοδική αναθεώρηση του αρχείου δραστηριοτήτων (πχ κάθε χρόνο) • Έλλειψη ελέγχων ελαχιστοποίησης των δεδομένων που μπορούν εύκολα να οδηγήσουν σε ταυτοποίηση του ονόματος/επιθέτου των υποκειμένων δεδομένων (π.χ. κρυπτογράφηση, ψευδωνυμοποιηση)	Αδυναμία διατήρησης ενημερωμένου αρχείου επεξεργασίας προσωπικών δεδομένων σύμφωνα με τις αρχές του ΓΚΠΔ ορίζεται ένας κίνδυνος μη συμμόρφωσης, ο οποίος μπορεί να έχει ως συνέπεια : • κυρώσεις (περιορισμοί/πρόστιμα) που θα εφαρμοστούν από τον Ρυθμιστή • νομικές δράσεις κατά του Πανεπιστημίου • ζημιά στο κύρος του Πανεπιστημίου • λειτουργικές αποτυχίες λόγω μεγάλου όγκου των αιτήσεων των υποκειμένων δεδομένων

Ενέργειες Αντιμετώπισης

11. Πολιτική / Διαδικασία Ελαχιστοποίησης των Δεδομένων: εφαρμογή, όπου είναι δυνατόν και απαραίτητο έλεγχο ελαχιστοποίησης δεδομένων.
12. Μητρώο Δραστηριοτήτων Επεξεργασίας: διατήρηση μητρώου δραστηριοτήτων επεξεργασίας σε ετήσια διαδικασία επικύρωσης για κάθε τομέα του Ιδρύματος.

5. Σχέδιο Συμμορφώσεως

4. ΕΚΤΙΜΗΣΗ ΑΝΤΙΚΤΥΠΟΥ ΕΠΕΞΕΡΓΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (DPIA):	Υψηλό	Μεσαίο	Χαμηλό	Ελάχιστο

Εύρημα	Επίπτωση Κινδύνου
• Ελλιπής διαδικασία και μεθοδολογία DPIA για την τεκμηρίωση και αιτιολόγηση πιθανών μελλοντικών ή / και υφιστάμενων σημαντικών επεξεργασιών • Έλλειψη διενεργειών εκτίμησης αντικτύπου για κρίσιμες επεξεργασίες (πχ. Ερευνητικά έργα και διαμοιρασμός δεδομένων εκτός Ε.Ε.) • Διενέργεια αναγκαιότητας εκτίμησης αντικτύπου για 10 ερευνητικά έργα (κωδ. Έργων : 569, 550, 61118, 4001, 448, 488, 61119, 542, 531, 486)	Αδυναμία σχεδιασμού, ανάπτυξης και υιοθέτησης μιας επίσημης διαδικασίας Εκτίμησης Κινδύνου/Αντικτύπου για όλες τις σημαντικές και κρίσιμες επεξεργασίες αποτελεί θέμα μη συμμόρφωσης, το οποίο μπορεί να οδηγήσει σε: • σημαντικούς κινδύνους και μη απαραίτητη έκθεση απορρήτου προσωπικών/ευαίσθητων δεδομένων • αδυναμία τεκμηρίωσης και αιτιολόγησης υφιστάμενης ή μελλοντικής επεξεργασίας δεδομένων • πιθανή απώλεια συνεργατών από την στιγμή που συνήθως το DPIA είναι μέρος των καλών πρακτικών της εταιρίας και είναι σημαντικό κριτήριο πριν από οποιαδήποτε συνεργασία • λειτουργικές αποτυχίες και ασάφειες στον ορισμό των κινδύνων απορρήτου

Ενέργειες Αντιμετώπισης
13. Διαδικασία DPIA: Βελτίωση της διαδικασίας DPIA και χρήση εάν/όταν συμβεί σημαντική επεξεργασία 14. Έλεγχος αναγκαιότητας για την διενέργεια εκτίμησης αντικτύπου για τα συγκεκριμένα έργα.

