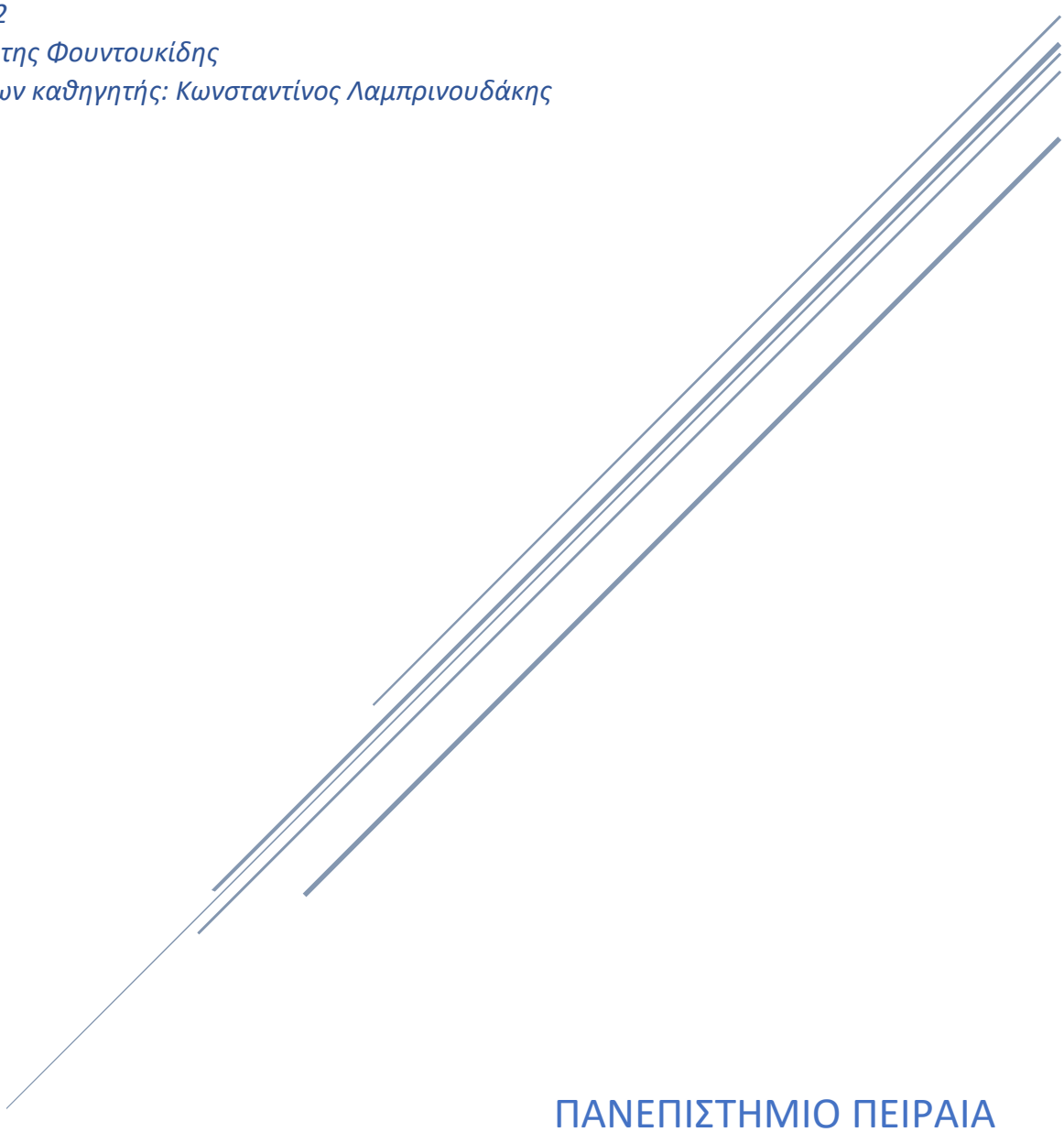
ΑΣΦΑΛΕΙΑ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑ ΣΤΗ ΜΕΤΑ GDPR ΕΠΟΧΗ, ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ ΥΓΕΙΑΣ ΚΑΙ ΤΗΣ ΑΣΦΑΛΙΣΗΣ.

A Case Study

MTE1732
Παναγιώτης Φουντουκίδης
Επιβλέπων καθηγητής: Κωνσταντίνος Λαμπρινουδάκης



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ
Ασφάλεια Ψηφιακών Συστημάτων

Ασφάλεια και ιδιωτικότητα στη μετά GDPR εποχή, στον τομέα της υγείας και της ασφάλισης.

Περιεχόμενα

ΕΙΣΑΓΩΓΗ

Πλαίσιο

Ένας χρόνος έχει ήδη κλείσει από την υποχρεωτική εφαρμογή του Γενικού Κανονισμού περί Προστασίας Δεδομένων (ΓΚΠΔ-GDPR) και ακόμα η πλειοψηφία των οργανισμών προσπαθεί να φτάσει το μέγιστο δυνατό επίπεδο συμμόρφωσης, χωρίς αυτό να είναι πάντα εφικτό ή υλοποιήσιμο με βάση το business της εκάστοτε επιχείρησης.

Πιο συγκεκριμένα οι μικρομεσαίες επιχειρήσεις πλέον έχουν μεγάλο μερίδιο της πίτας στο κομμάτι της αγοράς και προσφέρουν αρκετά στην Ευρωπαϊκή οικονομία. Προσπαθώντας λοιπόν να πετύχουν το στόχο τους, βασίζονται όλο και περισσότερο στην τεχνολογία και στα πληροφοριακά συστήματα, ενώ πολλές έχουν και online παρουσία προσφέροντας υπηρεσίες στους πελάτες τους. Ο μεγάλος όγκος λοιπόν των μικρομεσαίων επιχειρήσεων συνεπάγεται και μεγάλο όγκο δεδομένων που αυτές επεξεργάζονται, μεγάλο μέρος του οποίου είναι προσωπικά δεδομένα.

Στο τομέα της υγείας και της ασφάλειας τα πράγματα είναι ακόμα πιο δύσκολα και τα περιθώρια για ριζικές αλλαγές είναι ισχνά, ιδιαίτερα όταν μιλάμε για δημόσιους οργανισμούς ασφάλισης και δημόσιες υποδομές υγείας, σε ένα κράτος που η γραφειοκρατία είναι θεμέλιος λίθος της λειτουργίας τους και η είσοδος της τεχνολογίας στο συγκεκριμένο κλάδο γίνεται με πολύ αργούς ρυθμούς και βρίσκοντας σθεναρή αντίσταση από όσους δυσκολεύονται να προσαρμοστούν σε αλλαγές, είτε είναι σε επίπεδο κυβερνήσεων είτε σε επίπεδο νοοτροπίας και κουλτούρας υπαλλήλων.

Πρέπει όμως να γίνει αντιληπτό, πως πλέον ζούμε σε μια εποχή όπου τα προσωπικά δεδομένα έχουν αποκτήσει άλλη αξία και λογίζονται διαφορετικά. Είναι ο κύριος μοχλός κίνησης του σύγχρονου επιχειρηματικού κόσμου και γι’ αυτό το λόγο θεωρούνται και υψηλής αξίας. Πόσα και πόσα σκάνδαλα έχουν δει το φως της δημοσιότητας τον τελευταίο καιρό όπου η χρήση των προσωπικών δεδομένων γίνεται κακόβουλα και με σκοπό το κέρδος, όπως και να υπολογίζεται αυτό (ποιοτικό ή ποσοτικό);

Κατά συνέπεια καθίσταται λοιπόν σαφές ότι και τα ευαίσθητα προσωπικά δεδομένα, αυτά δηλαδή που διαχειρίζονται κατά κόρον οι οργανισμοί (δημόσιοι ή ιδιωτικοί) που αναφέραμε παραπάνω, χρήζουν ακόμα περισσότερης προσοχής. Η λήψη μέτρων, τεχνικών ή οργανωτικών, για την προστασία τους είναι η σημαντικότερη επένδυση στην οποία μπορεί να προβεί κάποιος οργανισμός όχι μόνο για να διαφυλάξει ένα τόσο πολύτιμο αγαθό, αλλά και για να αποφύγει διαρροές οι οποίες μπορούν να αποδειχθούν επιζήμιες δεδομένων των υψηλών προστίμων που μπορεί να επιβληθούν κατά περίπτωση. Βέβαια ένα υψηλό πρόστιμο δεν είναι το μόνο πρόβλημα που θα καλεστεί

κάποιος οργανισμός να αντιμετωπίσει, καθώς η δυσφήμιση που μπορεί να υποστεί θα είναι ακόμα μεγαλύτερο πλήγμα το οποίο σε μια εποχή που ο κόσμος έχει αρχίσει να ευαισθητοποιείται, δύναται να είναι και μη αναστρέψιμο.

Πεδίο

Το συγκεκριμένο case study αναφέρεται σε εταιρεία που δραστηριοποιείται στο χώρο της υγείας και έχει ως πελάτες μεγάλες φαρμακευτικές εταιρείες. Καθώς λειτουργεί ουσιαστικά ως ενδιάμεσος κρίκος μεταξύ των φαρμακευτικών και των ασθενών παρέχοντας υπηρεσίες εκπαιδεύσεων και υποστήριξης για θεραπείες που αφορούν χρόνιες παθήσεις διατηρεί μια τεράστια βάση που αποτελείται από στοιχεία ασθενών (ευαίσθητα προσωπικά δεδομένα) και κατά συνέπεια ορίζεται ως συνυπεύθυνος επεξεργασίας. Αυτό γιατί η ίδια ορίζει τον τρόπο με τον οποίο αποθηκεύει και διαχειρίζεται τα προσωπικά δεδομένα που εισέρχονται στο σύστημά της.

Μέσα από το case study -και αφού έχουν αναγνωριστεί οι ροές δεδομένων και ποιες χρήζουν DPIA- γίνεται αξιολόγηση κινδύνου και μέσω μιας διαδικασίας gap analysis και ελέγχεται κατά πόσο μια εταιρεία πιστοποιημένη με ISO 27001:2013 (με ένα αρκετά μεγάλο πεδίο εφαρμογής του προτύπου), όπως η συγκεκριμένη, μπορεί με τα μέτρα -τεχνικά ή οργανωτικά- που έχει πάρει ώστε να συμμορφώνεται με το πρότυπο, να πετύχει συμμόρφωση και με το GDPR σε ένα μεγάλο βαθμό.

ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

Ασφάλεια Πληροφορίας

Με τον όρο ασφάλεια πληροφορίας εννοούμε όλα εκείνα τα μέτρα που μπορεί να πάρει ένας οργανισμός ώστε να προστατέψει την πληροφορία που επεξεργάζεται μέσα σε ένα σύστημα (είτε ηλεκτρονικό, είτε φυσικό) από μη εξουσιοδοτημένη πρόσβαση και χρήση, αποκάλυψη, διακοπή παροχής, τροποποίηση, ανάγνωση, έλεγχο, καταγραφή ή καταστροφή. Το πιο διαδεδομένο μοντέλο πάνω στο οποίο βασίζεται η ανάπτυξη και η εφαρμογή ενός πλαισίου για τη διαχείριση της ασφάλειας της πληροφορίας είναι γνωστό με τον όρο CIA: εμπιστευτικότητα (**confidentiality**), ακεραιότητα (**integrity**) και διαθεσιμότητα (**availability**).

1) **Εμπιστευτικότητα**: με τον όρο εμπιστευτικότητα εννοούμε την ιδιότητα της πληροφορίας να μην αποκαλύπτεται σε μη εξουσιοδοτημένα πρόσωπα, οντότητες ή διεργασίες. Ταυτόχρονα βεβαιώνεται ότι αυτοί που πρέπει να έχουν πρόσβαση στην πληροφορία, θα έχουν όντως πρόσβαση σε αυτή.
2) **Ακεραιότητα**: με τον όρο ακεραιότητα εννοούμε την ιδιότητα της πληροφορίας να είναι ακριβής και ολοκληρωμένη, μια ιδιότητα που πρέπει να διατηρεί η πληροφορία καθ' όλο τον κύκλο της, από τη δημιουργία μέχρι την καταστροφή της, ενώ τυχόν αλλαγές πρέπει να μπορούν να είναι ανιχνεύσιμες.
3) **Διαθεσιμότητα**: με τον όρο διαθεσιμότητα εννοούμε την ιδιότητα της πληροφορίας να είναι προσβάσιμη και έτοιμη προς χρήση όταν ένα

εξουσιοδοτημένο άτομο τη ζητάει. Αυτό προϋποθέτει όλα τα συστήματα που αποθηκεύουν ή διαχειρίζονται την πληροφορίας να είναι πάντα πλήρως λειτουργικά.

ISO 27001

Στον τομέα της ασφάλειας της πληροφορίας υπάρχει πληθώρα από πρότυπα και πλαίσια τα οποία παρέχουν διαφορετικούς τύπους από μέτρα. Το πιο γνωστό και αυτό που χρησιμοποιείται σε μεγαλύτερο βαθμό είναι η οικογένεια προτύπων ISO 27000 η οποία παρέχει μια συστηματική και δομημένη προσέγγιση για την εφαρμογή και τη συντήρηση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφορίας (ΣΔΑΠ/ISMS). Ένα ISMS βοηθάει έναν οργανισμό στα παρακάτω:

- ✓ Να αναγνωρίσει τα περιουσιακά στοιχεία του που φέρουν πληροφορία καθώς και τις απαιτήσεις ασφαλείας που συνδέονται με αυτά
- ✓ Να αξιολογήσει και να περιορίσει τους κινδύνους που μπορεί να προκύπτουν
- ✓ Να επιλέξει τα κατάλληλα μέτρα ώστε να διαχειριστεί τους κινδύνους που δε μπορεί να αποδεχθεί
- ✓ Να μπορεί να ελέγχει και να συντηρεί/βελτιώνει την αποτελεσματικότητα των μέτρων που έχει λάβει και σχετίζονται με την πληροφορία ως περιουσιακό στοιχείο ενός οργανισμού.

Από την παραπάνω οικογένεια προτύπων αυτά που έχουν το μεγαλύτερο ενδιαφέρον είναι τα ISO 27001 και ISO 27002.

Το πρώτο είναι ένα ISMS ανεξάρτητο της τεχνολογίας και των προμηθευτών αλλά σε καμία περίπτωση δεν είναι οδηγός. Προσφέρει όμως την εξειδίκευση, δηλαδή το σύνολο των στοιχείων που μπορούν να ορίσουν ως αποτελεσματικό ένα ISMS.

Από την άλλη ενώ το ISO 27001 ουσιαστικά παρέχει τις απαιτήσεις, το ISO 27002 παρέχει οδηγίες και τις καλύτερες πρακτικές για να καλυφθούν οι προαναφερθείσες απαιτήσεις, λειτουργώντας ως ζευγάρι με το ISO 27001.

Οι σημαντικότεροι λόγοι που το ενδιαφέρον για τις πιστοποιήσεις πάνω στο ISO 27001 παρουσιάζει τέτοια άνοδο είναι η αύξηση των απειλών που σχετίζονται με την πληροφορία καθώς και οι κανονισμοί (όπως ο ΓΚΠΔ) που σχετίζονται με την προστασία της πληροφορίας.

Οι απειλές σχετικά με την ασφάλεια πληροφορίας στοχεύουν αδιάκριτα κάθε οργανισμό ή άτομο που χρησιμοποιεί κυρίως ηλεκτρονικά μέσα για τη διαχείριση της πληροφορίας, ενώ είναι αυτοματοποιημένες και ελεύθερες στο διαδίκτυο. Τα δεδομένα ωστόσο είναι ευάλωτα και σε άλλους παράγοντες όπως είναι οι φυσικές καταστροφές, η κλοπή, οι εξωτερικές επιθέσεις όπως και η δολιοφθορά εκ των έσω.

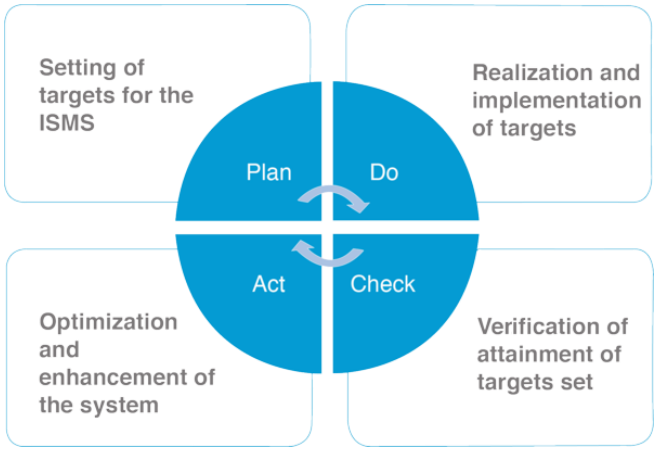
Τα τελευταία 20 χρόνια επίσης έχει παρατηρηθεί αύξηση των νομικών και κανονιστικών απαιτήσεων που σχετίζονται με την ασφάλεια της πληροφορίας και των δεδομένων. Κάποια από αυτά επικεντρώνονται στην προστασία των προσωπικών δεδομένων φυσικών προσώπων, ενώ κάποια άλλα σε εταιρικά οικονομικά, λειτουργικά δεδομένα ή συστήματα διαχείρισης κινδύνων.

Πάντως πέρα από την ενίσχυση της άμυνας ενός οργανισμού σε ότι αφορά τους κινδύνους που σχετίζονται με την πληροφορία και τα δεδομένα, το να πιστοποιηθεί με το συγκεκριμένο πρότυπο παρέχει και ένα ανταγωνιστικό πλεονέκτημα –κυρίως σε αγορές που εμπλέκονται προσωπικά δεδομένα– καθώς φαίνεται προς τα έξω πως ο οργανισμός κάνει τις απαραίτητες κινήσεις ώστε να προστατέψει το σημαντικότερο περιουσιακό του στοιχείο. Δεν είναι απλώς θέμα marketing, αλλά σε συνδυασμό με τη συμμόρφωση με τον ΓΚΠΔ καθώς και άλλες οδηγίες που αφορούν την ασφάλεια της πληροφορίας, η ικανότητα να αποδείξει ένας οργανισμός ότι συμμορφώνεται με το εν λόγω πρότυπο μπορεί να ανοίξει ευκαιρίες εργασίας σε όλο τον κόσμο.

Πολλοί είναι ωστόσο αυτοί που πιστεύουν ότι η ασφάλεια της πληροφορίας είναι θέμα που αφορά μόνο την τεχνολογία, αλλά αυτό απέχει πολύ από την πραγματικότητα. Είναι ο χρήστης της τεχνολογίας που θα αποφασίσει από ποιες απειλές πρέπει να προστατευτεί και πως θα κινηθεί στο δίλλημα ασφάλεια ή ελαστικότητα. Σαφώς όταν παρθούν αυτές οι αποφάσεις οι ειδικοί στην ασφάλεια πληροφορίας θα είναι αυτοί που θα εφαρμόσουν μια τεχνολογική λύση που θα επιφέρει τα επιθυμητά αποτελέσματα αλλά λειτουργούν πάντα με βάση την εκτίμηση κινδύνου του χρήστη. Σε έναν οργανισμό λοιπόν οι αποφάσεις αυτές πρέπει να παίρνονται από τα διοικητικά στελέχη και όχι από την ομάδα IT και αυτό είναι και κάτι που κάνει σαφές το ίδιο το πρότυπο. Συνεπώς η εφαρμογή ενός ISMS δεν είναι ένα project που θα «τρέξει» ένας ειδικός σε τεχνολογικά θέματα καθώς αυτό σε πολλές περιπτώσεις μπορεί να γίνει αντιπαραγωγικό.

Σε ότι αφορά το project αυτό καθαυτό, πρόκειται για μια αρκετά πολύπλοκη διαδικασία καθώς χρειάζεται τη συμβολή όλης της επιχείρησης, από τα ανώτατα διοικητικά στελέχη μέχρι την τελευταία θέση στο οργανόγραμμα, ενώ η εφαρμογή του μπορεί να χρειαστεί μήνες, ακόμα και χρόνια.

Αναφορικά με την εφαρμογή του προτύπου δεν υπάρχουν συγκεκριμένα στάδια που θα ακολουθηθούν μια φορά, αλλά πρόκειται για μια κυκλική διαδικασία με το μοτίβο του PDCA (Plan-Do-Check-Act) να είναι το πιο διαδεδομένο. Η διαδικασία ή η βελτίωση της διαδικασίας πρέπει πρώτα να σχεδιαστεί (Plan), μετά να εφαρμοστεί (Do) και η αποτελεσματικότητας της να ελέγχεται σε τακτά χρονικά διαστήματα (Check-Act). Συγκρίνοντας τα αποτελέσματα της φάσης ελέγχου με αυτά που έχουν σχεδιαστεί ο οργανισμός μπορεί να αναγνωρίσει πιθανές αποκλίσεις αλλά και να εντοπίσει περιθώρια βελτίωσης.



Το πιο χρονοβόρο μέρος της εφαρμογής ενός ISMS είναι η δημιουργία αρχείου και οδηγιών για το πως το ISMS δουλεύει και λειτουργεί στον οργανισμό. Υπάρχει πληθώρα προσεγγίσεων, από το να το αναλάβει εξωτερικός συνεργάτης μέχρι κάποιος μέσα στον οργανισμό.

ΓΚΠΔ (GDPR)

Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων 679/2016, τέθηκε σε εφαρμογή τον Μάιο του 2018, και αποτελεί το μόνο και βασικό νομικό πλαίσιο για την προστασία δεδομένων και είναι άμεσα εφαρμόσιμο σε όλα τα κράτη μέλη της

Ευρωπαϊκής Ένωσης και αντικατέστησε την ήδη υπάρχουσα ντιρεκτίβα περί Προστασίας Δεδομένων 95/46/ΕC, ενώ ουσιαστικά ξεδιάλυνε το τοπίο καθώς μέχρι τότε οι επιχειρήσεις στην Ευρωπαϊκή Ένωση είχαν να κάνουν με 28 διαφορετικούς νόμους που αφορούσαν την προστασία δεδομένων που δεν ήταν μόνο κάτι πολύπλοκο αλλά ταυτόχρονα και πολύ κοστοβόρο.

Μια από τις βασικές υποχρεώσεις όλων των επιχειρήσεων συμπεριλαμβανομένων και των μικρομεσαίων που λειτουργούν είτε ως εκτελούντες είτε ως υπεύθυνοι επεξεργασίας με βάση τον ΓΚΠΔ είναι η ασφάλεια των προσωπικών δεδομένων, δεδομένα δηλαδή μέσω των οποίων μπορεί να ταυτοποιηθεί ένα φυσικό πρόσωπο. Πιο συγκεκριμένα με τον όρο ασφάλεια, νοείται τόσο η εμπιστευτικότητα όσο και η διαθεσιμότητα αλλά και η ακεραιότητα των δεδομένων και θα έπρεπε να ελέγχεται με βάση μια προσέγγιση βασισμένη στο ρίσκο, κάτι που σημαίνει πως όσο ψηλότερο είναι το ρίσκο, τόσο πιο αυστηρά θα πρέπει να είναι τα μέτρα που ο υπεύθυνος ή ο εκτελών την επεξεργασία θα πρέπει να λάβει, ώστε να το διαχειριστεί και αν είναι εφικτό να το εξαλείψει.

Επιπλέον η επεξεργασία των δεδομένων θα πρέπει να διέπεται από την αρχή ελαχιστοποίησης των δεδομένων, κάτι που σημαίνει ότι μια επιχείρηση θα πρέπει να συγκεντρώνει και να επεξεργάζεται δεδομένα που είναι απολύτως απαραίτητα για την προσφορά των υπηρεσιών της και τίποτα παραπάνω. Σε ότι αφορά πάλι τα δεδομένα αυτά πρέπει να είναι ακριβή και να επικαιροποιούνται εφόσον αυτά απαιτούνται, να υπάρχουν εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση τους και να περιορίζεται η περίοδος τήρησης τους μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας, με εξαίρεση μόνο για σκοπούς δημοσίου συμφέροντος, επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς.

Επίσης θα πρέπει να είναι ξεκάθαρο σε κάθε περίπτωση αν μια επιχείρηση είναι υπεύθυνη ή εκτελών την επεξεργασία καθώς οι ευθύνες που προκύπτουν σε κάθε περίπτωση με βάση τον ΓΚΠΔ είναι διαφορετικές. Ακόμα και σε περιπτώσεις που μια

επιχείρηση είναι συνυπεύθυνη με μια άλλη θα πρέπει να προσδιορίζονται με σαφήνεια τα μεταξύ τους όρια. Έτσι ορίζεται ως:

1) Υπεύθυνος επεξεργασίας οποιοσδήποτε καθορίζει τον σκοπό και τον τρόπο της επεξεργασίας και φέρει την ευθύνη για την εφαρμογή του νόμου και δίνει οδηγίες στον εκτελούντα.
2) Εκτελών την επεξεργασία οποιοσδήποτε επεξεργάζεται δεδομένα για λογαριασμό του υπευθύνου επεξεργασίας.
3) Από κοινού υπεύθυνοι επεξεργασίας, δυο ή περισσότεροι υπεύθυνοι που καθορίζουν από κοινού τα μέσα και τους σκοπούς επεξεργασίας.

Παρακάτω παρουσιάζονται σύντομα τα βασικότερα σημεία του ΓΚΠΔ.

Ο ΓΚΠΔ εφαρμόζεται σε επιχειρήσεις που ανήκουν εντός της Ευρωπαϊκής Ένωσης, ωστόσο αν χώρες εκτός ΕΕ προσφέρουν αγαθά ή υπηρεσίες σε υποκείμενα εντός ΕΕ ή κάνουν profiling υποκειμένων, τότε και αυτές εμπίπτουν στον κανονισμό και οφείλουν να συμμορφώνονται με τις οδηγίες του.

Συνεπώς οι συγκεκριμένες επιχειρήσεις θα πρέπει να ορίσουν κάποιον εκπρόσωπο ο οποίος θα ασχολείται με το συγκεκριμένο θέμα.

Ο ΓΚΠΔ διατηρεί τις ίδιες βασικές αρχές με την προηγούμενη οδηγία που αφορούσε την προστασία δεδομένων, αλλά περιλαμβάνει και κάποιες αλλαγές. Διατηρεί το κύριο θέμα που αφορά τα ευαίσθητα προσωπικά δεδομένα, ενώ ταυτόχρονα το επεκτείνει με το να συμπεριλαμβάνει πλέον και γενετικά αλλά και βιομετρικά δεδομένα.

Αυτό μπορεί να έχεις ως επακόλουθο η χρήση στοιχείων που εμπίπτουν στις παραπάνω κατηγορίες σαν πειστήρια σε ποινικά αδικήματα να είναι πιο δύσκολη διαδικασία.

Η έννοια της συγκατάθεσης για τη χρήση των προσωπικών δεδομένων ενός υποκειμένου θωρακίζεται ακόμα περισσότερο. Πλέον η διαδικασία της λήψης της συγκατάθεσης πρέπει να είναι απόλυτα διαφανής και η συγκατάθεση αυτή καθαυτή να είναι ρητή. Επιπλέον τα υποκείμενα έχουν τη δυνατότητα να ανακαλούν τη συγκατάθεση τους ανά πάσα στιγμή.

Σαφής θα πρέπει να είναι και η συγκατάθεση όχι μόνο για τη λήψη και την επεξεργασία των προσωπικών δεδομένων, αλλά και για τη μεταφορά τους σε χώρες εκτός ΕΕ. Υπάρχουν βέβαια και οι εξαιρέσεις, για τις οποίες η λήψη συγκατάθεσης δεν απαιτείται.

Τα υποκείμενα πλέον έχουν σημαντικά περισσότερα δικαιώματα μεταξύ των οποίων και το «δικαίωμα στη λήθη» (την πλήρη διαγραφή των προσωπικών του δεδομένων), καθώς και το δικαίωμα μεταφοράς δεδομένων (σε περιπτώσεις για παράδειγμα παρόχων υπηρεσιών).

Ωστόσο η λίστα των δικαιωμάτων δεν είναι πολύ σαφής, ενώ σε κάποιες περιπτώσεις η εφαρμογή τους μπορεί να είναι και τεχνικά αδύνατη.

Όσες επιχειρήσεις ή οργανισμοί υπόκεινται στον ΓΚΠΔ δεν αρκεί να δηλώνουν συμμορφώνονται, αλλά πρέπει να είναι και σε θέση να αποδείξουν ότι το κάνουν.

Αν μια επιχείρηση ή οργανισμός πραγματοποιεί επεξεργασία που μπορεί να θεωρηθεί υψηλού ρίσκου, τότε πρέπει να διενεργεί DPIA και σε πολλές φορές να συμβουλεύεται κάποια ανώτερη αρχή. Αυτό βέβαια μπορεί να έχει σημαντικό αντίκτυπο σε χρόνο κατά τη διαδικασία εκκίνησης ενός καινούριου project.

Ο ΓΚΠΔ απαιτεί ένα μεγάλο όγκο πληροφορίας ο οποίος θα πρέπει να αναφέρεται από τις επιχειρήσεις και τους οργανισμούς σχετικά με τη λήψη, αποθήκευση, επεξεργασία, μεταφορά των δεδομένων, τα δικαιώματα των υποκειμένων κλπ. Πέρα από τον όγκο, η πληροφορία αυτή θα πρέπει να είναι σαφής και κατανοητή προς τα υποκείμενα, τα οποία θα πρέπει να είναι πάντα ενημερωμένα, ακόμα και αν αυτή η πληροφορία αλλάζει κατά καιρούς.

Ο κανονισμός ορίζει τη θέσπιση μιας καινούριας θέσης στους οργανισμούς και στις επιχειρήσεις, αυτή του Υπεύθυνου Προστασίας Δεδομένων (DPO), ο οποίος θα πρέπει να εμπλέκεται σε όλες τις διαδικασίες που αφορούν την προστασία δεδομένων και θα αναφέρεται απευθείας στην ανώτατη διοίκηση του οργανισμού ή της επιχείρησης.

Ο ορισμός ενός DPO δεν είναι υποχρεωτικός για όλες τις επιχειρήσεις, αλλά εξαρτάται από το μέγεθός τους αλλά και από το αν εμπλέκονται με προσωπικά δεδομένα. Μπορεί να είναι ένα άτομο στην επιχείρηση ή ακόμα και εξωτερικός συνεργάτης.

Οι επιχειρήσεις πρέπει να παίρνουν όλα τα απαραίτητα μέτρα ώστε να διαφυλάσσουν τα προσωπικά δεδομένα είτε αυτά είναι οργανωτικά είτε τεχνικά, όπως για παράδειγμα κρυπτογράφηση. Επιπλέον οφείλουν να αναφέρουν περιστατικά ασφαλείας στις ρυθμιστικές αρχές, ακόμα και στα υποκείμενα κατά περιπτώσεις.

Όπως αναφέρθηκε παραπάνω, ο κανονισμός ορίζει τους υπεύθυνους και τους εκτελούντες την επεξεργασία. Αυτό σημαίνει ότι πολλά συμβόλαια με εκτελούντες την επεξεργασία πρέπει να αναθεωρηθούν και να συμπεριλάβουν αντίστοιχες διευκρινήσεις.

Οι προμηθευτές λοιπόν που μέχρι πρότινος δεν είχαν κάποια νομική απαίτηση, πλέον όντας εκτελούντες την επεξεργασία σε πολλές περιπτώσεις, υπάγονται πλέον στον ΓΚΠΔ και οφείλουν να λάβουν τα αντίστοιχα μέτρα.

Η μεταφορά προσωπικών δεδομένων σε χώρες εκτός ΕΕ δεν επιτρέπεται από τον ΓΚΠΔ, εκτός και αν το επιβάλλουν συγκεκριμένες συνθήκες, οι οποίες ουσιαστικά είναι οι ίδιες με αυτές που περιλαμβάνονταν στη μέχρι τώρα ισχύουσα οδηγία για την προστασία δεδομένων. Αυτό έχει ως αποτέλεσμα οι απαιτήσεις από εξωτερικές αρχές να είναι πιο ιδιαίτερες.

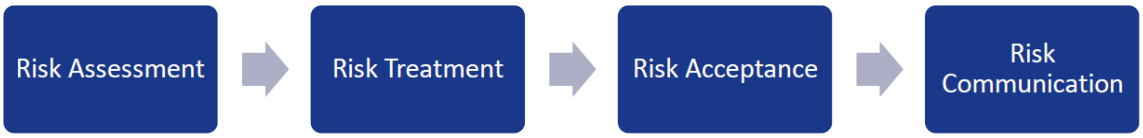
Τα πρόστιμα που μπορούν να επιβληθούν από τις αρχές σε παραβάσεις είναι αρκετά υψηλά πλέον και μπορεί να φτάσουν έως το 4% του ετήσιου τζίρου μιας εταιρείας ή το ποσό των 20 εκατομμυρίων ευρώ.

Τα υποκείμενα μπορούν να προχωρήσουν σε μηνύσεις τόσο σε ότι αφορά υλική ή μη υλική ζημιά που οφείλεται σε απώλεια προσωπικών δεδομένων. Αυτό σημαίνει λοιπόν πως οι οργανισμοί πρέπει να είναι πλέον πολύ προσεκτικοί και να λειτουργούν με γνώμονα την πλήρη εναρμόνιση με τις οδηγίες του κανονισμού.

Διαχείριση κινδύνου

Η διαχείριση κινδύνου στην ασφάλεια πληροφορίας είναι η διαδικασία κατά την οποία ένας οργανισμός αναγνωρίζει, εκτιμά και διαχειρίζεται κινδύνους που σχετίζονται με την ασφάλεια της πληροφορίας και έχει ως σκοπό να επιτευχθεί μια ισορροπία ανάμεσα στο να αντιληφθεί ένας οργανισμός ευκαιρίες βελτίωσης ενώ ταυτόχρονα θα ελαττώνει τις ευπάθειες και τις απώλειες.

Οι φάσεις-κλειδιά στη διαδικασία διαχείρισης κινδύνου είναι οι παρακάτω:



A. **Εκτίμηση κινδύνου (Risk Assessment):** Πρόκειται ουσιαστικά για την αναγνώριση των κινδύνων που αντιμετωπίζει ένας οργανισμό σε μια συγκεκριμένη χρονική στιγμή και αποτελεί μια εξίσωση της πιθανότητας να πραγματοποιηθεί μια απειλή σε συνδυασμό με την επίπτωση που αυτή θα έχει στον οργανισμό. Το πρώτο βήμα είναι η αναγνώριση των απειλών και ακολουθείται από τον ορισμό της πιθανότητας εμφάνισης και της επίπτωσης που έχει αυτή.
B. **Αντιμετώπιση κινδύνου (Risk Treatment):** Λαμβάνοντας υπόψη τα αποτελέσματα της εκτίμησης κινδύνου ο οργανισμός καθορίζει μέτρα ώστε να τους αντιμετωπίσει τα οποία μπορεί να έχουν διαφορετική προσέγγιση, όπως μείωση του κινδύνου, μεταφορά του σε τρίτο, αποφυγή ή διατήρηση. Πολλαπλά μέτρα ίσως και διαφορετικού τύπου μπορεί να επιλεχθούν για την αντιμετώπιση ενός συγκεκριμένου κινδύνου.

C. **Αποδοχή κινδύνου (Risk Acceptance):** Ακόμα και όταν ληφθούν μέτρα για την αντιμετώπιση ενός κινδύνου, ένα μέρος αυτού μπορεί να παραμείνει, όπως για παράδειγμα αν κάποια μέτρα δεν είναι εφικτό να παρθούν. Αυτό είναι ένα ποσοστό που στις περισσότερες περιπτώσεις θα πρέπει να το αποδεχθεί ο οργανισμός.
D. **Επικοινωνία του κινδύνου (Risk Communication):** Όλοι πρέπει να λάβουν γνώση των κινδύνων, των μέτρων που έχουν ληφθεί καθώς και των κινδύνων που έχει αποδεχτεί ο οργανισμός.

Ασφάλεια στην επεξεργασία προσωπικών δεδομένων

Τα προσωπικά δεδομένα είναι ακόμα ένα είδος πληροφορίας, συνεπώς η ασφάλεια στην επεξεργασία προσωπικών δεδομένων ακολουθεί τις ίδιες αρχές για την ασφάλεια της πληροφορίας καθώς και της διαχείρισης κινδύνου.

Υποχρεώσεις ασφαλείας με βάση τον ΓΚΠΔ

Σύμφωνα με το άρθρο 32 του ΓΚΠΔ:

«Λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση:

a) της ψευδωνυμοποίησης και της κρυπτογράφησης δεδομένων προσωπικού χαρακτήρα
b) της δυνατότητας διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση,
c) της δυνατότητας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος,
d) διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.

Κατά την εκτίμηση του ενδεδειγμένου επιπέδου ασφάλειας λαμβάνονται ιδίως υπόψη οι κίνδυνοι που απορρέουν από την επεξεργασία, ιδίως από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία λαμβάνουν μέτρα ώστε να διασφαλίζεται ότι κάθε φυσικό πρόσωπο που ενεργεί υπό την εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία το οποίο έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα τα επεξεργάζεται μόνο κατ' εντολή του υπευθύνου επεξεργασίας, εκτός εάν υποχρεούται προς τούτο από το δίκαιο της Ένωσης ή του κράτους μέλους.»