5. Σχέδιο Συμμορφώσεως

5. ΣΥΓΚΑΤΑΘΕΣΗ & ΑΠΟΚΑΛΥΨΗ ΔΕΔΟΜΕΝΩΝ:	Υψηλό	Μεσαίο	Χαμηλό	Ελάχιστο

Εύρημα	Επίπτωση Κινδύνου
• Ελλιπείς διαδικασίες ενημέρωσης υποκειμένων και διαχείρισης συναίνεσης για την επεξεργασία των δεδομένων ενδεικτικά, στο πλαίσιο των προωθητικών ενεργειών, συλλογής βιογραφικών, εγγραφή στην βιβλιοθήκη, διαχείριση cookies κ.α.	Αδυναμία παροχής επαρκούς πληροφόρησης στο υποκείμενο δεδομένων την στιγμή της συλλογής σχετικά με την επεξεργασία και μεταφορά των προσωπικών και ευαίσθητων δεδομένων του/της, αποτελεί κίνδυνο μη συμμόρφωσης, το οποίο μπορεί να οδηγήσει σε: • κυρώσεις (περιορισμοί/πρόστιμα) που θα εφαρμοστούν από την Αρχή • ζημιά στο σήμα του Πανεπιστημίου • νομική δράση κατά της εταιρίας από τα υποκείμενα δεδομένων

Ενέργειες Αντιμετώπισης

15. Διαχείριση/Εφαρμογή Μηχανισμών Λήψης Συναίνεσης: ανάπτυξη και διατήρηση μιας διαδικασίας για την διαχείριση αποδείξεων λήψης συναίνεσης στα σημεία συλλογής (πχ. λήψη βιογραφικών, συμμετοχή σε events/διαγωνισμούς κλπ.).
16. Ενημέρωση και Συγκατάθεση Υποκειμένων: εισαγωγή μηχανισμών ενημέρωσης υποκειμένων για κάθε συλλογή και επεξεργασία που δεν βασίζεται αμιγώς στην συμβατική παροχή υπηρεσιών του Ιδρύματος πχ newsletters, διατήρηση βιογραφικών υποψηφίων, διαβίβαση δεδομένων σε τρίτους κλπ.).
17. Πολιτική Απορρήτου: Σύνδεση της πολιτικής απορρήτου με κάθε συλλογή ΔΠΧ μέσω της ιστοσελίδας του Πανεπιστημίου για πληρέστερη ενημέρωση και λήψη συγκατάθεσης επεξεργασίας ΔΠΧ. Παράλληλη εισαγωγή λειτουργίας unsubscribe (opt-out) για όσα υποκείμενα επιθυμούν την άρση της πρότερης συγκατάθεσης. Υιοθέτηση back office μηχανισμών υλοποίησης των αιτημάτων των υποκειμένων.

5. Σχέδιο Συμμορφώσεως

6. ΔΗΛΩΣΕΙΣ & ΕΝΗΜΕΡΩΣΗ ΥΠΟΚΕΙΜΕΝΩΝ:	Υψηλό	Μεσαίο	Χαμηλό	Ελάχιστο

Εύρημα	Επίπτωση Κινδύνου
• Έλλειψη επίσημης πολιτικής ή/και διαδικασίας διαχείρισης αιτημάτων υποκειμένων • Βελτίωση επάρκειας πολιτικής απορρήτου. Η πολιτική απορρήτου θα πρέπει να υπόκειται σε περιοδική αναθεώρηση με βάση το αρχείο δραστηριοτήτων του Ιδρύματος. • Έλλειψη επαρκούς ενημέρωσης υποκειμένων για την συλλογή και διατήρηση δεδομένων για διαφορετικό επιχειρησιακό λόγο για τον οποίο αρχικά συλλέχθηκαν (πχ. βιογραφικά υποψηφίων σπουδαστών, στοιχεία επικοινωνίας συμμετεχόντων σε διαγωνισμούς, συνεργάτες και απόφοιτους που περιλαμβάνονται στις λίστες ενημερώσεων και newsletters) • Έλλειψη πολιτικής απορρήτου για χρήση στο Facebook	Αδυναμία παροχής επαρκούς πληροφόρησης για την επεξεργασία των προσωπικών δεδομένων μπορεί να οδηγήσει σε: • κυρώσεις (περιορισμοί/πρόστιμα) που θα εφαρμοστούν από την Ρυθμιστική Αρχή • επίπτωση στην φήμη του Ιδρύματος • νομική δράση κατά της εταιρίας από τα υποκείμενα δεδομένων • λειτουργικές δυσλειτουργίες