Σύμφωνα λοιπόν με τα παραπάνω σε ότι αφορά την ασφάλεια των προσωπικών δεδομένων με βάση τον ΓΚΠΔ μπορεί να καταλήξει κανείς στα παρακάτω:

1) **Προσέγγιση με βάση τον κίνδυνο:** Τα τεχνικά και οργανωτικά μέτρα για την προστασία των προσωπικών δεδομένων θα πρέπει να είναι ανάλογα του κινδύνου και να διασφαλίζουν τα δικαιώματα και τις ελευθερίες των προσώπων. Αυτό οδηγεί με τη σειρά του στην εφαρμογή αποτίμησης επίπτωσης σε ότι αφορά την προστασία δεδομένων (DPIA).
2) **Δημιουργία ενός ISMS για τα προσωπικά δεδομένα:** Με βάση το ΓΚΠΔ ένας οργανισμός δεν πρέπει να αρκεστεί στην εφαρμογή μέτρων, αλλά στην εφαρμογή ενός ISMS για την προστασία της εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας και της ανθεκτικότητας των προσωπικών δεδομένων.
3) **Ασφάλεια της ιδιωτικότητας:** Αν και ο ΓΚΠΔ δεν προσδιορίζει κάποιες συγκεκριμένες τεχνολογίες ενίσχυσης ιδιωτικότητας, αναφέρει ρητά την ψευδωνυμοποίηση και την κρυπτογράφηση ως τα μέτρα κλειδιά για την ασφάλεια των προσωπικών δεδομένων.

Διαχείριση κινδύνου για την επεξεργασία προσωπικών δεδομένων

Όπως έχει αναφερθεί και παραπάνω, η αξιολόγηση και η διαχείριση του κινδύνου είναι σημαντικό μέρος της ασφάλειας της πληροφορίας, με σκοπό την υιοθέτηση κατάλληλων μέτρων. Σε ότι αφορά όμως την ασφάλεια πληροφορίας στην επεξεργασία προσωπικών δεδομένων, θα πρέπει να ληφθούν υπόψη συγκεκριμένες παράμετροι και να ακολουθηθεί μια διαφορετική προσέγγιση. Πιο συγκεκριμένα:

i. Στις τυπικές διαδικασίες αποτίμησης κινδύνου, αυτοί αξιολογούνται με βάση την επίπτωση τους στον οργανισμό. Στην περίπτωση όμως των προσωπικών δεδομένων, η έννοια της επίπτωσης συνδέεται με τις ελευθερίες και τα

δικαιώματα των υποκειμένων, κάτι το οποίο αλλάζει όλη την οπτική της διαδικασίας. Ένα ακόμα σημαντικό κομμάτι είναι πως η επίπτωση είναι πολύ μεγάλη ακόμα και αν αφορά μόνο ένα άτομο.

ii. Η διαχείριση του κινδύνου αλλάζει αρκετά με βάση το παραπάνω. Για παράδειγμα, ακόμα και αν η πιθανότητα εμφάνισης ενός κινδύνου είναι μικρή, αν η επίπτωση του είναι μεγάλη το να τον αποδεχθεί ο οργανισμός θα είναι μια τελείως λάθος απόφαση. Σε τέτοιες περιπτώσεις, ο υπεύθυνος ή ο εκτελών την επεξεργασία θα πρέπει να αξιολογήσει ξανά τη διαδικασία επεξεργασίας ή να χρησιμοποιήσει πιο εξελιγμένες τεχνολογίες προστασίας προσωπικών δεδομένων.

Άρα αν σκεφτεί κανείς λίγο τον κύκλο PDCA αυτός αλλάζει λίγο δομή:

1) Αρχικά πρέπει να γίνει μια σωστή αποτύπωση των δεδομένων που επεξεργάζεται ένας οργανισμός.
2) Στη συνέχεια να οριστούν οι πιθανές απειλές και κίνδυνοι που ελλοχεύουν σχετικά με τα προσωπικά δεδομένα.
3) Ακολούθως να υπολογιστεί ο συνολικός κίνδυνος (πιθανότητα εμφάνισης και μέγεθος επίπτωσης) που αφορά τα υποκείμενα.
4) Να επιλεχθούν τα κατάλληλα μέτρα.
5) Τέλος να εφαρμοστούν και να ελέγχονται σε τακτά χρονικά διαστήματα.

ΜΕΘΟΔΟΛΟΓΙΑ

Σκοπός

Στο συγκεκριμένο case study εφαρμόστηκε η μεθοδολογία που περιγράφεται στο "Guidelines for SMEs on the security of Personal Data" που εκδόθηκε το Δεκέμβριο του 2016 από τον ENISA και είχε ως στόχο να παρέχει οδηγίες σε μικρομεσαίες επιχειρήσεις οι οποίες λειτουργούν ως υπεύθυνοι ή εκτελούντες επεξεργασίας, ώστε να υιοθετήσουν μέτρα ασφάλειας για την προστασία των προσωπικών δεδομένων με απώτερο σκοπό τη συμμόρφωση τους με το Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων.

Σύμφωνα με τον ΓΚΠΔ η ασφάλεια των προσωπικών δεδομένων βασίζεται τόσο στην εμπιστευτικότητα, όσο και στην ακεραιότητα και τη διαθεσιμότητα, κάτι που οδηγεί στη χρήση μιας προσέγγισης με βάση το ρίσκο. Όσο μεγαλύτερο δηλαδή είναι το ρίσκο τόσο πιο σκληρά μέτρα (τεχνικά ή οργανωτικά) πρέπει να λάβει ο υπεύθυνος ή ο εκτελών την επεξεργασία

Πιο συγκεκριμένα οι συγκεκριμένες οδηγίες έχουν δυο σκέλη:

1) Να παρέχουν μια απλοποιημένη προσέγγιση που θα βοηθήσει τις μικρομεσαίες επιχειρήσεις να καταλάβουν το νόημα της επεξεργασίας προσωπικών δεδομένων και να μπορούν να εκτιμήσουν τους κινδύνους που μπορούν να προκύψουν από την εν λόγω επεξεργασία.
2) Να παρέχουν κάποια πιθανά οργανωτικά και τεχνικά μέτρα που θα προστατέψουν τα προσωπικά δεδομένα από τους κινδύνους που θα αναγνωριστούν παραπάνω.

Η μεθοδολογία που θα αναλυθεί παρακάτω οδηγεί σε μια λίστα μέτρων που πρέπει να λάβει η επιχείρηση και τα οποία αντιστοιχούνται στη συνέχεια με τις παραγράφους του προτύπου ISO 27001:2013, ενώ στο τέλος ελέγχεται αν τα μέτρα που έχουν προαναφερθεί εφαρμόζονται από την επιχείρηση για τις αντίστοιχες ροές δεδομένων.

Προαπαιτούμενα

Σημαντικό είναι να αναφερθεί ότι για την εφαρμογή της συγκεκριμένης μεθοδολογίας θα πρέπει πρώτα να έχει προηγηθεί η διαδικασία της χαρτογράφησης των ροών δεδομένων, το οποίο είναι ένα από τα σημαντικότερα κομμάτια ώστε η επιχείρηση να μπορέσει να έχει μια ξεκάθαρη εικόνα των παρακάτω:

1) Τι είδους δεδομένα εισέρχονται στο σύστημα της.

2) Ποια είναι η προέλευση τους.
3) Που αποθηκεύονται.
4) Πως αποθηκεύονται.
5) Τι επεξεργασία υπόκεινται.
6) Που αποθηκεύονται μετά την επεξεργασία.
7) Πως αποθηκεύονται μετά την επεξεργασία.
8) Ποια είναι τα εξερχόμενα.
9) Προς τα που κατευθύνονται τα εξερχόμενα.

Αυτή η διαδικασία συνήθως υλοποιείται με τη βοήθεια εξωτερικών συνεργατών (κάτι το οποίο έγινε και στο συγκεκριμένο case study) και απαιτεί συνεντεύξεις με υπευθύνους του κάθε τμήματος ξεχωριστά ώστε να συλλεχθεί όλη η απαραίτητη πληροφορία.

Σε δεύτερο στάδιο ελέγχεται από το νομικό τμήμα της εταιρείας ή από εξωτερικούς νομικούς συμβούλους ποιες από τις παραπάνω αναγνωρισμένες ροές δεδομένων χρήζουν DPIA και οι οποίες στη συνέχεια θα εξεταστούν με βάση τη μεθοδολογία που αναφέρεται στο συγκεκριμένο case study.

Στάδια

Εκτίμηση κινδύνου

Η εκτίμηση κινδύνου είναι το πρώτο βήμα ώστε να υιοθετηθούν τα κατάλληλα μέτρα για την προστασία των προσωπικών δεδομένων. Η μεθοδολογία που θα περιγραφεί βασίζεται σε τέσσερα βήματα:

1) **Ορισμός της επεξεργασίας και του περιεχομένου της.**
2) **Κατανόηση και εκτίμηση της επίπτωσης ενός κινδύνου.**
3) **Ορισμός των πιθανών απειλών και εκτίμηση της πιθανότητας να εμφανιστούν.**
4) **Εκτίμηση του κινδύνου συνδυάζοντας την πιθανότητα αυτός να εμφανιστεί με την επίπτωση που μπορεί να έχει.**

Ορισμός της επεξεργασίας και του περιεχομένου της

Αυτό είναι το πρώτο και ίσως το σημαντικότερο βήμα για τον οργανισμό ώστε να μπορεί να κατανοήσει σε βάθος το σύστημα επεξεργασίας καθώς και το περιεχόμενο του. Για να το πετύχει αυτό, πρέπει να λάβει υπόψη όλες τις φάσης της επεξεργασίας, από τη

συλλογή μέχρι και την καταστροφή, καθώς και τις διάφορες παραμέτρους που τις πλαισιώνουν.

Για να μπορέσει να φτάσει εύκολα σε ένα συμπέρασμα, ο οργανισμός θα πρέπει να απαντήσει στις παρακάτω ερωτήσεις:

- *Με ποιο τρόπο επεξεργάζονται τα προσωπικά δεδομένα;* Ακόμα και αν χρησιμοποιούνται τα ίδια τεχνικά ή μη μέσα για την επεξεργασία διαφορετικής ομάδας δεδομένων, προτείνεται η εκτίμηση κινδύνου να γίνει για την κάθε ομάδα ξεχωριστά.
- *Ποιος είναι ο τύπος των προσωπικών δεδομένων που επεξεργάζονται;* Αν εμπλέκονται προσωπικά δεδομένα που φέρουν την ταμπέλα των «ευαίσθητων», τότε το ρίσκο αυτομάτως γίνεται υψηλότερο, σύμφωνα με το άρθρο 9 του ΓΚΠΔ.
- *Ποιος είναι ο σκοπός της επεξεργασίας;* Ακόμα και αν πρόκειται για τον ίδιο τύπο δεδομένων αν ο σκοπός για τον οποίο επεξεργάζονται διαφέρει, τότε πρέπει να αναπροσαρμοστεί το ρίσκο αναλόγως.
- *Ποια είναι τα μέσα με τα οποία γίνεται η επεξεργασία;* Αυτό σημαίνει ότι ο κίνδυνος διαφοροποιείται αν η επεξεργασία γίνεται με αυτοματοποιημένο μέσα ή όχι ή με συνδυασμό αυτών. Μπορεί επίσης η επιχείρηση να βασίζεται σε τεχνικά μέσα ενός τρίτου, π.χ. ενός παρόχου υπηρεσιών cloud.
- *Που λαμβάνει χώρα η επεξεργασία;* Αν η επεξεργασία των προσωπικών δεδομένων γίνεται σε χώρα εκτός Ευρωπαϊκής Ένωσης τότε πρέπει να ληφθούν επιπλέον μέσα προστασίας.
- *Ποια είναι η κατηγορία των υποκειμένων;* Για παράδειγμα αν η επεξεργασία αφορά προσωπικά δεδομένα ανηλίκων, τότε θα πρέπει να δίνεται ακόμα μεγαλύτερη προσοχή.
- *Ποιοι είναι οι παραλήπτες των δεδομένων;* Με τον ορισμό των παραληπτών είναι πιο εύκολο να κατανοήσει ο οργανισμός τις εξουσιοδοτημένες μεταφορές καθώς και τις συνθήκες μεταφοράς.

Κατανόηση και εκτίμηση της επίπτωσης ενός κινδύνου

Σε αυτό το βήμα ο οργανισμός θα πρέπει να εκτιμήσει τον πιθανό αντίκτυπο που μπορεί να έχει ένα περιστατικό ασφαλείας στα δικαιώματα και τις ελευθερίες των υποκειμένων. Η εκτίμηση αυτή μπορεί να είναι μόνο ποιοτική λόγω της ιδιαίτερης φύσης της επεξεργασίας των προσωπικών δεδομένων.

Επίπεδα αντικτύπου

Με βάση τις οδηγίες που έχουν δοθεί μέσα από τα «CNIL – Managing Privacy Risks Methodology» και «ENISA - Recommendations for a methodology of the assessment of severity of personal data breaches» τα επίπεδα αντικτύπου χωρίζονται σε τέσσερα επίπεδα όπως φαίνεται παρακάτω:

ΕΠΙΠΕΔΟ ΑΝΤΙΚΤΥΠΟΥ	ΠΕΡΙΓΡΑΦΗ
Χαμηλό	Τα υποκείμενα θα αντιμετωπίσουν κάποια προβλήματα τα οποία όμως θα αντιμετωπίσουν χωρίς δυσκολίες, όπως για παράδειγμα η επανάληψη εισαγωγής κάποιων στοιχείων σε ένα σύστημα.
Μεσαίο	Τα υποκείμενα θα αντιμετωπίσουν σημαντικά προβλήματα τα οποία θα ξεπεράσουν αντιμετωπίζοντας κάποιες δυσκολίες, όπως για παράδειγμα κάποια extra κόστη, άρνηση πρόσβασης σε υπηρεσίες, στρες κλπ.
Υψηλό	Τα υποκείμενα θα έχουν σημαντικές επιπτώσεις τις οποίες θα ξεπεράσουν αντιμετωπίζοντας σημαντικές δυσκολίες, όπως για παράδειγμα ζημιά στην περιουσία τους, απόλυση, επιπτώσεις στην υγεία τους κλπ.
Πολύ Υψηλό	Τα υποκείμενα θα έχουν σημαντικές επιπτώσεις που τις περισσότερες φορές δε θα μπορούν να αντιστρέψουν ή ξεπεράσουν, όπως για παράδειγμα αποκλεισμός από την αγορά εργασίας, θάνατος κλπ.

Πίνακας 1

Πως γίνεται η εκτίμηση της επίπτωσης

Όπως αναφέρθηκε και πιο πάνω η εκτίμηση της επίπτωσης μπορεί να είναι μόνο ποιοτική λαμβάνοντας υπόψη τις ιδιαιτερότητες στην επεξεργασία του συγκεκριμένου τύπου δεδομένων. Για να προκύψει ένα σωστό αποτέλεσμα πρέπει να ληφθούν υπόψη τα παρακάτω:

- *Ο τύπος των προσωπικών δεδομένων:* Αυτή η παράμετρος μπορεί αυτόματα να αυξήσει ή να μειώσει το επίπεδο επίπτωσης ανάλογα με την κρισιμότητα των δεδομένων. Για παράδειγμα αν τα δεδομένα περιλαμβάνουν ιατρικούς φακέλους ή πολιτικές πεποιθήσεις ή οποιαδήποτε άλλη ειδική κατηγορία σύμφωνα με τον

ΓΚΠΔ η επίπτωση ενός περιστατικού ασφαλείας μπορεί να είναι πολύ σοβαρή για τα υποκείμενα.

- *Η κρισιμότητα της ίδιας της επεξεργασίας ως διαδικασία:* Αυτό σημαίνει για παράδειγμα πως ιδιαίτερη προσοχή πρέπει να δοθεί στην επεξεργασία όταν αυτή γίνεται για ή μπορεί να οδηγήσει σε συστηματική παρακολούθηση των υποκειμένων.
- *Ο όγκος των προσωπικών δεδομένων που επεξεργάζονται:* Είναι λογικό, όσο περισσότερα δεδομένα εισάγονται και επεξεργάζονται από έναν οργανισμό, τόσο περισσότερες είναι οι απειλές που μπορεί να προκύψουν. Ο όγκος περιλαμβάνει δυο έννοιες:
    - την χρονική περίοδο που μπορεί να επηρεάσει ένα περιστατικό ασφαλείας (διαρροή δεδομένων μιας εβδομάδας σε αντίθεση με τη διαρροή δεδομένων ενός έτους)
    - το περιεχόμενο
- *Ειδικές περιπτώσεις υπευθύνου/εκτελούντος την επεξεργασία:* Αυτή η παράμετρος αναφέρεται στο πεδίο και το core business του οργανισμού, το οποίο με τη σειρά του σχετίζεται με το τι δεδομένα και πληροφορία αυτός αποκαλύπτει.
- *Ειδικές περιπτώσεις υποκειμένων:* Αν για παράδειγμα τα δεδομένα αφορούν ανηλίκους ή δημόσια πρόσωπα τότε αλλάζει και το επίπεδο του αντικτύπου.

Πέρα από τις προαναφερθείσες παραμέτρους, θα πρέπει να λαμβάνεται υπόψη και το κατά πόσο τα υποκείμενα μπορούν να ταυτοποιηθούν από τα δεδομένα που είναι διαθέσιμα, είτε αυτή η ταυτοποίηση είναι άμεση είτε όχι. Επίσης θα πρέπει να λαμβάνονται μέτρα για την μη αναγνωσιμότητα των δεδομένων σε περίπτωση μη εξουσιοδοτημένης πρόσβασης ή αποκάλυψης.

Κατά τη διάρκεια εκτίμησης αντικτύπου θα πρέπει να λαμβάνονται υπόψη και δευτερεύοντες επιπτώσεις. Αν για παράδειγμα η επεξεργασία περιλαμβάνει usernames και κωδικούς και δεδομένου ότι οι χρήστες τείνουν να χρησιμοποιούν τα ίδια usernames και κωδικούς σε πολλαπλές υπηρεσίες τότε το επίπεδο αντικτύπου αλλάζει αναλόγως.

Εκτίμηση της επίπτωσης

Η επίπτωση εκτιμάται ξεχωριστά για κάθε μία από τις τρεις αρχές της ασφάλειας (εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα) και με βάση το χειρότερο σενάριο. Το εκάστοτε τμήμα του οργανισμού και για τα δεδομένα που το αφορούν, μπορεί να απαντήσει στο παρακάτω ερωτηματολόγιο:

ΕΡΩΤΗΣΗ	ΕΚΤΙΜΗΣΗ ΕΠΙΠΤΩΣΗΣ
Τι επίπτωση θα έχει μια μη εξουσιοδοτημένη αποκάλυψη προσωπικών δεδομένων (εμπιστευτοκότητα) για ένα υποκείμνο; ***Σενάρια:*** *Ένα αρχείο hardcopy ή ένα laptop χάνονται κατά τη μεταφορά.* *Ο εξοπλισμός έχει πεταχτεί χωρίς να ακολουθηθούν οι κατάλληλες διαδικασίες καταστροφής.* *Προσωπικά δεδομένα έχουν αποσταλλεί λανθασμένα σε μη εξουσιοδοτημένους παραλήπτες.* *Πελάτες μπορούν να έχουν πρόσβαση σε δεδομένα άλλων πελατών σε μια online υπηρεσία.* *Προσωπικά δεδομένα διατίθενται στο internet ή σε P2P υπηρεσίες* *Ένα μέσα αποθήκευσης με δεδομένα πελατών έχει κλαπεί από τις εγκαταστάσεις.*	☐Χαμηλή ☐Μεσαία ☐Υψηλή ☐Πολύ Υψηλή
Τι επίπτωση θα έχει μια μη εξουσιοδοτημένη μεταβολή των δεδομένων (ακεραιότητα) για ένα υποκείμενο; ***Σενάρια:*** *Μία καταχώρηση που είναι απαραίτητη για την χρήση μιας online υπηρεσίας τροποποιήθηκε και ένα υποκείμενο πρέπει να τη ζητήσει offline.* *Μία καταχώρηση που είναι σημαντική για την ακρίβεια του ιατρικού φακέλου ενός υποκειμένου τροποποιήθηκε.*	☐Χαμηλή ☐Μεσαία ☐Υψηλή ☐Πολύ Υψηλή
Τι επίπτωση θα έχει μια μη εξουσιοδοτημένη καταστροφή ή απώλεια των δεδομένων (διαθεσιμότητα) για ένα υποκείμενο; ***Σενάρια:*** *Μια βάση δεδομένων πελατών έχει αλλοιωθεί και απαιτείται διαδικασία επαναφοράς για τη λειτουργία της υπηρεσίας.* *Ένα αρχείο προσωπικού χάθηκε και τα υποκείμενα πρέπει να συγκεντρώσουν ξανά έγγραφα και πληροφορία για την εταιρεία.* *Ένα αρχείο ή μια βάση δεδομένων έχει αλλοιωθεί και δεν υπάρχει αντίγραφο ασφαλείας.* *Μια κρίσιμη υπηρεσία έχει "πέσει" και δε μπορεί να επανέλθει άμεσα.*	☐Χαμηλή ☐Μεσαία ☐Υψηλή ☐Πολύ Υψηλή

Πίνακας 2

Αφού απαντηθεί το συγκεκριμένο ερωτηματολόγιο θα προκύψουν τρία διαφορετικά επίπεδα επίπτωσης (για κάθε μια αρχή). Το υψηλότερο από αυτά θα πρέπει να θεωρηθεί ως το τελικό αποτέλεσμα στην εκτίμηση αντικτύπου.

Η αντιστοίχιση του συνολικού βαθμού με τη συνολική επίπτωση ακολουθεί το παρακάτω μοτίβο:

- ***Βαθμός 1: Χαμηλή επίπτωση***
- ***Βαθμός 2: Μεσαία επίπτωση***

- ***Βαθμός 3: Υψηλή/Πολύ Υψηλή επίπτωση***

Ορισμός των πιθανών απειλών και εκτίμηση της πιθανότητας να εμφανιστούν.

Με τον όρο απειλή εννοούμε κάθε γεγονός που μπορεί να επηρεάσει αρνητικά την ασφάλεια των προσωπικών δεδομένων. Σε αυτό το βήμα λοιπόν ο οργανισμός θα πρέπει να κατανοήσει τις απειλές σε όλο τον κύκλο της επεξεργασίας και να εκτιμήσει την πιθανότητα να εμφανιστούν.

Μερικά παραδείγματα απειλών σε προσωπικά δεδομένα είναι τα παρακάτω:

i. Ένας επιτιθέμενος εισάγει κώδικα στη φόρμα ενός website, σκοπεύοντας να αποκτήσει πρόσβαση σε προσωπικά δεδομένα που φυλάσσονται στο σύστημα.
ii. Ένας επιτιθέμενος πραγματοποιεί μια man in the middle επίθεση με σκοπό να υποκλέψει μια επικοινωνία.
iii. Ένας υπάλληλος κλέβει αρχεία από το εσωτερικό σύστημα.
iv. Ένας υπάλληλος νοσοκομείου, κατά λάθος ή εσκεμμένα, αλλάζει μια παράμετρο στον ιατρικό φάκελο ενός ασθενή.
v. Λόγω μιας διακοπής ρεύματος, η βάση δεδομένων πελατών δεν είναι προσβάσιμη.
vi. Ένα USB με προσωπικά δεδομένα, χάνεται κατά τη μεταφορά.

Διαδικασία εκτίμησης απειλών

Με σκοπό την απλοποίηση της διαδικασίας ορίστηκε ένας αριθμός ερωτήσεων που μπορούν να βοηθήσουν τον οργανισμό είτε είναι υπεύθυνος είτε εκτελών την επεξεργασία να κατανοήσει τις απειλές και να υπολογίσει την πιθανότητα εμφάνισης τους και βασίζονται σε τέσσερις βασικούς άξονες.

Δίκτυο και τεχνολογικοί πόροι: Η διασύνδεση με το δίκτυο μπορεί να επιφέρει απειλές τόσο από εξωτερικούς παράγοντες όσο και από εσωτερικούς. Το ίδιο συμβαίνει και με τους τεχνολογικούς πόρους αν αυτοί δε συντηρούνται σωστά, ή δεν έχει γίνει σωστό configuration ή υπάρχουν backdoors. Οι πιο συνήθεις απειλές σχετικά με τον συγκεκριμένο τομέα είναι οι παρακάτω:

- υποκλοπή των καναλιών επικοινωνίας
- μη εξουσιοδοτημένη πρόσβαση σε βάσεις δεδομένων

- μη διαθεσιμότητα υπηρεσιών
- απώλεια επικοινωνιών
- κακή χρήση των συστημάτων

Διαδικασίες και διεργασίες σχετικά με την επεξεργασία δεδομένων: Πολλές φορές απειλές προκύπτουν από τη μη ύπαρξη σωστών εσωτερικών διαδικασιών και διεργασιών, με αποτέλεσμα κανόνες και πρακτικές να παρακάμπτονται. Οι πιο συνήθεις απειλές σχετικά με τον συγκεκριμένο τομέα είναι οι παρακάτω:

- πρόσβαση σε δεδομένα από μη εξουσιοδοτημένο προσωπικό
- εσκεμμένη ή μη αλλοίωση δεδομένων
- μη εξουσιοδοτημένη τροποποίηση ή καταστροφή δεδομένων
- απώλεια εξοπλισμού που επεξεργάζεται δεδομένα

Συμμετοχή πολλών μερών στην επεξεργασία δεδομένων: Υπάρχει περίπτωση πολλοί υπάλληλοι ενός οργανισμού να εμπλέκονται στην επεξεργασία δεδομένων, καθώς και εξωτερικοί συνεργάτες. Οι πιο συνήθεις απειλές σχετικά με τον συγκεκριμένο τομέα είναι οι παρακάτω:

- μη εσκεμμένη χρήση προσωπικών δεδομένων λόγω ανθρωπίνου λάθους
- μη εξουσιοδοτημένη αποκάλυψη δεδομένων από εξωτερικούς συνεργάτες

Τομέας της επιχείρησης και έκταση της επεξεργασίας: Αν τα προσωπικά δεδομένα ενός οργανισμού θεωρούνται ένα πολύτιμο αγαθό ή η επεξεργασία αφορά όλο τον πληθυσμό μιας χώρας τότε είναι πιο πιθανό να απειληθεί από εξωτερικούς επιτιθέμενους που θα ήθελα να έχουν πρόσβαση σε τέτοιους πόρους.

Παρακάτω υπάρχουν κάποιες ερωτήσεις ανά άξονα, ώστε να γίνει καλύτερη εκτίμηση αντικτύπου συνοδευόμενες από σχετικά παραδείγματα. Επιπλέον μια θετική απάντηση σε κάθε μία από αυτές υποδηλώνει και υψηλότερο ρίσκο.

|A| ΔΙΚΤΥΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΚΟΙ ΠΟΡΟΙ	
1.	**Διενεργείται οποιοδήποτε μέρος της επεξεργασίας δεδομένων προσωπικού χαρακτήρα μέσω του διαδικτύου;** *Ένα e-shop που δίνει τη δυνατότητα online αγορών.* *Ένα site νέων που παρέχει προσωποποιημένη ενημέρωση στους χρήστες του.* *Ένα CRM που παρέχεται σαν υπηρεσία cloud.*	Όταν η επεξεργασία των προσωπικών δεδομένων διενεργείται πλήρως ή ένα μέρος αυτής μέσω του διαδικτύου, οι πιθανές απειλές από εξωτερικούς εισβολείς αυξάνονται (π.χ. Denial of Service, SQL injection, Man-in-the-Middle επιθέσεις), ειδικότερα όταν η υπηρεσία είναι διαθέσιμη σε όλους τους χρήστες του διαδικτύου.
2.	**Είναι πιθανό να δοθεί πρόσβαση σε ένα εσωτερικό σύστημα επεξεργασίας δεδομένων προσωπικού χαρακτήρα μέσω διαδικτύου (π.χ. για συγκεκριμένους χρήστες ή ομάδες χρηστών);** *Μια ασφαλιστική εταιρεία δίνει απομακρυσμένη πρόσβαση στους managers για να έχουν πρόσβαση σε στοιχεία πελατών.* *Μια συμβουλευτική εταιρεία επιτρέπει απομακρυσμένη πρόσβαση στους υπαλλήλους της.* *Μια εταιρεία επιτρέπει απομακρυσμένη πρόσβαση σε εξωτερικό συνεργάτη για συντήρηση των συστημάτων.*	Όταν δίνεται η δυνατότητα πρόσβασης σε ένα εσωτερικό σύστημα επεξεργασίας δεδομένων προσωπικού χαρακτήρα μέσω διαδικτύου, η πιθανότητα εξωτερικών απειλών αυξάνεται. Ταυτόχρονα η πιθανότητα (τυχαία ή σκόπιμη) κατάχρησης δεδομένων από τους χρήστες αυξάνεται επίσης (π.χ. τυχαία αποκάλυψη προσωπικών δεδομένων όταν εργάζονται σε δημόσιο χώρο). Ιδιαίτερη προσοχή θα πρέπει να δίνεται στις περιπτώσεις όπου επιτρέπεται η απομακρυσμένη διαχείριση/υποστήριξη του συστήματος IT.
3.	**Είναι το σύστημα επεξεργασίας δεδομένων προσωπικού χαρακτήρα διασυνδεμένο με άλλον εξωτερικό ή εσωτερικό συνεργάτη (του οργανισμό), IT σύστημα ή υπηρεσία;** *Ένα ηλεκτρονικό βιβλιοπωλείο που είναι συνδεδεμένο με ένα online σύστημα πληρωμών.* *Το ERP μιας μικρής κλινικής συνδέεται με το σύστημα του ασφαλιστικού τομέα.* *Ένα CRM συνδεδεμένο με σύστημα παραγγελιών και πληρωμών.*	Η σύνδεση με εξωτερικό IT σύστημα μπορεί να προκαλέσει επιπλέον απειλές στις ήδη υπάρχουσες (και ενδεχόμενα σφάλματα ασφαλείας). Το ίδιο ισχύει επίσης στα εσωτερικά συστήματα, λαμβάνοντας υπόψη ότι εάν δεν είναι ρυθμισμένα κατάλληλα, τέτοιες συνδέσεις μπορούν να επιτρέψουν την πρόσβαση στα προσωπικά δεδομένα σε περισσότερα άτομα μέσα από τον οργανισμό που στην πραγματικότητα δεν έχουν εξουσιοδότηση.

4.	**Μπορούν μη εξουσιοδοτημένα άτομα να έχουν εύκολη πρόσβαση στο περιβάλλον επεξεργασίας προσωπικών δεδομένων;** *Μια μικρομεσαία επιχείρηση δεν έχει τα συστήματα σε απομονωμένο computer room.* *Μια μικρομεσαία επιχείρηση δίνει τα δεδομένα για φύλαξη σε εξωτερικό συνεργάτη χωρίς να είναι σαφή τα μέτρα που αυτός παίρνει για τη διαφύλαξη τους.*	Παρόλο που έχει δοθεί έμφαση στα ηλεκτρονικά συστήματα και υπηρεσίες, το φυσικό περιβάλλον (που σχετίζεται με αυτά τα συστήματα και τις υπηρεσίες) είναι μία σημαντική πτυχή η οποία, εάν δεν προστατεύεται επαρκώς, μπορεί να διακινδυνεύσει την ασφάλεια (π.χ. επιτρέποντας σε μη εξουσιοδοτημένα μέρη να έχουν φυσική πρόσβαση στον IT εξοπλισμό καθώς και στα εξαρτήματα/μέρη του δικτύου ή αποτυγχάνοντας να παρέχει ασφάλεια στο data center στην περίπτωση φυσικών καταστροφών).
5.	**Ο σχεδιασμός, η εγκατάσταση και η συντήρηση του συστήματος επεξεργασίας δεδομένων προσωπικού χαρακτήρα ακολουθεί σχετικές καλές πρακτικές;** *Τα συστήματα είναι δομημένα με βάση συγκεκριμένες διαδικασίες IT και πρωτόκολλα.* *Το hardware και το software παρέχονται από αξιόπιστους συνεργάτες και έχουν ακολουθηθεί συγκεκριμένες διαδικασίες για την παραγωγή τους.* *Ακολουθείται συγκεκριμένο πλάνο συντήρησης.*	Ένας φτωχός σχεδιασμός, κατά την εγκατάσταση ή/και συντήρηση των μηχανημάτων ή λογισμικού μπορεί να δημιουργήσει σοβαρά προβλήματα στην ασφάλεια πληροφοριών. Για το σκοπό αυτό, οι καλές πρακτικές συσσωρεύουν την εμπειρία των προηγούμενων γεγονότων και μπορούν να θεωρηθούν ως πρακτικές οδηγίες για το πώς να αποφευχθεί η έκθεση σε απειλές και να επιτευχθεί συγκεκριμένο επίπεδο ανθεκτικότητας.

Πίνακας 3

|Β| ΔΙΕΡΓΑΣΙΕΣ / ΔΙΑΔΙΚΑΣΙΕΣ ΠΟΥ ΣΧΕΤΙΖΟΝΤΑΙ ΜΕ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ		
6.	**Είναι οι ρόλοι και οι αρμοδιότητες που σχετίζονται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα ασαφής ή μη καθαρά διατυπωμένα;** *Οι βοηθοί στο λογιστήριο του οργανισμού μπορούν πέρα από το να εισάγουν, να τροποποιήσουν ή να διαγράψουν πληροφορία όπως οι managers.* *Οι νοσοκόμες σε μια κλινική μπορούν να τροποποιήσουν τον φάκελο ενός ασθενή, ενώ κάτι τέτοιο θα ήταν επιτρεπτό μόνο από τους γιατρούς.*	Όταν οι ρόλοι και οι αρμοδιότητες δεν είναι καθαρά διατυπωμένες, η πρόσβαση (και οι περαιτέρω επεξεργασίες) στα δεδομένα προσωπικού χαρακτήρα μπορεί να γίνει ανεξέλεγκτη, με αποτέλεσμα τη μη πιστοποιημένη χρήση των πόρων, διακινδυνεύοντας την ασφάλεια του όλου συστήματος.

7.	**Είναι η αποδεκτή χρήση του δικτύου, συστήματος και φυσικών πόρων εντός του οργανισμού ασαφής/διφορούμενη ή δεν είναι σαφώς διατυπωμένη;** *Δεν είναι σαφές αν οι υπάλληλοι μπορούν να χρησιμοποιήσουν τα επαγγελματικά τους mail για προσωπικούς λόγους.* *Δεν υπάρχει πολιτική που να καθορίζει το bandwith που δικαιούται να χρησιμοποιήσει ο υπάλληλος κάθε μέρα.*	Όταν δεν υπάρχει σαφής οδηγία για την αποδεκτή χρήση των πόρων, απειλές ασφαλείας μπορεί να προκύψουν λόγω εσκεμμένης, ή μη, κακής χρήσης του συστήματος. Ο σαφής ορισμός των πολιτικών του δικτύου, συστήματος και φυσικών πόρων μπορεί να μειώσει τους πιθανούς κινδύνους.
8.	**Επιτρέπεται στους υπαλλήλους να φέρουν δικές τους συσκευές και να τις χρησιμοποιήσουν συνδεόμενοι με το σύστημα επεξεργασίας δεδομένων προσωπικού χαρακτήρα;** *Οι υπάλληλοι μπορούν να συνδεθούν στο δίκτυο της εταιρείας με τα tablets τους ή άλλες συσκευές.* *Οι υπάλληλοι μπορούν να επεξεργαστούν δεδομένα χρησιμοποιώντας εφαρμογές που είναι όμως εγκατεστημένες στις προσωπικές τους συσκευές.*	Οι υπάλληλοι που χρησιμοποιούν τις προσωπικές τους συσκευές εντός του οργανισμού μπορούν να αυξήσουν τον κίνδυνο διαρροής ή μη εξουσιοδοτημένης πρόσβασης στο σύστημα πληροφόρησης. Επιπλέον, επειδή οι συσκευές αυτές δεν ελέγχονται από το κεντρικό σύστημα, μπορεί να εισαγάγουν επιπρόσθετα σφάλματα ή ιούς στο σύστημα.
9.	**Επιτρέπεται στους υπαλλήλους να μεταφέρουν, να αποθηκεύσουν ή να επεξεργαστούν με άλλον τρόπο δεδομένα προσωπικού χαρακτήρα εκτός των εγκαταστάσεων του οργανισμού;** *Μια επιχείρηση επιτρέπει στους υπαλλήλους της να χρησιμοποιούν τα εταιρικά laptop τους εκτός για την επεξεργασία δεδομένων πελατών.* *Μια εταιρεία παραδόσεων επιτρέπει στους υπαλλήλους να χρησιμοποιούν συγκεκριμένα tablets από τα οποία επιβεβαιώνουν τα στοιχεία του παραλήπτη.*	Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα εκτός των εγκαταστάσεων του οργανισμού μπορεί να προσφέρει μεγάλη ευελιξία, αλλά την ίδια στιγμή εισαγάγει κινδύνους, τόσο σε σχέση με τη μεταφορά της πληροφορίας μέσω μη ασφαλών δικτύων/καναλιών (π.χ. ανοικτό δίκτυο Wi-Fi), όσο και σε μη εξουσιοδοτημένη χρήση της πληροφορίας.
10.	**Μπορούν οι δραστηριότητες επεξεργασίας δεδομένων προσωπικού χαρακτήρα να διεξαχθούν χωρίς τη δημιουργία log files;** *Δεν υπάρχει λίστα ατόμων που έχουν πρόσβαση στο computer room καθημερινά.*	

	Η πρόσβαση στους ιατρικούς φακέλους μιας κλινικής δεν καταγράφεται. *Δεν υπάρχει πολιτική που να αναφέρει πως θα γίνονται monitor τα logs και τι γίνεται σε περίπτωση παραβιάσεων.*	Η έλλειψη κατάλληλων μηχανισμών καταγραφής και παρακολούθησης μπορεί να αυξήσει την σκόπιμη ή τυχαία κατάχρηση των πόρων, που έχει ως επακόλουθο την κατάχρηση των δεδομένων προσωπικού χαρακτήρα.