Ενέργειες Αντιμετώπισης
18. Χειρισμός Αιτημάτων Υποκειμένων: υιοθέτηση ή ενσωμάτωση στις ήδη υπάρχουσες διαδικασίες Διαχείρισης Παραπόνων την διαχείριση των αιτημάτων που σχετίζονται με τα δικαιώματα των υποκειμένων δεδομένων (δικαίωμα πρόσβασης, ενημέρωσης, διαγραφής, εναντίωσης κλπ.). 19. Ενημέρωση Υποκειμένων: διασφάλιση διαφανούς και πλήρους ενημέρωσης υποκειμένων για κάθε νέα επεξεργασία ή περιστατικό διαρροής ΔΠΧ. Τυχόν αιτήματα φυσικών προσώπων θα πρέπει να διαχειρίζονται σε συνεργασία με τους υπευθύνους επεξεργασίας στο πλαίσιο των εκατέρωθεν συμβατικών υποχρεώσεων. 20. Υιοθέτηση πολιτικής απορρήτου για το Facebook καθώς και αναθεώρηση της υπάρχουσας σε ισχύ πολιτικής απορρήτου της ιστοσελίδας.

5. Σχέδιο Συμμορφώσεως

7. ΔΙΚΑΙΩΜΑΤΑ ΥΠΟΚΕΙΜΕΝΩΝ	Υψηλό	Μεσαίο	Χαμηλό	Ελάχιστο

Εύρημα	Επίπτωση Κινδύνου
• Ελλειψη Πολιτικής Διαχείρισης Δικαιωμάτων Υποκειμένων • Έλλειψη συγκεκριμένου front και back-office μηχανισμών για την παροχή των μέσων για την άσκηση των δικαιωμάτων των υποκειμένων	Αδυναμία ανάπτυξης και εφαρμογής αποτελεσματικών λειτουργιών back office και καθορισμένων ρολών και αρμοδιοτήτων για την διαχείριση των δικαιωμάτων των υποκείμενων δεδομένων, το οποίο μπορεί να οδηγήσει σε: • σημαντικές καθυστερήσεις ή/και αδυναμία ανταπόκρισης σε αιτήματα δικαιωμάτων των υποκειμένων δεδομένων • κυρώσεις (περιορισμοί/πρόστιμα) θα εφαρμοστούν από την Αρχή σαν αποτέλεσμα της μη ανταπόκρισης μέσα στις προθεσμίες που έχουν καθοριστεί από τον νομό • πιθανή ζημία στο κύρος του σήματος του Ιδρύματος • λειτουργικές αποτυχίες

Ενέργειες Αντιμετώπισης

21. Διαχείριση Δικαιωμάτων Δεδομένων Υποκείμενων: οργάνωση ειδικά για αυτό το σκοπό ομάδας για την λήψη και διαχείριση των αιτημάτων των δικαιωμάτων υποκείμενων διασφαλίζοντας
    α) τον τρόπο λήψης αιτημάτων,
    β) έγκαιρη απάντηση γραπτώς,
    γ) την παρακολούθηση της έκβασης / αποτελέσματος των αιτήσεων των υποκείμενων δεδομένων,
    δ) την ενημέρωση των ατόμων που λειτουργούν ως υπεύθυνοι επεξεργασίας.

22. Πολιτική / Διαδικασία Διαχείρισης Δικαιωμάτων Υποκείμενων Δεδομένων: τεκμηρίωση διαδικασιών διαχείρισης Δικαιωμάτων Υποκειμένων και καθοδήγηση αυτών αναφορικά με ποιον τρόπο που μπορούν να ασκήσουν τα δικαιώματα τους (ανακοινώσεις, προφορικές ενημερώσεις, γραπτές οδηγίες, πολιτική απορρήτου κλπ.).

5. Σχέδιο Συμμορφώσεως

8. ΔΙΑΒΙΒΑΣΗ & ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΑΠΟ/ΠΡΟΣ ΤΡΙΤΟΥΣ:	Υψηλό	Μεσαίο	Χαμηλό	Ελάχιστο

Εύρημα	Επίπτωση Κινδύνου
• Ελλιπής διαχείριση του συμβατικού πλαισίου-μοντέλου Υπεύθυνου Επεξεργασίας / Εκτελούντα την Επεξεργασία για χρήση σε όλες τις υφιστάμενες και μελλοντικές συμβάσεις που διαβιβάζονται και επεξεργάζονται ΔΠΧ προς και από τρίτους.	Πιθανή αντισυμβατική ή / και μη εγκεκριμένη επεξεργασία ΔΠΧ από συνεργαζόμενους τρίτους ελλείψει επίσημων συμβατικών μοντέλων για τους εκτελούντες την επεξεργασία, δύναται να οδηγήσει σε: • μη εγκεκριμένες επεξεργασίες από τρίτους • απώλεια ελέγχου της μεταφοράς και επεξεργασίας δεδομένων • περιορισμός ευθύνη των τρίτων μερών • υποτίμηση σοβαρών κινδύνων ασφάλειας • ζημιά κυρούς του εμπορικού σήματος της εταιρίας • καταγγελίες υποκειμένων και επιβολή προστίμων / ποινών

Ενέργειες Αντιμετώπισης

23. Ρυθμίσεις Συμφωνητικών Προστασίας ΔΠΧ (DPA): ανάπτυξη και συμφωνία όρων προστασίας προσωπικών δεδομένων με όλα τα τρίτα μέρη με τα οποία γίνεται ανταλλαγή και επεξεργασία προσωπικών δεδομένων.
24. Μητρώο Τρίτων Μερών: ανάπτυξη και τήρηση μητρώου με όλα τα τρίτα μέρη / υποπαρόχους με τους οποίους ανταλλάσσονται ΔΠΧ .
25. Πρόγραμμα Παρακολούθησης Ασφάλειας και Προστασίας ΔΠΧ Εκτελούντων την Επεξεργασία: Να δοθεί προτεραιότητα σε λειτουργίες των τρίτων μερών όσον αφορά την προστασία των δεδομένων και δημιουργία ενός προγράμματος ελέγχου προστασίας ΔΠΧ σε εκτελούντες την επεξεργασία.
26. Συνιστάται να ορίσετε με σαφήνεια μια διαδικασία επιλογής προμηθευτή / συνεργάτη που θα παραμένει ίδια στο σύνολο του Ιδρύματος, η οποία αντιμετωπίζει τους κινδύνους απορρήτου που προκύπτουν από μια επιλογή προμηθευτή, αξιολογώντας τα επίπεδα επάρκειας απορρήτου πριν από την υπογραφή της σύμβασης.
27. Σύνταξη Τυποποιημένων συμβατικών ρητρών για τη διαχείριση μεταφορών δεδομένων εκτός ΕΕ

5. Σχέδιο Συμμορφώσεως

9. ΕΚΠΑΙΔΕΥΣΗ & ΕΝΗΜΕΡΩΣΗ:	Υψηλό	Μεσαίο	Χαμηλό	Ελάχιστο

Εύρημα	Επίπτωση Κινδύνου
• Έλλειψη προγράμματος περιοδικής εκπαίδευσης - ενημέρωσης για την ανάγκη προστασίας δεδομένων προσωπικού χαρακτήρα καθώς και παρακολούθηση αφομοίωσης και κατανόησης υποχρεώσεων και ευθυνών.	Αδυναμία δημιουργίας ενός πλήρους προγράμματος εκπαίδευσης / ενημέρωσης δημιουργεί προϋποθέσεις άγνοιας συμμόρφωσης και πιθανής υποτίμησης σημαντικών θεμάτων - κινδύνων επεξεργασίας ΔΠΧ.

Ενέργειες Αντιμετώπισης
28. Προγράμματα Κατάρτισης / Εκπαίδευσης / Ευαισθητοποίησης για την Προστασία των Δεδομένων: ανάπτυξη και εκτέλεση τακτικών και έκτακτων προγραμμάτων ενημέρωσης, εκπαίδευσης και ενημέρωσης προστασίας δεδομένων. Παρακολούθηση και επίσημη τεκμηρίωση ποσοστών αφομοίωσης / κατανόησης υποχρεώσεων και ευθυνών (KPIs).