Πίνακας 4

|Γ| ΟΜΑΔΕΣ/ ΑΤΟΜΑ ΠΟΥ ΕΜΠΛΕΚΟΝΤΑΙ ΣΤΗ ΔΙΑΔΙΚΑΣΙΑ ΕΠΕΞΕΡΓΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ		
11.	**Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα διεξάγεται από μη καθορισμένο αριθμό υπαλλήλων;** *Το σύστημα του HR είναι προσβάσιμο από όλους τους υπαλλήλους.* *Ιατρικά αρχεία μπορούν να επεξεργαστούν από τη γραμματεία ενώ μόνο συγκεκριμένο προσωπικό μπορεί.*	Όταν η πρόσβαση (και η περαιτέρω επεξεργασία) των δεδομένων προσωπικού χαρακτήρα είναι ανοικτή σε μεγάλο αριθμό υπαλλήλων, η πιθανότητα κακής διαχείρισης λόγω ανθρώπινου παράγοντα αυξάνονται. Πρέπει να καθοριστεί σαφώς ποιος πραγματικά χρειάζεται να έχει πρόσβαση στα δεδομένα προσωπικού χαρακτήρα και να περιοριστεί η πρόσβαση μόνο σε αυτούς που μπορούν να συνεισφέρουν στην ασφάλεια τον δεδομένων προσωπικού χαρακτήρα.
12.	**Διεξάγεται κάποιο μέρος της διαδικασίας επεξεργασίας από υπεργολάβο/τρίτο μέρος;** *Το σύστημα ενός ιδιωτικού σχολείου είναι hosted σε εξωτερικό data center.* *Τα αρχεία πελατών μιας ασφαλιστικής μπορούν να επεξεργαστούν από εξωτερικούς συνεργάτες.* *Μια εξειδικευμένη εταιρεία έχει αναλάβει την καταστροφή του αρχείου των ασθενών μιας κλινικής.* *Μια εταιρεία χρησιμοποιεί μια cloud υπηρεσία για τη διαχείριση των πόρων της.*	Όταν η διαδικασία εκτελείται από εξωτερικό υπεργολάβο, ο οργανισμός μπορεί να χάσει εν μέρει τον έλεγχο των δεδομένων. Επιπλέον, επιπρόσθετες απειλές μπορεί να εμφανιστούν λόγω των ενυπαρχόντων στους υπεργολάβους. Είναι σημαντικό για τον οργανισμό να επιλέξει υπεργολάβους, οι οποίοι μπορούν να προσφέρουν υψηλό επίπεδο ασφαλείας και να καθορίσουν σαφώς ποιο κομμάτι της διαδικασίας τους έχει ανατεθεί, διατηρώντας έτσι όσο το δυνατόν υψηλό επίπεδο ελέγχου.
13.	**Είναι οι υποχρεώσεις των μερών/ατόμων που εμπλέκονται στη διαδικασία δεδομένων προσωπικού χαρακτήρα διφορούμενη ή μη σαφώς καθορισμένη;** *Οι υπάλληλοι δε γνωρίζουν ότι διαχειρίζονται εμπιστευτική πληροφορία.* *Οι εξωτερικοί συνεργάτες μιας εταιρείας δεν έχουν σαφής οδηγίες για το επίπεδο ασφάλειας που πρέπει να τηρούν σχετικά με τα δεδομένα που επεξεργάζονται.*	Όταν οι υπάλληλοι δεν είναι ξεκάθαρα ενημερωμένοι για τις υποχρεώσεις τους, απειλές από τυχαία κακή χρήση (π.χ. αποκάλυψη ή καταστροφή) των δεδομένων αυξάνουν σημαντικά.

14.	**Το προσωπικό που εμπλέκεται με τη διαδικασία δεδομένων προσωπικού χαρακτήρα είναι εξοικειωμένο με θέματα ασφαλείας πληροφοριών;** *Το προσωπικό που κάνει επεξεργασία προσωπικών δεδομένων δεν είναι ενημερωμένο για πιθανές απειλές και τη σωστή χρήση των πόρων.* *Οι υπάλληλοι ενός τηλεφωνικού κέντρου δεν είναι ενημερωμένοι για πιθανές επιθέσεις phishing.*	Όταν οι υπάλληλοι δεν γνωρίζουν την ανάγκη εφαρμογής μέτρων ασφαλείας, μπορούν να δημιουργήσουν κατά λάθος περαιτέρω απειλές για το σύστημα. Η εκπαίδευση μπορεί να συμβάλει τα μέγιστα στην ευαισθητοποίηση των υπαλλήλων τόσο για τις υποχρεώσεις προστασίας των δεδομένων τους, όσο και για την εφαρμογή ειδικών μέτρων ασφαλείας.
15.	**Τα άτομα/μέρη που εμπλέκονται στη διαδικασία δεδομένων προσωπικού χαρακτήρα αμελούν να αποθηκεύσουν με ασφάλεια ή/και να καταστρέψουν προσωπικά δεδομένα;** *Τα αρχεία του HR δεν είναι κλειδωμένα σε ντουλάπες.* *Αντίγραφα τιμολογίων με αριθμούς καρτών και λογαριασμών δεν καταστρέφονται καταλλήλως.*	Πολλές παραβιάσεις δεδομένων προσωπικού χαρακτήρα συμβαίνουν εξαιτίας της έλλειψης φυσικών μέτρων προστασίας. Τα χειρόγραφα αρχεία αποτελούν συνήθως μέρος της διαδικασίας εισαγωγής και εξαγωγής δεδομένων σε ένα σύστημα πληροφόρησης ενώ μπορεί να περιέχουν δεδομένα προσωπικού χαρακτήρα και θα έπρεπε επίσης να προστατεύονται από μη εξουσιοδοτημένη αποκάλυψη ή επαναχρησιμοποίηση.

Πίνακας 5

	|Δ| ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΣ ΤΟΜΕΑΣ ΚΑΙ ΚΛΙΜΑΚΑ ΕΠΕΞΕΡΓΑΣΙΑΣ	
16.	**Θεωρείτε ότι ο επιχειρηματικός σας τομέας είναι επιρρεπής σε διαδικτυακές εισβολές;** *Ένας μεγάλος αριθμός από εταιρείες του ίδιου τομέα δέχθηκαν επίθεση τη χρονιά που μας πέρασε.* *Έχουν δοθεί στη δημοσιότητα ευπάθειες του συγκεκριμένου τομέα.*	Όταν ένας συγκεκριμένος επιχειρηματικός τομέας έχει ήδη δεχθεί εισβολή στο σύστημα ασφαλείας, αυτό αποτελεί μία ένδειξη ότι ο οργανισμός έχει πιθανότατα την ανάγκη να λάβει επιπρόσθετα μέτρα με σκοπό να αποφύγει παρόμοια περιστατικά.
17.	**Έχει υποστεί ο οργανισμός σας κάποιου είδους διαδικτυακής εισβολής ή παραβίαση οποιουδήποτε άλλου είδους τα τελευταία δύο χρόνια;** *Έχουν ανακαλυφθεί πολλαπλές προσπάθειες εισόδου στη βάση δεδομένων από μη εξουσιοδοτημένα εξωτερικά συστήματα.* *Οι κλειδαριές στο data center έχουν παραβιαστεί.*	Εάν ο οργανισμός έχει ήδη δεχθεί επίθεση ή υπάρχουν ενδείξεις ότι αυτό έχει συμβεί, θα πρέπει να ληφθούν επιπρόσθετα μέτρα για να αποτρέψουν την δημιουργία παρόμοιων γεγονότων στο μέλλον.

18.	**Έχετε λάβει οποιαδήποτε ειδοποίηση ή/και παράπονα που να σχετίζονται με την ασφάλεια του συστήματος τεχνολογίας πληροφοριών που χρησιμοποιείται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα τα τελευταία χρόνια;** *Χρήστες ενός online καταστήματος έχουν ενημερώσει ότι μπορούν κατά λάθος να έχουν πρόσβαση σε λογαριασμούς άλλων χρηστών. Μετά από audit διαπιστώθηκε ότι η πολιτική κωδικών ασφαλείας είναι ανεπαρκής.*	Κενά ασφαλείας μπορούν να χρησιμοποιηθούν για την εκτέλεση εισβολών (δικτυακές ή φυσικές) στο σύστημα και τις υπηρεσίες. Τα αρχεία τέτοιων reports περιέχουν σημαντικές πληροφορίες σχετικά με τις ευπάθειες ασφαλείας που μπορούν να επηρεάσουν το προαναφερθέν σύστημα/υπηρεσίες θα πρέπει να ληφθούν υπόψη.
19.	**Σχετίζεται κάποια διαδικασία επεξεργασίας με μεγάλο όγκο υποκειμένων ή/και δεδομένων προσωπικού χαρακτήρα;** *Ένα online αρχείο ασθενών ενός νοσοκομείου που αποθηκεύει δεδομένα ασθενών με χρόνιες παθήσεις από όλη τη χώρα.* *Ένα online site γνωριμιών που αποθηκεύει στοιχεία εκατοντάδων χρηστών.*	Ο τύπος και ο όγκος των δεδομένων προσωπικού χαρακτήρα (κλίμακα) μπορεί να κάνει τη διαδικασία επεξεργασίας ελκυστική στους εισβολείς (λόγω της δεδομένης αξίας των συγκεκριμένων δεδομένων)
20.	**Υπάρχουν Καλές Πρακτικές Ασφαλείας στον επιχειρησιακό σας τομέα όπου δεν έχουν ακολουθηθεί επαρκώς;**	Τα Ειδικά Μέτρα Ασφαλείας ανά Τομέα συνήθως προσαρμόζονται στις ανάγκες (και κινδύνους) του κάθε Τομέα. Έλλειψη συμμόρφωσης με σχετικές Καλές Πρακτικές μπορεί να αποτελεί έναν δείκτη φτωχής διαχείρισης ασφαλείας.

Πίνακας 6

Εκτίμηση της πιθανότητας εμφάνισης της απειλής.

Όπως και στην περίπτωση της εκτίμησης της επίπτωσης, έτσι και εδώ η εκτίμηση της πιθανότητας εμφάνισης μπορεί να είναι μόνο ποιοτική, επομένως σύμφωνα με την προσέγγιση αυτής της μεθοδολογίας καθορίζονται τρία επίπεδα πιθανότητας εμφάνισης:

1. **Χαμηλό:** Η απειλή είναι δύσκολο να πραγματοποιηθεί.
2. **Μεσαίο:** Είναι δυνατόν η απειλή να πραγματοποιηθεί.
3. **Υψηλό:** Η απειλή πιθανότατα θα πραγματοποιηθεί.

Σε συνδυασμό λοιπόν με τις ερωτήσεις που παρουσιάστηκαν στους παραπάνω πίνακες ανά τομέα μπορεί να συμπληρωθεί και ο παρακάτω πίνακας. Πιο συγκεκριμένα αν σε κάποιο τομέα οι απαντήσεις είναι όλες **«όχι»**, τότε η πιθανότητα εμφάνισης αξιολογείται ως **χαμηλή**. Αν όλες είναι **«ναι»** τότε η πιθανότητα εμφάνισης αξιολογείται ως **υψηλή**.

Αν πάλι δυο με τρεις απαντήσεις είναι **«ναι»** τότε η πιθανότητα εμφάνισης αξιολογείται ως **μέτρια**.

ΤΟΜΕΑΣ ΤΟΥ ΟΡΓΑΝΙΣΜΟΥ	ΠΙΘΑΝΟΤΗΤΑ	
	Επίπεδο	Τιμή
ΔΙΚΤΥΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΚΟΙ ΠΟΡΟΙ	Χαμηλό	1
	Μεσαίο	2
	Υψηλό	3
ΔΙΕΡΓΑΣΙΕΣ / ΔΙΑΔΙΚΑΣΙΕΣ ΠΟΥ ΣΧΕΤΙΖΟΝΤΑΙ ΜΕ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ	Χαμηλό	1
	Μεσαίο	2
	Υψηλό	3
ΟΜΑΔΕΣ/ ΑΤΟΜΑ ΠΟΥ ΕΜΠΛΕΚΟΝΤΑΙ ΣΤΗ ΔΙΑΔΙΚΑΣΙΑ ΕΠΕΞΕΡΓΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ	Χαμηλό	1
	Μεσαίο	2
	Υψηλό	3
ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΣ ΤΟΜΕΑΣ ΚΑΙ ΚΛΙΜΑΚΑ ΕΠΕΞΕΡΓΑΣΙΑΣ	Χαμηλό	1
	Μεσαίο	2
	Υψηλό	3

Πίνακας 7

Η τελική τιμή της πιθανότητας εμφάνισης υπολογίζεται ως το άθροισμα των διαφορετικών τιμών για κάθε τομέα της επιχείρησης. Η αντιστοίχιση με το τελικό αποτέλεσμα φαίνεται στον παρακάτω πίνακα.

ΕΥΡΟΣ ΤΙΜΩΝ ΠΙΘΑΝΟΤΗΤΑΣ ΕΜΦΑΝΙΣΗΣ ΑΠΕΙΛΗΣ	ΕΠΙΠΕΔΟ ΠΙΘΑΝΟΤΗΤΑΣ ΕΜΦΑΝΙΣΗΣ ΑΠΕΙΛΗΣ
4-5	Χαμηλό
6-8	Μεσαίο
9-12	Υψηλό

Πίνακας 8

Εκτίμηση του κινδύνου συνδυάζοντας την πιθανότητα αυτός να εμφανιστεί με την επίπτωση που μπορεί να έχει.

Έχοντας λοιπόν υπολογίσει το επίπεδο επίπτωσης που θα έχει μια απειλή στον οργανισμό καθώς και το επίπεδο πιθανότητας εμφάνισης, μπορεί πλέον να εκτιμηθεί το επίπεδο του κινδύνου.

		ΕΠΙΠΕΔΟ ΕΠΙΠΤΩΣΗΣ		
		Χαμηλό	Μεσαίο	Υψηλό/Πολύ Υψηλό
Πιθανότητα εμφάνισης απειλής	Χαμηλό			
	Μεσαίο			
	Υψηλό			

Πίνακας 9

Όπου:

- Χαμηλός κίνδυνος
- Μεσαίος κίνδυνος
- Υψηλός κίνδυνος

Μέτρα ασφαλείας

Αφού ολοκληρωθεί η εκτίμηση του κινδύνου ο οργανισμός μπορεί να επιλέξει τα κατάλληλα μέτρα ασφαλείας για την προστασία των προσωπικών δεδομένων και όπως έχει αναφερθεί και στην αρχή της περιγραφής της μεθοδολογίας, αυτά τα μέτρα μπορεί να είναι είτε **οργανωτικά** είτε **τεχνικά**. Αυτά με τη σειρά τους έχουν χωριστεί σε μικρότερες κατηγορίες η κάθε μία από τις οποίες εφαρμόζεται ανάλογα με το επίπεδο κινδύνου που έχει αναγνωριστεί. Μέτρα που σχετίζονται με χαμηλό κίνδυνο είναι εφαρμόσιμα σε όλα τα επίπεδα κινδύνων, μέτρα που σχετίζονται με μεσαίο κίνδυνο στα επίπεδα μεσαίο και υψηλό, ενώ αυτά που σχετίζονται με υψηλό κίνδυνο, μόνο με το υψηλό επίπεδο.

Φυσικά σε κάθε κίνδυνο μπορούν να αντιστοιχιστούν περισσότερα του ενός μέτρα, αναλόγως με το επίπεδο κινδύνου. Ταυτόχρονα τα μέτρα που αναφέρονται έχουν αντιστοιχιστεί με τα μέτρα που προτείνονται από το πρότυπο 27001:2013, κάτι που δίνει τη δυνατότητα στον οργανισμό να προχωρήσει σε ένα gap analysis σε περίπτωση που είναι ήδη πιστοποιημένος στο συγκεκριμένο πρότυπο.

Οργανωτικά μέτρα

Πολιτικές ασφαλείας και διαδικασίες για την προστασία των προσωπικών δεδομένων

A.1	Η εταιρεία θα πρέπει να τεκμηριώνει την πολιτική της σε ότι αφορά την επεξεργασία των προσωπικών δεδομένων ως μέρος της πολιτικής ασφαλείας πληροφοριών.	
A.2	Η πολιτική ασφάλειας θα πρέπει να επανεξετάζεται και να αναθεωρείται, εάν είναι απαραίτητο, σε ετήσια βάση.	
A.3	Η εταιρεία θα πρέπει να τηρεί ξεχωριστή πολιτική ασφαλείας για τα προσωπικά δεδομένα η οποία να έχει εγκριθεί από τη Διοίκηση και να έχει διανεμηθεί προς ενημέρωση σε όλο το προσωπικό της εταιρείας και τους τρίτους που σχετίζονται με την επεξεργασία των προσωπικών δεδομένων.	
A.4	Η πολιτική ασφαλείας θα πρέπει να περιέχει κατ' ελάχιστο: ρόλοι και αρμοδιότητες προσωπικού, το επίπεδο των τεχνικών και οργανωτικών μέτρων που έχουν ληφθεί για την προστασία των προσωπικών δεδομένων, τους εκτελούντες και τους αποδέκτες.	
A.5	Βάσει της γενικής πολιτικής ασφαλείας θα πρέπει να δημιουργηθεί και να διατηρείται κατάλογος πολιτικών και διαδικασιών που σχετίζονται με τα προσωπικών δεδομένων.	
A.6	Η πολιτική ασφάλειας πρέπει να επανεξετάζεται και αναθεωρείται, εάν είναι απαραίτητο ανά εξάμηνο.	
ISO 27001:2013 – § A.5 Πολιτική Ασφαλείας		

Ρόλοι και υποχρεώσεις

Σύμφωνα με το άρθρο 32 του ΓΚΠΔ και την παράγραφο 4: «*Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία λαμβάνουν μέτρα ώστε να διασφαλίζεται ότι κάθε φυσικό πρόσωπο που ενεργεί υπό την εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία το οποίο έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα τα επεξεργάζεται μόνο κατ' εντολή του υπευθύνου επεξεργασίας, εκτός εάν υποχρεούται προς τούτο από το δίκαιο της Ένωσης ή του κράτους μέλους.*»

B.1	Ρόλοι και ευθύνες που σχετίζονται με επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να ορίζονται σαφώς και να κατανέμονται σύμφωνα με την πολιτική ασφαλείας.	
B.2	Κατά τη διάρκεια εσωτερικών αναδιοργανώσεων ή λήξη συνεργασιών και αλλαγών προσωπικού θα πρέπει να καθορίζεται με σαφείς διαδικασίες η ανάκληση δικαιωμάτων και αρμοδιοτήτων.	
B.3	Σαφής καθορισμός αρμοδίων επί των θεμάτων ασφαλείας συμπεριλαμβανομένου του Υπευθύνου Ασφαλείας.	

B.4	Ο καθορισμός του υπευθύνου ασφαλείας πρέπει να τεκμηριώνεται. Τα καθήκοντα και οι αρμοδιότητες του υπεύθυνου ασφαλείας πρέπει επίσης να είναι σαφώς καθορισμένα και τεκμηριωμένα.
B.5	Τα συγκρουόμενα καθήκοντα και πεδία ευθύνης, για παράδειγμα ο ρόλος του υπεύθυνου ασφαλείας, του επιθεωρητή ασφάλειας και του DPO, θα πρέπει να διαχωρίζονται ώστε να ελαχιστοποιούνται οι περιπτώσεις μεταβολών ή κατάχρησης προσωπικών δεδομένων λόγω αμέλειας ή μη εξουσιοδοτημένης χρήσης.
ISO 27001:2013 – § A.6.1.1 Ρόλοι και αρμοδιότητες για την ασφάλεια πληροφορίας	

Πολιτική ελέγχου πρόσβασης

Σύμφωνα με τον ΓΚΠΔ η πρόσβαση στα συστήματα που επεξεργάζονται προσωπικά δεδομένα θα πρέπει να χορηγείται μόνο σε εξουσιοδοτημένα άτομα.

C.1	Η κατανομή των δικαιωμάτων πρόσβασης σε ρόλους που εμπλέκονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα) θα πρέπει να ακολουθεί την αρχή «Ανάγκη Γνώσης».
C.2	Η πολιτική ελέγχου προσβάσεων θα πρέπει να είναι αναλυτική και τεκμηριωμένη. Εντός της οποίας να καθορίζονται οι κατάλληλοι κανόνες ελέγχου πρόσβασης, δικαιώματα πρόσβασης και περιορισμούς για συγκεκριμένους ρόλους χρηστών σε σχέση με την επεξεργασία και διαδικασίες που σχετίζονται με τα προσωπικά δεδομένα.
C.3	Ο διαχωρισμός των ρόλων ελέγχου πρόσβασης (π.χ. αίτημα πρόσβασης, εξουσιοδότηση πρόσβασης, διαχείριση πρόσβασης) θα πρέπει να είναι σαφής και να τεκμηριώνεται.
C.4	Οι ρόλοι που συγκεντρώνουν υψηλού επιπέδου δικαιώματα πρόσβασης πρέπει να είναι σαφώς ορισμένοι και να δίνονται σε περιορισμένο αριθμό προσωπικού.
ISO 27001:2013 – § A.9.1.1 Πολιτική ελέγχου πρόσβασης	

Διαχείριση πόρων

D.1	Η εταιρεία θα πρέπει να διατηρεί αρχείο των παγίων που χρησιμοποιούνται για την επεξεργασία δεδομένων προσωπικού χαρακτήρα (υλικό, λογισμικό και δίκτυο). Η λίστα παγίων θα μπορούσε να περιλαμβάνει κατ' ελάχιστο: κατηγορία παγίων IT (π.χ. server, workstation), σημείο τήρησης (φυσικό ή ηλεκτρονικό). Θα πρέπει να καθοριστεί ο αρμόδιος διατήρησης και επικαιροποίησης αρχείου (π.χ. IT officer).
D.2	Τα πάγια του IT θα πρέπει να ελέγχονται και να ενημερώνονται σε τακτική βάση.

D.3	Οι ρόλοι με πρόσβαση σε πηγές δεδομένων πρέπει να καθορίζονται και να τεκμηριώνονται σαφώς.	
D.4	Τα πάγια θα πρέπει να ελέγχονται και να συντηρούνται/ενημερώνονται ετησίως.	
ISO 27001:2013 – § A.8 Διαχείριση πόρων		

Διαχείριση αλλαγών

E.1	Θα πρέπει να καθοριστεί υπεύθυνος καταγραφής και παρακολούθησης όλων των αλλαγών του πληροφοριακού συστήματος (π.χ. IT ή security officer). Η παρακολούθηση αυτής της διαδικασίας θα πρέπει να γίνεται συστηματικά.	
E.2	Η ανάπτυξη λογισμικού θα πρέπει γίνεται σε ειδικό περιβάλλον το οποίο δεν θα πρέπει να συνδέεται με το πληροφοριακό σύστημα που χρησιμοποιείται για την επεξεργασία προσωπικών δεδομένων. Όταν απαιτείται δοκιμή, πρέπει να χρησιμοποιούνται demo δεδομένα. Σε περιπτώσεις που αυτό δεν είναι εφικτό, τότε θα πρέπει να εφαρμόζονται ειδικές διαδικασίες για την προστασία των δεδομένων προσωπικού χαρακτήρα που χρησιμοποιούνται στη δοκιμή.	
E.3	Θα πρέπει να τηρείται λεπτομερής και τεκμηριωμένη πολιτική αλλαγών. Θα πρέπει να περιλαμβάνει: διαδικασία εισαγωγής αλλαγής, ρόλους/χρήστες με δικαίωμα αλλαγών και χρονοδιαγράμματα για την εισαγωγή των αλλαγών. Η πολιτική αλλαγών θα πρέπει να επικαιροποιείται τακτικά.	
ISO 27001:2013 – § A.12.1 Διαδικασίες και υποχρεώσεις		

Εκτελούντες την επεξεργασία

Σύμφωνα με το άρθρο 28, παράγραφο 1 του ΓΚΠΔ: «*Όταν η επεξεργασία πρόκειται να διενεργηθεί για λογαριασμό υπευθύνου επεξεργασίας, ο υπεύθυνος επεξεργασίας χρησιμοποιεί μόνο εκτελούντες την επεξεργασία που παρέχουν επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων, κατά τρόπο ώστε η επεξεργασία να πληροί τις απαιτήσεις του παρόντος κανονισμού και να διασφαλίζεται η προστασία των δικαιωμάτων του υποκειμένου των δεδομένων.*»

F.1	Οι οδηγίες και διαδικασίες που καλύπτουν την επεξεργασία προσωπικών δεδομένων από τους εκτελούντες (εργολάβοι / εξωτερικοί συνεργάτες) πρέπει είναι σαφώς καθορισμένες, τεκμηριωμένες και να έχουν συμφωνηθεί μεταξύ του υπευθύνου και του εκτελούντα την επεξεργασία πριν την έναρξη των ενεργειών επεξεργασίας. Αυτές οι οδηγίες και διαδικασίες πρέπει να εφαρμόζουν υποχρεωτικά στο ίδιο επίπεδο ασφαλείας προσωπικών δεδομένων σύμφωνα με την πολιτική ασφαλείας της εταιρείας.	

F.2	Σε περίπτωση εντοπισμού παραβίασης προσωπικών δεδομένων ο εκτελών οφείλει να ενημερώσει τον υπεύθυνο επεξεργασίας χωρίς περαιτέρω καθυστέρηση.	
F.3	Οι απαιτήσεις και υποχρεώσεις μεταξύ του υπεύθυνου και του εκτελούντα την επεξεργασία θα πρέπει να συμφωνηθούν επισήμως. Ο εκτελών θα πρέπει να παρέχει επαρκή τεκμηρίωση συμμόρφωσης.	
F.4	Θα πρέπει να διενεργούνται τακτικές επιθεωρήσεις του εκτελούντα ώστε να ελέγχεται το επίπεδο συμμόρφωσης επί των συμφωνηθέντων απαιτήσεων και των υποχρεώσεων από τον υπεύθυνο επεξεργασίας.	
F.5	Οι εργαζόμενοι του εκτελούντα την επεξεργασία πρέπει δεσμεύονται μέσω συμφωνητικών εμπιστευτικότητας και τήρησης απορρήτου.	
ISO 27001:2013 – § A.15 Σχέσεις με παρόχους		

Διαχείριση περιστατικών ασφαλείας

G.1	Θα πρέπει να καθοριστεί σχέδιο αντιμετώπισης περιστατικών που σχετίζονται με προσωπικά δεδομένα το οποίο να περιλαμβάνει λεπτομερείς διαδικασίες ώστε να διασφαλιστεί η αποτελεσματική και ορθή αντιμετώπιση τους.	
G.2	Οι παραβιάσεις δεδομένων προσωπικού χαρακτήρα θα πρέπει να αναφέρονται άμεσα στη διοίκηση. Οι διαδικασίες κοινοποίησης της αναφοράς του συμβάντος παραβίασης στις αρμόδιες αρχές και στα υποκείμενα των δεδομένων πρέπει να ακολουθούν τα άρθρα 33 και 34 του ΓΚΠΔ.	
G.3	Το σχέδιο αντιμετώπισης περιστατικών θα πρέπει να τεκμηριώνεται και να περιλαμβάνει όλες τις πιθανές ενέργειες μετριασμού και σαφή καθορισμό αρμοδιοτήτων.	
G.4	Τα περιστατικά παραβίασης δεδομένων προσωπικού χαρακτήρα πρέπει να καταγράφονται με λεπτομέρειες σχετικά με το περιστατικό και τις επόμενες ενέργειες μετριασμού που θα υλοποιηθούν.	
ISO 27001:2013 – § A.16 Διαχείριση περιστατικών ασφαλείας		

Επιχειρησιακή συνέχεια

H.1	Η εταιρεία θα πρέπει να διασφαλίσει ότι οι βασικές διαδικασίες και έλεγχοι τηρούνται ώστε να διασφαλίζεται το απαιτούμενο επίπεδο συνέχειας και διαθεσιμότητας του πληροφοριακού συστήματος επεξεργασίας προσωπικών δεδομένων σε περίπτωση συμβάντος/παραβίασης προσωπικών δεδομένων.	

H.2	Ένα BCP πρέπει να είναι λεπτομερές και τεκμηριωμένο (σύμφωνα με τη γενική πολιτική ασφαλείας). Θα πρέπει να περιλαμβάνει σαφείς ενέργειες και καθορισμό αρμοδιοτήτων.	
H.3	Το επίπεδο ποιότητας υπηρεσιών των βασικών τομέων δραστηριότητας θα πρέπει να καθορίζεται από το BCP και να παρέχει επαρκή προστασία των προσωπικών δεδομένων.	
H.4	Πρέπει να καθοριστεί εξειδικευμένο προσωπικό με την απαραίτητη ευθύνη, αρμοδιότητα και ικανότητα για τη διαχείριση της επιχειρηματικής συνέχειας σε περίπτωση περιστατικού παραβίασης δεδομένων προσωπικού χαρακτήρα.	
H.5	Θα πρέπει να καθοριστεί εφεδρική μονάδα παροχής ενέργειας βάσει της εταιρείας και του αποδεκτού χρόνου διακοπής λειτουργίας του πληροφοριακού συστήματος.	
ISO 27001:2013 – § A.17 Επιχειρησιακή συνέχεια στην ασφάλεια πληροφορίας		

Προσωπικό και εμπιστευτικότητα

I.1	Ο οργανισμός θα πρέπει να εξασφαλίσει ότι όλοι οι εργαζόμενοι τους κατανοούν τις αρμοδιότητες και υποχρεώσεις που σχετίζονται με την επεξεργασία των προσωπικών δεδομένων. Οι ρόλοι και αρμοδιότητες πρέπει να κοινοποιούνται με σαφήνεια κατά τη διάρκεια ένταξης νέων εργαζομένων ή κατά την περίοδο δοκιμαστικής εργασίας .	
I.2	Πριν από την ανάληψη των καθηκόντων τους οι εργαζόμενοι πρέπει να κληθούν να επανεξετάσουν και να συμφωνήσουν με την πολιτική ασφαλείας της εταιρείας και να υπογράψουν τα αντίστοιχα συμφωνητικά εμπιστευτικότητας και τήρησης απορρήτου.	
I.3	Οι υπάλληλοι που εμπλέκονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα με υψηλό κίνδυνο πρέπει να δεσμεύονται με συγκεκριμένες ρήτρες εμπιστευτικότητας (μέσα στη σύμβαση εργασίας τους ή άλλη νομική πράξη).	
ISO 27001:2013 – § A.7 Ασφάλεια ανθρωπίνου δυναμικού.		

Εκπαίδευση

J.1	Η εταιρεία θα πρέπει να διασφαλίσει ότι όλοι οι εργαζόμενοι είναι επαρκώς ενημερωμένοι σχετικά με τους ελέγχους ασφαλείας του πληροφοριακού συστήματος που σχετίζεται με την καθημερινή εργασία τους. Οι εργαζόμενοι που εμπλέκονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει επίσης να είναι κατάλληλα ενημερωμένοι για τις σχετικές απαιτήσεις προστασίας δεδομένων προσωπικού χαρακτήρα καθώς και τις νομικές υποχρεώσεις μέσω προγραμματισμένων εκπαιδεύσεων.	

J.2	Η εταιρεία θα πρέπει προγραμματίζει και να υλοποιεί εκπαιδεύσεις επί των θεμάτων που σχετίζονται με την προστασία των προσωπικών δεδομένων όπως επίσης και εισαγωγικές εκπαιδεύσεις για τους νεοπροσληφθέντες.
J.3	Σχέδιο εκπαίδευσης με καθορισμένους στόχους και σκοπούς πρέπει να προετοιμάζεται και να εκτελείται ετησίως.
ISO 27001:2013 – § A.7.2. Εκπαίδευση και ενημέρωση πάνω σε θέματα ασφάλειας πληροφορίας	

Τεχνικά μέτρα

Έλεγχος πρόσβασης και αυθεντικοποίηση

K.1	Θα πρέπει να εφαρμόζεται σύστημα ελέγχου πρόσβασης για όλους τους χρήστες του πληροφοριακού συστήματος. Το σύστημα θα πρέπει να επιτρέπει τη δημιουργία, την έγκριση, την επανεξέταση και τη διαγραφή των λογαριασμών χρηστών.
K.2	Η χρήση κοινών λογαριασμών χρηστών πρέπει να αποφεύγεται. Σε περιπτώσεις όπου αυτό είναι απαραίτητο, θα πρέπει να διασφαλιστεί ότι όλοι οι χρήστες του κοινού λογαριασμού έχουν τους ίδιους ρόλους και ευθύνες.
K.3	Πρέπει να υπάρχει ένας μηχανισμός ελέγχου ταυτότητας επιτρέποντας πρόσβαση στο πληροφοριακό σύστημα βάσει της πολιτικής και του συστήματος ελέγχου προσβάσεων. Θα πρέπει να χρησιμοποιείται κατ' ελάχιστο ένας συνδυασμός ονόματος χρήστη και κωδικού πρόσβασης. Οι κωδικοί πρόσβασης πρέπει να διατηρούν ένα καθορισμένο επίπεδο πολυπλοκότητας.
K.4	Το σύστημα ελέγχου πρόσβασης θα πρέπει να έχει τη δυνατότητα να ανιχνεύει και να απαγορεύει τη χρήση των κωδικών πρόσβασης που δεν τηρούν ένα καθορισμένο επίπεδο πολυπλοκότητας.
K.5	Θα πρέπει να καθοριστεί και να τεκμηριωθεί πολιτική κωδικών χρήστη η οποία να περιλαμβάνει κατ' ελάχιστο τον αριθμό των χαρακτήρων του κωδικού πρόσβασης, πολυπλοκότητα, περίοδος ισχύος, καθώς και τον αριθμό των αποδεκτών ανεπιτυχών προσπαθειών σύνδεσης.
K.6	Οι κωδικοί πρόσβασης χρηστών πρέπει να αποθηκεύονται σε κρυπτογραφημένη μορφή.
K.7	Κατά προτίμηση θα πρέπει να χρησιμοποιείται διπλή εξουσιοδότηση για την πρόσβαση σε συστήματα που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα. Οι μέθοδοι εξουσιοδότησης χρηστών θα μπορούσαν να είναι κωδικοί πρόσβασης, ψηφιακά πιστοποιητικά, USB με Ασφαλή Διάταξη Δημιουργίας Υπογραφής, βιομετρικά κ.λπ.
K.8	Θα πρέπει να γίνεται ταυτοποίηση συσκευών εντός δικτύου για να διασφαλίζεται ότι η επεξεργασία των προσωπικών δεδομένων γίνεται από καθορισμένους πόρους του δικτύου.

ISO 27001:2013 – § A.9 Έλεγχος πρόσβασης		

Logging και παρακολούθηση

L.1	Τα αρχεία καταγραφής ενεργειών (log files) θα πρέπει να ενεργοποιούνται για κάθε ένα σύστημα/εφαρμογή που χρησιμοποιείται για την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Αυτά πρέπει να περιλαμβάνουν όλα τα είδη προσβάσεων στα δεδομένα (πρόσβαση, τροποποίηση, διαγραφή).	
L.2	Τα αρχεία καταγραφής ενεργειών (log files) θα πρέπει να φέρουν χρονική σήμανση και να προστατεύονται από τυχόν αλλοιώσεις και μη εξουσιοδοτημένη πρόσβαση. Τα ρολόγια θα πρέπει να συγχρονίζονται με μία μοναδική πηγή χρόνου αναφοράς	
L.3	Θα πρέπει να πραγματοποιείται καταγραφή ενεργειών των διαχειριστών των συστημάτων και εφαρμογών συμπεριλαμβανομένων των ενεργειών προσθήκης/διαγραφής/αλλαγής δικαιωμάτων χρηστών	
L.4	Δεν θα πρέπει να υπάρχει δυνατότητα διαγραφής ή τροποποίησης αρχείων καταγραφής (log files) περιεχόμενου. Η πρόσβαση στα αρχεία καταγραφής πρέπει επίσης να καταγράφεται έτσι ώστε να εντοπίζεται τυχόν ασυνήθιστη δραστηριότητα.	
L.5	Ένα σύστημα παρακολούθησης πρέπει να επεξεργάζεται τα αρχεία καταγραφής και να εξάγει αναφορές σχετικά με την κατάσταση του συστήματος και να ειδοποιεί για πιθανούς κινδύνους.	

ISO 27001:2013 – § A.12.4 Logging και παρακολούθηση		

Ασφάλεια βάσεων δεδομένων και servers

M.1	Οι βάσεις δεδομένων και οι εφαρμογές θα πρέπει να έχουν ρυθμιστεί ώστε να λειτουργούν χρησιμοποιώντας ξεχωριστό λογαριασμό, με τα ελάχιστα δικαιώματα λειτουργικού συστήματος ώστε να λειτουργούν σωστά.	
M.2	Οι βάσεις δεδομένων και οι εφαρμογές θα πρέπει να επεξεργάζονται μόνο τα προσωπικά δεδομένα που πραγματικά χρειάζονται για την επεξεργασία ώστε να επιτευχθεί ο σκοπός επεξεργασίας.	
M.3	Θα πρέπει να εφαρμόζονται λύσεις κρυπτογράφησης σε καθορισμένα αρχεία με την χρήση υλικού/λογισμικού.	
M.4	Η κρυπτογράφηση των σκληρών δίσκων και μονάδων αποθήκευσης πρέπει να ληφθεί υπόψη.	