5. Σχέδιο Συμμορφώσεως

10. ΕΛΕΓΧΟΣ ΚΑΙ ΠΑΡΑΚΟΛΟΥΘΗΣΗ:	Υψηλό	Μεσαίο	Χαμηλό	Ελάχιστο

Εύρημα	Επίπτωση Κινδύνου
Δεδομένης της έλλειψης ομάδας έργου προστασίας δεδομένων προσωπικού χαρακτήρα, παρατηρείται ανεπαρκές πρόγραμμα ενημέρωσης και παρακολούθησης των διαδικασιών συμμόρφωσης.	Αδυναμία δημιουργίας οργανωμένων και τακτικών ελέγχων προστασίας δεδομένων και προγραμμάτων παρακολούθησης μπορεί να οδηγήσουν σε : • δυσανάλογες κυρώσεις (περιορισμοί/πρόστιμα) λόγω της έλλειψης αποδείξεων ευθύνης • κίνδυνο υποτίμησης σοβαρών θεμάτων προστασίας δεδομένων και μη συμμόρφωσης ή άγνοια κινδύνων • λειτουργικές απώλειες

Ενέργειες Αντιμετώπισης

29. Εκτίμηση Κίνδυνου Προστασίας Δεδομένων: ανάπτυξη και εκτέλεση εκτιμήσεων κίνδυνου προστασίας δεδομένων και παρακολούθηση της εφαρμογής/μετριασμού του κίνδυνου. Ενσωμάτωση της ιδιωτικότητας, προστασίας και ασφάλειας στα προγράμματα ελέγχου του ιδρύματος και να γίνει επίσημη αναφορά των αποτελεσμάτων στην Επιτροπή/Ομάδα Ελέγχου/Συμμόρφωσης.
30. Ανάπτυξη και τήρηση ενός μητρώου κινδύνου προστασίας δεδομένων ακολουθούμενο από την αντίστοιχη πολιτική διαχείρισης κινδύνων όπου να αναδεικνύει τον εντοπισμό, καταγραφή και διαχείριση των κινδύνων που σχετίζονται με το μητρώο προσωπικών δεδομένων.

5. Σχέδιο Συμμορφώσεως

11. ΔΙΑΧΕΙΡΙΣΗ ΠΑΡΑΒΙΑΣΕΩΝ:	Υψηλό	Μεσαίο	Χαμηλό	Ελάχιστο

Εύρημα	Επίπτωση Κινδύνου
• Έλλειψη επίσημης πολιτικής/διαδικασίας διαχείρισης παραβιάσεων με ρόλους και ευθύνες. • Έλλειψη μεθοδολογίας ειδοποιήσεων μετά από διαρροή δεδομένων.	Αδυναμία αναγνώρισης μιας πιθανής παραβίασης δεδομένων / συμβάντος ασφάλειας μπορεί να οδηγήσει σε : • σοβαρή διαρροή προσωπικών δεδομένων που θα μπορούσε να είχε αποφευχθεί • αδυναμία παροχής έγκαιρης (72 ωρών) ανταπόκριση και επίσημη κοινοποίηση στα υποκείμενα δεδομένων και στον Ρυθμιστή Απορρήτου • σοβαρές κυρώσεις (περιορισμοί/πρόστιμα) λόγω της αδυναμίας της παροχής αποδείξεων συμμόρφωσης ή καλής πρακτικής • σημαντική ζημία στο κύρος του εμπορικού σήματος της εταιρίας • σοβαρές οικονομικές ζημίες λόγω των πιθανών κυρώσεων ή/και απώλεια πελατών/υποκειμένων δεδομένων

Ενέργειες Αντιμετώπισης
31. Διαδικασία Διαχείρισης Διαρροής Δεδομένων: ανάπτυξη και διατήρηση μιας διαδικασίας διαρροής/παραβίασης των δεδομένων για να αντιμετωπιστούν επαρκώς οι νομικές απαιτήσεις που σχετίζονται με τις πιθανές παραβιάσεις των δεδομένων έγκαιρα (ενημέρωση υποκειμένων και Αρχής εντός 72 ωρών). 32. Διαδικασία Διαχείρισης Διαρροής Δεδομένων: καθορισμός στην διαδικασία παραβίασης των δεδομένων συγκεκριμένων εργασιών και αρμοδιοτήτων σχετικά με την επίσημη ανακοίνωση στα υποκείμενα δεδομένων και στις αρμόδιες αρχές. 33. Διαδικασία Διαχείρισης / Ενημέρωσης Διαρροής Δεδομένων: δημιουργία και τήρηση μητρώου περιστατικών.