M.5	Οι τεχνικές ψευδωνυμοποίησης θα πρέπει να εφαρμόζονται με διαχωρισμό των προσωπικών δεδομένων από στοιχεία τα οποία θα μπορούσαν να οδηγήσουν σε ταυτοποίηση του υποκειμένου.
M.6	Στις βάσεις δεδομένων θα πρέπει να εφαρμόζονται συμπληρωματικοί κανόνες για την προστασία των δεδομένων. Τέτοια παραδείγματα είναι η εξουσιοδότηση για την υλοποίηση ενεργειών αναζήτησης στη βάση, απαγόρευση πράξεων αναζήτησης, κρυπτογράφηση επί των αναζητήσεων, κτλ.
ISO 27001:2013 – § A.12 Ασφάλεια στις διεργασίες	

Ασφάλεια σταθμών εργασίας

N.1	Οι χρήστες δεν θα πρέπει να είναι σε θέση να απενεργοποιήσουν ή παρακάμψουν τις ρυθμίσεις ασφαλείας.
N.2	Λειτουργίες anti-virus scan και update πρέπει να εκτελούνται εβδομαδιαία.
N.3	Οι χρήστες δεν πρέπει να έχουν δικαιώματα εγκατάστασης μη εξουσιοδοτημένων εφαρμογών λογισμικού.
N.4	Το σύστημα θα πρέπει να έχει καθορισμένο χρόνο λήξης συνεδρίας όταν ο χρήστης δεν έχει υπάρξει ενεργός για ορισμένο χρονικό διάστημα.
N.5	Όλες οι κρίσιμες ενημερώσεις λογισμικών που σχετίζονται με την ασφάλεια θα πρέπει να εγκαθίστανται συστηματικά
N.6	Λειτουργίες anti-virus scan και update πρέπει να εκτελούνται καθημερινά.
N.7	Δεν πρέπει να επιτρέπεται η μεταφορά δεδομένων προσωπικού χαρακτήρα από τους σταθμούς εργασίας σε συσκευές εξωτερικής αποθήκευσης (π.χ. USB, DVD, εξωτερικούς σκληρούς δίσκους).
N.8	ΟΙ σταθμοί εργασίας που χρησιμοποιούνται για την επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει κατά προτίμηση να μην είναι συνδεδεμένοι στο διαδίκτυο εκτός εάν έχουν ληφθεί μέτρα ασφαλείας για την αποτροπή μη εξουσιοδοτημένης επεξεργασίας, αντιγραφής και διαβίβασης δεδομένων προσωπικού χαρακτήρα σε αποθηκευτικό χώρο.
N.9	Πλήρης κρυπτογράφηση δίσκου πρέπει να είναι ενεργοποιημένη στους δίσκους που έχουν εγκαταστημένα τα λειτουργικά συστήματα
ISO 27001:2013 – § A.14.1 Απαιτήσεις ασφαλείας για πληροφοριακά συστήματα	

Ασφάλεια και ιδιωτικότητα στη μετά GDPR εποχή, στον τομέα της υγείας και της ασφάλισης.

Ασφάλεια δικτύων και επικοινωνιών

O.1	Κάθε φορά που η πρόσβαση γίνεται μέσω του Διαδικτύου, η επικοινωνία θα πρέπει να κρυπτογραφείται με τη χρήση κρυπτογραφικών πρωτοκόλλων (TLS/SSL).	
O.2	Η ασύρματη πρόσβαση στο πληροφοριακό σύστημα θα πρέπει να επιτρέπεται σε καθορισμένους χρήστες και επεξεργασίες και να προστατεύεται με μηχανισμούς κρυπογράφησης.	
O.3	Απομακρυσμένη πρόσβαση στο σύστημα θα πρέπει γενικά να αποφεύγεται. Σε περιπτώσεις όπου αυτό είναι απολύτως απαραίτητο θα πρέπει να εκτελείται μόνο κάτω από το τον έλεγχο και την παρακολούθηση ενός συγκεκριμένου ατόμου από τον οργανισμό (π.χ. διαχειριστής/υπεύθυνος ασφαλείας) μέσω προκαθορισμένων συσκευών.	
O.4	Κάθε κίνηση από και προς το πληροφοριακό σύστημα θα πρέπει να παρακολουθείται και να ελέγχεται μέσω firewall.	
O.5	Η σύνδεση στο διαδίκτυο δεν πρέπει να επιτρέπεται σε servers και σταθμούς εργασίας που χρησιμοποιούνται για την επεξεργασία δεδομένων προσωπικού χαρακτήρα.	
O.6	Το δίκτυο του πληροφοριακού συστήματος πρέπει να διαχωρίζεται από τα υπόλοιπα δίκτυα του υπευθύνου επεξεργασίας.	
O.7	Η πρόσβαση στο πληροφοριακό σύστημα πρέπει να επιτρέπεται μόνο από εκ των προτέρων εξουσιοδοτημένες συσκευές και τερματικά με χρήση τεχνικών όπως MAC filtering ή έλεγχο πρόσβασης δικτύου (Network Access Control (NAC))	
ISO 27001:2013 – § A.13 Ασφάλεια επινοικωνιών		

Αντίγραφα ασφαλείας

P.1	Οι διαδικασίες δημιουργίας αντιγράφων ασφαλείας και επαναφοράς δεδομένων πρέπει να είναι καθορισμένες, τεκμηριωμένες και να συνδέονται σαφώς με ρόλους και αρμοδιότητες.	
P.2	Οι παράμετροι ασφαλείας του φυσικού περιβάλλοντος όπου διατηρείται το backup να είναι συναφή των προδιαγραφών ασφαλείας που τίθενται εξαρχής στα πρωτογενή δεδομένα.	
P.3	Η υλοποίηση της διαδικασίας λήψης αντιγράφων ασφαλείας θα πρέπει να παρακολουθείται για να εξασφαλιστεί η πληρότητα.	
P.4	Η λήψη πλήρους αρχείου αντιγράφου ασφαλείας θα πρέπει να υλοποιείται τακτικά.	
P.5	Τα πάγια backup θα πρέπει να ελέγχονται τακτικά ώστε να διασφαλίζεται η αξιοπιστία τους σε περίπτωση επείγουσας χρήσης.	

P.6	Προγραμματισμένες λήψεις back up για τις αλλαγές στα αρχεία (incremental backups) θα πρέπει να διεξάγονται καθημερινά.	
P.7	Τα backups θα πρέπει να αποθηκεύονται με ασφάλεια σε χωριστές τοποθεσίες.	
P.8	Σε περίπτωση που η αποθήκευση backup παρέχεται από τρίτους, θα πρέπει να κρυπτογραφείται πριν τη διαβίβαση από τον υπεύθυνο επεξεργασίας.	
P.9	Τα backup θα πρέπει να είναι κρυπτογραφημένα και αποθηκευμένα με ασφάλεια και εκτός σύνδεσης.	
ISO 27001:2013 – § A.12.3 Αντίγραφα ασφαλείας		

Φορητές συσκευές

Q.1	Οι διαδικασίες διαχείρισης των κινητών και φορητών συσκευών πρέπει να είναι καθορισμένες και να προσδίδουν σαφείς κανόνες ορθής χρήσης.	
Q.2	Θα πρέπει να γίνεται εγγραφή και έγκριση των κινητών συσκευών που αποκτούν πρόσβαση στα πληροφοριακά συστήματα πριν την χρήση τους.	
Q.3	Οι κανόνες ασφαλείας των κινητών συσκευών θα πρέπει να είναι σε πλήρη αντιστοιχία με αυτές του υπόλοιπου τερματικού εξοπλισμού.	
Q.4	Οι ρόλοι και οι αρμοδιότητες που σχετίζονται με διαχείριση κινητών και φορητών συσκευών πρέπει να καθορίζονται σαφώς.	
Q.5	Ο οργανισμός πρέπει να είναι σε θέση να διαγράψει απομακρυσμένα προσωπικά δεδομένα που εμπεριέχονται σε κινητές συσκευές που έχουν κλαπεί/χαθεί.	
Q.6	Οι κινητές συσκευές θα πρέπει να υποστηρίζουν τον διαχωρισμό του προσωπικού κι εταιρικού περιβάλλοντος λειτουργίας μέσω εφαρμογών ασφαλούς διαχωρισμού περιβάλλοντος.	
Q.7	Οι κινητές συσκευές θα πρέπει έχουν φυσική προστασία από κλοπή όταν είναι εκτός χρήσης.	
Q.8	Πρέπει να πραγματοποιείται έλεγχος ταυτότητας δύο παραγόντων (two factor authentication) για πρόσβαση σε κινητές συσκευές.	
Q.9	Προσωπικά δεδομένα που αποθηκεύονται σε κινητές συσκευές (ως μέρος της λειτουργίας διαχείρισης δεδομένων προσωπικού χαρακτήρα της λειτουργίας) πρέπει να είναι κρυπτογραφημένα.	
ISO 27001:2013 – § A.6.2 Φορητές συσκευές και τηλεργασία		

Ασφάλεια στον κύκλο ζωής εφαρμογών

R.1	Κατά τη διάρκεια του κύκλου ζωής της ανάπτυξης λογισμικού θα πρέπει να ακολουθούνται οι βέλτιστες πρακτικές.	
R.2	Οι παράμετροι ασφαλείας του λογισμικού θα πρέπει να καθορίζονται στα πρώτα στάδια ζωής του λογισμικού.	
R.3	Εξειδικευμένες τεχνολογίες και τεχνικές που σχεδιάζονται για την υποστήριξη της ιδιωτικότητας και της προστασίας των δεδομένων (Τεχνολογίες Βελτίωσης Προστασίας της Ιδιωτικότητας - Privacy Enhancing Technologies (PETs)) θα πρέπει να εφαρμόζονται κατ' αναλογία με τις απαιτήσεις ασφάλειας.	
R.4	Πρέπει να ακολουθούνται ασφαλή πρότυπα κωδικοποίησης και πρακτικές.	
R.5	Κατά την ανάπτυξη λογισμικού θα πρέπει να γίνονται έλεγχοι για την ορθότητα των κανόνων ασφαλείας που έχουν τεθεί από τον σχεδιασμό	
R.6	Πριν τη χρήση ενός λειτουργικού συστήματος θα πρέπει να πραγματοποιείται αξιολόγηση ευπάθειας και δοκιμές διείσδυσης (penetration tests) σε συστήματα και υποδομές από αξιόπιστο τρίτο μέρος. Η εφαρμογή δεν πρέπει να εγκρίνεται αν δεν διασφαλίζεται το απαιτούμενο επίπεδο ασφάλειας	
R.7	Οι δοκιμές διείσδυσης (penetration tests) πρέπει να διεξάγονται τακτικά.	
R.8	Θα πρέπει να λαμβάνονται πληροφορίες για τα τρωτά σημεία του πληροφοριακού συστήματος που χρησιμοποιείται.	
R.9	Οι επιδιορθώσεις λογισμικού θα πρέπει να ελέγχονται και αξιολογούνται πριν την εγκατάστασή τους σε λειτουργικό περιβάλλον.	
ISO 27001:2013 – § A.12.6 Διαχείριση τεχνικών ευπαθειών, § A.14.2 Ασφάλεια στην ανάπτυξη λογισμικού		

Διαγραφή και καταστροφή δεδομένων

S.1	Πριν την καταστροφή των παγίων θα πρέπει να γίνεται ovewrite των δίσκων για εκκαθάριση με τη χρήση εφαρμογών software-based overwriting.	
S.2	Θα πρέπει να πραγματοποιείται συστηματική καταστροφή του φυσικού αρχείου και των παγίων που εμπεριέχουν προσωπικά δεδομένα.	
S.3	Πολλαπλό overwrite από ειδικά λογισμικά επανεγγραφής δίσκων θα πρέπει να υλοποιούνται πριν την τελική καταστροφή/απόρριψη των παγίων που φέρουν δεδομένα.	

S.4	Εάν χρησιμοποιούνται υπηρεσίες τρίτων για την ασφαλή καταστροφή φυσικού και ηλεκτρονικού αρχείου, θα πρέπει να υπάρχει μια σύμβαση παροχής υπηρεσιών καθώς και ένα αρχείο καταγραφής των αρχείων που καταστρέφονται το οποίο θα συμπληρώνεται όταν κριθεί απαραίτητο.
S.5	Μετά τη διαγραφή του λογισμικού που βρίσκεται εντός παγίων προς καταστροφή επιπρόσθετες πράξεις όπως απομαγνητισμός δίσκου θα έπρεπε να εφαρμόζονται. Συμπληρωματικά, με βάση το είδος του παγίου θα μπορούσε να εφαρμοστεί και η φυσική καταστροφή του (σπάσιμο με σφυρί).
S.6	Εάν γίνεται χρήση τρίτου μέρους (εκτελούντα) για την τελική καταστροφή φυσικού αρχείου ή παγίων θα πρέπει να αξιολογηθεί η δυνατότητα οι πράξεις καταστροφής να γίνονται εντός εγκαταστάσεων του Υπευθύνου Επεξεργασίας για να μην απαιτείται η μεταφορά εκτός έδρας των προσωπικών δεδομένων

ISO 27001:2013 – § A.8.3 Καταστροφή μέσων, § A.11.2.7 Ασφαλής καταστροφή ή επαναχρησιμοποίηση του εξοπλισμού

Φυσική ασφάλεια

T.1	Η φυσική περίμετρος των χώρων όπου φυλάσσονται οι υποδομές του IT δεν θα πρέπει να είναι προσβάσιμη από μη εξουσιοδοτημένο προσωπικό.
T.2	Θα πρέπει να υπάρχει σαφής ταυτοποίηση του προσωπικού και των επισκεπτών που έχουν πρόσβαση στις εγκαταστάσεις του οργανισμού με χρήση κατάλληλων μέσων π.χ. κάρτες πρόσβασης.
T.3	Θα πρέπει να υπάρχουν καθορισμένες ζώνες ασφαλείας οι οποίες να προστατεύονται με κατάλληλους ελέγχους εισόδου. Το βιβλίο εισόδου ή η ηλεκτρονική καταγραφή κινήσεων όλων των προσβάσεων πρέπει να τηρούνται και να ελέγχονται.
T.4	Συναγερμός πρέπει να είναι εγκατεστημένα σε όλες τις ζώνες ασφαλείας.
T.5	Θα πρέπει να τοποθετηθούν φυσικά εμπόδια όπου χρειάζεται ώστε να αποτρέπεται κάθε μη εξουσιοδοτημένη φυσική πρόσβαση.
T.6	Οι περιοχές εκτός συστήματος ασφαλείας πρέπει να κλειδώνονται και να ελέγχονται συστηματικά.
T.7	Στο server room θα πρέπει να υπάρχει αυτόματο σύστημα καταστολής φωτιάς, ξεχωριστό σύστημα κλιματισμού κλειστού ελέγχου και UPS.
T.8	Το προσωπικό των εξωτερικών συνεργατών παροχής τεχνικής υποστήριξης πρέπει να έχει περιορισμένη πρόσβαση σε ασφαλείς χώρους.

ISO 27001:2013 – § A.11 Φυσική ασφάλεια

CASE STUDY

Η εταιρεία

Ο οργανισμός πάνω στον οποίο πραγματοποιήθηκε το case study δραστηριοποιείται στον τομέα της υγείας και έχει στο πελατολόγιο του μεγάλες φαρμακευτικές εταιρείες. Σαν core business λειτουργεί ως ενδιάμεσος κρίκος μεταξύ των φαρμακευτικών εταιριών και των ασθενών, καθώς οι πρώτες βάση νομοθεσίας δεν έχουν το δικαίωμα να έρχονται σε απευθείας επικοινωνία με τους δεύτερους. Συνεπώς το κομμάτι αυτό το έχει αναλάβει η εταιρεία για την οποία γίνεται λόγος, έχοντας ένα τηλεφωνικό κέντρο μέσω του οποίου ο ασθενής μπορεί να μάθει πληροφορίες για τη θεραπεία του, να αναφέρει τυχόν ανεπιθύμητες ενέργειες, καθώς και να κανονίσει κάποια εκπαίδευση (σε περίπτωση που κάνει χρήση κάποια συσκευής για τη χορήγηση) ή να ζητήσει υπηρεσία υπενθύμισης για τη συνταγογράφηση/χορήγηση του φαρμάκου.

Προσωπικά Δεδομένα

Η όλη διαδικασία προϋποθέτει φυσικά τη συγκατάθεση του υποκειμένου, αλλά και τη διατήρηση στοιχείων επικοινωνίας και ιστορικού σε ηλεκτρονική βάση δεδομένων. Γίνεται λοιπόν αντιληπτό ότι ένας τέτοιος όγκος ευαίσθητων προσωπικών δεδομένων έκανε επιτακτική την ανάγκη ορισμού ενός πλαισίου τεχνικών και οργανωτικών μέτρων ώστε να διαφυλάσσεται ανά πάσα στιγμή η διαθεσιμότητα, η ακεραιότητα και η εμπιστευτικότητα των συγκεκριμένων πληροφοριών. Ως εκ τούτου η εταιρεία το 2015 πιστοποιήθηκε από την TUV Austria στο ISO 27001:2013 πράγμα που δεν της έδωσε μόνο ανταγωνιστικό πλεονέκτημα, αλλά της προσέφερε και μια εργαλειοθήκη για την ομαλή μετάβαση στην εφαρμογή του ΓΚΠΔ.

Πέρα από τα τεχνικά μέτρα, στα οποία επένδυσε η εταιρεία από την ίδρυση της, σε συνεργασία με ομάδες συμβούλων επιχειρήσεων δημιούργησε ένα πλέγμα διαδικασιών και διεργασιών ώστε αυτές να δέσουν με τα παραπάνω μέτρα και να ενισχύσουν την κουλτούρα του προσωπικού και την ευαισθητοποίηση του σε θέματα ασφάλειας πληροφορίας. Σε ένα παραπάνω βήμα στα τέλη του 2017 όντας ήδη πιστοποιημένη στο ISO 9001:2015 προχώρησε στην ενοποίηση των δυο συστημάτων με σκοπό να καταστεί πιο σαφές το όλο πλαίσιο λειτουργίας της εταιρείας σε θέματα ασφάλειας και ποιότητας, αλλά ταυτόχρονα να θέσει τη βάση ώστε όλο αυτό το σύνολο διαδικασιών να πατήσει πάνω στο νομικό και κανονιστικό πλαίσιο του ΓΚΠΔ.