6. ΣΥΝΟΠΤΙΚΟ ΣΧΕΔΙΟ ΔΡΑΣΗΣ

Συνοπτικές ενέργειες για τις γενικές διατάξεις του ΓΚΠΔ

1. Σύσταση Ομάδας Έργου για την προστασία δεδομένων – (μέρος της υλοποίησης εσωτερικά)
2. Περιοδική ενημέρωση του Αρχείου Δραστηριοτήτων Επεξεργασίας και αποτύπωση των τυχόν αλλαγών στην Πολιτική Απορρήτου – (μέρος της υλοποίησης εσωτερικά)
3. Σύνταξη Πολιτικών Απορρήτου και Διαδικασιών (Πολιτική διαχείρισης περιστατικών, μεθοδολογία DPIA, Πολιτική παραβίασης δεδομένων, διαδικασία επικοινωνίας με τις τοπικές αρχές, κ.λπ.) – (Παραδόθηκαν)
4. Σύνταξη διαδικασίας και δημιουργία μηχανισμών για τη διαχείριση των αιτημάτων για δικαιώματα υποκειμένων – (Παραδόθηκαν / μέρος της υλοποίησης εσωτερικά)
5. Διαχείριση τρίτων μερών αναφορικά με την αξιολόγηση του επιπέδου συμμόρφωσης με τον ΓΚΠΔ, τις συμβατικές ρήτρες και την μεταφορά δεδομένων εκτός Ε.Ε. – (Παραδόθηκαν / μέρος της υλοποίησης εσωτερικά)
6. Σύνταξη και υιοθέτηση ενιαίου πλαισίου πολιτικών ασφάλειας πληροφοριών. – (Παραδόθηκαν / μέρος της υλοποίησης εσωτερικά)
7. Βελτίωση των τεχνικών και οργανωτικών μέτρων των υποδομών πληροφορικής. – (Παραδόθηκαν / μέρος της υλοποίησης εσωτερικά)
8. Σύνταξη, διατήρηση και διαχείριση των ρίσκων προστασίας δεδομένων και της αντίστοιχης πολιτικής – (Παραδόθηκαν / μέρος της υλοποίησης εσωτερικά)
9. Αξιολόγηση ερευνητικών έργων ως προς την αναγκαιότητα για την διενέργεια εκτίμησης αντικτύπου για την προστασία προσωπικών δεδομένων (Baker Tilly / μέρος της υλοποίησης εσωτερικά)
10. Εκπαίδευση όλων των υπαλλήλων σχετικά με τις διατάξεις του ΓΚΠΔ, τις ευθύνες και τις υποχρεώσεις τους. – (Παραδόθηκαν / μέρος της υλοποίησης εσωτερικά)
11. Συνεχής παρακολούθηση των πτυχών της Προστασίας Δεδομένων – (μέρος της υλοποίησης εσωτερικά)

5 Στάδια Ετοιμότητας

Στάδιο	Εκτίμηση	Σχεδιασμός	Μετασχηματισμός	Λειτουργία	Συμμόρφωση
Δραστηριότητα	• Αξιολογήσεις κινδύνου και απορρήτου δεδομένων για τη διακυβέρνηση, τους ανθρώπους, τις διαδικασίες, τα δεδομένα, την ασφάλεια • Ανάπτυξη χάρτη πορείας ετοιμότητας • Προσδιορισμός και χαρτογράφηση προσωπικών δεδομένων	• Σχεδιασμός προτύπων εκπαίδευσης διακυβέρνησης, επικοινωνίας και διαδικασιών • Σχεδιασμός προτύπων απορρήτου, διαχείρισης δεδομένων και διαχείρισης ασφάλειας	• Ανάπτυξη και ενσωμάτωση διαδικασιών και εργαλείων • Παροχή Εκπαίδευσης • Ανάπτυξη και ενσωμάτωση προτύπων και πολιτικών χρησιμοποιώντας την ασφάλεια εξ ορισμού • Λεπτομερής χαρτογράφηση δεδομένων	• Εκτέλεση σχετικών επιχειρησιακών διαδικασιών • Επίβλεψη της ασφάλειας και του απορρήτου με την χρήση ΕΤΜΑ / ΕΟΜΑ • Διαχείριση δικαιωμάτων συναίνεσης και πρόσβασης υποκειμένου δεδομένων	• Παρακολούθηση, εκτίμηση, έλεγχος, αναφορά και αξιολόγηση της τήρησης των διατάξεων του ΓΚΠΔ
Αποτέλεσμα	Εκτιμήσεις και χάρτης υλοποίησης	Καθορισμένο σχέδιο δράσης	Ολοκλήρωση των βελτιώσεων των διαδικασιών	Λειτουργικό πλαίσιο σε εφαρμογή	Συνεχής παρακολούθηση και αναφορά
	Προσδιορισμός του αντικτύπου του ΓΚΠΔ και σχεδιασμός ελάχιστων τεχνικών και οργανωτικών μέτρων	Περιλαμβάνει ελέγχους, διαδικασίες και λύσεις προστασίας δεδομένων που θα εφαρμοστούν	Περιλαμβάνει ελέγχους, διαδικασίες και λύσεις προστασίας δεδομένων που θα εφαρμοστούν	Νέος τρόπος λειτουργίας συμμορφούμενος με τον ΓΚΠΔ	Επίβλεψη της εκτέλεσης των ΕΤΜΑ / ΕΟΜΑ, παράδοση αποδεικτικών στοιχείων συμμόρφωσης σε εσωτερικά και εξωτερικά ενδιαφερόμενα μέρη

Σχέδιο Συμμορφώσεως

1. Πολιτικές, Πρότυπα και Οδηγίες

Πολιτική απορρήτου δεδομένων υπαλλήλων
Πολιτική/Διαδικασία Ακρίβειας Δεδομένων
Πολιτική ελαχιστοποίησης δεδομένων
Πολιτική διαχείρισης συναίνεσης
Πολιτική αποδεκτής χρήσης
Πολιτική Cloud
Πολιτική Social Media

2. Δικαιώματα υποκειμένων δεδομένων

Πολιτική / Διαδικασία δικαιωμάτων υποκειμένου δεδομένων

3. Ευθύνη και Λογοδοσία

Ορισμός ΥΠΔ
Ανακοίνωση ΥΠΔ
Ομάδα Έργου
Πολιτική Διατήρησης Δεδομένων
Πολιτική Αποδεκτής Χρήσης

4. Μόρφωση, Εκπαίδευση και Ευαισθητοποίηση

Εκπαίδευση και ευαισθητοποίηση για την προστασία δεδομένων

5. Ασφάλεια & Ακεραιότητα Δεδομένων

Ελάχιστα Τεχνικά & Οργανωτικά Μέτρα Ασφάλειας & Προστασίας Δεδομένων
Σχέδιο Επιχειρησιακής Συνέχειας
Στρατηγική Διαβάθμισης Δεδομένων

6. Privacy by Design

Εκτίμηση Αντικτύπου σε νέα έργα
Συμμετοχή του ΥΠΔ σε νέα έργα

7. Τρίτα Μέρη

Τυπικές συμβατικές ρήτρες
Συμφωνίες Προστασίας Δεδομένων
Έλεγχος απορρήτου τρίτων μερών

8. Αρχείο Δραστηριοτήτων

Αρχεία Δραστηριοτήτων Επεξεργασίας
Νομικές Βάσεις επεξεργασίας
Αναθεώρηση αρχείου δραστηριοτήτων

9. Διαχείριση παραβίασης δεδομένων

Διαδικασία διαχείρισης παραβίασης δεδομένων

10. Διαφάνεια

Μητρώο Μηχανισμών Μεταφοράς ΔΠΧ
Γενική Πολιτική Προστασίας Δεδομένων
Διαδικασία Διαχείρισης Συγκατάθεσης
Έγκαιρη ενημέρωση υποκειμένων
Διαχείριση συγκατάθεσης Cookies
Πολιτική Απορρήτου
Ευαισθητοποίηση του προσωπικού

11.Συγκατάθεση

Προϋποθέσεις ζήτησης συγκαταθέσεων
Τήρηση Μητρώου Συγκαταθέσεων

12. Χαρτογράφηση Δεδομένων

Εκτίμηση Κινδύνου Απορρήτου
Τήρηση Μητρώου Κινδύνων

Υπόμνημα
Δεν εφαρμόζεται
Χρήζει Βελτίωσης
Εφαρμόζεται