Φυσικά κάτι τέτοιο δε θα αρκούσε για να εναρμονιστεί η εταιρεία με τον ΓΚΠΔ. Χρειάστηκε ένα σύνολο ενεργειών για να μπορέσει να αξιολογήσει την κατάσταση πριν

και μετά και κατόπιν με την εφαρμογή της μεθοδολογίας που θα παρουσιαστεί παρακάτω να μπορεί να αποδείξει ότι μέσω των προτύπων και ιδίως του ISO 27001 έχει καταφέρει να φτάσει σε ένα μέγιστο επίπεδο συμμόρφωσης σε ότι αφορά την προστασία των δεδομένων που διαχειρίζεται.

Αρχικά βήματα

Πριν την υλοποίηση του συγκεκριμένου case study προηγήθηκαν βήματα στα πλαίσια του εναρμονισμού του οργανισμού με τις απαιτήσεις του GDPR.

Αρχικώς πραγματοποιήθηκε το λεγόμενο data mapping, το οποίο έδωσε σαν παραγόμενο το αρχείο ροής δεδομένων, δηλαδή όλο το flow από τη στιγμή που γίνεται η αρχική λήψη της πληροφορίας ως και το που καταλήγει. Με τον όρο πληροφορία στο συγκεκριμένο οργανισμό εννοούμε οικονομικά στοιχεία, στοιχεία ασθενών, στοιχεία υπαλλήλων κλπ τα οποία μπορεί να εισάγονται στην εταιρεία είτε προφορικά, είτε σε έντυπη μορφή, είτε ηλεκτρονικά.

Αφού λοιπόν ταυτοποιήθηκαν όλες οι ροές δεδομένων, αυτές δόθηκαν στο νομικό σύμβουλο της εταιρείας με σκοπό να κριθεί ποιες από αυτές απαιτείται να περάσουν από διαδικασία DPIA. Έτσι σύμφωνα με την απόφαση που βγήκε τότε το επόμενο στάδιο είναι η αξιολόγηση της επίπτωσης στα θεμελιώδη δικαιώματα και στις ελευθερίες που έχει το υποκείμενο, λόγω της πιθανής απώλειας ασφάλειας των προσωπικών δεδομένων.

Αξιολόγηση κινδύνου

Σύμφωνα λοιπόν με την απόφαση του νομικού συμβούλου ταυτοποιήθηκαν έξι ροές δεδομένων στις οποίες θα έπρεπε να γίνει αξιολόγηση του κινδύνου:

ΚΩΔΙΚΟΣ	ΠΕΡΙΓΡΑΦΗ PROCESSING ACTIVITY	ΤΥΠΟΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ	ΟΓΚΟΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ	ΥΠΟΚΕΙΜΕΝΟ
1	ΕΛΕΓΧΟΣ ΥΠΗΡΕΣΙΑΣ ΑΠΌ ΦΑΡΜΑΚΕΥΤΙΚΕΣ με σκοπό την παρακολούθηση παρεχόμενων υπηρεσιών	ΔΕΔΟΜΕΝΑ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ	-	Συνεργάτες εταιρείας
2	CCTV Η βιντεοσκόπηση μέσω κλειστού κυκλώματος τηλεόρασης για τον σκοπό της προστασίας των εγκαταστάσεων και των περιουσιακών στοιχείων της APC καθώς και του συνόλου των πληροφοριών εμπιστευτικού χαρακτήρα που αφορούν πελάτες και ασθενείς που εξυπηρετεί η APC.	ΔΕΔΟΜΕΝΑ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ	-	Συνεργάτες εταιρείας

3	Drug @ clinics Με σκοπό την παροχή υπηρεσίας μεταφοράς και παράδοσης φαρμάκου στον ασθενή	ΔΕΔΟΜΕΝΑ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ	-	Κάθε ασθενής που δύναται να κάνει χρήση της υπηρεσίας (δυνητικά και ανήλικοι)
4	Drug @ home Με σκοπό την παροχή υπηρεσίας μεταφοράς και παράδοσης φαρμάκου στον ασθενή	ΔΕΔΟΜΕΝΑ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ	-	Κάθε ασθενής που δύναται να κάνει χρήση της υπηρεσίας (δυνητικά και ανήλικοι)
5	ΦΑΡΜΑΚΟΕΠΑΓΡΥΠΝΙΣΗ (ΔΗΜΙΟΥΡΓΙΑ / ΤΗΡΗΣΗ ΑΡΧΕΙΟΥ ΦΑΡΜΑΚΟΕΠΑΓΡΥΠΝΙΣΗΣ) Με σκοπό τη συλλογή και επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων για σκοπούς φαρμακοεπαγρύπνησης όπως αυτοί προβλέπονται και ορίζονται από την ισχύουσα τοπική και ευρωπαϊκή νομοθεσία.	ΔΕΔΟΜΕΝΑ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ	-	Κάθε ασθενής έχει ανεπιθύμητες ενέργειες από κάποιο σκεύασμα (δυνητικά και ανήλικοι)
6	SUPPORT CENTER (ΔΗΜΙΟΥΡΓΙΑ / ΤΗΡΗΣΗ ΑΡΧΕΙΟΥ SUPPORT CENTER) Με σκοπό τη συλλογή και επεξεργασία προσωπικών δεδομένων ειδικών κατηγοριών στο πλαίσιο παροχής προγραμμάτων υποστήριξης ασθενών, τα οποία συνίστανται στην εκπαίδευση τους αναφορικά με τον θεμιτό τρόπο χορήγησης φαρμακευτικών σκευασμάτων καθώς και την ψυχολογική υποστήριξη αυτών απο εξειδικευμένο νοσηλευτικό προσωπικό.	ΔΕΔΟΜΕΝΑ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ	-	Κάθε ασθενής που δύναται να κάνει χρήση της υπηρεσίας (δυνητικά και ανήλικοι)

Έχοντας πλέον τις ροές δεδομένων και χρησιμοποιώντας τις οδηγίες που δίνονται από τους **πίνακες 1 & 2** που αναφέρονται στη μεθοδολογία, αξιολογούνται οι επιπτώσεις στη διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα για αυτές.

Έτσι προκύπτουν τρεις τιμές, μια για κάθε αρχή και επιλέχθηκε η υψηλότερη ώστε να αξιολογηθεί η συνολική επίπτωση στα προσωπικά δεδομένα των υποκειμένων, όπως φαίνεται στο παρακάτω παράδειγμα.

ΑΙΤΙΟΛΟΓΗΣΗ ΕΠΙΠΤΩΣΗΣ ΣΤΗΝ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ	ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ		ΑΙΤΙΟΛΟΓΗΣΗ ΕΠΙΠΤΩΣΗΣ ΣΤΗΝ ΑΚΕΡΑΙΟΤΗΤΑ	ΑΚΕΡΑΙΟΤΗΤΑ		ΑΙΤΙΟΛΟΓΗΣΗ ΕΠΙΠΤΩΣΗΣ ΣΤΗΝ ΔΙΑΘΕΣΙΜΟΤΗΤΑ	ΔΙΑΘΕΣΙΜΟΤΗΤΑ		ΣΥΝΟΛΙΚΟΣ ΒΑΘΜΟΣ	ΣΥΝΟΛΙΚΗ ΕΠΙΠΤΩΣΗ
Μία μη εξουσιοδοτημένη αποκάλυψη (απώλεια εμπιστευτικότητας) δεδομένων προσωπικού χαρακτήρα σε τρίτους θα μπορούσε να προκαλέσει στο υποκείμενο προσπελάσιμες δυσκολίες (πχ. Άγχος, δυσκολία εύρεσης νέας εργασίας).	Μεσαία	2	Μία μη εξουσιοδοτημένη μεταβολή (απώλεια ακεραιότητας) δεδομένων προσωπικού χαρακτήρα θα μπορούσε να φέρει το υποκείμενο αντιμέτωπο με σημαντικές συνέπειες, οι οποίες θα πρέπει να μπορούν να ξεπεραστούν με σημαντική δυσκολία (πχ. αλλοίωση δεδομένων απόδοσης μπορεί να προκαλέσει απώλεια εργασίας)	Υψηλή	3	Η επίπτωση μίας μη εξουσιοδοτημένης καταστροφής ή απώλειας (απώλεια διαθεσιμότητας) δεδομένων προσωπικού χαρακτήρα θα μπορούσε να προκαλέσει προσπελάσιμα προβλήματα στο υποκείμενο.	Χαμηλή	1	3	Υψηλή / Πολύ Υψηλή

Στη συνέχεια, ακολουθώντας τους **πίνακες 3 έως και 7** εκτιμάται η πιθανότητα εμφάνισης της απειλής ανά περιοχή αξιολόγησης.

ΑΙΤΙΟΛΟΓΗΣΗ ΠΙΘΑΝΟΤΗΤΑΣ (ΔΙΚΤΥΟ & ΤΕΧΝΙΚΟΙ ΠΟΡΟΙ)	ΔΙΚΤΥΟ & ΤΕΧΝΙΚΟΙ ΠΟΡΟΙ		ΑΙΤΙΟΛΟΓΗΣΗ ΠΙΘΑΝΟΤΗΤΑΣ (ΔΙΑΔΙΚΑΣΙΕΣ / ΕΝΕΡΓΕΙΕΣ ΕΠΕΞΕΡΓΑΣΙΑΣ)	ΔΙΑΔΙΚΑΣΙΕΣ / ΕΝΕΡΓΕΙΕΣ ΕΠΕΞΕΡΓΑΣΙΑΣ	
Το σύστημα δεν είναι συνδεδεμένο στο διαδίκτυο και δεν επιτρέπει πρόσβαση από το Διαδίκτυο σε εσωτερικούς πόρους και άλλα συστήματα πληροφορικής. Θεωρείται ότι για τη συγκεκριμένη περίπτωση χρήσης εμποδίζεται η μη εξουσιοδοτημένη πρόσβαση, ακολουθώντας τους απαραίτητους μηχανισμούς ασφάλειας συστημάτων και back up Policies.	Χαμηλή	1	Οι ρόλοι και οι ευθύνες του ανθρώπινου δυναμικού καθορίζονται σαφώς σύμφωνα με πολιτική προσβάσεων, η επεξεργασία των προσωπικών δεδομένων περιορίζεται στις εγκαταστάσεις του οργανισμού.	Χαμηλή	1

ΑΙΤΙΟΛΟΓΗΣΗ ΠΙΘΑΝΟΤΗΤΑΣ (ΕΜΠΛΕΚΟΜΕΝΟΙ ΣΕ ΕΠΕΞΕΡΓΑΣΙΑ)	ΕΜΠΛΕΚΟΜΕΝΟΙ ΣΕ ΕΠΕΞΕΡΓΑΣΙΑ		ΑΙΤΙΟΛΟΓΗΣΗ ΠΙΘΑΝΟΤΗΤΑΣ (ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΣ ΤΟΜΕΑΣ & ΚΛΙΜΑΚΑ ΕΠΕΞΕΡΓΑΣΙΑΣ)	ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΣ ΤΟΜΕΑΣ & ΚΛΙΜΑΚΑ ΕΠΕΞΕΡΓΑΣΙΑΣ	
Οι υπάλληλοι της εταιρείας έχουν λάβει σχετική εκπαίδευση και υπάρχουν πολιτικές πρόσβασης, συστήματα ελέγχου πρόσβασης, συμφωνητικά εμπιστευτικότητας και κώδικας δεοντολογίας.	Χαμηλή	1	Ο επιχειρηματικός τομέας της εταιρείας θεωρείται επιρρεπής σε επιθέσεις. Επιπλέον έχει πραγματοποιηθεί επίθεση σε πληροφοριακό σύστημα στο παρελθόν. Παρόλα αυτά ο όγκος των υποκειμένων και ΔΠΧ δε θεωρείται μεγάλος.	Μεσαία	2

Ως τελικός βαθμός ορίζεται το άθροισμα των επιμέρους βαθμών για κάθε τομέα της επιχείρησης και η αντιστοιχία στον **πίνακα 8** χαρακτηρίζει το τελικό επίπεδο πιθανότητας εμφάνισης της απειλής.

Έχοντας λοιπόν πλέον και την πιθανότητα εμφάνισης μιας απειλής, καθώς και την επίπτωση που θα έχει αυτή στα προσωπικά δεδομένα που διαχειρίζεται η εταιρεία, από τον **πίνακα 9** ο οργανισμός λαμβάνει την αξιολόγηση κινδύνου για την εκάστοτε ροή δεδομένων.

GAP Analysis

Το τελικό βήμα στο συγκεκριμένο case study είναι ουσιαστικά να δει ο οργανισμός κατά πόσο οι ενέργειες και τα οργανωτικά/τεχνικά μέτρα που έχουν γίνει/ληφθεί στα πλαίσια της πιστοποίησης για το πρότυπο ISO 27001:2013 καλύπτουν τις απειλές που προέκυψαν από την εκτίμηση κινδύνου.

Για κάθε ροή δεδομένων και με βάση τα μέτρα που αναφέρονται στην παράγραφο **«Μέτρα Ασφαλείας»** της μεθοδολογίας ελέγχεται ποια από αυτά εφαρμόζονται και σε ποιο επίπεδο, όπως φαίνεται παρακάτω:

	Access control policy	C.2	A.9.1.1 Access control policy	An access control policy should be detailed and documented. The organization should determine in this document the appropriate access control rules, access rights and restrictions for specific user roles towards the processes and procedures related to personal data.	Η πολιτική ελέγχου προσβάσεων θα πρέπει να είναι αναλυτική και τεκμηριωμένη. Εντός της οποίας να καθορίζονται οι κατάλληλοι κανόνες ελέγχου πρόσβασης, δικαιώματα πρόσβασης και περιορισμούς για συγκεκριμένους ρόλους χρηστών σε σχέση με την επεξεργασία και διαδικασίες που σχετίζονται με τα προσωπικά δεδομένα.	Βάσει των οδηγιών Κανόνες Απόδοσης Δικαιωμάτων Πρόσβασης (G3) και Βασικές Οδηγιές Ασφάλειας Πληροφοριών (G5).	ΕΦΑΡΜΟΖΕΤΑΙ

Γίνεται αντιληπτό πως όσο πιο πολλά μέτρα εφαρμόζονται για κάθε ροή δεδομένων, τόσο ελαχιστοποιείται ο κίνδυνος που αφορά την επεξεργασία προσωπικών δεδομένων.

Για μια πιο αναλυτική παρουσίαση των εργαλείων και σε βάθος επεξήγηση του case study, μπορείτε να επικοινωνήσετε με τον συγγραφέα της διπλωματικής εργασίας.

ΕΠΙΛΟΓΟΣ

Η συμμόρφωση με τον ΓΚΠΔ δεν είναι μια εύκολη υπόθεση, ιδιαίτερα για τις μικρομεσαίες επιχειρήσεις, καθώς οι απαιτήσεις ασφαλείας είναι ιδιαιτέρως υψηλές, κάτι που επιφέρει και μεγάλα έξοδα στο τεχνολογικό κομμάτι, αλλά και στην πρόσληψη προσωπικού που θα εφαρμόσει και θα ελέγξει τα οργανωτικά μέτρα που θεωρούνται απαραίτητα από το νομικό πλαίσιο (Υπεύθυνος Διασφάλισης Ποιότητας, DPO).

Η συγκεκριμένη μεθοδολογία που προτείνεται από τον ENISA βοηθάει τους οργανισμούς να αντιληφθούν τους κινδύνους που ελλοχεύουν πίσω από την επεξεργασία των προσωπικών δεδομένων και να τους αξιολογήσουν καταλλήλως ώστε να μετριάσουν την επίπτωση των διάφορων απειλών.

Ταυτόχρονα προτείνονται και μέτρα αντιμετώπισης μέσω των οποίων μπορεί να περιοριστεί ο παραπάνω αντίκτυπος, μέτρα τα οποία προκύπτουν από το ίδιο το πρότυπο ISO 27001:2013 τα οποία μπορεί να είναι τόσο οργανωτικά όσο και τεχνικά.

Στον τομέα της υγείας και σε όσες επιχειρήσεις δραστηριοποιούνται σε αυτόν, τα πράγματα είναι ακόμα πιο δύσκολα καθώς έχουμε να κάνουμε πλέον με ευαίσθητα προσωπικά δεδομένα, μεγαλύτερους δηλαδή κινδύνους και μεγαλύτερη προσοχή.

Υλοποιώντας το συγκεκριμένο case study όμως, γίνεται φανερό πως αν υπάρχουν κάποιες βάσεις τότε οι δυσκολίες σε ότι αφορά τη συμμόρφωση με τον ΓΚΠΔ μπορούν να μετριαστούν αισθητά. Εφαρμόζοντας αυτή τη μεθοδολογία σε μια εταιρεία που από την έναρξη των δραστηριοτήτων της δούλεψε προς την κατεύθυνση της πιστοποίησης στο πρότυπο ISO 27001:2013, διαπιστώθηκε πως πολλές από τις απαιτήσεις του κανονιστικού πλαισίου καλύπτονται με μέτρα που ήδη ισχύουν από το ίδιο το πρότυπο.

Αν λοιπόν υπάρχουν ισχυρές βάσεις και μια επιχείρηση έχει ως κύριο μέλημα της την ασφάλεια της πληροφορίας, η συμμόρφωση με τον ΓΚΠΔ μπορεί να γίνει μια σχετικά απλή διαδικασία, χωρίς αυτό βέβαια να σημαίνει ότι δε θα χρειάζονται επιπλέον διορθωτικές κινήσεις.

Η ασφάλεια πληροφορίας λοιπόν δεν είναι υπόθεση ενός, αλλά οφείλει να είναι νοοτροπία ολόκληρου του οργανισμού και πρέπει όλοι εμπλεκόμενοι να δουλέψουν για τα επιθυμητά αποτελέσματα.

ΑΚΡΩΝΥΜΙΑ

SME: Small and Medium Enterprises

ENISA: European Union Agency for Network and Information Security

DPIA: Data Privacy Impact Assessment

GDPR: General Data Protection Regulation

ΓΚΠΔ: Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων

DPO: Data Protection Officer

ΣΔΑΠ: Σύστημα Διαχείρισης Ασφάλειας Πληροφορίας

ISMS: Information Security Management System

DPIA: Data Privacy Impact Assessment

ΑΝΑΦΟΡΕΣ

WP2016 3-2 6 Data Controllers Risk

WP2017 O-2-2-5 GDPR Measures Handbook

ISO/IEC 27000:2016 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary : http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=66435

General_Data Protection_RegulationGDPR_Brochure_WEB_FINAL_Spreads4

CNIL – Managing Privacy Risks Methodology https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf

35 ENISA - Recommendations for a methodology of the assessment of severity of personal data breaches https://www.enisa.europa.eu/publications/dbn-severity

The CNIL methodology for privacy risk assessment (appendices) provides a detailed list of threats related to personal data processing, see in: https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf