ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗΝ
ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ (MBA)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ ΣΤΑ ΠΛΑΙΣΙΑ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ»

ΠΑΡΑΣΚΕΥΗ Α. ΦΟΥΣΕΚΗ

Επιβλέπων Καθηγητής: Παναγιώτης Αρτίκης

Πειραιάς 2019

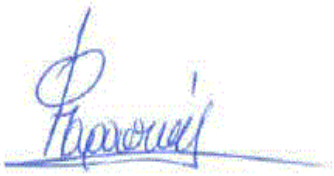
ΒΕΒΑΙΩΣΗ ΕΚΠΟΝΗΣΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

«Δηλώνω υπεύθυνα ότι η διπλωματική εργασία για τη λήψη του μεταπτυχιακού τίτλου σπουδών, του Πανεπιστημίου Πειραιώς, στη Διοίκηση Επιχειρήσεων : MBA» με τίτλο «Διαχείριση Κινδύνων στα πλαίσια προστασίας των προσωπικών δεδομένων» έχει συγγραφεί από εμένα αποκλειστικά και στο σύνολό της. Δεν έχει υποβληθεί ούτε έχει εγκριθεί στο πλαίσιο κάποιου άλλου μεταπτυχιακού προγράμματος ή προπτυχιακού τίτλου σπουδών, στην Ελλάδα ή στο εξωτερικό, ούτε είναι εργασία ή τμήμα εργασίας ακαδημαϊκού ή επαγγελματικού χαρακτήρα.

Δηλώνω επίσης υπεύθυνα ότι οι πηγές στις οποίες ανέτρεξα για την εκπόνηση της συγκεκριμένης εργασίας, αναφέρονται στο σύνολό τους, κάνοντας πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου»

Υπογραφή Μεταπτυχιακού Φοιτητή - Ονοματεπώνυμο

Παρασκευή Φουσέκη



ΑΦΙΕΡΩΣΕΙΣ

Αφιερώνεται στην οικογένεια μου…

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία αποτελεί προϊόν μεταπτυχιακής διατριβής που πραγματοποιήθηκε στα πλαίσια του «Μεταπτυχιακού Προγράμματος Σπουδών στην Διοίκηση Επιχειρήσεων» του Πανεπιστημίου Πειραιώς. Σκοπός της είναι ο εντοπισμός των βασικότερων κινδύνων, τους οποίους καλείται να αντιμετωπίσει η σύγχρονη επιχείρηση, αναφορικά με την προστασία των προσωπικών δεδομένων που αυτή συλλέγει και επεξεργάζεται, καθώς και η ανάδειξη των πλέον πρόσφορων μεθόδων και διαδικασιών για την διαχείριση των κινδύνων αυτών μέσω ενός ενδεδειγμένου μοντέλου συμμόρφωσης με τις ισχύουσες κανονιστικές διατάξεις.

Λέξεις κλειδιά: επιχείρηση, κίνδυνος, αποτίμηση κινδύνου, διαχείριση κινδύνου, προσωπικά δεδομένα, ιδιωτικότητα, Γενικός Κανονισμός Προστασίας Δεδομένων, ΓΚΠΔ, General Data Protection Regulation, GDPR, 2016/679, προστασία δεδομένων προσωπικού χαρακτήρα, συμμόρφωση, εκτίμηση αντικτύπου, ανάλυση αποκλίσεων

ABSTRACT

The present thesis was carried out in the framework of the postgraduate program “Master in Business Administration” of the University of Piraeus. Its purpose is to identify the most important risks that modern business is required to face regarding personal data protection and the most appropriate methods and procedures for managing those risks through a model of compliance with the applicable regulations.

Keywords: enterprise, risk, risk valuation, risk management, personal data, privacy, General Data Protection Regulation, GDPR, 2016/679, protection of personal data, compliance, data privacy impact assessment, gap analysis

ΕΥΧΑΡΙΣΤΙΕΣ

Κατόπιν ολοκλήρωσης της διπλωματικής μου εργασίας, θα ήθελα να ευχαριστήσω την οικογένειά μου που είναι δίπλα μου σε κάθε ακαδημαϊκό και επαγγελματικό μου βήμα, καθώς και όλους τους ανθρώπους που με συνέδραμαν ενεργά κατά την διάρκεια εκπόνησής της. Επιπλέον, οφείλω να ευχαριστήσω θερμά τον καθηγητή μου, Παναγιώτη Αρτίκη, για την καθοδήγησή του και όλες τις συμβουλές που μου παρείχε επί της δομής, της οργάνωσης και του περιεχομένου της παρούσας μεταπτυχιακής διατριβής. Τέλος, ευχαριστώ ιδιαίτερα όλους τους διδάσκοντες του μεταπτυχιακού προγράμματος σπουδών που είχα την ευκαιρία να παρακολουθήσω, καθώς χάρη στην κατάρτισή και την πολυετή εμπειρία τους κατόρθωσαν να εμπλουτίσουν το νομικό μου υπόβαθρο με αξιοσημείωτες γνώσεις από τον τομέα της διοίκησης επιχειρήσεων και της χρηματοοικονομικής επιστήμης.

ΚΑΤΑΣΤΑΣΗ ΑΚΡΩΝΥΜΙΩΝ

ΕΕ: Ευρωπαϊκή Ένωση

ΓΚΠΔ: Γενικός Κανονισμός για την Προστασία Δεδομένων

ΕΑΠΔ: Εκτίμηση Αντικτύπου στην Προστασία Δεδομένων

ΑΠΔΠΧ: Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

ΕΣΔΑ: Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου

DPO: Data Protection Officer

GDPR: General Data Protection Regulation

ERM: Enterprise Risk Management

IoT: Internet of Things

DPIA: Data Privacy Impact Assessment

CMM: Capability Maturity Model

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

Οι ραγδαίες τεχνολογικές εξελίξεις στα πλαίσια μίας απόλυτα παγκοσμιοποιημένης οικονομίας έχουν οδηγήσει σήμερα στην αύξηση τόσο της συλλογής όσο και της επεξεργασίας προσωπικών δεδομένων από δημόσιες αρχές, επιχειρήσεις και ιδιώτες, δημιουργώντας έτσι ένα από τα πιο σύνθετα προβλήματα της σύγχρονης ψηφιακής εποχής. Η ανταλλαγή πληροφοριών και δεδομένων έχει διευρυνθεί αισθητά μεταξύ των οργανισμών κατά την διεξαγωγή των οικονομικών τους συναλλαγών, ενώ παράλληλα η διαθεσιμότητα και η δημοσιοποίηση πλήθους προσωπικών δεδομένων στο διαδίκτυο αποτελεί πλέον σύνηθες φαινόμενο. Η αλματώδης ανάπτυξη των δικτύων και η λειτουργική ολοκλήρωση των πληροφοριακών και επικοινωνιακών συστημάτων διαμορφώνουν ένα ριζικά διαφορετικό πλαίσιο παραγωγής και επεξεργασίας των προσωπικών δεδομένων. Οι μεταβολές αυτές δεν θα μπορούσαν προφανώς να αφήσουν ανεπηρέαστη την σύγχρονη επιχείρηση, καθώς η συχνότητα και η σοβαρότητα των κινδύνων για την προστασία των προσωπικών δεδομένων που αυτή επεξεργάζεται, παρουσιάζουν διαρκώς αυξητικές τάσεις, επιφυλάσσοντας αρνητικές επιπτώσεις για την λειτουργία της συνολικά και κατ' επέκταση για την βιωσιμότητά της.

Η παρούσα εργασία αποσκοπεί να προσεγγίσει τις πλέον κατάλληλες μεθόδους διαχείρισης των επιχειρησιακών κινδύνων που εγκυμονεί η επεξεργασία προσωπικών δεδομένων από τον οργανισμό καθώς και η πιθανή μη συμμόρφωση αυτού με τις ισχύουσες κανονιστικές διατάξεις που διέπουν την προστασία των εν λόγω δεδομένων. Συγκεκριμένα, στο δεύτερο κεφάλαιο πραγματοποιείται εκτενής αναφορά στο νομικό πλαίσιο που διέπει την προστασία των προσωπικών δεδομένων, με ιδιαίτερη έμφαση στον Γενικό Κανονισμό Προστασίας Δεδομένων (ΕΕ) 2016/679 (General Data Protection Regulation – GDPR), ο οποίος τέθηκε σε εφαρμογή στις 25/5/2018 και αναπτύσσει άμεση και δεσμευτική ισχύ για όλες τις χώρες της Ευρωπαϊκής Ένωσης. Στο τρίτο κεφάλαιο, προσδιορίζονται οι πιθανοί κίνδυνοι για την ασφάλεια και την προστασία των προσωπικών δεδομένων που η εκάστοτε επιχείρηση φέρει στην κατοχή της, ενώ παράλληλα αποτυπώνεται η διαδικασία αποτίμησης αυτών και ειδικότερα ο τρόπος διεξαγωγής της προβλεπόμενης από τον Κανονισμό εκτίμησης αντικτύπου στην ιδιωτικότητα. Στο τέταρτο κατά σειρά κεφάλαιο, εξειδικεύονται οι διαδικασίες και τα μέτρα που συνιστούν την μέθοδο αποτελεσματικής διαχείρισης των ανωτέρω κινδύνων, ενώ στο πέμπτο παρουσιάζεται η μελέτη περίπτωσης μίας εμπορικής εταιρείας, κατά την οποία εντοπίστηκαν οι υφιστάμενες αποκλίσεις της από τις διατάξεις του

Κανονισμού και οι δυνητικοί κίνδυνοι για την προστασία των προσωπικών δεδομένων, για την αποτελεσματική διαχείριση των οποίων συνιστάται ένα ολοκληρωμένο και σαφώς οριοθετημένο πλάνο κανονιστικής συμμόρφωσης.

ΚΕΦΑΛΑΙΟ 2

Τα Προσωπικά Δεδομένα και η προστασία τους

2.1 Ιστορική αναδρομή

Το δικαίωμα στην ιδιωτική ζωή αποτελεί ένα από τα θεμελιώδη δικαιώματα του ανθρώπου, το οποίο διαμορφώθηκε αρχικά στα φιλελεύθερα συνταγματικά κείμενα του 18ου αιώνα και αναγνωρίστηκε αργότερα τόσο από την Οικουμενική Διακήρυξη Δικαιωμάτων του Ανθρώπου του Οργανισμού Ηνωμένων Εθνών το 1948 όσο και από την Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ) το 1950. Αργότερα, την δεκαετία του 1970, κατά την διάρκεια της οποίας κατέστη εμφανής ο κίνδυνος παραβίασης της ιδιωτικής ζωής σαν απόρροια της ραγδαίας τεχνολογικής εξέλιξης, εμφανίστηκε για πρώτη φορά στην ευρωπαϊκή και αμερικάνικη νομοθεσία το δικαίωμα του ατόμου στην προστασία των προσωπικών του δεδομένων, σαν μία ειδικότερη έκφανση του δικαιώματος στην ιδιωτικότητα. Το 1981, το Συμβούλιο της Ευρωπαϊκής Ένωσης προέβη στην κατάρτιση της διεθνούς σύμβασης 108 αναφορικά με την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία των δεδομένων προσωπικού χαρακτήρα, η οποία υπεγράφη από την Ελλάδα στις 17/2/1983 και τέθηκε σε ισχύ στη 1/12/1995. Η εν λόγω σύμβαση δεν ήταν μεν άμεσα εφαρμοστέα για τα κράτη μέλη, επηρέασε ωστόσο σε μεγάλο βαθμό τη νοοτροπία τους σε νομοθετικό επίπεδο.

Η ανάδειξη της προστασίας των προσωπικών δεδομένων σε αυτοτελές ατομικό δικαίωμα πραγματοποιήθηκε μέσα από μία σειρά νομικών κειμένων που ακολούθησαν, τα οποία και θέσπιζαν μέτρα αυξημένης ισχύος για την αποτελεσματική αντιμετώπιση δυνητικών κινδύνων και παραβιάσεων. Πρόκειται για την Οδηγία 95/46/ΕΚ που αποτέλεσε ορόσημο της προστασίας προσωπικών δεδομένων και ενσωματώθηκε στην ελληνική έννομη τάξη με τον Ν. 2472/1997 (Α'50), την Συνθήκη της Λισαβόνας και συγκεκριμένα το άρθρο 16 αυτής για την λειτουργία της Ευρωπαϊκής Ένωσης, καθώς επίσης και τον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, δυνάμει του οποίου κατοχυρώθηκαν οι βασικές αρχές της προστασίας των προσωπικών δεδομένων και ο κανόνας της νομιμότητας της επεξεργασίας τους.

Ωστόσο, στην πορεία αποδείχτηκε ότι οι διατάξεις της Οδηγίας 95/46/ΕΕ δεν επέφεραν την απαιτούμενη συνεκτικότητα στον χώρο της Ευρωπαϊκής Ένωσης, εξ' ου και κρίθηκε αναγκαία η διαμόρφωση ενός ισχυρότερου νομικού πλαισίου για την προστασία των προσωπικών δεδομένων με την μορφή Κανονισμού, με σκοπό την ενιαία και

ομοιόμορφη εφαρμογή του στην ευρωπαϊκή επικράτεια. Τον ρόλο αυτό καλείται να διαδραματίσει ο νέος Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα (General Data Protection Regulation – GDPR), γνωστός και ως «Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων» (εφεξής «Κανονισμός») που τέθηκε σε εφαρμογή την 25η Μαΐου 2018. Ο εν λόγω Κανονισμός, ο οποίος αντικατέστησε την Οδηγία 95/46/ΕΚ και δεν απαιτεί την ενσωμάτωσή του με νόμους από τα κράτη μέλη, στοχεύει στον επαναπροσδιορισμό της προστασίας των προσωπικών δεδομένων και την ενίσχυση του σεβασμού της ιδιωτικής ζωής του ατόμου μέσω ενός αυστηρότερου πλέγματος διαδικασιών και μεθόδων ελέγχου. Ωστόσο, πρόκειται αναμφίβολα για ένα άκρως δυναμικό νομοθέτημα, άρρηκτα συνδεδεμένο με τις σύγχρονες κοινωνικοοικονομικές τάσεις και τεχνολογικές εξελίξεις και ως εκ τούτου η εφαρμογή του δεν δύναται να εξασφαλίσει στον μέγιστο βαθμό την ασφάλεια των προσωπικών δεδομένων, ούτε να εξαλείψει τους κινδύνους που απειλούν την προστασία τους, Αποτελεί, παρ' όλα αυτά, μία άρτια νομική βάση που θέτει τα θεμέλια για τον αποτελεσματικό περιορισμό των εκάστοτε απειλών που ελλοχεύουν καθημερινά και συνιστούν σημαντική προσβολή για τον πυρήνα της ιδιωτικότητας του ατόμου.

2.2 Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων(GDPR)

2.2.1 Βασικοί όροι και έννοιες

Η έννοια των δεδομένων συχνά συγχέεται με εκείνη των πληροφοριών, διότι στην πραγματικότητα η διαφοροποίηση μεταξύ των δύο εννοιών είναι τόσο λεπτή που εύκολα μπορεί να οδηγήσει σε ερμηνευτικά προβλήματα. Τα δεδομένα αποτελούν ένα σύνολο καταγεγραμμένων συμβόλων, τα οποία αντιπροσωπεύουν διάφορες πτυχές τόσου του πραγματικού όσο και του νοητού μας κόσμου. Από την άλλη πλευρά, ως πληροφορία θεωρούνται τα δεδομένα αυτά συμπεριλαμβανομένης της υποκειμενικής ερμηνείας που εμπερικλείουν. Τα δεδομένα αποτελούν το μέσο παραγωγής, αποθήκευσης και μετάδοσης των πληροφοριών. Στην πράξη, ωστόσο, η διασφάλιση των πληροφοριών καθίσταται πιο δύσκολη σε σχέση με την διασφάλιση των δεδομένων, εξ' ου και τις περισσότερες φορές ο όρος «ασφάλεια πληροφοριών» αντικαθίσταται από τον όρο «ασφάλεια δεδομένων».

Ως εκ τούτου, για την αποφυγή παρερμηνειών, κρίνεται αναγκαίο στο σημείο αυτό να δοθούν οι ορισμοί των βασικότερων εννοιών που θα χρησιμοποιηθούν στην συνέχεια, μεταξύ των οποίων η έννοια των προσωπικών δεδομένων, όπως ακριβώς προσδιορίζονται από το άρθρο 4 του Γενικού Κανονισμού για την Προστασία των Προσωπικών Δεδομένων:

- **«δεδομένα προσωπικού χαρακτήρα**: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου

- **επεξεργασία**: κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή

- **περιορισμός της επεξεργασίας**: η επισήμανση αποθηκευμένων δεδομένων προσωπικού χαρακτήρα με στόχο τον περιορισμό της επεξεργασίας τους στο μέλλον

- **κατάρτιση προφίλ**: οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου

- **ψευδωνυμοποίηση**: η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών εφόσον οι εν λόγω

συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο

- **υπεύθυνος επεξεργασίας**: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους

- **εκτελών την επεξεργασία**: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας

- **αποδέκτης**: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, στα οποία κοινολογούνται τα δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για τρίτον είτε όχι. Ωστόσο, οι δημόσιες αρχές που ενδέχεται να λάβουν δεδομένα προσωπικού χαρακτήρα στο πλαίσιο συγκεκριμένης έρευνας σύμφωνα με το δίκαιο της Ένωσης ή κράτους μέλους δεν θεωρούνται ως αποδέκτες· η επεξεργασία των δεδομένων αυτών από τις εν λόγω δημόσιες αρχές πραγματοποιείται σύμφωνα με τους ισχύοντες κανόνες προστασίας των δεδομένων ανάλογα με τους σκοπούς της επεξεργασίας

- **τρίτος**: οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέας, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα

- **συγκατάθεση του υποκειμένου των δεδομένων**: κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν

- **παραβίαση δεδομένων προσωπικού χαρακτήρα**: η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία

- **γενετικά δεδομένα**: τα δεδομένα προσωπικού χαρακτήρα που αφορούν τα γενετικά χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν, όπως προκύπτουν, ιδίως, από ανάλυση βιολογικού δείγματος του εν λόγω φυσικού προσώπου και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με την φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου

- **βιομετρικά δεδομένα**: δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα

- **δεδομένα που αφορούν την υγεία**: δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, περιλαμβανομένης της παροχής υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του

- **κύρια εγκατάσταση**: α) όταν πρόκειται για υπεύθυνο επεξεργασίας με εγκαταστάσεις σε περισσότερα του ενός κράτη μέλη, ο τόπος της κεντρικής του διοίκησης στην Ένωση, εκτός εάν οι αποφάσεις όσον αφορά τους σκοπούς και τα μέσα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα λαμβάνονται σε άλλη εγκατάσταση του υπευθύνου επεξεργασίας στην Ένωση και η εγκατάσταση αυτή έχει την εξουσία εφαρμογής των αποφάσεων αυτών, οπότε ως κύρια εγκατάσταση θεωρείται η εγκατάσταση στην οποία έλαβε τις αποφάσεις αυτές,

  β) όταν πρόκειται για εκτελούντα την επεξεργασία με εγκαταστάσεις σε περισσότερα του ενός κράτη μέλη, ο τόπος της κεντρικής του διοίκησης στην Ένωση ή, εάν ο εκτελών την επεξεργασία δεν έχει κεντρική διοίκηση στην Ένωση, η εγκατάσταση του εκτελούντος την επεξεργασία στην Ένωση στην οποία εκτελούνται οι κύριες δραστηριότητες επεξεργασίας στο πλαίσιο των δραστηριοτήτων εγκατάστασης του εκτελούντος την επεξεργασία, στον βαθμό που ο εκτελών την επεξεργασία υπόκειται σε ειδικές υποχρεώσεις δυνάμει του παρόντος κανονισμού

- **επιχείρηση**: φυσικό ή νομικό πρόσωπο που ασκεί οικονομική δραστηριότητα, ανεξάρτητα από τη νομική του μορφή, περιλαμβανομένων των προσωπικών εταιρειών ή των ενώσεων που ασκούν τακτικά οικονομική δραστηριότητα

- **όμιλος επιχειρήσεων**: μια ελέγχουσα επιχείρηση και οι ελεγχόμενες από αυτήν επιχειρήσεις

- **δεσμευτικοί εταιρικοί κανόνες**: οι πολιτικές προστασίας δεδομένων προσωπικού χαρακτήρα τις οποίες ακολουθεί ένας υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία εγκατεστημένος στο έδαφος κράτους μέλους για διαβιβάσεις ή δέσμη διαβιβάσεων δεδομένων προσωπικού χαρακτήρα σε υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία σε μία ή περισσότερες τρίτες χώρες εντός ομίλου επιχειρήσεων, ή ομίλου εταιρειών που ασκεί κοινή οικονομική δραστηριότητα

- **εποπτική αρχή**: ανεξάρτητη δημόσια αρχή που συγκροτείται από κράτος μέλος σύμφωνα με το άρθρο 51 το Κανονισμού

- **διασυνοριακή επεξεργασία**: α) η επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία γίνεται στο πλαίσιο των δραστηριοτήτων διάφορων εγκαταστάσεων σε περισσότερα του ενός κράτη μέλη υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση όπου ο υπεύθυνος επεξεργασίας ή ο εκτελών επεξεργασία είναι εγκατεστημένος σε περισσότερα του ενός κράτη μέλη ή

  β) η επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία γίνεται στο πλαίσιο των δραστηριοτήτων μίας μόνης εγκατάστασης υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση αλλά που επηρεάζει ή ενδέχεται να επηρεάσει ουσιωδώς υποκείμενα των δεδομένων σε περισσότερα του ενός κράτη μέλη

- **σχετική και αιτιολογημένη ένσταση**: ένσταση σε ένα σχέδιο απόφασης ως προς την ύπαρξη παράβασης του παρόντος κανονισμού, ή ως προς τη συμφωνία με τον παρόντα κανονισμό της προβλεπόμενης ενέργειας σε σχέση με τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία, η οποία καταδεικνύει σαφώς τη σημασία των κινδύνων που εγκυμονεί το σχέδιο απόφασης όσον αφορά τα θεμελιώδη δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και, κατά περίπτωση, την ελεύθερη κυκλοφορία δεδομένων προσωπικού χαρακτήρα εντός της Ένωσης

- **διεθνής οργανισμός**: οργανισμός και οι υπαγόμενοι σε αυτόν φορείς που διέπονται από το δημόσιο διεθνές δίκαιο ή οποιοσδήποτε άλλος φορέας που έχει ιδρυθεί δυνάμει ή επί τη βάσει συμφωνίας μεταξύ δύο ή περισσότερων χωρών»

2.2.2 Αρχές επεξεργασίας των προσωπικών δεδομένων

Σημείο αναφοράς για την προστασία των προσωπικών δεδομένων αποτελούν οι αρχές που πρέπει να διέπουν την επεξεργασία τους, η οποία και συνιστά ουσιώδη επέμβαση στα θεμελιώδη δικαιώματα του ατόμου και την σφαίρα της ιδιωτικής του ζωής. Συγκεκριμένα, πρόκειται για τις ακόλουθες αρχές, όπως ακριβώς προσδιορίζονται στο άρθρο 5 του Κανονισμού:

- ✓ **Αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας**, η οποία ορίζει ότι τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο αναφορικά με το υποκείμενο των δεδομένων. Διαφανής καθίσταται η επεξεργασία των προσωπικών δεδομένων όταν υφίσταται προγενέστερη συνοπτική, κατανοητή και σαφής ενημέρωση του υποκειμένου αυτών. Για να μπορεί δε να χαρακτηριστεί νόμιμη, θα πρέπει να θεμελιώνεται σε μία από τις λεγόμενες βάσεις νομιμότητας της επεξεργασίας που αποτυπώνονται στο άρθρο 6 του Κανονισμού, μεταξύ των οποίων η συγκατάθεση του υποκειμένου των δεδομένων, η εκπλήρωση συμβατικών ή εκ του νόμου υποχρεώσεων, η διαφύλαξη ζωτικών συμφερόντων του υποκειμένου, η εξυπηρέτηση έργου δημοσίου συμφέροντος και η ικανοποίηση εννόμων συμφερόντων του υπεύθυνου επεξεργασίας. Ο όρος «σύννομη» δεν υποδηλώνει μόνο την γενικότερη υποχρέωση συμμόρφωσης με τον νόμο, αλλά καταδεικνύει την ανάγκη άμεσης νομοθετικής παρέμβασης, ούτως ώστε η συλλογή και η επεξεργασία των προσωπικών δεδομένων να καθίσταται σύμφωνη με τα συνταγματικά κατοχυρωμένα δικαιώματα του ανθρώπου τόσο σε εθνικό όσο και σε ευρωπαϊκό επίπεδο.

- ✓ **Αρχή του περιορισμού του σκοπού**, σύμφωνα με την οποία τα δεδομένα πρέπει να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο με αυτούς. Η αρχή αυτή οριοθετεί τις δυνατότητες επέμβασης και συλλογής των δεδομένων, περιορίζει ποιοτικά την εμβέλεια της επεξεργασίας και καθορίζει την διάρκειά της. Η αξία της έγκειται στον περιορισμό της χρήσης δεδομένων του προσώπου κατά τρόπο τέτοιο ώστε να μην καταστρατηγούνται τα δικαιώματα αυτού μέσω ανεπίτρεπτων χρήσεων.

Η γνώση και η κατανόηση των σκοπών της επεξεργασίας από το υποκείμενο των δεδομένων αποτελεί απαραίτητη προϋπόθεση για την υποβολή της συγκατάθεσής του και την άσκηση των δικαιωμάτων του και ως εκ τούτου οι σκοποί αυτοί θα πρέπει να είναι σαφώς οριοθετημένοι και συμβατοί με όλους τους κανόνες προστασίας προσωπικών δεδομένων.

- ✓ **Αρχή της αναλογικότητας** («ελαχιστοποίηση των δεδομένων»), δυνάμει της οποίας τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να είναι πρόσφορα, συναφή και αναγκαία σε σχέση με τους επιδιωκόμενους σκοπούς της επεξεργασίας. Η εν λόγω αρχή, η οποία τελεί σε άρρηκτη σχέση με την αμέσως προηγούμενη, συνίσταται στην απαίτηση ύπαρξης εύλογης σχέσης μεταξύ αφενός του νόμιμου σκοπού που επιδιώκεται κάθε φορά μέσω της επεξεργασίας των προσωπικών δεδομένων και αφετέρου της έντασης, έκτασης και διάρκειας του συνακόλουθου περιορισμού που υφίστανται τα δικαιώματα του υποκειμένου από την επεξεργασία αυτή.

- ✓ **Αρχή της ακρίβειας των δεδομένων:** Τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι ακριβή, καθώς και να επικαιροποιούνται, όταν κάτι τέτοιο καθίσταται αναγκαίο. Συγχρόνως προβλέπεται η άμεση διαγραφή και διόρθωση με εύλογα μέτρα εκείνων των δεδομένων που θεωρούνται ανακριβή σε σχέση με τους σκοπούς της επεξεργασίας.

- ✓ **Αρχή της ακεραιότητας και της εμπιστευτικότητας:** Πρόκειται για μία αρχή που δεν απαντάται σε προγενέστερα ευρωπαϊκά νομοθετήματα για την προστασία των προσωπικών δεδομένων αλλά εισάγεται για πρώτη φορά μέσω των διατάξεων του Κανονισμού. Τα δεδομένα θα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που εξασφαλίζει με την χρήση κατάλληλων τεχνικών και οργανωτικών μέτρων την ενδεδειγμένη ασφάλειά τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά.

- ✓ **Αρχή του καθορισμού της χρονικής διάρκειας της επεξεργασίας** («περιορισμός της περιόδου αποθήκευσης»), η οποία αποτελεί μία ειδικότερη έκφανση της αρχής της αναλογικότητας, προσδιορίζει ως νόμιμο χρονικό όριο διατήρησης των προσωπικών δεδομένων το διάστημα εκείνο που απαιτείται αποκλειστικά και μόνο για την επίτευξη των σκοπών της επεξεργασίας. Εξαίρεση από την αρχή της περιορισμένης χρονικής διάρκειας διατήρησης των δεδομένων αποτελεί η διατήρηση αυτών για μελλοντική χρήση μόνο για επιστημονικούς, ιστορικούς, στατιστικούς σκοπούς ή σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, υποκείμενη

ωστόσο σε επιπρόσθετα μέτρα ασφαλείας και ειδικές εγγυήσεις δυνάμει του εθνικού δικαίου.

- ✓ **Αρχή της λογοδοσίας του υπεύθυνου επεξεργασίας:** Η αρχή αυτή, γνωστή και ως “accountability principle”, αποτελεί μία από τις σημαντικότερες ρυθμίσεις του Κανονισμού, η οποία αποτυπώνει την προσπάθεια του ευρωπαϊκού νομοθέτη να θέσει υπόψη των υπεύθυνων επεξεργασίας την σοβαρότητα της ανάληψης ευθύνης από πλευράς τους για τα προσωπικά δεδομένα τα οποία αυτοί συλλέγουν και διαχειρίζονται. Η έννοια της λογοδοσίας, η οποία συνίσταται στην υποχρέωση μίας οντότητας να αιτιολογεί τις ενέργειές της, σχετίζεται αλλά δεν ταυτίζεται με την έννοια της ευθύνης (responsibility), καθώς αποτελούν αλληλοσυμπληρούμενες πτυχές του μοντέλου χρηστής διακυβέρνησης. Ειδικότερα, στην δεύτερη παράγραφο του άρθρου 5 του Κανονισμού, ορίζεται ότι ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και πρέπει να είναι σε θέση να αποδείξει την συμμόρφωση του με όλες τις ανωτέρω αρχές προστασίας προσωπικών δεδομένων. Σημειώνεται ότι δεν απαιτείται κατά κυριολεξία από τους υπεύθυνους επεξεργασίας η παροχή συγκεκριμένων αποδείξεων, αλλά εισάγεται μία γενικότερη υποχρέωση αυτών για την εφαρμογή εκείνων των μέτρων που θα διασφαλίζουν την συμμόρφωση τους με το σύνολο των κανονιστικών διατάξεων στον μεγαλύτερο δυνατό βαθμό, αφήνοντάς τους παράλληλα περιθώρια ελεύθερης επιλογής των ειδικότερων μέσων και πολιτικών.

2.2.3 Δικαιώματα του υποκειμένου των δεδομένων

Ένας από τους βασικούς πυλώνες της προστασίας των προσωπικών δεδομένων αποτελεί η κατοχύρωση των δικαιωμάτων των προσώπων. Υπό το πρίσμα αυτό, ο νέος Κανονισμός αναγνωρίζει νέα δικαιώματα, επικαιροποιεί άλλα ήδη υπάρχοντα και θεσπίζει νέους κανονισμούς για την αποτελεσματική ενίσχυση της προστασίας τους. Ορισμένα από τα πιο σημαντικά δικαιώματα του υποκειμένου είναι:

Δικαίωμα ενημέρωσης (άρθρα 13 και 14): Το δικαίωμα ενημέρωσης του υποκειμένου πηγάζει από την αρχή της διαφάνειας, σύμφωνα με την οποία, όπως χαρακτηριστικά αναφέρεται στην αιτιολογική σκέψη 39, κάθε πληροφορία και ανακοίνωση σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα πρέπει να είναι εύκολα προσβάσιμη και κατανοητή με σαφή και απλή γλώσσα, μη επιδεχόμενης παρερμηνειών. Η υποχρέωση ενημέρωσης υφίσταται είτε η οι σχετικές πληροφορίες προς επεξεργασία συλλέγονται από το ίδιο το υποκείμενο των δεδομένων (άρθρο 13)

είτε από άλλες πηγές (άρθρο 14). Βασικά στοιχεία της ενημέρωσης του υποκειμένου είναι η ταυτότητα του υπεύθυνου επεξεργασίας, τα στοιχεία επικοινωνίας του, οι σκοποί της επεξεργασίας, οι αποδέκτες των δεδομένων και η πρόθεση του υπεύθυνου επεξεργασίας να διαβιβάσει τα δεδομένα σε τρίτη χώρα ή οργανισμό. Επιπλέον, τα φυσικά πρόσωπα θα πρέπει να είναι πλήρως ενήμερα για την ύπαρξη πιθανών κινδύνων καθώς και για τα δικαιώματά τους και τον τρόπο άσκησης σε αυτών. Οι σκοποί της επεξεργασίας δε, θα πρέπει να είναι σαφείς, νόμιμοι και προσδιορισμένοι κατά τον χρόνο συλλογής των δεδομένων. Το δικαίωμα ενημέρωσης, το οποίο αποτελεί έκφανση του δικαιώματος πληροφοριακού αυτοκαθορισμού του ατόμου, αποσκοπεί να βελτιώσει αισθητά το επίπεδο προστασίας του υποκειμένου και να καταστήσει σαφές ότι κρίσιμη δεν καθίσταται μόνο η παραβίαση των προσωπικών δεδομένων αλλά και διαχείριση αυτής με τον κατάλληλο τρόπο από τον υπεύθυνο επεξεργασίας μέσω της ουσιαστικής ενημέρωσης των άμεσα ενδιαφερόμενων προσώπων.

Δικαίωμα πρόσβασης (άρθρο 15): Για την άσκηση του εν λόγω δικαιώματος από το υποκείμενο των δεδομένων, προαπαιτούμενο αποτελεί η έγκαιρη και πλήρης πληροφόρηση αυτού, όπως αναφέρθηκε αναλυτικά κατά τα ανωτέρω. Πρόκειται για ένα δικαίωμα που διασφαλίζει στο άτομο την δυνατότητα να λαμβάνει επιβεβαίωση από τον υπεύθυνο επεξεργασίας για το κατά πόσον ή όχι τα δεδομένα προσωπικού χαρακτήρα που το αφορούν υφίστανται επεξεργασία, καθώς και την πρόσβαση, σε περίπτωση που τούτο συμβαίνει, σε πληροφορίες που αφορούν ενδεικτικά στους σκοπούς της επεξεργασίας, τις κατηγορίες των δεδομένων, τους εκάστοτε αποδέκτες και την ύπαρξη αυτοματοποιημένης λήψης των αποφάσεων. Προβλέπεται μάλιστα η παροχή από τον υπεύθυνο επεξεργασίας αντιγράφου των δεδομένων προσωπικού χαρακτήρα που υπόκεινται σε επεξεργασία προς το υποκείμενο αυτό, κατόπιν σχετικού αιτήματος.

Δικαίωμα διαγραφής ή «Δικαίωμα στη λήθη» (άρθρο 17) : Πρόκειται για ένα δικαίωμα που συνιστά απόρροια της γενικότερης ελευθερίας αναπτύξεως της προσωπικότητας του ατόμου (άρθρο 5 παρ. 1 Συντάγματος) συνδυαστικά με την κατοχύρωση της αξίας του ανθρώπου (άρθρο 3 παρ. 1 Συντάγματος) και το δικαίωμα προστασίας της ιδιωτικής ζωής (άρθρο 9 Συντάγματος). Με βάση το δικαίωμα αυτό, ο υπεύθυνος επεξεργασίας υποχρεούται να προβεί, κατόπιν αιτήσεως του υποκειμένου των δεδομένων, στην διαγραφή των προσωπικών του δεδομένων, χωρίς αδικαιολόγητη καθυστέρηση και δίχως να απαιτείται η επίκληση ζημίας εκ μέρους του υποκειμένου. Διασφαλίζεται έτσι ένα σημαντικό επίπεδο αυτονομίας του ατόμου, η οποία αντικατοπτρίζεται στην προστασία αυτού από την ακούσια έκθεση των δεδομένων του και την αλόγιστη επεξεργασία τους από δημόσιους ή ιδιωτικούς φορείς, ιδίως μέσω της

χρήσης του διαδικτύου και των μηχανών αναζήτησης. Το εν λόγω δικαίωμα τυγχάνει εφαρμογής σε περίπτωση που συντρέχουν συγκεκριμένοι λόγοι, συμπεριλαμβανομένης της ανάκλησης συγκατάθεσης του υποκειμένου, της έλλειψης νόμιμης επεξεργασίας, της υπέρβασης του αναγκαίου για τον σκοπό της επεξεργασίας χρόνου τήρησης και της προβλεπόμενης εκ του νόμου διαγραφής. Ωστόσο, το δικαίωμα της διαγραφής δεν είναι απεριόριστο αλλά αντίθετα οριοθετείται, για παράδειγμα, από λόγους δημοσίου συμφέροντος, την ύπαρξη νόμιμης βάσης επεξεργασίας και από σκοπούς επιστημονικής ή ιστορικής έρευνας.

Δικαίωμα περιορισμού της επεξεργασίας (άρθρο 18): Σε περίπτωση που διαζευκτικά και όχι σωρευτικά α) η ακρίβεια των προσωπικών δεδομένων αμφισβητείται από το υποκείμενο τους, β) η επεξεργασία καθίσταται παράνομη και το υποκείμενο αιτείται τον περιορισμό αυτής αντί της διαγραφής των δεδομένων, γ) ο υπεύθυνος επεξεργασίας δεν χρειάζεται πλέον τα δεδομένα για τους σκοπούς της επεξεργασίας αλλά τα δεδομένα αυτά απαιτούνται από το υποκείμενο για την θεμελίωση νομικών του αξιώσεων ή δ) το υποκείμενο των δεδομένων έχει αντιρρήσεις για την επεξεργασία σύμφωνα με το άρθρο 21 παρ.1 του Κανονισμού(δικαίωμα εναντίωσης), εν αναμονή επαληθεύσεως του κατά πόσον οι νόμιμοι λόγοι του υπεύθυνου επεξεργασίας υπερτερούν έναντι των δικών του, τότε δικαιούται να εξασφαλίζει τον περιορισμό της επεξεργασίας των προσωπικών του δεδομένων από τον υπεύθυνο επεξεργασίας. Πρόκειται επί της ουσίας για ένα δικαίωμα που παρέχει προσωρινή προστασία στο υποκείμενο των δεδομένων, ιδίως στην περίπτωση που εκκρεμεί η διαλεύκανση μίας νομικής κατάστασης.

Δικαίωμα στην φορητότητα (άρθρο 20): Δυνάμει του δικαιώματος αυτού, το οποίο συνιστά καινοτομία του Κανονισμού και απορρέει από την γενικότερη ανάγκη ελέγχου των πληροφοριών, δίνει την δυνατότητα στο υποκείμενο των δεδομένων να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν και που ήδη έχει παράσχει σε έναν υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και να τα διαβιβάζει σε άλλον υπεύθυνο επεξεργασίας, υπό τον όρο ότι η επεξεργασία των δεδομένων διενεργείται με αυτοματοποιημένα μέσα και βασίζεται αποκλειστικά και μόνο στην νόμιμη βάση της συγκατάθεσης ή της συμβάσεως. Σύμφωνα με τον Κανονισμό, μάλιστα, η άσκηση του δικαιώματος φορητότητας δεν θα πρέπει θίγει τα δικαιώματα και τις ελευθερίες άλλων υποκειμένων των δεδομένων. Πρόκειται για ένα δικαίωμα που στην ουσία διευκολύνει την διαβίβαση των δεδομένων από τον ένα πάροχο στον άλλον, ενώ παράλληλα εξυπηρετεί την

επαναχρησιμοποίηση των δεδομένων από το υποκείμενο αυτό για διαφορετικούς σκοπούς και σε διαφορετικές υπηρεσίες.

Δικαίωμα εναντίωσης (άρθρα 20 και 21): Ο Κανονισμός παρέχει το δικαίωμα στο υποκείμενο των δεδομένων να αντιτάσσεται ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του στην επεξεργασία των προσωπικών του δεδομένων, η οποία αφορά είτε στην εκπλήρωση δημοσίου συμφέροντος είτε την ικανοποίηση έννομου συμφέροντος. Στην προκειμένη περίπτωση, το βάρος απόδειξης φέρει ο υπεύθυνος επεξεργασίας, ο οποίος θα πρέπει να αποδείξει τόσο το σύννομο της επεξεργασία όσο και την συνδρομή επιτακτικών λόγων που οδήγησαν σε αυτή και υπερισχύουν των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων. Ιδιόμορφο δικαίωμα εναντίωσης αποτελεί το δικαίωμα του προσώπου να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο. Για παράδειγμα, τέτοια περίπτωση μπορεί να συνιστά η αυτόματη άρνηση επιγραμμικής αίτησης πίστωσης ή πρακτικές ηλεκτρονικών προσλήψεων χωρίς ανθρώπινη παρέμβαση.

2.2.4 Κυρώσεις του Κανονισμού

Το σύστημα προστασίας των προσωπικών δεδομένων διέπεται από ένα σύνολο κυρωτικών μηχανισμών, οι οποίοι τίθενται σε εφαρμογή όταν παραβιάζονται οι κανόνες και οι υποχρεώσεις που προβλέπονται από τις διατάξεις του Κανονισμού. Πρόκειται για κυρώσεις, τόσο ποινικές όσο και διοικητικές, που δεν συνιστούν απλά μία μέθοδο εξαναγκασμού της συμμόρφωσης και επιβολής του δικαίου, αλλά αναπτύσσουν μία γενικότερη αποτρεπτική λειτουργία, λαμβάνοντας υπόψη την κοινωνική απαξία που ενέχει η οποιαδήποτε προσβολή της προστασίας των προσωπικών δεδομένων. Καίρια κανονιστική παρέμβαση του ευρωπαίου νομοθέτη αποτελεί η ρύθμιση περί επιβολής προστίμων, ενώ ταυτόχρονα θεσπίζονται περισσότεροι και πιο εξειδικευμένοι κανόνες για την αντιμετώπιση των παραβιάσεων, με απώτερο σκοπό την συνεκτική και εναρμονισμένη εφαρμογή τους από όλα τα κράτη μέλη της Ένωσης.

Τα διοικητικά πρόστιμα αποτελούν την ισχυρότερη μορφή των προβλεπόμενων από τον Κανονισμό κυρώσεων και επιβάλλονται επιπρόσθετα ή αντί των μέτρων που εφαρμόζονται από την εκάστοτε αρμόδια εποπτική αρχή στα πλαίσια των λεγόμενων διορθωτικών της εξουσιών (corrective powers). Ως διορθωτικές δε εξουσίες ορίζονται,

μεταξύ άλλων, στο άρθρο 58 του Κανονισμού, οι προειδοποιήσεις ή επιπλήξεις της εποπτικής αρχής προς τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία, σε περίπτωση παράβασης των κανονιστικών διατάξεων από πλευράς τους, οι εντολές για συμμόρφωση προς τα αιτήματα του υποκειμένου των δεδομένων, η επιβολή προσωρινού ή οριστικού περιορισμού της επεξεργασίας ή η απαγόρευση αυτής και η εντολή διόρθωσης ή διαγραφής των προσωπικών δεδομένων.

Ειδικότερα, στο άρθρο 83 του Κανονισμού προσδιορίζεται τόσο το ύψος των διοικητικών προστίμων όσο και το πεδίο των παραβάσεων για τις οποίες αυτά επιβάλλονται. Οι παραβάσεις των διατάξεων που αφορούν σε υποχρεώσεις του υπεύθυνου επεξεργασίας και του εκτελούντος την επεξεργασία, του φορέα πιστοποίησης καθώς και του φορέα παρακολούθησης ενδέχεται να επισύρουν διοικητικά πρόστιμα έως δέκα εκατομμύρια ευρώ ή, σε περίπτωση επιχειρήσεων, έως το 2% του συνολικού παγκόσμιου κύκλου εργασιών του προηγούμενου οικονομικού έτους. Οι παραβάσεις που αφορούν στις αρχές επεξεργασίας των προσωπικών δεδομένων, την διαβίβαση αυτών σε αποδέκτη τρίτης χώρας ή σε διεθνή οργανισμό, τα δικαιώματα του υποκειμένου των δεδομένων, την μη συμμόρφωση με τις εντολές της εποπτικής αρχές και τις ειδικότερες υποχρεώσεις που θεσπίζονται από τα εθνικά δίκαια των κρατών μελών, δύνανται να επισύρουν διοικητικά πρόστιμα έως είκοσι εκατομμύρια ευρώ ή, σε περίπτωση επιχειρήσεων, έως το 4% του συνολικού παγκόσμιου κύκλου εργασιών του προηγούμενου οικονομικού έτους. Σε αμφότερες τις περιπτώσεις, ο Κανονισμός προβλέπει ότι επιβάλλεται το υψηλότερο κάθε φορά πρόστιμο.

Κρίσιμοι παράγοντες για τον καθορισμό του ύψους τους επιβαλλόμενου προστίμου καθίστανται η φύση, η βαρύτητα και η διάρκεια της παράβασης, λαμβανομένων υπόψη της φύσης, της έκτασης ή του σκοπού της επεξεργασίας, του αριθμού των υποκειμένων των δεδομένων που έθιξε η παράβαση, καθώς και τον βαθμό ζημίας που αυτά υπέστησαν. Άλλα στοιχεία που λαμβάνονται υπόψη για την επιβολή του διοικητικού προστίμου και τον προσδιορισμό του ύψος αυτού είναι η ύπαρξη δόλου ή αμέλειας, ο βαθμός ευθύνης του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία αναφορικά με την λήψη τεχνικών και οργανωτικών μέτρων προστασίας, οι προσπάθειες και ενέργειες μετριασμού των επιπτώσεων της παράβασης, η ύπαρξη προηγούμενων παραβάσεων, ο βαθμός συνεργασίας με την εποπτική αρχή, καθώς και η τήρηση κωδίκων δεοντολογίας ή εγκεκριμένων μηχανισμών πιστοποίησης. Παρατηρείται, λοιπόν, ότι πέρα από τον καθορισμό του ανώτατου ύψους των προστίμων, ο Κανονισμός κατοχυρώνει επίσης ένα σύνολο κριτηρίων, προκειμένου να τηρείται η αρχή της αναλογικότητας κατά την επιβολή των προστίμων από τις εποπτικές αρχές και

να προστατεύονται έτσι οι υπεύθυνοι επεξεργασίας ή οι εκτελούντες την επεξεργασία από τυχόν δυσανάλογες κυρώσεις.

Τέλος, επισημαίνεται ότι ο Κανονισμός αφήνει περιθώρια στα κράτη μέλη να θεσπίζουν περαιτέρω κανόνες που θα ρυθμίζουν την επιβολή αποτελεσματικών, αναλογικών και αποτρεπτικών κυρώσεων για τις παραβάσεις των διατάξεών του, ιδίως δε για εκείνες που δεν αποτελούν αντικείμενο διοικητικών προστίμων, καθώς και να λαμβάνουν όλα τα αναγκαία μέτρα που θα εξασφαλίζουν την τήρησή τους.

2.3 Το εθνικό νομικό πλαίσιο προστασίας των προσωπικών δεδομένων

Στην ελληνική έννομη τάξη, η προστασία των προσωπικών δεδομένων απαντάται κατ' αρχήν στην διάταξη του άρθρου 9^{A} του Συντάγματος, σύμφωνα με το οποίο «Καθένας έχει δικαίωμα προστασίας από την συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει». Η διάταξη αυτή, η οποία προστέθηκε με το ψήφισμα της Ζ' Αναθεωρητικής Βουλής των Ελλήνων της 6^{ης} Απριλίου 2001, κατοχυρώνοντας για πρώτη φορά συνταγματικά την προστασία των δεδομένων προσωπικού χαρακτήρα στην Ελλάδα, αποτέλεσε καίρια νομοθετική ρύθμιση, καθώς υπό την ισχύ του Συντάγματος του 1975 προστατευόταν μεν η ιδιωτική και οικογενειακή ζωή του ατόμου, δεν υπήρχε ωστόσο συγκεκριμένη πρόβλεψη για την προστασία των προσωπικών του δεδομένων.

Έκτοτε, ακολούθησε μία σειρά από εθνικά νομοθετήματα, τα οποία εισήγαγαν ειδικότερες διατάξεις αναφορικά με την προστασία των προσωπικών δεδομένων, όπως χαρακτηριστικά αναφέρονται ως κάτωθι:

Νόμος 2472/1997 «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.»: Εκδόθηκε από το ελληνικό κράτος προς συμμόρφωση με την υπ' αριθμό 95/46 Οδηγία του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, η οποία υποχρέωνε τα κράτη-μέλη να προβούν στις αναγκαίες νομοθετικές, κανονιστικές και διοικητικές διατάξεις και αποτέλεσε αναμφίβολα την μήτρα του ελληνικού δικαίου.

Νόμος 3051/2002: «Συνταγματικά κατοχυρωμένες ανεξάρτητες αρχές, τροποποίηση και συμπλήρωση του συστήματος προσλήψεων στο δημόσιο τομέα και συναφείς ρυθμίσεις»

Νόμος 3471/2006: «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν. 2472/97»

Νόμος 3783/2009: «Ταυτοποίηση των κατόχων και χρηστών εξοπλισμού και υπηρεσιών κινητής τηλεφωνίας και άλλες διατάξεις»

Νόμος 3917/2011: «Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις»

Νόμος 4070/2012: «Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις»

Νόμος 4624/2019: «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις»

Ο νέος νόμος 4624/2019, ο οποίος δημοσιεύθηκε στο ΦΕΚ (137/Α/29-8-2019) στις 29 Αυγούστου 2019, συμπληρώνει τις διατάξεις του Γενικού Κανονισμού Προστασίας Δεδομένων και ενσωματώνει την Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου. Πρόκειται για ένα νομοθέτημα που εξειδικεύει τις λεγόμενες «ρήτρες ανοίγματος» που παρέχει ο Κανονισμός προς τα κράτη μέλη, ενώ παράλληλα καταργεί τον προγενέστερο Ν. 2472/1997 περί «Προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα», διατηρώντας σε ισχύ ορισμένες μόνο διατάξεις αυτού, μεταξύ των οποίων η δημοσιοποίηση προσωπικών δεδομένων από τις εισαγγελικές αρχές στην περίπτωση συγκεκριμένων αδικημάτων, η χρήση οπτικοακουστικού υλικού στις δημόσιες συναθροίσεις, η διάταξη σύστασης της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και αμοιβές των μελών της, καθώς και τα πλαίσια επιβολής διοικητικών προστίμων στους ιδιωτικούς φορείς.

Οι βασικότερες προβλέψεις του νέου εθνικού νόμου αφορούν στην οργάνωση και την λειτουργία της ΑΠΔΠΧ, την ενίσχυση της προστασίας των ανηλίκων μέσω της συγκατάθεσης αυτών ή των νόμιμων αντιπροσώπων τους για την επεξεργασία των προσωπικών τους δεδομένων, την απαλλαγή κατά περιπτώσεις του υπεύθυνου επεξεργασίας από την υποχρέωση ενημέρωσης του υποκειμένου των δεδομένων, την επεξεργασία προσωπικών δεδομένων στα πλαίσια σχέσεων απασχόλησης, καθώς και περιορισμούς στα δικαιώματα πρόσβασης, διαγραφής και εναντίωσης των προσώπων. Επιπροσθέτως, βάσει του Ν. 4624/2019, αρμόδιο για την διαπίστευση φορέων πιστοποίησης του άρθρου 43 του ΓΚΠΔ, αναφορικά με την συμμόρφωσή τους με την κείμενη νομοθεσία και σύμφωνα με το πρότυπο EN-ISO/IEC17065:2012, καθίσταται το Εθνικό Σύστημα Διαπίστευσης (Ε.ΣΥ.Δ.).

Σημαντική είναι επίσης και η ρύθμιση για την επιβολή ποινικών κυρώσεων, σύμφωνα με την οποία, όποιος με οποιονδήποτε τρόπο επεμβαίνει σε σύστημα αρχειοθέτησης προσωπικών δεδομένων, το διαγράφει, το αντιγράφει και εν γένει το χρησιμοποιεί παρανόμως, τιμωρείται με ποινή φυλάκισης ενός έτους. Εάν μάλιστα η παράνομη ως άνω πράξη αφορά σε δεδομένα ειδικών κατηγοριών, εκτός από την ποινή φυλάκισης προβλέπεται και χρηματική ποινή έως 100.000 ευρώ. Στην περίπτωση δε που ο υπαίτιος σκοπεύει με τις αξιόποινες πράξεις του να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος ή να προκαλέσει περιουσιακή ζημία και το συνολικό όφελος αυτής υπερβαίνει τα 120.000 ευρώ τιμωρείται με κάθειρξη έως δέκα χρόνια.

ΚΕΦΑΛΑΙΟ 3

Οι κίνδυνοι και η αποτίμησή τους

3.1 Οριοθέτηση της έννοιας του κινδύνου

3.1.1 Γενική εννοιολογική προσέγγιση

Η έννοια του κινδύνου εμφανίστηκε αρχικά κατά τον 17ο αιώνα σαν μία μαθηματική προσέγγιση της σχέσης μεταξύ της πιθανότητας και του μεγέθους των δυνητικών κερδών ή απωλειών που προέρχονταν από τα τυχερά παιχνίδια. Αργότερα, τον 18ο αιώνα, η έννοια του κινδύνου χρησιμοποιήθηκε για να αποδώσει κατά έναν ουδέτερο τρόπο τα κέρδη και τις απώλειες στον κλάδο της ναυτιλιακής ασφάλισης, ενώ τον 19ο αιώνα εμφανίστηκε για πρώτη φορά με μία πιο αρνητική χροιά στην οικονομική επιστήμη, οπότε και σχετίστηκε με την ανάληψη ρίσκου από πλευράς των επιχειρηματιών για την πραγματοποίηση επενδύσεων. Τον 20ο αιώνα, η έννοια του κινδύνου καθίσταται άμεσα συνυφασμένη με τα αποτελέσματα της επιστημονικής και τεχνολογικής προόδου και ως εκ τούτου απόκτα μία ακόμα περισσότερο αρνητική ερμηνεία.

Σήμερα, ο όρος κίνδυνος (risk) εμπεριέχει πολλές και διαφορετικές έννοιες στην εμπορική και καθημερινή ζωή. Σε γενικές γραμμές, χρησιμοποιείται για να αποτυπώσει μία κατάσταση στην οποία ενυπάρχει αβεβαιότητα ως προς το αναμενόμενο αποτέλεσμα. Στην στατιστική επιστήμη, την οικονομική διαχείριση αλλά και τον επενδυτικό τομέα, ο κίνδυνος αντιπροσωπεύει την πιθανή απόκλιση μίας αναμενόμενης τιμής. Όσο μεγαλύτερος είναι ο κίνδυνος, τόσο μικρότερη θα είναι η εκτιμώμενη κάθε φορά αξία, πράγμα το οποίο οφείλεται στην θετική σχέση μεταξύ κινδύνου και απόδοσης. Με άλλα λόγια, ένας υψηλός κίνδυνος συνεπάγεται υψηλή απαιτούμενη απόδοση, γεγονός που οδηγεί σε υψηλό κόστος κεφαλαίου και συνεπώς χαμηλή αξία.

Η έννοια του κινδύνου είναι άρρηκτα συνδεδεμένη με τις έννοιες της αβεβαιότητας και της πιθανότητας, εξ' ου και γίνεται κατανοητό ότι ο κίνδυνος περιλαμβάνει όχι μόνο την αρνητική έκβαση μίας κατάστασης, ήτοι απόδοση χαμηλότερη από την αναμενόμενη, αλλά και τη θετική έκβαση αυτής, ήτοι απόδοση μεγαλύτερη από την αναμενόμενη. Καθημερινά, τα άτομα και οι επιχειρήσεις καλούνται να αντιμετωπίσουν κινδύνους ικανούς να προκαλέσουν ζημίες ή να αποτελέσουν ευκαιρίες κέρδους. Κατά την εξέταση δε των δυνητικών ζημιών, χρήζουν ενδελεχούς διερεύνησης τόσο οι άμεσες ζημίες (direct losses) που ενδέχεται να προέλθουν εξαιτίας μίας επικίνδυνης

κατάστασης, όσο και οι έμμεσες ζημίες (indirect losses) που προκύπτουν ως παρεπόμενο αυτών. Για τις επιχειρήσεις, μάλιστα, οι έμμεσες ζημίες κρίνονται ιδιαίτερα σημαντικές και η πιθανότητα εμφάνισης αυτών αποτελεί έναν από τους βασικότερους λόγους που ωθούν τα διοικητικά στελέχη στην άμεση λήψη αποφάσεων για τον περιορισμό των επικείμενων κινδύνων. Για την αποφυγή των εκάστοτε οικονομικών ή άλλου είδους ζημιών, η έλευση των οποίων ενδέχεται να καταστήσει επισφαλή την βιωσιμότητα της επιχείρησης, κρίνεται απαραίτητη η έγκαιρη εφαρμογή των κατάλληλων μεθόδων διαχείρισης κινδύνων, όπως αυτές θα αναλυθούν εκτενώς στα κεφάλαια που ακολουθούν.

3.1.2 Η έννοια του κινδύνου για τα προσωπικά δεδομένα

Στον τομέα της ασφάλειας των προσωπικών δεδομένων, ο κίνδυνος αποτελεί το ενδεχόμενο μία συγκεκριμένη απειλή να εκμεταλλευτεί τις ευπάθειες ενός ή περισσότερων προστατευόμενων από την επιχείρηση αγαθών, προκαλώντας σοβαρές ζημίες σε αυτήν. Ο κίνδυνος (R) ορίζεται ως το γινόμενο της πιθανότητας (P) να συμβεί ένας συγκεκριμένος αριθμός περιστατικών παραβίασης ασφάλειας μέσα σε ένα συγκεκριμένο χρονικό διάστημα επί το κόστος (C) της ζημιάς που θα προκύψει (R= P x C). Στο σημείο αυτό, κρίνεται σκόπιμο να αποδοθούν σημασιολογικά οι παρακάτω βασικές έννοιες, οι οποίες συμβάλλουν στην κατανόηση της έννοιας του κινδύνου, των προϋποθέσεων εμφάνισής του και του τρόπου διαχείρισης αυτού:

- **Απειλή (threat):** είναι η δυνητική αιτία πρόκλησης ενός περιστατικού παραβίασης της ασφάλειας των δεδομένων, η οποία ενδέχεται να προκαλέσει ζημίες στα συστήματα του οργανισμού και κατ' επέκταση στην λειτουργία του γενικότερα. Κατηγοριοποιούνται σε απειλές φυσικές, τεχνικής φύσεως, καθώς και ανθρώπινες. Σύμφωνα με το άρθρο 4 του Γενικού Κανονισμού για την προστασία των προσωπικών δεδομένων, ως απειλή θεωρείται κάθε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατά άλλο τρόπο σε επεξεργασία. Προϋπόθεση εμφάνισης της απειλής αποτελεί η ευπάθεια του προβαλλόμενου αγαθού.

- **Ευπάθεια (vulnerability) :** είναι η αδυναμία που παρουσιάζει ένα αγαθό ή μία ομάδα αγαθών, η οποία καθίσταται εύκολα εκμεταλλεύσιμη από μία ή περισσότερες απειλές. Ενδεικτικά αναφέρονται οι ευπάθειες λογισμικού, όπως η παράλειψη αποσύνδεσης των χρηστών, οι ευπάθειες δικτύου, όπως λόγου χάριν η μη κρυπτογραφημένη μετάδοση εμπιστευτικών πληροφοριών και οι ευπάθειες

προσωπικού, όπως η έλλειψη διαδικασιών ασφάλειας ή ελλιπής ενημέρωση των εργαζομένων για την διαχείριση των εκάστοτε περιστατικών ασφάλειας.

- **Γεγονός (event) :** είναι ένα περιστατικό ή μία κατάσταση του δικτύου και των συστημάτων της επιχείρησης, που υποδεικνύει πιθανή παραβίαση της πολιτικής ασφάλειας των δεδομένων ή αναποτελεσματική εφαρμογή των μέτρων ασφάλειας.

- **Περιστατικό παραβίασης ασφάλειας (security incident):** πρόκειται για εκείνο το περιστατικό, το οποίο προκαλείται από ένα μεμονωμένο γεγονός ή μία σειρά ανεπιθύμητων γεγονότων ικανών να οδηγήσουν στην παραβίαση της ασφάλειας των προσωπικών δεδομένων ή άλλων εμπιστευτικών πληροφοριών της επιχείρησης.

- **Αντίμετρο ή μέτρο ασφάλειας (counter measure):** ως αντίμετρο θεωρείται κάθε μέτρο ικανό να συντελέσει στην αποτελεσματική διαχείριση του κινδύνου, όπως πολιτικές, κανόνες, διαδικασίες ή οργανωσιακές πρακτικές.

3.2 Κατηγορίες Κινδύνων

3.2.1 Οι κίνδυνοι της επιχείρησης γενικά

Από την πρώτη στιγμή λειτουργίας της, η επιχείρηση έρχεται καθημερινά αντιμέτωπη με πολλαπλούς κινδύνους, οι οποίοι μπορεί να χαρακτηρίζονται από διαφορετικό βαθμό σημαντικότητας και έντασης, χρήζουν ωστόσο μίας συνολικής και αποτελεσματικής διαχείρισης. Οι κίνδυνοι, ανάλογα με τα ιδιαίτερα χαρακτηριστικά τους και τους παράγοντες που συντελούν στην διαμόρφωσή τους, διακρίνονται σε πολλές επιμέρους κατηγορίες, μερικές από τις βασικότερες παρουσιάζονται αναλυτικά στην συνέχεια.

Μία από τις κύριες διακρίσεις των κινδύνων αυτών αποτελεί η κατηγοριοποίησή τους σε ενδογενείς και εξωγενείς. **Ενδογενείς** είναι οι κίνδυνοι οι οποίοι προέρχονται από το εσωτερικό της επιχείρησης και οφείλονται σε ελαττωματικές λειτουργίες ή διαδικασίες αυτής και οι οποίες σχετίζονται, παραδείγματος χάριν, με τον τομέα διαχείρισης του ανθρωπίνου δυναμικού, τον οικονομικό τομέα, την παραγωγή, την διαφήμιση και προώθηση των προϊόντων της (marketing) ή το κομμάτι της τεχνολογικής και μηχανογραφικής υποστήριξης γενικότερα. Αντίθετα, **εξωγενείς** χαρακτηρίζονται όσοι κίνδυνοι προέρχονται εξ' ολοκλήρου από το εξωτερικό περιβάλλον τις επιχείρησης, όπως μακροοικονομικό, πολιτικό, κοινωνικό και θεσμικό. Η αντιμετώπιση των εξωγενών κινδύνων καθίσταται περισσότερο δυσχερής, σε σχέση με τους ενδογενείς,

λόγω του πολύ μικρού βαθμού επιρροής που δύναται να ασκήσει η επιχείρηση πάνω τους.

Ειδικότερα, οι κίνδυνοι που καλείται να αντιμετωπίσει η σύγχρονη επιχείρηση μπορούν να ομαδοποιηθούν στις τέσσερις παρακάτω βασικές κατηγορίες:

- **Φυσικοί κίνδυνοι (natural risks)** : περιλαμβάνουν απρόβλεπτα γεγονότα, τα οποία δεν πηγάζουν από τις συνθήκες φυσιολογικής λειτουργίας της επιχείρησης αλλά προέρχονται από τις φυσικές διεργασίες του περιβάλλοντος, όπως σεισμός, τυφώνας ή πλημμύρα. Η πιθανότητα συχνότητάς τους είναι πολύ χαμηλή, η πιθανή τους ένταση όμως, σε περίπτωση που επέλθουν, είναι πολύ μεγάλη με σοβαρές επιπτώσεις για τον ανθρώπινο παράγοντα.

- **Οικονομικοί κίνδυνοι (financial risks)**: ως οικονομικός κίνδυνος ορίζεται η μεταβλητότητα των δυνητικών αποτελεσμάτων μιας επένδυσης γύρω από την αναμενόμενη τιμή ή τον αριθμητικό τους μέσο. Σχετίζεται επίσης με την εισροή και την εκροή των χρημάτων στην επιχείρησης, καθώς και με την πιθανότητα μίας ξαφνικής οικονομικής απώλειας. Οι οικονομικοί κίνδυνοι πηγάζουν από τους κινδύνους αγοράς, ήτοι την έκθεση της επιχείρησης στην αλλαγή της αξίας των πρώτων υλών, των εμπορευμάτων, των αποθεμάτων και την μεταβλητότητα στις τιμές των διάφορων χρηματοοικονομικών εργαλείων και μεγεθών, όπως των μετοχών, των επιτοκίων και των συναλλαγματικών ισοτιμιών. Στην κατηγορία αυτή ενδεικτικά συμπεριλαμβάνονται ο κίνδυνος ρευστότητας, ο πιστωτικός κίνδυνος, ο κεφαλαιακός κίνδυνος, καθώς και ο συναλλαγματικός.

- **Λειτουργικοί κίνδυνοι (operational risks)**: Λειτουργικός ή επιχειρησιακός κίνδυνος είναι ο κίνδυνος που αντιμετωπίζει μία επιχείρηση κατά την διάρκεια της παραγωγικής διαδικασίας και οφείλεται στον ανθρώπινο παράγοντα. Περιλαμβάνει τα προβλήματα που παρουσιάζονται στις εσωτερικές διεργασίες, τις εργασιακές σχέσεις, τα πληροφοριακά συστήματα της επιχείρησης και κάθε άλλη δυσλειτουργία που οφείλεται στον άνθρωπο. Είναι κατανοητό ότι οι επιχειρήσεις με μικρότερες απαιτήσεις για ανθρώπινο κεφάλαιο θα έχουν και χαμηλότερο επιχειρησιακό κίνδυνο.

- **Επιχειρηματικοί κίνδυνοι (business risks)**: Πρόκειται για τους κινδύνους μείωσης της αποδοτικότητας και της παραγωγικότητας μιας επιχείρησης λόγω λανθασμένων αποφάσεων της διοίκησης, που έχουν ως συνέπεια την εμφάνιση ζημιών. Στην κατηγορία αυτή εντάσσεται και ο κίνδυνος φήμης (reputational risk) της επιχείρησης, ο οποίος κατά γενική ομολογία θεωρείται κίνδυνος υψηλής συχνότητας και έντασης.

3.2.2 Οι κίνδυνοι για τα προσωπικά δεδομένα σήμερα

Για να είναι εφικτός ο εντοπισμός και αξιολόγηση των κινδύνων με τους οποίους απειλούνται σήμερα τα προσωπικά δεδομένα της εκάστοτε επιχειρησιακής οντότητας, θα πρέπει πρώτα να ληφθεί υπόψη το σύγχρονο περιβάλλον της επικινδυνότητας καθώς και οι τάσεις εξέλιξης του.

Σύμφωνα με την μη κερδοσκοπική αμερικανική οργάνωση «Identity Theft Resource Center», έως την 19η Οκτωβρίου του περασμένου έτους είχαν καταγραφεί 783 παραβιάσεις δεδομένων, με αποτέλεσμα την έκθεση περισσοτέρων από 29 εκατομμύρια αρχείων. Σημειωτέον, η πλειοψηφία των παραβιάσεων δεν έχει αναφερθεί από τις εταιρείες. Οι παραβιάσεις των δεδομένων γίνονται όλο και πιο διαδεδομένες και οι τάσεις των επιθέσεων δεν παρουσιάζουν ενδείξεις επιβράδυνσης. Στοχεύουν κυρίως σε δεδομένα υψηλής αξίας, όπως αριθμούς κοινωνικής ασφάλισης, πληροφορίες για την υγεία, αριθμούς πιστωτικών και χρεωστικών καρτών, ηλεκτρονικά μηνύματα, κωδικούς και άλλες πληροφορίες πρόσβασης του χρήστη.

Στην συνέχεια, παρατίθενται οι σημαντικότερες τάσεις και τεχνολογικές εξελίξεις που χαρακτηρίζουν το εξωτερικό περιβάλλον της σημερινής επιχείρησης, καθώς και οι πιο κρίσιμες απειλές των προσωπικών δεδομένων προερχόμενες από αυτό:

- **Κινητή τηλεφωνία (Mobile):** Αναμφισβήτητα, τόσο η εμπιστευτικότητα όσο και η ακεραιότητα των πληροφοριών μέσω κινητών τηλεφώνων βάλλονται από πολλούς κινδύνους, τεχνικής και μη φύσεως. Το πολυμεσικό περιεχόμενο που αποθηκεύεται στα κινητά τηλέφωνα, όπως φωτογραφίες, βίντεο και άλλα σχετικά αρχεία δεδομένων, μπορούν πλέον εύκολα να βρεθούν στην κατοχή του εκάστοτε επιτιθέμενου υποκλοπέα, ενώ ιδιαίτερα συχνή είναι η υποκλοπή κλήσεων και μηνυμάτων. Λαμβάνοντας υπόψη ότι οι επιθέσεις σε κινητές συσκευές καθίστανται διαρκώς αυξανόμενες, αναμένονται όλο και περισσότερες παραβιάσεις τέτοιας μορφής και στις επιχειρήσεις, με αποτέλεσμα να προκαλείται ιδιαίτερη ανησυχία σχετικά με την ασφάλεια των εταιρικών δεδομένων.

- **Κρίσιμες Υποδομές (Critical infrastructures):** Ως κρίσιμες υποδομές ή υποδομές ζωτικής σημασίας ορίζονται αγαθά, συστήματα ή υποσυστήματα, τα οποία καθίστανται αναγκαία για τη διατήρηση των ζωτικών λειτουργιών της κοινωνίας, την υγεία, τη φυσική προστασία, την ασφάλεια, την οικονομική και κοινωνική ευημερία. Τα συστήματα επικοινωνιών και πληροφορικής συγκαταλέγονται μεταξύ των κρίσιμων

υποδομών της Χώρας, η ασφάλεια των οποίων αποτελεί πλέον μείζον θέμα εθνικού ενδιαφέροντος. Στα πλαίσια αυτά, δημοσιεύθηκε η υπ' αριθμ. 1027/2019 Υπουργική Απόφαση (ΦΕΚ 3739/Β/8-10-2019), με βάση την οποία καθορίζονται όλες εκείνες οι κρίσιμες υποδομές που σε περίπτωση διαταραχής της ομαλής τους λειτουργίας, θα επέλθουν κρίσιμες συνέπειες για την εύρυθμη λειτουργία ολόκληρου του κρατικού μηχανισμού. Η απόφαση αυτή, η οποία αποτελεί στην ουσία την συμμόρφωση της Χώρας με την υπ' αριθμ.2016/1148 ευρωπαϊκή οδηγία, γνωστή και ως NIS-Network and Information Systems, προβλέπει επίσης την διαδικασία παροχής πληροφοριών και κοινοποίησης συμβάντων ασφαλείας στις αρμόδιες αρχές, την έκδοση των βασικών απαιτήσεων ασφαλείας των δικτυακών συστημάτων, καθώς και συγκεκριμένα πρωτόκολλα διαχείρισης περιστατικών κυβερνοασφάλειας.

- **Διαδίκτυο των πραγμάτων (Internet of Things)**: Αποτελεί το δίκτυο επικοινωνίας πληθώρας ηλεκτρονικών συσκευών καθώς και κάθε αντικειμένου που ενσωματώνει ηλεκτρονικά μέσα, λογισμικό, αισθητήρες και συνδεσιμότητα σε δίκτυο, ώστε να επιτρέπεται η σύνδεση και η ανταλλαγή δεδομένων. Τα δίκτυα των κυβερνοεγκληματιών συχνά εκμεταλλεύονται την ελαστικότητα της ασφάλειας τέτοιου είδους συσκευών, με σκοπό την εξάπλωση κακόβουλων λογισμικών (malware), τα οποία προσβάλλουν τον χρήστη, ζητώντας στην συνέχεια χρηματικό αντάλλαγμα από αυτόν για την άρση της πραγματοποιηθείσας προσβολής. Το μεγαλύτερο ποσοστό των επιθέσεων αυτών στοχεύουν συνήθως σε συσκευές κοινής χρήσης, όπως servers, routers, συστήματα τηλεοράσεων κλειστού τύπου (CCTV), συσκευές δικτυακής αποθήκευσης και βιομηχανικά συστήματα ελέγχου.

Σύμφωνα με πρόσφατη έρευνα της «Irdeto Global Connected Industries», οκτώ στους δέκα οργανισμούς έχουν υποστεί μια κυβερνοεπίθεση σε συσκευές διαδικτύου των πραγμάτων τους τελευταίους 12 μήνες. Για το 90%, μάλιστα, των παθόντων οργανισμών, τα αποτελέσματα της κυβερνοεπίθησης είχαν καίριες επιδράσεις συμπεριλαμβανομένων των λειτουργικών διακοπών, της έκθεσης δεδομένων των πελατών και της ασφάλεια των τελικών χρηστών. Η έρευνα της Irdeto αποκαλύπτει επίσης ότι οι οργανισμοί δραστηριοποιούμενοι στους τομείς των μεταφορών, των κατασκευών και της υγειονομικής περίθαλψης υπέστησαν σημαντικές απώλειες λόγω των τρωτών σημείων που σχετίζονται με τη διαδικτυακή πύλη, με το μέσο οικονομικό αντίκτυπο μιας στοχευμένης IoT κυβερνοεπίθεσης να κοστίζει περισσότερα από 330 εκατομμύρια δολάρια.

- **Υπολογιστικό Νέφος (Cloud Computing):** Πρόκειται για την διάθεση υπολογιστικών πόρων μέσω διαδικτύου (π.χ. servers, apps κλπ), από κεντρικά συστήματα που βρίσκονται απομακρυσμένα από τον τελικό χρήστη, τα οποία τον εξυπηρετούν αυτοματοποιώντας διαδικασίες, παρέχοντας ευκολίες και ευελιξία σύνδεσης. Οι επιχειρήσεις σήμερα διοχετεύουν όλο και περισσότερα δεδομένα μέσω της νεφοϋπολογιστικής, παρέχοντας έτσι την δυνατότητα σε επίδοξους εισβολείς να αποκτήσουν πρόσβαση στα συστήματά τους, γεγονός που θέτει σε κίνδυνο το σύνολο των δεδομένων που αυτές διαχειρίζονται. Όλο και περισσότεροι οργανισμοί, δημόσιοι αλλά και ιδιωτικοί, καταφεύγουν στην λύση της εν λόγω τεχνολογίας, με αποτέλεσμα οι εκάστοτε επιτιθέμενοι να βρίσκουν τρόπους ώστε να εισβάλουν στις επιχειρησιακές υποδομές, όπως, για παράδειγμα, μέσω κρυπτογραφημένων αρχείων που εξαπλώνονται από σύννεφο σε σύννεφο.

- **Πρόγραμμα πληρωμής λύτρων (Ransomware):** Αποτελεί ένα είδος κακόβουλου λογισμικού, το οποίο απειλεί να δημοσιοποιήσει τα προσωπικά δεδομένα του θύματος ή να διακόψει την πρόσβασή του σε αυτά μέσω της κρυπτογράφησης των αρχείων του, εμφανίζοντας, στην συνέχεια μία απαίτηση καταβολής λύτρων. Σε αντάλλαγμα, οι δημιουργοί του κακόβουλου αυτού κώδικα υπόσχονται, άνευ εγγυήσεως, την αποκατάσταση της πρόσβασης του χρήστη στο «μολυσμένο» λειτουργικό σύστημα ή στα αρχεία των δεδομένων του. Σε περιπτώσεις επιθέσεων τέτοιου είδους, η ανάκτηση των προσβαλλόμενων αρχείων χωρίς το λεγόμενο «κλειδί αποκρυπτογράφησης» καθίσταται ανέφικτη, ενώ παράλληλα τα ψηφιακά νομίσματα που χρησιμοποιήθηκαν ως λύτρα για την συναλλαγή, όπως κρυπτονομίσματα (bitcoins), δεν δύνανται να εντοπιστούν με ευκολία, εξ' ου και η σύλληψη του δράστη ενέχει μεγάλο βαθμό δυσκολίας. Πλην δύο περιπτώσεων, οι 50 και πλέον διαφορετικές εκδόσεις τέτοιων ιών δεν μπορούν να αντιμετωπιστούν από τα συμβατικά λογισμικά αντιμετώπισης κακόβουλου κώδικα, παρά μόνο από εξειδικευμένο λογισμικό εξομοίωσης απειλών.

3.2.3. Οι κίνδυνοι μη συμμόρφωσης με τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων

Η υποχρέωση συμμόρφωσης της επιχείρησης με τις επιταγές του Γενικού Κανονισμού για την Προστασία των Προσωπικών Δεδομένων συνεπάγεται την εμφάνιση διάφορων επιχειρησιακών κινδύνων, οι βασικότεροι από τους οποίους παρουσιάζονται ως ακολούθως:

- **Κίνδυνος συμμόρφωσης (Compliance risk)**

Ως «Κανονιστική Συμμόρφωση» ορίζεται η προσαρμογή και η συνεχής λειτουργία της επιχείρησης σύμφωνα με την υπάρχουσα νομοθεσία, το ισχύον ρυθμιστικό πλαίσιο αλλά και το σύνολο των κανόνων που τίθενται από την εκάστοτε Διοίκηση και αποτελούν πρότυπα εταιρικής κουλτούρας. Υπό το πρίσμα αυτό, ο κίνδυνος συμμόρφωσης είναι η έκθεση του οργανισμού σε νομικές κυρώσεις, οικονομικές απώλειες, επιβολή διοικητικών προστίμων και υλικές ζημίες, όταν αυτός αποτυγχάνει να ενεργήσει σύμφωνα με τους υφιστάμενους νόμους και κανονισμούς, τις εσωτερικές πολιτικές ή τις βέλτιστες πρακτικές.

Ο κίνδυνος από την μη συμμόρφωση με τον Γενικό Κανονισμό Προστασίας των Προσωπικών Δεδομένων, αλλά και με την ισχύουσα κάθε φορά εθνική νομοθεσία, φαίνεται να έχει τρεις βασικές πτυχές για την επιχείρηση. Πρώτη και ίσως η σημαντικότερη έκφανση αυτού, είναι η επιβολή προστίμων από τις εποπτικές αρχές (**οικονομικός κίνδυνος**), το μέγεθος των οποίων δύναται να φτάσει τα 20 εκατομμύρια ευρώ ή το 4% του ετήσιου παγκόσμιου κύκλου εργασιών μιας εταιρείας. Δεύτερον, η αποτυχία συμμόρφωσης με τις επιταγές του Κανονισμού μπορεί να οδηγήσει σε δυσφήμιση της επιχείρησης (**κίνδυνος φήμης**) και τρίτον, ενδέχεται να επιφέρει προσωπικές ευθύνες στους εργαζόμενους του οργανισμού.

Στο σύγχρονο επιχειρησιακό γίγνεσθαι, ωστόσο, παρατηρούνται συχνά λάθη και αβλεψίες των Διοικητικών Συμβουλίων, που παρακωλύουν και επιβραδύνουν τους ρυθμούς υλοποίησης της κανονιστικής συμμόρφωσης της επιχείρησης. Πολλές φορές, για παράδειγμα, τα διοικητικά στελέχη ενδέχεται να μην κατανοούν το εύρος του εξωγενούς κινδύνου συμμόρφωσης που καλείται να αντιμετωπίσει η επιχείρηση από ενέργειες τρίτων μερών. Σύμφωνα με έρευνα της «Thomson Reuters», διαπιστώθηκε ότι μόλις το 62% των οργανισμών διεξάγει έλεγχο δέουσας επιμέλειας (due diligence) σε προμηθευτές, διανομείς και λοιπούς εξωτερικούς συνεργάτες. Άλλοτε πάλι το Διοικητικό Συμβούλιο εσφαλμένα διαχωρίζει την συμμόρφωση από την γενικότερα στρατηγική της εταιρείας, ενώ στην πραγματικότητα πρόκειται για δύο έννοιες άρρηκτα συνδεδεμένες μεταξύ τους.

- **Κίνδυνος φήμης (Reputational risk)**

Πρωταρχικό μέλημα οποιασδήποτε επιχείρησης αποτελεί η διαμόρφωση, η βελτίωση και η απρόσκοπτη διατήρηση της φήμης της στον κλάδο εντός του οποίου δραστηριοποιείται. Με άλλα λόγια, πρόκειται για την αναγνωρισιμότητα του ονόματός

της, γνωστού και ως “brand-name”, καθώς και με τον τρόπο που αυτό γίνεται αντιληπτό από τον καταναλωτή, δημιουργώντας αξία σε αυτόν για το παρεχόμενο προϊόν ή την υπηρεσία. Ως κίνδυνος φήμης ορίζεται η πιθανή απώλεια χρηματικών κεφαλαίων ή μεριδίου αγοράς που μπορεί να υποστεί μία επιχείρηση λόγω ζημιών στο όνομα και στην φήμη της. Συχνά μετριέται σε απώλεια εσόδων, αύξηση των λειτουργικών δαπανών ή καταστροφή της αξίας των μετόχων.

Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων παρέχει στα υποκείμενα των δεδομένων μια σειρά από νέα δικαιώματα, συμπεριλαμβανομένου του δικαιώματος πρόσβασης αυτών στα προσωπικά τους δεδομένα που τυγχάνουν επεξεργασίας από την επιχείρηση, το δικαίωμα διαγραφής ή διόρθωσης, το δικαίωμα στη φορητότητα των δεδομένων τους και το δικαίωμα να μην υπόκεινται σε αυτοματοποιημένη λήψη αποφάσεων. Σε περίπτωση δε, που η επιχείρηση δεν λάβει όλα τα δέοντα μέτρα ασφαλείας για την προστασία των προσωπικών δεδομένων ή αποτύχει να ικανοποιήσει επαρκώς ένα εκ των ανωτέρω δικαιωμάτων του υποκειμένου, κατόπιν σχετικής αιτήσεως αυτού, ενδέχεται να υποβληθεί καταγγελία από πλευράς του υποκειμένου στην αρμόδια εποπτική αρχή, γεγονός που σίγουρα θα λειτουργήσει αρνητικά για την φήμη της επιχείρησης δημιουργώντας παράλληλα δυσπιστία και επιφυλάξεις στους πελάτες, τους συνεργάτες και τους εργαζομένους αυτής, υφιστάμενους ή και υποψηφίους.

- **Κίνδυνος στον κυβερνοχώρο (Cyber risk)**

Η παραβίαση των ηλεκτρονικών συστημάτων της επιχείρησης και η συνακόλουθη διαρροή εμπιστευτικών πληροφοριών αποτελεί πλέον καθημερινό φαινόμενο. Συγκεκριμένα, η παραβίαση μπορεί να οφείλεται σε μη εξουσιοδοτημένη πρόσβαση στα συστήματα της εταιρείας, την οποία διαδέχεται η απώλεια πελατειακών δεδομένων, περιλαμβανομένων κατά κύριο λόγο οικονομικών στοιχείων, δεδομένων υγείας, ή άλλων διαφόρων εταιρικών δεδομένων, όπως εμπορικών μυστικών ή ζητημάτων πνευματικής ιδιοκτησίας. Η φύση, ωστόσο, των απειλών στον κυβερνοχώρο συνεχώς μεταβάλλεται, πράγμα το οποίο εμποδίζει σημαντικά την προσπάθεια συμμόρφωσης των επιχειρήσεων με τις επιταγές ασφαλείας των προσωπικών δεδομένων που θέτει ο ΓΚΠΔ, ενώ η εφαρμογή των κατάλληλων διαδικασιών ανίχνευσης και διερεύνησης παραβίασης προσωπικών δεδομένων (data breach) καθίσταται όλο και πιο σύνθετη στην πράξη.

- **Κίνδυνος ανθρώπινου δυναμικού (Human resources risk)**

Τα προσωπικά δεδομένα που τηρεί και επεξεργάζεται η επιχείρηση δεν εντοπίζονται μόνο στις πελατειακές βάσεις δεδομένων αλλά και στο συνολικό πλαίσιο οργάνωσης και λειτουργίας των ανθρώπινων πόρων αυτής. Οι διευθύνσεις ανθρώπινου δυναμικού συλλέγουν, αποθηκεύουν και επεξεργάζονται μεγάλο εύρος προσωπικών δεδομένων, όχι μόνο των ήδη υφιστάμενων υπαλλήλων της επιχείρησης, αλλά και εκείνων που έχουν ήδη αποχωρήσει ή αποτελούν δυνητικούς υποψηφίους προς απασχόληση. Οι πληροφορίες που έχουν στην κατοχή τους οι εν λόγω διευθύνσεις περιλαμβάνουν μάλιστα ευαίσθητα προσωπικά δεδομένα, όπως πληροφορίες υγείας, ιατρικά αρχεία ή μισθολογικά στοιχεία. Ως εκ τούτου, είναι εξαιρετικά σημαντικό οι υπάλληλοι της διεύθυνσης ανθρώπινου δυναμικού της επιχείρησης να γνωρίζουν και να κατανοούν απόλυτα τις απαιτήσεις του Κανονισμού για την προστασία των προσωπικών δεδομένων, καθώς η οποιαδήποτε απώλεια, καταστροφή ή λανθασμένη διαχείριση αυτών μπορεί να θέσει σε κίνδυνο την λειτουργία της επιχείρησης, προκαλώντας διαταραχές στις εργασιακές σχέσεις.

- **Νομικός κίνδυνος (Legal risk)**

Οι επιχειρήσεις που δραστηριοποιούνται και σε χώρες εκτός Ευρωπαϊκής Ένωσης ενδέχεται να κληθούν να αντιμετωπίσουν το φαινόμενο της σύγκρουσης των τοπικών κανονισμών ξένων κρατών με τις απαιτήσεις του Ευρωπαϊκού Κανονισμού για την προστασία των προσωπικών δεδομένων, οπότε και θα πρέπει να υιοθετήσουν ένα πιο εξειδικευμένο και σαφώς οριοθετημένο πλαίσιο λειτουργίας. Σημειώνεται ότι και στην ελληνική νομική πραγματικότητα, ο πρόσφατος υπ' αριθμ. 4624/2019 εθνικός νόμος, ο οποίος προβλέπει μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα καθώς και την ενσωμάτωση της Οδηγίας (ΕΕ) 2016/680 στην εθνική νομοθεσία, δημιουργεί ένα ακόμα πιο σύνθετο πλέγμα υποχρεώσεων για τις επιχειρήσεις, ενώ ορισμένες από τις διατάξεις του τυγχάνουν αμφισβήτησης από την επιστημονική κοινότητα ως προς την νομιμότητά τους.

- **Κίνδυνος νέου προϊόντος (New product risk)**

Μία από τις πιο σημαντικές απαιτήσεις του Κανονισμού είναι η λεγόμενη εκτίμηση αντικτύπου στην προστασία των προσωπικών δεδομένων (Data Protection Impact Assessment), την οποία θα πρέπει υποχρεωτικά να διεξάγουν οι επιχειρήσεις όταν ένα

είδος επεξεργασίας, ιδίως με την χρήση νέων τεχνολογιών, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Μία τέτοια περίπτωση συνιστά ο σχεδιασμός και η ανάπτυξη νέων προϊόντων. Η συλλογή στοιχείων συμπεριφοράς του καταναλωτή μέσω των ιστοσελίδων, η διεξαγωγή ερευνών ικανοποίησης πελατών με σκοπό την βελτιστοποίηση των υπαρχόντων προϊόντων και οι ενέργειες μάρκετινγκ στα πλαίσια προώθησης νέων καινοτόμων προϊόντων, αποτελούν μερικές από τις δραστηριότητες της επιχείρησης οι οποίες τελούν πλέον υπό το πρίσμα της προηγούμενης συγκατάθεσης του καταναλωτή, χωρίς την ύπαρξη της οποίας δεν μπορούν να θεωρηθούν νόμιμα υφιστάμενες.

3.3 Η αποτίμηση των κινδύνων

3.3.1 Διαδικασία αποτίμησης των κινδύνων

Η διαδικασία αποτίμησης των κινδύνων που απειλούν την σύγχρονη επιχείρηση δύναται να συνοψιστεί στα ακόλουθα στάδια, η επιτυχής διεκπεραίωση των οποίων αποτελεί τον ακρογωνιαίο λίθο της αποτελεσματικής διαχείρισης των κινδύνων που πρόκειται να αναλυθεί εκτενώς στο επόμενο κεφάλαιο:

Αναγνώριση των κινδύνων: Αποτελεί το πρώτο και σημαντικότερο στάδιο αποτίμησης των κινδύνων της επιχείρησης, θέτοντας τα θεμέλια για την αποτελεσματική διαχείριση αυτών στην συνέχεια. Στοχεύει στον ακριβή προσδιορισμό κάθε ενδεχόμενου συμβάντος δυνάμενου να οδηγήσει στην εμφάνιση ζημιογόνων αποτελεσμάτων. Περιλαμβάνει την αναγνώριση των δυνητικά προσβαλλόμενων αγαθών, κύριων και υποστηρικτικών, την αναγνώριση των απειλών, των ευπαθειών, των υπαρχόντων μέτρων ασφαλείας καθώς και όλων των πιθανών συνεπειών. Το στάδιο της αναγνώρισης των κινδύνων καθίσταται ζωτικής σημασίας για την επιχείρηση, καθώς αποδεικνύει ότι δεν αγνοούνται από αυτή γεγονότα, τα οποία μπορεί να αποβούν καταστροφικά για την λειτουργία της.

Ανάλυση των κινδύνων: Η ανάλυση των κινδύνων μπορεί να είναι είτε ποσοτική είτε ποιοτική, ανάλογα με την πιθανότητα εμφάνισης αυτών και τις αναμενόμενες συνέπειες που θα επιφέρει η έλευσή τους. Για την περιγραφή της πιθανότητας επέλευσης του εκάστοτε κινδύνου και των παρεπόμενων συνεπειών αυτού, η ποσοτική ανάλυση χρησιμοποιεί μία κλίμακα αριθμητικών τιμών, ενώ η ποιοτική ανάλυση μία κλίμακα χαρακτηριστικών κατάταξης. Στην πράξη είθισται να χρησιμοποιείται αρχικά η ποιοτική ανάλυση, ούτως ώστε να αποτυπωθεί η γενικότερη εικόνα του επιπέδου των κινδύνων

και δευτερευόντως η εφαρμογή της ποσοτικής ανάλυσης για την εκτίμηση των σοβαρότερων κινδύνων.

Προφίλ των κινδύνων: Η διεργασία της ανάλυσης των κινδύνων μπορεί να οδηγήσει στην δημιουργία ενός προφίλ για καθένα εξ' αυτών (risk profiling). Πρόκειται για μία διαδικασία, δυνάμει της οποίας επιτυγχάνεται η μέτρηση της συχνότητας και της έντασης των κινδύνων, παρέχοντας έτσι στην επιχείρηση ένα αξιόλογο εργαλείο για τον καθορισμό προτεραιοτήτων κατά το στάδιο διαχείρισης αυτών με κριτήριο τον βαθμό σημαντικότητάς τους.

Χαρτογράφηση των κινδύνων: Αποτέλεσμα της εξέτασης του προφίλ των κινδύνων αποτελεί η ολιστική χαρτογράφηση αυτών (risk mapping), η οποία περιλαμβάνει την γραφική απεικόνιση όλων των πιθανών για την επιχείρηση κινδύνων σε ένα διάγραμμα διαχείρισης κινδύνων. Με άλλα λόγια, ο χάρτης κινδύνων οπτικοποιεί τους κινδύνους που καλείται να αντιμετωπίσει μία εταιρεία, προκειμένου να καταστεί κατανοητή η σχέση που τους συνδέει μεταξύ τους, αποτελώντας έτσι ένα μέσο για την αιτιολόγηση και την επικοινωνία αυτών τόσο στα διοικητικά στελέχη όσο και στους εργαζόμενους. Στον χάρτη αυτόν οι κίνδυνοι εμφανίζονται με σειρά κατάταξης, ανάλογα με την ένταση και την συχνότητα τους.

Αξιολόγηση των κινδύνων: Το στάδιο της ανάλυσης των κινδύνων διαδέχεται η διεργασία αξιολόγησης αυτών, κατά την οποία πραγματοποιείται η σύγκριση των ήδη αναγνωρισμένων από την επιχείρηση κινδύνων με κάποια συγκεκριμένα κριτήρια, τα οποία η ίδια έχει θέσει και θεωρεί σημαντικά. Για τον καθορισμό των κριτηρίων αξιολόγησης των κινδύνων που σχετίζονται με τις πληροφορίες και τα δεδομένα της επιχείρησης, λαμβάνονται υπόψη η στρατηγική αξία των πληροφοριών, η κρισιμότητα των εμπλεκόμενων πληροφοριακών αγαθών, οι ενδεχόμενες κανονιστικές και νομικές υποχρεώσεις, τις πιθανές επιπτώσεις ενός επικίνδυνου περιστατικού ασφαλείας για την φήμη και το όνομα της εταιρείας, καθώς και τις αντιλήψεις των μετόχων.

3.3.2 Η αποτίμηση των κινδύνων για τα προσωπικά δεδομένα

Η κατηγοριοποίηση των επαπειλούμενων για τα προσωπικά δεδομένα κινδύνων σε συνδυασμό με την κλιμάκωση εκείνων των διαδικασιών που συμβάλλουν στην εξασφάλιση της συμμόρφωσης με τις ισχύουσες κανονιστικές διατάξεις και εν τέλει της προστασίας των δεδομένων, είναι γνωστή με τον όρο «προσέγγιση με βάση τον κίνδυνο» (risk based approach). Οι υποστηρικτές της θεωρούν ως προαπαιτούμενο για την εφαρμογή των εκάστοτε προστατευτικών κανόνων την διαπίστωση «βλάβης»

(harm) για το υποκείμενο των δεδομένων. Πρόκειται για μια προσέγγιση που αναδεικνύει τον βαθμό του κινδύνου ως βασικό κριτήριο για τον προσδιορισμό της έκτασης των υποχρεώσεων του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία, ενώ παράλληλα αποσκοπεί στην εστίαση των υπεύθυνων επεξεργασίας σε αυξημένης επικινδυνότητας επεξεργασίες, όπως είναι για παράδειγμα η επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων. Ωστόσο, δεν θα πρέπει να συγχέεται με την προσέγγιση με βάση την βλάβη (harm-base approach), η οποία λαμβάνει υπόψη οποιαδήποτε ενδεχόμενη επίπτωση της επεξεργασίας ανεξαρτήτως κλιμάκωσης και έντασης.

Η προσέγγιση με βάση των κίνδυνων αντικατοπτρίζεται στο πνεύμα συγκεκριμένων διατάξεων του Κανονισμού, μεταξύ των οποίων σημαντικότερη θεωρείται η διάταξη του άρθρου 35, η οποία εισάγει την υποχρέωση διενέργειας εκτίμησης των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας για την προστασία των προσωπικών δεδομένων. Επιπλέον, το κριτήριο του υψηλού βαθμού κινδύνου εντοπίζεται στην επιλογή της προηγούμενης διαβούλευσης με την εποπτική αρχή (άρθρο 36 παρ.1), στην τήρηση αρχείων επεξεργασίας (άρθρο 30 παρ. 5), στις ρυθμίσεις που αφορούν στην γνωστοποίηση της παραβίασης των δεδομένων στην εποπτική αρχή (άρθρα 33 και 34), στις διατάξεις που σχετίζονται με την υποχρέωση εφαρμογής κατάλληλων οργανωτικών και τεχνικών μέτρων ασφαλείας (άρθρο 32), καθώς και σε εκείνες που αναφέρονται στην προστασία των δεδομένων από τον σχεδιασμό και εξ’ ορισμού (άρθρο 25).

Προς αποσαφήνιση της έννοιας του κινδύνου και των προσδιοριστικών στοιχείων που τον καθιστούν υψηλό, ο ενωσιακός νομοθέτης προέβη σε σχετικές αιτιολογικές σκέψεις. Για παράδειγμα, στην αιτιολογική σκέψη 75 του Κανονισμού, παρατίθεται οι κίνδυνοι για τα δικαιώματα του φυσικού προσώπου, η σοβαρότητα των οποίων δύναται να οδηγήσει σε σωματική, υλική ή μη βλάβη, σε οποιοδήποτε οικονομικό ή κοινωνικό μειονέκτημα, στην στέρηση θεμελιωδών ελευθεριών των προσώπων ή σε παρακώλυση αυτών στην άσκηση ελέγχου από πλευράς τους επί της επεξεργασίας των προσωπικών τους δεδομένων. Η έννοια της σοβαρότητας του κινδύνου παραπέμπει στην φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της εκάστοτε επεξεργασίας των προσωπικών δεδομένων.

Ωστόσο, υποστηρίζεται ευρέως η άποψη ότι η προσέγγιση με βάση τον κίνδυνο προσκρούει στην θεμελιώδη παραδοχή του σεβασμού της προστασίας των προσωπικών δεδομένων του ατόμου ανεξάρτητα από το επίπεδο των κινδύνων που προκύπτουν από την επεξεργασία. Εξάλλου, η εν λόγω παραδοχή έχει επιδοκιμαστεί

και νομολογιακά μέσω αποφάσεων του Δικαστηρίου της Ευρωπαϊκής Ένωσης (ΔΕΕ), σύμφωνα με το οποίο η παραβίαση των δικαιωμάτων του προσώπου για την προστασία των δεδομένων του δεν εξαρτάται από την υφιστάμενη υλική βλάβη.

3.3.3 Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

Πριν από την εφαρμογή του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων (GDPR), η αξιολόγηση των κινδύνων που σχετίζονταν με την επεξεργασία προσωπικών δεδομένων δεν ήταν υποχρεωτική βάσει της Οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών». Παρόλο που στην προαναφερθείσα Οδηγία είχε ήδη ενσωματωθεί μία προσέγγιση του κινδύνου αναφορικά με την επιστημονική έρευνα και την ασφάλεια των δεδομένων, δεν είχε ωστόσο προβλεφθεί μια τυποποιημένη μεθοδολογία αξιολόγησης του κινδύνου προστασίας των δεδομένων. Το κενό αυτό καλείται να καλύψει ο Γενικός Κανονισμός για την Προστασίας Δεδομένων, ο οποίος καθιστά υποχρεωτική την εκπόνηση αξιολόγησης αντικτύπου σχετικά με την προστασία των δεδομένων πριν από την υλοποίηση οποιασδήποτε επικίνδυνης επεξεργασίας αυτών.

Το άρθρο 35 του Κανονισμού εισάγει την έννοια της Εκτίμησης Αντικτύπου σχετικά με την προστασία των προσωπικών δεδομένων, γνωστή και με τον αγγλικό όρο «**Data Privacy Impact Assessment** (DPIA)». Σκοπός της είναι η εκτίμηση της πιθανότητας επέλευσης και της σοβαρότητας ενός υψηλού κινδύνου, λαμβάνοντας υπόψη την φύση, την έκταση, το πλαίσιο και τους σκοπούς της επεξεργασίας. Σύμφωνα με την Ομάδα Εργασίας του άρθρου 29, πρόκειται για μια διαδικασία που έχει σχεδιαστεί για να περιγράψει την επεξεργασία των προσωπικών δεδομένων, να αξιολογήσει την αναγκαιότητα και την αναλογικότητα αυτής και να συνδράμει στη διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων που συνεπάγεται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, μέσω της αξιολόγησής τους και του καθορισμού των απαραίτητων μέτρων για την αντιμετώπισή τους.

Ειδικότερα, στην πρώτη παράγραφο του άρθρου 35 του Κανονισμού ορίζεται ότι «όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να

επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους».

Η εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων απαιτείται ιδίως στην περίπτωση α) συστηματικής και εκτενούς αξιολόγησης προσωπικών δεδομένων φυσικών προσώπων, η οποία συνίσταται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο είτε επηρεάζουν σημαντικά το φυσικό πρόσωπο β) μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων ή δεδομένων που αφορούν σε ποινικές καταδίκες και αδικήματα και γ) συστηματικής και μεγάλης κλίμακας παρακολούθησης δημόσιου χώρου (άρθρο 35 παράγραφος 3 ΓΚΠΔ). Επιπλέον, η εκτίμηση αντικτύπου θα πρέπει να περιέχει κατ' ελάχιστο:

- την περιγραφή των προβλεπόμενων πράξεων επεξεργασίας των προσωπικών δεδομένων και των σκοπών της επεξεργασίας
- την εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς
- την εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων
- τα προβλεπόμενα μέτρα αντιστάθμισης των δυνητικών κινδύνων, όπως η παροχή εγγυήσεων και οι μηχανισμοί ασφαλείας, ούτως ώστε να εξασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα και να αποδεικνύεται η συμμόρφωση της επιχείρησης με τις επιταγές του Κανονισμού.

Σημειωτέον, η παράλειψη διενέργειας αντικτύπου, η εσφαλμένη διενέργεια αυτής ή η παράλειψη διαβούλευσης με την αρμόδια εποπτική αρχή, εφόσον τούτο απαιτείται, ενδέχεται να επιφέρουν διοικητικό πρόστιμο ύψους έως 10 εκατομμυρίων ευρώ ή, σε περίπτωση επιχείρησης, έως ποσοστό 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου έτους, λαμβάνοντας υπόψη όποιο από τα δύο είναι μεγαλύτερο κάθε φόρα.

ΚΕΦΑΛΑΙΟ 4

Διαχείριση των κινδύνων

4.1 Τι είναι η διαχείριση των κινδύνων

Στην σύγχρονη εποχή, η διαχείριση των κινδύνων (risk management) καθίσταται σημείο αναφοράς για την λήψη των εκάστοτε επιχειρηματικών αλλά και κοινωνικών αποφάσεων. Αποτελεί ένα διακριτό πεδίο μελέτης, το οποίο αντλεί γνώσεις από το δίκαιο, την οικονομική επιστήμη, τα μαθηματικά και την στατιστική, την μηχανική αλλά και την ψυχολογία, με απώτερο σκοπό την δημιουργία ενός πλαισίου ολιστικής διαδικασίας λήψης των αποφάσεων, οι οποίες θα προσδίδουν αξία στην επιχείρηση και θα εξασφαλίζουν την βιωσιμότητά της. Η αξία της επιχείρησης για τους μετόχους, όπως αυτή αντανακλάται στην αξία των κοινών της μετοχών, εξαρτάται από το αναμενόμενο μέγεθος, τον χρόνο και τον κίνδυνο που σχετίζονται με τις μελλοντικές χρηματοροές της εταιρείας. Οποιαδήποτε απροσδόκητη αλλαγή στην μελλοντική ρευστότητα της επιχείρησης δύναται να αποτελέσει σημαντικό παράγοντα διακύμανσης της αξίας της.

Η διαχείριση των κινδύνων των επιχειρήσεων, ευρέως γνωστή με τον όρο «Enterprise Risk Management» (ERM), αποτελεί μία προσέγγιση διαχείρισης κινδύνου, η οποία εμφανίστηκε για πρώτη φορά σαν έννοια την δεκαετία του 1990. Σήμερα, έχει καταστεί καίρια επιχειρηματική λειτουργία με αντικειμενικό στόχο την μεγιστοποίηση της αξίας της επιχείρησης, μέσω της μείωσης του κόστους των εμφανιζόμενων κάθε φορά κινδύνων. Συγκεκριμένα, το ERM αποτελεί μία ταυτόχρονη εξέταση των λεγόμενων καθαρών κινδύνων (pure risks), ήτοι εκείνων που ενέχουν πιθανότητα ζημίας και μηδενική πιθανότητα κέρδους, καθώς και των επονομαζόμενων κερδοσκοπικών κινδύνων (speculative risks), οι οποίοι χαρακτηρίζονται από την πιθανότητα είτε για κέρδος είτε για ζημία. Οι φυσικοί κίνδυνοι, όπως ο κίνδυνος πυρκαγιάς ή πλημμύρας, εντάσσονται στην κατηγορία των καθαρών κινδύνων, ενώ ο κίνδυνος επενδύσεων ή ο κίνδυνος εταιρικής φήμης συγκαταλέγονται μεταξύ των κερδοσκοπικών κινδύνων.

Στην σύγχρονη εποχή, δεδομένου ότι τα αίτια εμφάνισης των ζημιών ποικίλουν ανάλογα με τις δραστηριότητες της επιχείρησης, θεωρείται σκόπιμο η διαδικασία διαχείρισης των κινδύνων να αποτελεί επακόλουθο μιας συντονισμένης και καλά οργανωμένης προσπάθειας όλων των τμημάτων της, συμπεριλαμβανομένων της παραγωγής, της οικονομικής και νομική διεύθυνσης, του τμήματος μάρκετινγκ καθώς και της διεύθυνσης ανθρώπινου δυναμικού, με σκοπό την δημιουργία του βέλτιστου δυνατού αποτελέσματος

4.2 Διαδικασία και μέθοδοι διαχείρισης των κινδύνων

Ανεξάρτητα από το είδος των κινδύνων που καλείται να αντιμετωπίσει σε καθημερινή βάση η επιχείρηση, το γενικότερο πλαίσιο διαχείρισης αυτών αποτελείται από τα ακόλουθα στάδια:

- ✓ Αναγνώριση όλων των ενδεχόμενων κινδύνων
- ✓ Εκτίμηση της πιθανότητας επέλευσης ζημιών και της σοβαρότητας αυτών
- ✓ Επιλογή και ανάπτυξη των κατάλληλων μεθόδων για την διαχείριση των κινδύνων
- ✓ Εφαρμογή των επιλεγμένων μεθόδων διαχείρισης των κινδύνων
- ✓ Διαρκής αξιολόγηση της αποδοτικότητας των εφαρμοστέων μεθόδων

Οι μέθοδοι διαχείρισης των επιχειρησιακών κινδύνων μπορούν να διακριθούν σε τρεις βασικές κατηγορίες, ήτοι τον έλεγχο των ζημιών, την χρηματοδότηση των ζημιών και τον εσωτερικό περιορισμό των κινδύνων, δυνάμενες να εφαρμοστούν είτε μεμονωμένα είτε από κοινού, χωρίς η μία να αποκλείει την άλλη. Κατά κύριο λόγο, η μέθοδος χρηματοδότησης των ζημιών αφορά στις αποφάσεις που λαμβάνει η Διοίκηση της επιχείρησης σχετικά με την αποκατάσταση-πληρωμή των ζημιών, σε περίπτωση επέλευσής τους, ενώ οι άλλες δύο μέθοδοι περιλαμβάνουν κατεξοχήν αποφάσεις επενδύσεων σε συστήματα ασφαλείας, προκειμένου να περιοριστούν οι αναμενόμενες ζημίες.

Ως **έλεγχος ζημιών** (loss control) χαρακτηρίζεται το σύνολο των ενεργειών στις οποίες προβαίνει η επιχείρηση για τον περιορισμό του αναμενόμενου κόστους των δυνητικών ζημιών, μέσω της ελαχιστοποίησης της συχνότητας και της σοβαρότητας αυτών. Ενέργειες οι οποίες επηρεάζουν την συχνότητα εμφάνισης των ζημιών είναι γνωστές με τον όρο «μέθοδοι πρόληψης των ζημιών» (loss prevention methods), ενώ οι ενέργειες εκείνες που επιδρούν σημαντικά στο μέγεθος των ζημιών αποκαλούνται «μέθοδοι περιορισμού των ζημιών» (loss reduction methods). Σε γενικές γραμμές, η μέθοδος ελέγχου των ζημιών συνίσταται αφενός στην μείωση του επιπέδου των επικίνδυνων δραστηριοτήτων και αφετέρου στην αύξηση των μέτρων προφύλαξης της επιχείρησης από αυτές. Ο περιορισμός των επικίνδυνων δραστηριοτήτων ελαττώνει την συχνότητα επέλευσης των ζημιών, ενώ η ολική εξάλειψη των επικίνδυνων δραστηριοτήτων, γνωστή και ως στρατηγική αποφυγής κινδύνου (risk avoidance), εκμηδενίζει τις πιθανότητες εμφάνισης ζημιών. Από την άλλη πλευρά, η αύξηση των μέτρων ασφαλείας για τις επικίνδυνες δραστηριότητες, όπως για παράδειγμα η εγκατάσταση εξοπλισμού ασφαλείας ή η βελτιστοποίηση των πληροφοριακών συστημάτων και του

δικτύου της επιχείρησης, συμβάλλει αισθητά στην μείωση όχι μόνο της συχνότητας αλλά και του μεγέθους των ζημιών.

Οι μέθοδοι **χρηματοδότησης των ζημιών** (loss financing) αντικατοπτρίζουν την προσπάθεια εξεύρεσης των απαιτούμενων κεφαλαίων, εσωτερικών ή εξωτερικών, για την αντιστάθμιση των υφιστάμενων ζημιών και διακρίνονται στην ίδια κράτηση (retention), την ασφάλιση (insurance), την αντιστάθμιση (hedging), καθώς και άλλες συμβατικές μεταφορές κινδύνων. Μέσω της ιδίας κράτησης η επιχείρηση αναλαμβάνει την υποχρέωση να αποκαταστήσει εν όλω ή εν μέρει την εκάστοτε ζημία, ενώ μέσω της ασφάλισης, μέρος του κινδύνου μεταφέρεται από την επιχείρηση στις ασφαλιστικές εταιρείες , οι οποίες αναλαμβάνουν την προμήθεια των κεφαλαίων για την πληρωμή των ζημιών αντί καταβολής ασφαλίστρου. Η μέθοδος της αντιστάθμισης (hedging) χρησιμοποιείται κυρίως για την αντιστάθμιση των χρηματοοικονομικών κινδύνων μέσω παραγώγων χρηματοοικονομικών προϊόντων, όπως είναι τα προθεσμιακά συμβόλαια (forward based derivatives) ή τα συμβόλαια δικαιωμάτων προαίρεσης (options based derivatives). Επιπλέον, συνήθη μέθοδο στην επιχειρησιακή πρακτική αποτελεί και η χρήση συμβατικών μορφών μεταφοράς κινδύνων (contractual risk transfers), όπως για παράδειγμα οι λεγόμενες «συμβάσεις αποζημίωσης» ή «εγγυήσεις καλής εκτέλεσης έργων» που συνάπτει η επιχείρηση με τρίτα μέρη, τα οποία και αναλαμβάνουν τον κίνδυνο των επερχόμενων ζημιών.

Τέλος, ο **εσωτερικός περιορισμός των κινδύνων** (internal risk reduction) διακρίνεται σε δύο βασικές κατηγορίες, την διασπορά (diversification) και την επένδυση στην πληροφόρηση. Η διασπορά του κινδύνου συνίσταται συνήθως στην διαφοροποίηση των δραστηριοτήτων της επιχείρησης, ενώ η επένδυση στην πληροφόρηση εξασφαλίζει στα διοικητικά στελέχη καλύτερες προβλέψεις αναφορικά με την πιθανότητα εμφάνισης ενδεχόμενων ζημιών και ως εκ τούτου αποτελεσματικότερη διαδικασία λήψης των αποφάσεων.

4.3 Διαχείριση κινδύνων σχετικά με τα προσωπικά δεδομένα

Η διαχείριση κινδύνων στα πλαίσια προστασίας των προσωπικών δεδομένων της επιχείρησης καθίσταται μία ιδιαίτερη δυσχερής και σύνθετη διαδικασία για πολλούς και διαφορετικούς λόγους, οι κυριότεροι εκ των οποίων κατά βάση εντοπίζονται στον χαμηλό βαθμό ασφάλειας των πληροφορικών της συστημάτων. Η ενσωμάτωση νέων μέτρων ασφάλειας ή η βελτίωση των ήδη υπαρχόντων συχνά προσκρούουν σε εμπόδια που σχετίζονται με την εσωτερική λειτουργία του οργανισμού, όπως είναι για παράδειγμα το υψηλό κόστος ενσωμάτωσης των μέτρων ασφαλείας, η αδυναμία

επικοινωνίας και συνεργασίας μεταξύ διοικητικού και τεχνικού προσωπικού της επιχείρησης, η λανθασμένη άποψη ότι η ασφάλεια των δεδομένων αποτελεί ένα αμιγώς τεχνικό θέμα, η ελλιπής υποστήριξη της Διοίκησης, η πλημμελής ενημέρωση και εκπαίδευση των εργαζομένων, η δυσκολία ανάπτυξης ενός ολοκληρωμένου σχεδίου ασφάλειας των δεδομένων αλλά και η αδυναμία αναγνώρισης και εκτίμησης των επιπτώσεων που τυχόν θα επιφέρει στην επιχείρηση η μη υλοποίηση αυτού.

Παρόλο που ο Γενικός Κανονισμός δεν εξειδικεύει τον τρόπο συμμόρφωσης με τις επιταγές του, προβλέπει ωστόσο μία σειρά από αναγκαίες ενέργειες, στις οποίες θα πρέπει να προβούν οι επιχειρήσεις, προκειμένου να καταστεί δυνατή η διαχείριση των επαπειλούμενων κινδύνων για τα προσωπικά δεδομένα που αυτές συλλέγουν, αποθηκεύουν και επεξεργάζονται. Ενδεικτικά αναφέρονται :

- **Αρχεία δραστηριοτήτων επεξεργασίας** (άρθρο 30): Ο υπεύθυνος ή ο εκτελών την επεξεργασία και, κατά περίπτωση, ο εκπρόσωπός τους, τηρεί έγγραφο ή ηλεκτρονικό αρχείο των δραστηριοτήτων επεξεργασίας, για τις οποίες φέρει την ευθύνη. Η τήρηση του εν λόγω αρχείου προϋποθέτει ότι η επιχείρηση απασχολεί περισσότερα από 250 άτομα καθώς και ότι η επεξεργασία δεν είναι περιστασιακή και δεν περιλαμβάνει ειδικές κατηγορίες δεδομένων ή δεδομένων που αφορούν σε ποινικές καταδίκες και αδικήματα. Επιπλέον, σύμφωνα με την Ομάδα Εργασίας του άρθρου 29, ο υπεύθυνος ή ο εκτελών την επεξεργασία μπορούν να αναθέτουν την τήρηση αρχείου δραστηριοτήτων στον Υπεύθυνο Προστασίας προσωπικών δεδομένων (DPO). Ωστόσο, υποστηρίζεται έντονα η άποψη ότι η ανάληψη τέτοιου καθήκοντος από πλευράς του Υπεύθυνου Προστασίας αφενός αναιρεί την επιταγή ανεξαρτησίας αυτού και αφετέρου παραβιάζει την αρχή της λογοδοσίας, δεδομένου ότι αρμόδιος για τις πράξεις επεξεργασίας αλλά και την απόδειξη συμμόρφωσης με τις επιταγές του Κανονισμού είναι αποκλειστικά ο υπεύθυνος επεξεργασίας.

- **Ασφάλεια επεξεργασίας** (άρθρο 32): Η επιχείρηση, έχοντας τον ρόλο του υπεύθυνου επεξεργασίας των προσωπικών δεδομένων, θα πρέπει να εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα, ούτως ώστε να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των επικείμενων κινδύνων. Μεταξύ των μέτρων αυτών συμπεριλαμβάνονται η ψευδωνυμοποίηση και η κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα, η δυνατότητα διαρκούς διασφάλισης του απορρήτου και της αξιοπιστίας των συστημάτων επεξεργασίας των δεδομένων, η δυνατότητα αποκατάστασης της διαθεσιμότητας και της πρόσβασης στα δεδομένα ανά πάσα στιγμή σε περίπτωση φυσικού ή τεχνικού συμβάντος, καθώς και η τακτική αξιολόγηση της αποτελεσματικότητας των τεχνικών και οργανωτικών μέτρων.

➢ **Γνωστοποίηση παραβίασης** (άρθρα 33 και 34): Σε περίπτωση παραβίασης των δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας φέρει την υποχρέωση γνωστοποίησης του συμβάντος τόσο στην αρμόδια εποπτική αρχή όσο και στο υποκείμενο των δεδομένων υπό ορισμένες προϋποθέσεις. Συγκεκριμένα, η γνωστοποίηση στην εποπτική αρχή ορίζεται ότι θα πρέπει να γίνει αμελλητί και εντός 72 ωρών από την στιγμή που ο υπεύθυνος της επεξεργασίας λαμβάνει γνώση για την παραβίαση, εκτός εάν αυτή δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Η γνωστοποίηση απαιτείται να είναι σαφώς και επαρκώς αιτιολογημένη, αναφέροντας αναλυτικά τα πραγματικά περιστατικά, τις επελθούσες συνέπειες και τα ληφθέντα διορθωτικά μέτρα. Το ίδιο σαφής, άμεση και τεκμηριωμένη θα πρέπει να είναι και η γνωστοποίηση της παραβίασης στο υποκείμενο των δεδομένων, η οποία, ωστόσο, δεν υπόκειται σε αυστηρή χρονική προθεσμία. Ο υπεύθυνος επεξεργασίας απαλλάσσεται από την υποχρέωση γνωστοποίησης προς το υποκείμενο των δεδομένων, σε περίπτωση που έχουν ληφθεί από πλευράς του όλα τα κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας, ούτως ώστε να διασφαλίζεται ότι η παραβίαση δεν ενέχει κίνδυνο για τα δικαιώματα του υποκειμένου, ή σε περίπτωση που η εν λόγω γνωστοποίηση απαιτεί δυσανάλογες προσπάθειες από εκείνον, ενώ παράλληλα υπάρχει κάποιο άλλο παρόμοιο μέτρο με βάση το οποίο μπορεί να επιτευχθεί εξίσου η επαρκής ενημέρωση του υποκειμένου.

➢ **Εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων** (άρθρο 35): Όπως ήδη αναφέρθηκε και σε προηγούμενο κεφάλαιο, ο Κανονισμός προβλέπει ρητά την υποχρέωση της επιχείρησης να διεξάγει μελέτη εκτίμησης των επιπτώσεων των σχεδιαζόμενων από αυτήν πράξεων επεξεργασίας προσωπικών δεδομένων, σε περίπτωση που η εν λόγω επεξεργασία ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ιδίως εάν αυτή πραγματοποιείται με την χρήση νέων τεχνολογιών. Αυτό το μέτρο αντιστάθμισης των πιθανών κινδύνων μπορεί να καταταχθεί στην κατηγορία των μεθόδων ελέγχου των ζημιών και συγκεκριμένα στην κατηγορία των μεθόδων πρόληψης των ζημιών.

➢ **Προηγούμενη διαβούλευση** (άρθρο 36): Όταν μία εκτίμηση αντικτύπου σχετικά με την προστασία των προσωπικών δεδομένων, που έχει διεξαχθεί από τον υπεύθυνο επεξεργασίας, υποδεικνύει την άμεση πρόκληση κινδύνων για την ασφάλεια των δεδομένων, αυτός δύναται να ζητήσει την γνώμη της εποπτικής αρχής, η οποία με την σειρά της καλείται να αποφανθεί παρέχοντας εγγράφως συμβουλές στον υπεύθυνο

επεξεργασίας εντός προθεσμίας οκτώ εβδομάδων από την παραλαβή του σχετικού αιτήματος διαβούλευσης.

- **Ορισμός Υπεύθυνου Προστασίας Δεδομένων** (άρθρο 37): Εισάγεται ο ρόλος του Υπεύθυνου Προστασίας προσωπικών δεδομένων (Data Protection Officer), ο οποίος μπορεί να ορίζεται από την επιχείρηση, όταν οι βασικές δραστηριότητες της συνιστούν πράξεις επεξεργασίας, οι οποίες λόγω της φύσης, του πεδίου εφαρμογής και των σκοπών τους, απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα, ή όταν αυτές συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα ή δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα. Ο θεσμός του Υπεύθυνου Προστασίας Δεδομένων αποτελεί τον ακρογωνιαίο λίθο για την εφαρμογή της αρχής της λογοδοσίας, καθώς είναι επιφορτισμένος με την έγγραφη τεκμηρίωση πράξεων επεξεργασίας, την διεξαγωγή μελέτης εκτίμησης αντικτύπου και την τήρηση αρχείου δραστηριοτήτων επεξεργασίας.

- **Κώδικες δεοντολογίας και πιστοποίηση** (άρθρα 40 και 42): Οι επιχειρήσεις υποχρεούνται να εκπονούν κώδικες δεοντολογίας ή να τροποποιούν τους ήδη υφιστάμενους, προκειμένου να διασφαλίζουν την συμμόρφωσή τους με τις διατάξεις του Κανονισμού, ιδίως αυτές που αφορούν στην διαφανή και αθέμιτη επεξεργασία των προσωπικών δεδομένων, την ενημέρωση των υποκειμένων των δεδομένων και την άσκηση των δικαιωμάτων τους, τις διαδικασίες και τα μέτρα ασφάλειας της επεξεργασίας των δεδομένων και την γνωστοποίηση των συμβάντων παραβίασης. Επιπλέον, προβλέπεται η θέσπιση από τα κράτη μέλη και τις εποπτικές αρχές μηχανισμών πιστοποίησης της προστασίας δεδομένων, με σκοπό την απόδειξη της συμμόρφωσης των υπεύθυνων και εκτελούντων την επεξεργασία με τις διατάξεις του Γενικού Κανονισμού προστασίας προσωπικών δεδομένων.

Κεφάλαιο 5

Μελέτη Περίπτωσης Διαχείρισης Κινδύνων

5.1 Αντικείμενο και στόχοι της μελέτης

Αντικείμενο της παρούσας μελέτης περίπτωσης αποτελεί η διαχείριση των κινδύνων που προκύπτουν από την εκάστοτε διαδικασία επεξεργασίας προσωπικών δεδομένων στα πλαίσια λειτουργίας της εμπορικής εταιρείας Χ (εφεξής καλούμενης η «εταιρεία»), μέσω της πρότασης ενός συγκεκριμένου σχεδίου συμμόρφωσης αυτής με τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR), κατόπιν προηγούμενης αξιολόγησης των κινδύνων αυτών σε σχέση με τους σκοπούς της επεξεργασίας και διεξαγωγής της απαιτούμενης ανάλυσης χάσματος (gap analysis) από τις διατάξεις του Κανονισμού. Η ανάλυση χάσματος αποτελεί μία τεχνική της επιστήμης διοίκησης, η οποία χρησιμοποιείται για τον καθορισμό εκείνων των βημάτων που απαιτούνται, προκειμένου η παρούσα κατάσταση των πραγμάτων να μετασχηματιστεί σε μία άλλη επιθυμητή κατάσταση.

Κατά την εκπόνηση της μελέτης, ελήφθησαν υπόψη ο υπ’ αριθμ. 2016/679 Γενικός Κανονισμός Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης (General Data Protection Regulation), τα πρότυπα ασφάλειας ISO/IEC 27001 και ISO/IEC 27002, τα πρότυπα ISO/IEC 29134 και ISO/IEC 29100, οι κατευθυντήριες γραμμές για τον Κανονισμό που δημοσιεύονται από την Ομάδα Εργασίας του άρθρου 29 για την προστασία δεδομένων, οι υφιστάμενες διαδικασίες και λειτουργίες της εταιρείας, οι τρέχουσες εξελίξεις στις Τεχνολογίες Πληροφοριών και Επικοινωνιών, καθώς επίσης η αρχιτεκτονική και η υποδομή των υπολογιστικών και επικοινωνιακών συστημάτων.

Στόχοι της μελέτης είναι η σαφής καταγραφή του επιπέδου συμμόρφωσης της εταιρείας με τον Κανονισμό και ο συνακόλουθος ο προσδιορισμός του απαραίτητου πλάνου ενεργειών, στις οποίες θα πρέπει αυτή να προβεί, ούτως ώστε να επιτευχθεί η καλύτερη δυνατή συμμόρφωση με τις κανονιστικές διατάξεις και ως εκ τούτου η αποτελεσματική διαχείριση των επαπειλούμενων κινδύνων για την προστασία των προσωπικών δεδομένων που αυτή συλλέγει, αρχειοθετεί, αποθηκεύει και επεξεργάζεται.

5.2 Μεθοδολογία της έρευνας

Στην παρούσα ενότητα παρουσιάζονται η γενική μεθοδολογική προσέγγιση που ακολουθήθηκε για την διεξαγωγή της εν λόγω μελέτης περίπτωσης, καθώς και οι επιμέρους μεθοδολογίες που χρησιμοποιήθηκαν για την υλοποίηση συγκεκριμένων τμημάτων αυτής. Ο στρατηγικός χαρακτήρας της μελέτης προσδιορίζει τη σπουδαιότητα εφαρμογής μιας συνεκτικής και δομημένης προσέγγισης, που θα αποδίδει την απαιτούμενη έμφαση σε όλες τις ενότητες των εργασιών της, εξασφαλίζοντας την μεταξύ τους ολοκλήρωση και συνέχεια, προκειμένου το σύνολο των δραστηριοτήτων της εταιρείας να συνθέσει ένα νέο ολοκληρωμένο πλαίσιο προστασίας των προσωπικών δεδομένων.

Λαμβάνοντας υπόψη τα ανωτέρω, υιοθετήθηκε μια προσέγγιση που αποτελείται από τις πλέον ενδεδειγμένες, δοκιμασμένες και επιστημονικά καταξιωμένες μεθοδολογίες που συμπληρώνονται από ειδικότερες διαδικασίες, τεχνικές και εργαλεία. Συγκεκριμένα, μεθοδολογία που υιοθετήθηκε για την υλοποίηση της έρευνας είναι η διεθνής μεθοδολογία PRINCE 2, η οποία εξειδικεύεται:

α) στη μεθοδολογία αποτίμησης του αντίκτυπου στην ιδιωτικότητα (Privacy Impact Assessment (PIA)) σύμφωνα με το πρότυπο ISO/IEC 29134

β) στη μεθοδολογία «Plan-Do-Check-Act» για την υλοποίηση του συστήματος διαχείρισης της ασφάλειας των προσωπικών δεδομένων. Πρόκειται για μία διεργασιοκεντρική προσέγγιση (process-based approach), η οποία αποτελεί επαναληπτική μέθοδο τεσσάρων βημάτων, ήτοι του σχεδιασμού (plan), της υλοποίησης των σχεδίων (do), του ελέγχου (check) των αποτελεσμάτων συγκριτικά με τους στόχους που έχουν τεθεί και της διόρθωσης (act) όποιων δραστηριοτήτων απαιτείται για την επίτευξη του καλύτερου δυνατού αποτελέσματος.

Ειδικότερα, για την εκπόνηση της μελέτης πραγματοποιήθηκαν οι ακόλουθες επιμέρους ενέργειες:

1) **Αρχικός Προγραμματισμός Έργου**

Στόχος του αρχικού προγραμματισμού ήταν η διασφάλιση ότι όλες οι προαπαιτούμενες ενέργειες είχαν ολοκληρωθεί και συνεπώς το έργο ήταν σε θέση να ξεκινήσει. Η διαδικασία πρόβλεπε ενέργειες που είχαν ως αποτέλεσμα τη δημιουργία των παρακάτω προϊόντων:

- καθορισμός του οργανωτικού σχήματος της εταιρείας

- συνοπτική περιγραφή του έργου, δηλαδή τους στόχους και το εύρος του έργου, καθώς και την προσέγγιση υλοποίησής του, δηλαδή μια πρώτη εκτίμηση του τεχνικού σχεδίου και του σχεδίου πόρων υλοποίησης (ανάλυση του έργου σε δραστηριότητες, χρονοπρογραμματισμός και απαιτούμενοι πόροι για την υλοποίησή τους)
- επισκόπηση και προσαρμογή των φάσεων υλοποίησης του έργου καθώς και των αποτελεσμάτων ανά φάση
- αναθεώρηση του συνολικού χρονοδιαγράμματος το οποίο αποτέλεσε την βάση παρακολούθησης της πορείας του έργου
- ενημέρωση του προσωπικού της εταιρείας που ενεπλάκη άμεσα ή έμμεσα στην ανάπτυξη του συστήματος προστασίας και διαχείρισης των προσωπικών δεδομένων

2) **Εκπαίδευση**

Εκπαιδεύτηκε κατάλληλα το προσωπικό που θα συμμετείχε ενεργά στην διεξαγωγή της μελέτης με έμφαση στις απαιτήσεις του Κανονισμού, ενώ παράλληλα ενημερώθηκε για την μεθοδολογία και για τα έντυπα που χρησιμοποιήθηκαν. Η εκπαίδευση του προσωπικού στηρίχθηκε στη μεθοδολογία Plan-Do-Check-Act (PDCA) και παρουσίασε από όλες τις οπτικές γωνίες, νομική, τεχνολογική και διοικητική, τα πλέον κρίσιμα ζητήματα του Γενικού Κανονισμού Προστασίας των Δεδομένων.

3) **Καταγραφή της Πληροφοριακής Υποδομής**

Σκοπός του σταδίου αυτού ήταν η αναγνώριση και οριοθέτηση του λειτουργικού περιβάλλοντος της εταιρείας, καθώς και η καταγραφή των πληροφοριακών συστημάτων αυτής, τα οποία επεξεργάζονται ή αποθηκεύουν προσωπικά δεδομένα. Η καταγραφή αυτή αφορά στους κρίσιμους πληροφοριακούς πόρους (information assets) της εταιρείας, κατά την λειτουργία των οποίων πραγματοποιείται επεξεργασία των προσωπικών δεδομένων. Ο προσδιορισμός των κρίσιμων περιουσιακών στοιχείων (assets), αποτελεί σημαντική πληροφόρηση για την ορθή και αποτελεσματική αξιολόγηση των κινδύνων ασφάλειας πληροφοριών. Ως εκ τούτου, κρίθηκε απαραίτητη η δημιουργία ενός καταλόγου στον οποίο να περιλαμβάνονται όλοι οι πόροι, οι οποίοι συμμετέχουν στις διεργασίες της εν λόγω περιοχής ελέγχου και σχετίζονται με την επεξεργασία των προσωπικών δεδομένων. Ο συγκεκριμένος κατάλογος προσδιόρισε το εύρος, το αντικείμενο και το σχεδιασμό υλοποίησης της εκάστοτε αξιολόγησης κινδύνων. Κάθε τέτοιος πόρος φέρει κάποια αξία για την εταιρεία, γι’ αυτό και χρήζει της ανάλογης προστασίας.

4) **Προσδιορισμός Νομικού και Κανονιστικού Πλαισίου Ασφάλειας Πληροφοριών**

Κατά την φάση αυτή, πραγματοποιήθηκε ο απαιτούμενος νομικός έλεγχος με βάση τα ευρήματα της χαρτογράφησης ροής δεδομένων, σε σχέση με τις τρέχουσες χρήσεις της εταιρείας. Ειδικότερα, ελέγχθηκαν οι συμβάσεις με επιχειρηματικούς εταίρους, προμηθευτές και πελάτες, οι εφαρμοσμένες διαδικασίες και οι υφιστάμενες εταιρικές πολιτικές, περιλαμβανομένης της διαδικασίας διαχείρισης απειλών, αιτιάσεων και κινδύνων που εμπίπτουν στο πεδίο του Κανονισμού ΕΕ 2016/679, οι τυχόν μεταφορές δεδομένων εκτός της ΕΕ καθώς και όλοι τρόποι επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

5) **Δημιουργία του αρχείου επεξεργασίας των προσωπικών δεδομένων**

Η χαρτογράφηση των προσωπικών δεδομένων, τα οποία επεξεργάζεται η εταιρεία, σε ένα ενιαίο αρχείο, βασίστηκε στην συλλογή στοιχείων μέσω συνεντεύξεων που πραγματοποιήθηκαν με αντιπροσώπους της κάθε επιμέρους διεύθυνσης και στην συνακόλουθη επεξεργασία των στοιχείων αυτών περαιτέρω. Κατά το στάδιο των συνεντεύξεων έγινε συστηματική καταγραφή της υφιστάμενης κατάστασης των προσωπικών δεδομένων που τυγχάνουν επεξεργασίας, ήτοι η καταγραφή των κατηγοριών των δεδομένων και των υποκειμένων τους, του σκοπού της επεξεργασίας ανά είδος δεδομένων, των αποδεκτών στους οποίους γνωστοποιούνται τα δεδομένα ανά κατηγορία, των προβλεπόμενων χρόνων τήρησης/προθεσμίες διαγραφής των διάφορων κατηγοριών δεδομένων και των τεχνικών και οργανωτικών μέτρων που λαμβάνονται για την ασφάλεια αυτών. Στην συνέχεια, εξετάστηκε συγκριτικά με τις απαιτήσεις του Κανονισμού κάθε κατηγορία προσωπικών δεδομένων και κάθε σκοπός επεξεργασίας, ώστε να διαπιστωθεί ο βαθμός συμμόρφωσης της εταιρείας σε θέματα νομιμότητας των σκοπών, συναίνεσης και ενημέρωσης των υποκειμένων, ελαχιστοποίησης των δεδομένων και περιορισμού της περιόδου αποθήκευσης αυτών.

6) **Επισκόπηση της Αρχιτεκτονικής Ασφαλείας**

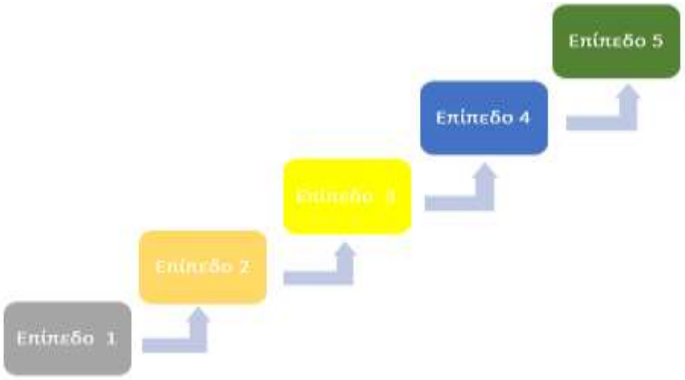
Σκοπό του σταδίου αυτού αποτέλεσε η εξέταση και καταγραφή των υφιστάμενων δικλείδων ασφάλειας που έχουν υιοθετηθεί και εφαρμόζονται από την εταιρεία, οργανωτικής ή τεχνικής φύσης, γεγονός το οποίο συνέβαλε στην αρχική εκτίμηση των αδυναμιών και των κινδύνων που καλείται αυτή να αντιμετωπίσει σχετικά με την προστασία των προσωπικών δεδομένων που επεξεργάζεται. Ενδεικτικά αναφέρονται οι ακόλουθες ενέργειες που πραγματοποιήθηκαν:

- Επανεξέταση της υφιστάμενης αρχιτεκτονικής υποδομών των δικτύων και των τεχνολογιών πληροφορικής σε τεχνικό και επιχειρησιακό επίπεδο
- Ανασκόπηση της υπάρχουσας τεκμηρίωσης δικτύων και πληροφορικής
- Τεχνικές συνεντεύξεις με τους ιδιοκτήτες συστημάτων (π.χ. διαχειριστές δικτύων και συστημάτων, διαχειριστές ασφαλείας, κλπ)
- Αξιολόγηση των ελέγχων ασφαλείας που εφαρμόζονται και ανίχνευση κρίσιμων περιοχών όσον αφορά την ασφάλεια των πληροφοριών
- Επισκόπηση των αντίστοιχων πολιτικών και διαδικασιών ασφαλείας που διέπουν το δίκτυο και την υποδομή πληροφορικής.

7) **Ανάλυση Αποκλίσεων και Πλάνο Συμμόρφωσης**

Η αποτίμηση της συμμόρφωσης της επιχείρησης με το Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR), τις βέλτιστες πρακτικές και τα διεθνή πρότυπα διαρθρώνεται στους ακόλουθους τομείς:

Η ποσοτικοποίηση της εκτίμησης της τρέχουσας κατάστασης της εταιρείας βασίσθηκε στο Μοντέλο Ικανότητας και Ωριμότητας (CMM) διαδικασιών, το οποίο αναπτύχθηκε στο Πανεπιστήμιο Carnegie Mellon. Ο όρος «ωριμότητα» δηλώνει την ύπαρξη σαφώς προσδιορισμένων, διαχειριζόμενων, ελεγχόμενων και αποτελεσματικών διαδικασιών σε έναν οργανισμό. Το πρότυπο CMM ορίζει μία συγκεκριμένη κλίμακα πέντε επιπέδων για τη μέτρηση της ωριμότητας της επιχείρησης σε ό,τι αφορά στις διεργασίες της, όπως ακριβώς αποτυπώνονται στην συνέχεια:



Σχήμα 1: Επίπεδα Ικανότητας και Ωριμότητας

- Επίπεδο 1 - Αρχικό επίπεδο (Initial level): Οι επιχειρήσεις ακολουθούν ad hoc διαδικασίες, τις οποίες μεταβάλλουν ανάλογα με τις ανάγκες τους.
- Επίπεδο 2 - Επίπεδο επαναληψιμότητας (Repeatable level): Η εταιρεία ακολουθεί επαναλαμβανόμενες διαδικασίες βάση της εμπειρίας αλλά και της ικανότητας του προσωπικού.
- Επίπεδο 3 - Καθορισμένο επίπεδο (Defined level): Η εταιρεία ακολουθεί τυποποιημένες και επαναλαμβανόμενες διαδικασίες.
- Επίπεδο 4 - Διαχειριζόμενο επίπεδο (Managed level): Η εταιρεία έχει υιοθετήσει τις βασικές πρακτικές για κάθε διαδικασία ενώ αναλύει την απόδοσης τους για περαιτέρω βελτίωση.
- Επίπεδο 5 - Επίπεδο βελτιστοποίησης (Optimizing level): Η εταιρεία έχει υιοθετήσει πλήρως τις βασικές πρακτικές για κάθε διαδικασία και αναλύει την απόδοσης τους για περαιτέρω βελτίωση.

8) **Αποτίμηση του αντικτύπου στην ιδιωτικότητα**

Η μέθοδος αποτίμησης των προσωπικών και ευαίσθητων προσωπικών δεδομένων της εταιρίας βασίστηκε στην πρότυπη μεθοδολογία ISO/IEC 29134. Η μεθοδολογία αυτή αποτελείται από δύο βασικά στάδια:

✓ Ανάλυση επικινδυνότητας (risk analysis)
✓ Διαχείριση επικινδυνότητας (risk management)

<u>Στάδιο 1ο: Ανάλυση επικινδυνότητας</u>

Στο στάδιο αυτό υπολογίζονται οι δύο παράγοντες που επηρεάζουν την επικινδυνότητα της ιδιωτικότητας, ήτοι η πιθανότητα εμφάνισης της απειλής και η επίπτωση στην πραγματοποίηση μίας απειλής. Ο συνδυασμός των δύο παραγόντων δίνει το βαθμό

επικινδυνότητας των προσωπικών δεδομένων, έτσι ώστε να επιλεγούν τα κατάλληλα αντίμετρα.

α) Προσδιορισμός της πιθανότητας εμφάνισης της απειλής

Η πιθανότητα εμφάνισης μίας απειλής υπολογίζεται βάσει της ευπάθειας, την αποτελεσματικότητα των μηχανισμών προστασίας των δεδομένων και την δυνατότητα εκμετάλλευσης των ευπαθειών ως ακολούθως:

Επίπεδο	Περιγραφή	Τιμή
Μέγιστο	Η πιθανότητα να εκμεταλλευτεί η απειλή μία ή περισσότερες ευπάθειες για το συγκεκριμένο αγαθό είναι πολύ υψηλή (π.χ. κλοπή φυσικών εγγράφων αποθηκευμένα σε ένα ντουλάπι σε δημόσιο χώρο).	4
Σημαντικό	Η πιθανότητα να εκμεταλλευτεί η απειλή μία ή περισσότερες ευπάθειες για το συγκεκριμένο αγαθό είναι πιθανή κάτω από προϋποθέσεις (π.χ. κλοπή φυσικών εγγράφων που είναι αποθηκευμένα σε γραφεία αλλά δεν είναι προσβάσιμα χωρίς πρώτα έλεγχο στη υποδοχή).	3
Περιορισμένο	Η πιθανότητα να εκμεταλλευτεί η απειλή μία ή περισσότερες ευπάθειες για το συγκεκριμένο αγαθό είναι δύσκολη (π.χ. κλοπή των φυσικών εγγράφων που είναι αποθηκευμένα σε ένα χώρο αποθήκευσης που προστατεύεται από σύστημα ελέγχου πρόσβασης).	2
Αμελητέο	Η πιθανότητα να εκμεταλλευτεί η απειλή μία ή περισσότερες ευπάθειες για το συγκεκριμένο αγαθό είναι πολύ μικρές (π.χ. κλοπή των φυσικών εγγράφων που είναι αποθηκευμένα σε ένα χώρο αποθήκευσης που προστατεύεται από σύστημα ελέγχου πρόσβασης και κλειστό κύκλωμα τηλεόρασης).	1

Πίνακας 1: Πίνακας πιθανότητας εμφάνισης της απειλής

β) Εκτίμηση επίπτωσης εμφάνισης της απειλής

Για κάθε περίπτωση εκτιμάται το δυσμενέστερο πιθανό σενάριο και υπολογίζονται οι επιπτώσεις για το υποκείμενο από την πραγματοποίηση της απειλής σε κλίμακα τεσσάρων βαθμίδων (Μέγιστη, Σημαντική, Περιορισμένη και Αμελητέα).

Επίπεδο	Περιγραφή	Τιμή
Μέγιστη	Τα υποκείμενα ενδέχεται να αντιμετωπίσουν σημαντικές ή ακόμη και μη αναστρέψιμες συνέπειες, τις οποίες δεν μπορούν να ξεπεράσουν (ανικανότητα προς εργασία, μακροχρόνιες ψυχολογικές ή σωματικές ασθένειες, θάνατος κλπ.).	4
Σημαντική	Τα υποκείμενα ενδέχεται να αντιμετωπίσουν σημαντικές συνέπειες, τις οποίες θα πρέπει να μπορέσουν να ξεπεράσουν με σοβαρές δυσκολίες (υπεξαίρεση κεφαλαίων, μαύρη λίστα από χρηματοπιστωτικά ιδρύματα, υλικές ζημιές, απώλεια απασχόλησης, κλήτευση, επιδείνωση της υγείας κ.λπ.).	3
Περιορισμένη	Τα υποκείμενα μπορεί να αντιμετωπίσουν κάποιες ενοχλήσεις, τις οποίες θα μπορέσουν να ξεπεράσουν παρά ορισμένες δυσκολίες (επιπλέον κόστος, άρνηση πρόσβασης στις υπηρεσίες των επιχειρήσεων, φόβος, έλλειψη κατανόησης, άγχος, μικρές σωματικές ασθένειες κλπ.).	2
Αμελητέα	Τα υποκείμενα μπορεί να αντιμετωπίσουν μερικές μικρές ενοχλήσεις, τις οποίες θα ξεπεράσουν χωρίς κανένα πρόβλημα (χρόνος ξοδεύοντας πληροφορίες, ενόχληση, κλπ.).	1

γ) Υπολογισμός επικινδυνότητας

Στην παρούσα μελέτη περίπτωσης, ο βαθμός επικινδυνότητας δεν υπολογίζεται για όλα τα προσωπικά δεδομένα συνολικά, αλλά αποτιμάται μεμονωμένα για κάθε συνδυασμό Δεδομένα- Πιθανότητα Εμφάνισης της Απειλής -Επίπτωση της Απειλής. Συγκεκριμένα, η επικινδυνότητα υπολογίζεται με βάση την ακόλουθη σχέση: Επικινδυνότητα = Πιθανότητα Εμφάνισης της απειλής + Επίπτωση της απειλής.

Πιθανότητα εμφάνισης της απειλής	**Επίπτωση**			
	1	2	3	4
1	2	3	4	5
2	3	4	5	6
3	4	5	6	7
4	5	6	7	8

Πίνακας 2: Κλίμακα επικινδυνότητας

Επίπεδο Επικινδυνότητας

Επίπεδο Κινδύνου	Τιμές
Υψηλό – Μη αποδεκτό	7-8
Μέτριο - Μη αποδεκτό	6
Χαμηλό – Αποδεκτό	3-5
Μηδενικό	2

Πίνακας 3: Επίπεδα επικινδυνότητας

Στάδιο 2ο: Διαχείριση της επικινδυνότητας

Με βάση τα αποτελέσματα που προέκυψαν από την ανάλυσης επικινδυνότητας, προτείνεται ένα σχέδιο ασφάλειας το οποίο διαρθρώνεται σε επιμέρους πυλώνες, οι οποίοι περιγράφονται λεπτομερώς στις επόμενες ενότητες. Ο κάθε πυλώνας αποτελείται από μία σειρά αντιμέτρων, τα οποία κρίνονται απαραίτητα για την διαχείριση της επικινδυνότητας και θα πρέπει να εφαρμοστούν. Το σχέδιο ασφάλειας περιλαμβάνει και μία σειρά επιλογών και εναλλακτικών λύσεων, ώστε να παρέχεται ευελιξία στην εφαρμογή του. Η τελική επιλογή των αντιμέτρων που θα εφαρμοστούν λαμβάνει υπόψη και το κόστος που ενέχουν τα αντίμετρα για την εταιρεία.

Τα αντίμετρα χωρίζονται σε ομάδες, ανάλογα με το είδος των απειλών που καλούνται να αντιμετωπίσουν και ανάλογα με το είδος των δεδομένων που καλούνται να προστατέψουν. Η βάση των αντιμέτρων περιλαμβάνει τόσο τις εναλλακτικές λύσεις, δηλαδή ποιο αντίμετρο μπορεί να χρησιμοποιηθεί εναλλακτικά άλλου, καθώς και τις επιλογές υλοποίησής αυτών. Τα κριτήρια που λαμβάνονται υπόψη στην τελική επιλογή περιλαμβάνουν τα εξής:

- Την επίδραση που θα έχουν τα αντίμετρα στη λειτουργία του οργανισμού.
- Το κόστος εγκατάστασης και λειτουργίας των αντιμέτρων.
- Την άποψη της διοίκησης και τους στόχους της.
- Ενδεχόμενες ενδείξεις ότι οι απειλές θα αυξηθούν στο μέλλον.
- Διαθέσιμος προϋπολογισμός για την ασφάλεια των πληροφοριακών συστημάτων.

9) **Αξιοποίηση των αποτελεσμάτων της μελέτης**

Κατά την μελέτη προσδιορίστηκαν με επιστημονική μεθοδολογία, τα κατάλληλα αντίμετρα τα οποία είναι ανάλογα με την επικινδυνότητά. Το σύνολο των αντιμέτρων αποτελεί το Σχέδιο Συμμόρφωσης και Προστασίας των Προσωπικών Δεδομένων.

Συνοπτικά το σχέδιο ασφάλειας προσδιορίζεται ως ένα σύνολο από προτεινόμενες διαδικασίες, πολιτικές, οργανωτικές δομές και τεχνικά έργα που επιτρέπουν στην εταιρεία να καθορίσει και να διαμορφώσει κάθε φορά κατανοητούς στόχους, σκοπούς, κανόνες και αρχιτεκτονικές που επιτυγχάνουν την, κατά τα ανωτέρω, συμμόρφωση με τον κανονισμό και την προστασία των δεδομένων προσωπικού χαρακτήρα. Η κατάσταση με τα αντίμετρα που περιλαμβάνεται πρέπει να χρησιμοποιηθεί για την παρακολούθηση της υλοποίησης του σχεδίου ασφαλείας. Κατά την υλοποίησή του, για κάθε μέτρο πρέπει να σημειώνεται η αντίστοιχη κατάσταση αυτού (state), η οποία μπορεί να είναι:

Α.Α	Κατάσταση	Περιγραφή
1	Εξάλειψη	Επιλογή των μηχανισμών ελέγχου για την εξάλειψη του κινδύνου εντελώς, με απόσυρση της δραστηριότητας ή του συνόλου των δραστηριοτήτων ή την αλλαγή των συνθηκών υπό τις οποίες παρέχεται η υπηρεσία.
2	Αποδοχή	Αναλαμβάνεται η επικινδυνότητα (accept level of risk) και δεν υλοποιείται κανένας μηχανισμός ελέγχου.
3	Μείωση	Επιλογή κατάλληλων μηχανισμών ελέγχου που δεν εξαλείφουν τον κίνδυνο αλλά μειώνουν την επίπτωση ή την πιθανότητα εμφάνισης της απειλής. Οι έλεγχοι επικεντρώνονται συνήθως στη μείωση των τρωτών σημείων ή των απειλών.
4	Μεταφορά	Μεταφορά της επικινδυνότητας σε τρίτη εταιρεία όπως οι ασφαλιστικές εταιρείες και παρόχοι υπηρεσιών ασφαλείας. Η μεταφορά κινδύνου μπορεί να δημιουργήσει νέους κινδύνους ή να τροποποιήσει τους υφιστάμενους.

Επισημαίνεται ότι σημείο έναρξης για την υλοποίηση του σχεδίου συμμόρφωσης αποτελεί η ενεργοποίηση του οργανωτικού σχήματος της ασφάλειας και η θέσπιση των πολιτικών ασφαλείας και προστασίας προσωπικών δεδομένων.

5.3 Εκτίμηση του Αντίκτυπου στην Ιδιωτικότητα

5.3.1 Εισαγωγή

Όπως ήδη αναφέρθηκε, προκειμένου να ενισχυθεί η συμμόρφωση προς τον παρόντα Κανονισμό, όταν οι πράξεις επεξεργασίας ενδέχεται να έχουν ως αποτέλεσμα υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας (= η εταιρεία) θα πρέπει να προβαίνει σε διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων, ώστε να αξιολογήσει, ιδίως, την προέλευση, τη φύση, την πιθανότητα και τη σοβαρότητα του εν λόγω κινδύνου. Το αποτέλεσμα της εκτίμησης θα πρέπει να λαμβάνεται υπόψη όταν καθορίζεται ποια μέτρα ενδείκνυται να ληφθούν ώστε να αποδειχθεί ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα είναι σύμφωνη με τον παρόντα κανονισμό. Εάν η εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων υποδεικνύει ότι οι πράξεις επεξεργασίας συνεπάγονται υψηλό κίνδυνο που ο υπεύθυνος επεξεργασίας δεν μπορεί να μετριάσει με τα κατάλληλα μέτρα από άποψη διαθέσιμης τεχνολογίας και κόστους εφαρμογής, θα πρέπει να πραγματοποιείται διαβούλευση με την αρχή ελέγχου πριν από την επεξεργασία.

5.3.2 Προσδιορισμός των απειλών

Οι απειλές των προσωπικών δεδομένων που επεξεργάζεται η εταιρεία χωρίζονται στις ακόλουθες βασικές κατηγορίες:

Φυσικές και περιβαλλοντικές απειλές: Αστοχία συστήματος παροχής ενέργειας, αστοχία συστήματος κλιματισμού, πυρκαγιά, καταστροφή από νερό (πλημμύρα), φυσική καταστροφή (σεισμός), κλοπή από άτομα εντός της Εταιρείας, κλοπή από συνεργάτες, κλοπή από τρίτους, τρομοκρατική ενέργεια, ανάκτηση φυσικού αρχείου ή μέσων που περιέχουν προσωπικά δεδομένα από απορρίμματα

Λογικές απειλές: Μη εξουσιοδοτημένη πρόσβαση από τρίτους (Hackers), εσωτερικούς χρήστες και παρόχους υπηρεσιών, κακόβουλος κώδικας, κατάχρηση των πόρων του συστήματος, συνακρόαση μέσω δικτύου, παραποίηση μέσω δικτύου, λανθασμένη διαχείριση, λανθασμένη συντήρηση και λανθασμένη χρήση.

Αστοχία εξοπλισμού: Τεχνική αστοχία υπολογιστή, μέσων αποθήκευσης, μέσων εκτύπωσης, δικτυακού εξοπλισμού και επικοινωνιών.

Αστοχία λογισμικού: Αστοχία λογισμικού συστήματος/ δικτύου και λογισμικού εφαρμογών

5.3.3 Διαχείριση των κινδύνων

Στις παραγράφους που ακολουθούν περιγράφεται σε επιμέρους πυλώνες το σχέδιο ασφάλειας των προσωπικών δεδομένων της εταιρείας, στα πλαίσια εφαρμογής της καλύτερης δυνατής διαδικασίας διαχείρισης των υφιστάμενων κινδύνων, εξαιτίας των οποίων καθίσταται επισφαλής τόσο η ακεραιότητα των δεδομένων όσο και η βιωσιμότητα της επιχείρησης γενικότερα.

Πυλώνας 1ος : Πολιτική Ασφαλείας

Κρίνεται απαραίτητο η εταιρεία να θεσπίσει την πολιτική ασφάλειας των πληροφοριακών της συστημάτων, η οποία αφενός θα περιγράφει με σαφήνεια τις βασικές επιλογές της Διοίκησης για την προώθηση της ασφάλειας των δεδομένων και τις γενικές αρχές προστασίας τους και αφετέρου θα παρέχει μία σειρά από οδηγίες και κατευθυντήριες γραμμές για την υλοποίηση των ανωτέρω. Το κείμενο της πολιτικής ασφάλειας πληροφοριών θα πρέπει ενδεικτικά να περιλαμβάνει:

- Τον ορισμό της ασφάλειας των πληροφοριών, το σκοπό της και τη σπουδαιότητά της ως μηχανισμού που επιτρέπει την ανταλλαγή πληροφοριών.
- Τους σκοπούς της διοίκησης και την υποστήριξή της αναφορικά με την ασφάλεια.
- Την επεξήγηση της πολιτικής ασφάλειας, των αρχών, των προτύπων και των απαιτήσεων που πρέπει να ικανοποιήσει η εταιρεία, όπως η σχετική νομοθεσία
- Τον ορισμό γενικών και ειδικών καθηκόντων για τη διαχείριση της ασφάλειας
- Πιθανές αναφορές σε άλλα κείμενα που μπορούν να υποστηρίξουν την πολιτική ασφάλειας, όπως περιγραφές συγκεκριμένων διαδικασιών και κανονισμών.

Η Διοίκηση της εταιρείας θα πρέπει να επικυρώσει την πολιτική ασφάλειας των πληροφοριών, η οποία θα είναι διαθέσιμη σε κάθε υπάλληλο και εξωτερικό συνεργάτη της εταιρείας. Παράλληλα, θα πρέπει να ελέγχεται ετησίως η αποτελεσματικότητά της, καθώς και να αναθεωρείται, όταν τούτο απαιτείται. Υπεύθυνος για τη διαχείριση της πολιτικής ασφαλείας καθίσταται ο υπεύθυνος ασφαλείας πληροφοριών.

Πυλώνας 2ος: Οργάνωση, διαχείριση και διοίκηση ασφάλειας

➢ **Στρατηγική, οργάνωση και υποστήριξη της ασφάλειας**

Η εταιρεία θα πρέπει να οριοθετήσει ένα βασικό οργανωτικό και κανονιστικό πλαίσιο για την οργάνωση, διαχείριση και διοίκηση της προστασίας των προσωπικών δεδομένων. Ωστόσο, η τελική ευθύνη για τη στρατηγική αντιμετώπιση του θέματος της ασφάλειας ανήκει στη Διοίκηση και ως εκ τούτου θα πρέπει να διασφαλίζεται η ενεργός συμμετοχή αυτής στα θέματα που σχετίζονται με την ασφάλεια πληροφοριών. Εν ολίγοις, η Διοίκηση θα πρέπει:

- Να εγκρίνει την μελέτη και συνεπώς το Σχέδιο Συμμόρφωσης και το Σχέδιο Διαχείρισης της Επικινδυνότητας.
- Να επικυρώσει την πολιτική προστασίας των προσωπικών δεδομένων και την πολιτική ασφαλείας.
- Να ανακοινώσει στους υπαλλήλους, στους πελάτες και στους συνεργάτες της την σπουδαιότητα της επεξεργασίας των προσωπικών δεδομένων και την ενεργή υποστήριξη της στην συμμόρφωση με τον νέο κανονισμό (αποστολή e-mail, ανακοίνωση στον ιστότοπο).
- Να ευαισθητοποιήσει τους υπαλλήλους της στο θέμα της επεξεργασίας και της προστασίας των προσωπικών δεδομένων.

Για την υλοποίηση, την επίβλεψη και την υποστήριξη του οργανωτικού και κανονιστικού πλαισίου ασφάλειας των δεδομένων, θα πρέπει να οριστεί από την εταιρεία μία **Επιτροπή Διαχείρισης της Συμμόρφωσης και της Προστασίας προσωπικών δεδομένων**, η οποία θα αποτελείται, κατ' ελάχιστον, από τον Υπεύθυνο Προστασίας Δεδομένων, τον Υπεύθυνο Ασφάλειας Πληροφοριών, τον Διευθυντή Πληροφορικής καθώς και τον Νομικό Σύμβουλο.

➢ **Εκτίμηση του Αντίκτυπου στην Ιδιωτικότητα**

Η Εταιρεία θα πρέπει να αναπτύξει και να εφαρμόζει Σύστημα Διαχείρισης του Αντίκτυπου στην Ιδιωτικότητα, σύμφωνα με το πρότυπο ISO/IEC 29134, το οποίο θα υποστηρίζει τη Διοίκηση στη λήψη στρατηγικών αποφάσεων αναφορικά με τον εντοπισμό, την αξιολόγηση, την αντιμετώπιση των κινδύνων και την επικοινωνία αυτών στα υποκείμενα των δεδομένων, συμπεριλαμβάνοντας όλα τα στρατηγικά, επιχειρησιακά και οργανωτικά μέτρα ελέγχου και παρακολούθησης που χρησιμοποιούνται στη διαχείριση κινδύνων. Στο πλαίσιο εφαρμογής του συστήματος

αυτού, θα πρέπει να καθορισθεί η στρατηγική για την παρακολούθηση, ανταπόκριση και διαχείριση των κινδύνων, έτσι ώστε να:

- διασφαλίζεται ότι οι υφιστάμενοι κίνδυνοι εντοπίζονται συστηματικά, αναλύονται και αξιολογούνται και, οι πληροφορίες που σχετίζονται με τους κινδύνους και τις αντίστοιχες ευκαιρίες, κοινοποιούνται αμέσως στα αρμόδια όργανα λήψης αποφάσεων.
- καταγράφεται η ανταπόκριση τη εταιρείας στον τρόπο που αντιμετωπίζει κινδύνους που έχουν αναγνωριστεί και να αξιολογούνται εναλλακτικές επιλογές (όπως μεταφορά των κινδύνων σε τρίτους φορείς, π.χ. ασφαλιστικές εταιρείες).

Η Αξιολόγηση Κινδύνων (Risk Assessment) θα πρέπει να αποτελεί μία δομημένη διεργασία όσων αφορά στην αναγνώριση, ανάλυση, αποτίμηση και την αντιμετώπιση των κινδύνων των υποκειμένων, με στόχο τη λήψη βέλτιστων αποφάσεων από τα αρμόδια όργανα της εταιρείας για τη διαχείριση και αντιμετώπισή τους και την παρακολούθηση υλοποίησης των σχετικών μέτρων. Για τον σκοπό αυτό, προτείνεται η διεθνή μεθοδολογία Αξιολόγησης Κινδύνων σε όλες τις επιχειρησιακές μονάδες με βάση καθολικά κριτήρια εκτίμησης και αξιολόγησης, σύμφωνα με τις απαιτήσεις του προτύπου ISO/IEC 29134. Επιπλέον, οι κίνδυνοι και οι σχετικές απειλές θα πρέπει να προσδιορίζονται σε ετήσια βάση, εάν αυτό απαιτείται, ενώ τα επίπεδα των κινδύνων θα πρέπει να προσδιορίζονται σύμφωνα με την πιθανότητα εμφάνισης και της επίπτωσης της απειλής.

Πυλώνας 3ος: Ασφάλεια προσωπικού

- **Πρόσληψη προσωπικού**

Κατά το στάδιο αξιολόγησης υποψήφιων υπαλλήλων, κρίνεται σκόπιμο η διεύθυνση Ανθρώπινου Δυναμικού της εταιρείας να μεριμνά για την ενημέρωση τους, μέσω σχετικού εντύπου, αναφορικά με όλα τα προσωπικά τους δεδομένα, τα οποία τυγχάνουν επεξεργασίας από την εν λόγω διεύθυνση με αποκλειστικό σκοπό την εκτίμηση της καταλληλότητας των αιτούντων για την εκάστοτε διαθέσιμη θέση εργασίας. Τα δεδομένα αυτά συλλέγονται από την εταιρεία μέσω των βιογραφικών σημειωμάτων που αποστέλλονται από τους υποψηφίους. Σε περίπτωση μη επιλογής του υποψηφίου για την κάλυψη συγκεκριμένης θέσης εργασίας, ως ένα εύλογο χρονικό διάστημα διατήρησης των δεδομένων τους προτείνεται αυτό των δύο ετών.

Επιπλέον, η εταιρεία θα πρέπει να δημιουργήσει ένα **εγχειρίδιο ενημέρωσης των εργαζομένων** της αναφορικά με την προστασία των προσωπικών τους δεδομένων, για το οποίο θα λαμβάνει γνώση κάθε νέος υπάλληλος που εισέρχεται στο εργατικό της δυναμικό και συνακόλουθα θα το υπογράφει, παράλληλα με την ατομική του σύμβαση εργασίας. Εναλλακτικά, μπορεί να δίνεται προς ενημέρωση και υπογραφή στους νέους υπαλλήλους η Πολιτική Προστασίας Προσωπικών Δεδομένων της εταιρείας ή Κώδικας Δεοντολογίας.

- **Εργασία προσωπικού**

Στα πλαίσια της ευρύτερης εργασίας και λειτουργίας του προσωπικού της εταιρείας, προτείνεται η υλοποίηση των παρακάτω ενεργειών για την αποφυγή περιστατικών που θέτουν σε κίνδυνο την προστασία των προσωπικών δεδομένων:

- Διαχωρισμός των καθηκόντων: πρόκειται για μια μέθοδο που αποσκοπεί στη μείωση του κινδύνου κατάχρησης των συστημάτων, είτε από αμέλεια είτε από δόλο, ενώ παράλληλα ελαχιστοποιεί τις πιθανότητες κατάχρησης ή μη εξουσιοδοτημένων αλλαγών στα δεδομένα ή τις υπηρεσίες. Η εταιρεία θα πρέπει να θεσπίσει τις απαραίτητες αρμοδιότητες του προσωπικού της σε θέματα επεξεργασίας προσωπικών δεδομένων ανά τμήμα/ρόλο.

- Διαδικασία συμμόρφωσης: τα περιστατικά παραβίασης της ασφάλειας, για τα οποία ευθύνεται προσωπικό της εταιρείας, θα πρέπει να αντιμετωπίζονται με βάση συγκεκριμένη και σαφώς οριοθετημένη διαδικασία συμμόρφωσης.

- Εκπαίδευση και ενημέρωση: θα πρέπει να πραγματοποιείται τακτικά εκπαίδευση και ενημέρωση του προσωπικού της εταιρείας σε θέματα προστασίας προσωπικών δεδομένων. Οι υπάλληλοι της εταιρείας θα πρέπει να εκπαιδευτούν κατ' ελάχιστο στις διαδικασίες διαχείρισης και προστασίας των προσωπικών δεδομένων ώστε να ελαχιστοποιηθούν οι πιθανοί κίνδυνοι. Ειδικότερα, η ενημέρωση και η ευαισθητοποίησή τους θα πρέπει ενδεικτικά να περιλαμβάνει τις θεμελιώδεις δομές και την ορολογία του Γενικού Κανονισμού προστασίας των δεδομένων, τα δικαιώματα και τις ελευθερίες των υποκείμενων των δεδομένων, την διαχείριση των αιτήσεων πρόσβασης των υποκειμένων, την συμμόρφωση με τον Νέο Κανονισμό, την διαδικασία γνωστοποίησης περιστατικών ασφαλείας, καθώς και τις διαδικασίες και πολιτικές προστασίας προσωπικών δεδομένων.

- **Τερματισμός ή μεταβολή της εργασιακής σχέσης**

Οι υπάλληλοι υποχρεούνται, με τον τερματισμό της εργασίας τους, να παραδώσουν στην εταιρεία όλον τον εταιρικό εξοπλισμό που βρισκόταν στην δική τους κατοχή κατά την διάρκεια της συνεργασίας τους με την εταιρεία, καθώς και όλα τα φυσικά ή ηλεκτρονικά αρχεία και έγγραφα που περιέχουν προσωπικά δεδομένα. Παράλληλα, η εταιρεία δύναται να ζητήσει από αυτούς την προσκόμιση έγγραφης βεβαίωσης, με την οποία θα δηλώνουν ότι δεν διατηρούν στην κατοχή τους οποιασδήποτε μορφής αντίγραφα των προσωπικών δεδομένων της εταιρείας, τα οποία και θα πρέπει να διαγραφούν από κάθε ηλεκτρονική συσκευή που διαθέτουν. Επιπλέον, τα δικαιώματα πρόσβασης των χρηστών στα συστήματα της εταιρείας θα πρέπει να αφαιρούνται κατά τον τερματισμό της εργασιακής σχέσης των υπαλλήλων, ενώ ο σκληρός δίσκος του Η/Υ του πρώην υπαλλήλου θα πρέπει να διαγράφεται οριστικά, εφόσον πρώτα ενημερωθεί, ούτως ώστε να αφαιρέσει τυχόν υπάρχοντα προσωπικά του δεδομένα.

- **Συστήματα εντοπισμού γεωγραφικής θέσης (GPS)**

Οι τεχνολογίες που επιτρέπουν στους εργοδότες να παρακολουθούν τα οχήματά τους έχουν υιοθετηθεί ευρέως, ιδίως μεταξύ των οργανισμών των οποίων οι δραστηριότητες συνεπάγονται τη μεταφορά ή έχουν σημαντικούς στόλους οχημάτων. Κάθε εργοδότης που χρησιμοποιεί την τηλεματική των οχημάτων συλλέγει δεδομένα τόσο για το όχημα όσο και για τον υπάλληλο που χρησιμοποιεί αυτό το όχημα, συμπεριλαμβανομένης της τοποθεσίας του οχήματος ή ακόμα και της συμπεριφοράς οδήγησης. Ωστόσο, ακόμη και αν οι εργοδότες έχουν έννομο συμφέρον να επιτύχουν αυτούς τους σκοπούς, θα πρέπει πρώτα να αξιολογείται κατά πόσον είναι αναγκαία η εν λόγω επεξεργασία και αν η πραγματική εφαρμογή τηρεί τις αρχές της αναλογικότητας. Συγκεκριμένα, για να είναι θεμιτή η επεξεργασία των προσωπικών δεδομένων των εργαζομένων μέσω των συστημάτων εντοπισμού γεωγραφικής θέσης, θα πρέπει να υφίστανται, κατά κύριο λόγο, οι παρακάτω προϋποθέσεις:

- Η επεξεργασία πραγματοποιείται στο πλαίσιο της παρακολούθησης της μεταφοράς ατόμων ή αγαθών ή στη βελτίωση της κατανομής πόρων για υπηρεσίες σε διάσπαρτες τοποθεσίες (π.χ. προγραμματισμός πράξεων σε πραγματικό χρόνο) ή όταν επιδιώκεται ένας στόχος ασφάλειας σε σχέση με τον ίδιο τον εργαζόμενο ή με τα αγαθά ή τα οχήματα που είναι υπό την ευθύνη του.
- Ο υπάλληλος θα πρέπει να έχει τη δυνατότητα προσωρινής απενεργοποίησης της παρακολούθησης της τοποθεσίας όταν υπάρχουν ειδικές περιστάσεις που δικαιολογούν αυτήν την ενέργεια, όπως επίσκεψη σε γιατρό. Με αυτόν τον τρόπο, ο εργαζόμενος μπορεί με δική του πρωτοβουλία να προστατεύσει ορισμένα δεδομένα τοποθεσίας ως ιδιωτικά.

- Η εταιρεία πρέπει να διασφαλίσει ότι τα δεδομένα που συλλέγονται δεν χρησιμοποιούνται για παράνομη περαιτέρω επεξεργασία, όπως η παρακολούθηση και η αξιολόγηση των εργαζομένων.
- Η εταιρεία πρέπει επίσης να ενημερώσει με σαφήνεια τους εργαζόμενους ότι έχει εγκατασταθεί συσκευή παρακολούθησης στα εταιρικά οχήματα που οδηγούν και ότι οι κινήσεις τους καταγράφονται κατά τη χρήση του οχήματος.

Πυλώνας 4ος: Διαχείριση Προσωπικών Δεδομένων

➢ **Αρχείο των δραστηριοτήτων επεξεργασίας προσωπικών δεδομένων**

Υπεύθυνος για την δημιουργία και τη διαχείριση του αρχείου των δραστηριοτήτων επεξεργασίας που τηρούνται από την εταιρεία είναι ο Υπεύθυνος Προστασίας Δεδομένων, ο οποίος θα πρέπει να αναπτύξει μια διαδικασία για να εξασφαλιστεί ότι το αρχείο θα ενημερώνεται τακτικά, ώστε να αντικατοπτρίζει τις αλλαγές που συσχετίζονται με τα προσωπικά δεδομένα που επεξεργάζεται η εταιρεία. Η δημιουργία του αρχείου δραστηριοτήτων επεξεργασίας των προσωπικών δεδομένων συμβάλλει στην σωστή προστασία τους και την συμμόρφωση της εταιρείας με τον Κανονισμό. Η διαδικασία της καταγραφής τους είναι σημαντικό τμήμα της διαδικασίας εκτίμησης του αντίκτυπου σχετικά με την προστασία των δεδομένων. Για κάθε κατηγορία προσωπικών δεδομένων θα πρέπει, ενδεικτικά και όχι περιοριστικά, να καταγράφονται ο σκοπός επεξεργασίας, οι κατηγορίες των υποκειμένων των δεδομένων και τρόπος συγκατάθεσής αυτών, ο τρόπος συλλογής των δεδομένων από την εταιρεία, ο προβλεπόμενος χρόνος διατήρησής τους και τα μέτρα προστασίας που λαμβάνονται από την εταιρεία. Τέλος, η πληρότητα και η ορθότητα του αρχείου θα πρέπει να ελέγχεται σε ετήσια βάση.

➢ **Ταξινόμηση των προσωπικών δεδομένων**

Τα προσωπικά δεδομένα θα πρέπει να κατατάσσονται σε κατηγορίες προκειμένου να καταδεικνύονται η ανάγκη, ο βαθμός και η προτεραιότητα της προστασίας που χρειάζονται. Κάποια δεδομένα μπορεί να χρειάζονται ειδική μεταχείριση και επιπλέον μέτρα προστασίας. Για τον καθορισμό των απαιτούμενων επιπέδων προστασίας, καθώς και για την επισήμανση τυχόν ανάγκης για ειδική μεταχείριση, μπορεί να χρησιμοποιείται ένα σύστημα διαβάθμισης των πληροφοριών σε τρία επίπεδα (δημόσιες, εταιρικές, ευαίσθητες). Κατά την ταξινόμηση των προσωπικών δεδομένων θα πρέπει να λαμβάνονται υπόψη, εκτός του Γενικού Κανονισμού Προστασίας

Δεδομένων, οι συμβατικές και οποιεσδήποτε άλλες νομικές απαιτήσεις, όπως η ασφαλιστική ή φορολογική νομοθεσία.

- **Διαχείριση των προσωπικών δεδομένων**

Η εταιρεία θα πρέπει να αναπτύξει τις διαδικασίες διαχείρισης των προσωπικών δεδομένων. Η μετάδοση των προσωπικών δεδομένων εκτός της εταιρείας, για παράδειγμα, θα πρέπει να γίνεται με χρήση κρυπτογραφικών τεχνικών αλλά και η αποθήκευση αυτών θα πρέπει να γίνεται σε εξυπηρετητές και σταθμούς εργασίας (π.χ. file servers, DB, laptop) μέσω μηχανισμών κρυπτογράφησης.

Τα προσωπικά δεδομένα θα πρέπει επίσης να καταστρέφονται με ασφαλή τρόπο μετά το πέρας του χρόνου διατήρησης, ώστε να αποκλειστεί η περαιτέρω μη νόμιμη και αθέμιτη επεξεργασία τους, όπως είναι η κάθε μορφής διάθεση σε τρίτους. Ως ασφαλής τρόπος καταστροφής των δεδομένων θεωρείται κάθε σύνολο διαδικασιών και μέτρων που μετά από την ολοκλήρωση της εφαρμογής τους δεν επιτρέπει την αναγνώριση των δεδομένων, όπως είναι για παράδειγμα ο καταστροφέας εγγράφων τύπου «cross cut», ο οποίος ενδείκνυται για την καταστροφή των φυσικών εγγράφων.

- **Χειρισμός Μέσων**

Είναι σκόπιμο να θεσπιστούν κατάλληλες λειτουργικές διαδικασίες για την προστασία μέσων υπολογιστή (π.χ. ταινίες, CD-ROM, DVD-ROM) που περιέχουν προσωπικά δεδομένα από μη εγκεκριμένη αποκάλυψη, τροποποίηση αφαίρεση και καταστροφή τους. Τα φορητά μέσα που περιέχουν προσωπικά δεδομένα θα πρέπει να προστατεύονται σε φωριαμό ή συρτάρι ασφαλείας, ενώ για τα μέσα εκείνα που περιέχουν ευαίσθητα προσωπικά δεδομένα προτείνεται η μέθοδος της κρυπτογράφησης. Σημειώνεται ότι τα προσωπικά δεδομένα μπορεί να είναι ευάλωτα σε κάθε μορφής υποκλοπή, κατάχρηση ή μη εξουσιοδοτημένη παρέμβαση κατά τη μεταφορά τους, γι' αυτό και θα πρέπει να χρησιμοποιούνται αξιόπιστα μέσα και υπηρεσίες μεταφοράς, ενώ θα πρέπει να συσκευάζονται κατάλληλα, ώστε να προστατευθούν από το ενδεχόμενο φθοράς. Κατά την απόσυρση από τη λειτουργία τους δε, τα μέσα αυτά θα πρέπει να καταστρέφονται φυσικά χωρίς να είναι δυνατή η επαναλειτουργία αυτών ή να ανακυκλώνονται πριν επαναχρησιμοποιηθούν.

- **Πρόληψη από διαρροή Δεδομένων**

Για την αποτελεσματική προστασία των προσωπικών δεδομένων της εταιρείας προτείνεται η υλοποίηση ενός ολοκληρωμένου συστήματος πρόληψης δεδομένων από την διαρροή. Το εν λόγω σύστημα θα πρέπει να διασφαλίζει την προστασία και των

προσωπικών δεδομένων μέσα και έξω από την εταιρεία, καθώς και να εμποδίζει την απώλεια «ευαίσθητων» πληροφοριών ως αποτέλεσμα των ενεργειών του χρήστη, όπως η παράνομη αντιγραφή σε οπτικά ή αλλά εξωτερικά αποθηκευτικά μέσα, η εκτύπωση, η μεταφορά μέσω δικτύου ή η αποστολή μέσω ηλεκτρονικού ταχυδρομείου. Επιπροσθέτως, θα πρέπει να επιτρέπει την εκτεταμένη καταγραφή καθώς και την παραγωγή αναλυτικών αναφορών σχετικά με τις παραβιάσεις της υπάρχουσας πολιτικής ασφάλειας. Σε κάθε περίπτωση παραβίασης της εφαρμοζόμενης πολιτικής ασφάλειας εταιρικών δεδομένων, το σύστημα θα πρέπει να παράγει τις αντίστοιχες ειδοποιήσεις (alerts), οι οποίες θα προωθούνται αυτόματα στους διαχειριστές της υποδομής, ενημερώνοντας ταυτόχρονα και τους ίδιους τους τελικούς χρήστες σχετικά με την ισχύουσα πολιτική προστασίας δεδομένων της εταιρείας.

Πυλώνας 5ος : Έλεγχος Πρόσβασης

Για τον έλεγχο της πρόσβασης των χρηστών στα προσωπικά δεδομένα που διαχειρίζεται η εταιρεία και την διαχείριση των κινδύνων που ενδέχεται να προκαλέσει μία μη εξουσιοδοτημένη πρόσβαση, κρίνονται αναγκαίες οι παρακάτω ενέργειες:

- ✓ Η αποτύπωση των αναγκών της εταιρείας για τον έλεγχο της πρόσβασης στα προσωπικά της δεδομένα σε μία σαφώς οριοθετημένη πολιτική ελέγχου
- ✓ Καθορισμός μοναδικών στοιχείων ταυτοποίησης του κάθε χρήστη (όνομα χρήστη και κωδικός πρόσβασης) καθώς και της πολιτικής πρόσβασης αυτών ανάλογα με τον ρόλο που κατέχουν στην ιεραρχική δομή της εταιρείας.
- ✓ Οι χρήστες να έχουν πρόσβαση μόνο στα προσωπικά δεδομένα που είναι απαραίτητα για την εκτέλεση των εργασιών που συνδέονται με το ρόλο τους.
- ✓ Η εφαρμογή μηχανισμών αυθεντικοποίησης των χρηστών, οι οποίοι θα είναι ανάλογοι με τους ρόλους που αποδίδονται σε καθένα εξ αυτών.
- ✓ Πλήρης ενημέρωση των χρηστών για τις ευθύνες τους σχετικά με τους μηχανισμούς προστασίας των προσωπικών δεδομένων.
- ✓ Οι χρήστες θα πρέπει να εξασφαλίζουν την επαρκή προστασία εξοπλισμού της εταιρείας, όπως για παράδειγμα να αποσυνδέονται από την εκάστοτε εφαρμογή που χρησιμοποιούν όταν έχουν ολοκληρώσει την εργασία τους.

Πυλώνας 6ος: Φυσική και περιβαλλοντική ασφάλεια

- **Φυσική ασφάλεια**

Τα φυσικά έγγραφα που περιέχουν ευαίσθητα προσωπικά δεδομένα θα πρέπει να στεγάζεται σε περιοχές ασφάλειας, προστατευμένες σύμφωνα με κατάλληλους περιορισμούς ασφάλειας και ελέγχους εισόδου. Για παράδειγμα, μπορούν να στεγάζονται σε ειδικά δωμάτια φύλαξης με πόρτα ασφαλείας και πυρασφαλείας, τα οποία θα παραμένουν κλειδωμένα. Προτείνεται, επίσης η εγκατάσταση συστήματος ελέγχου πρόσβασης, με βάση το οποίο θα ελέγχεται η είσοδος και η έξοδος από κάθε χώρο μέσω ειδικών μαγνητικών κλειδαριών και αναγνωστών καρτών. Παρόμοιο σύστημα ελέγχου πρόσβασης μπορεί να εγκατασταθεί και στην αίθουσα ασφάλειας των υπολογιστών. Αποτελεσματική θεωρείται και η εγκατάσταση συστήματος παρακολούθησης των χώρων φύλαξης του φυσικού αρχείου της εταιρείας και ψηφιακής καταγραφής.

- **Σύστημα βιντεοεπιτήρησης (CCTV)**

Η εταιρεία οφείλει να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για το απόρρητο και την ασφάλεια των δεδομένων καθώς και για την προστασία τους από κάθε μορφής αθέμιτη επεξεργασία. Η επεξεργασία δεδομένων εικόνας και ήχου μέσω κλειστού κυκλώματος τηλεόρασης επιτρέπεται όταν είναι απαραίτητη για την προστασία αγαθών και προσώπων και των θεμελιωδών δικαιωμάτων αυτών. Τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται θα πρέπει να είναι πρόσφορα και όχι περισσότερα από όσα απαιτούνται σε σχέση με τον επιδιωκόμενο σκοπό, ο οποίος θα πρέπει να μη δύναται να επιτευχθεί με ηπιότερα μέσα. Εφόσον από τη λήψη δεδομένων ήχου και εικόνας που αποθηκεύονται ή τη λήψη που γίνεται σε πραγματικό χρόνο δεν προκύπτει επέλευση συμβάντος που εμπίπτει στον επιδιωκόμενο σκοπό, τα δεδομένα πρέπει να καταστρέφονται το αργότερο μέσα σε δεκαπέντε (15) ημερολογιακές ημέρες. Σε περίπτωση συμβάντος που αφορά τον σκοπό της επεξεργασίας, η εταιρεία επιτρέπεται να τηρεί τις λήψεις, στις οποίες έχει καταγραφεί το συγκεκριμένο συμβάν σε χωριστό αρχείο για τρεις (3) μήνες. Μετά την πάροδο του ανωτέρω χρονικού διαστήματος η εταιρεία μπορεί να τηρεί τα δεδομένα για μεγαλύτερο συγκεκριμένο χρονικό διάστημα μόνο σε εξαιρετικές περιπτώσεις όπου το συμβάν χρήζει περαιτέρω διερεύνησης. Στην περίπτωση αυτή η εταιρεία έχει την υποχρέωση να ενημερώσει την ΑΠΔΠΧ για το αναγκαίο χρονικό διάστημα τήρησης των εν λόγω λήψεων.

Πυλώνας 7ος : Λειτουργίες της εταιρείας

➢ Λειτουργικές διαδικασίες και αρμοδιότητες

Οι διαδικασίες για τη διαχείριση και τη λειτουργία των εφαρμογών που διαχειρίζονται προσωπικά δεδομένα θα πρέπει να είναι σαφώς καθορισμένες και να θεωρούνται επίσημα έγγραφα της εταιρείας. **Θ**α πρέπει μάλιστα να αναθεωρούνται όποτε υπάρχουν σημαντικές αλλαγές στις εφαρμογές της εταιρείας και να υπόκεινται σε ετήσιο έλεγχο. Οι αλλαγές στα συστήματα που επεξεργάζονται προσωπικά δεδομένα πρέπει να ελέγχονται, καθώς αποτελούν αρκετά συχνά αιτία προβλημάτων. Κρίνεται επίσης αναγκαίο να τεκμηριώνονται οι επίσημες διαδικασίες έγκρισης των προτεινόμενων αλλαγών, καθώς και να ελέγχονται οι πιθανές συνέπειες των αυτών κυρίως σε θέματα ασφάλειας και επεξεργασίας των προσωπικών δεδομένων.

➢ Προστασία από κακόβουλο λογισμικό

Απαιτείται ειδική μέριμνα για τον εντοπισμό και την προστασία των προσωπικών δεδομένων από κακόβουλο λογισμικό μηδενικού χρόνου. Ειδικότερα απαιτείται να εγκατασταθεί λογισμικό ανίχνευσης κακόβουλου λογισμικού σε όλα τα τελικά σημεία (σταθμοί εργασίας, εξυπηρετητές, έξυπνα τηλέφωνα, ταμπλέτες) και όχι μόνο στην υπηρεσία ηλεκτρονικού ταχυδρομείου, ενώ τα τεχνικά χαρακτηριστικά του αυτού θα πρέπει να είναι κατ' ελάχιστο τα εξής:

- Υποστήριξη των ακόλουθων τύπων αρχείων: Adobe PDF, Microsoft Office, Exe, Files in archives, Flash, Java Applets, PIF
- Υποστήριξη των ακόλουθων περιβαλλόντων εξομοίωσης: Microsoft Windows XP/7/8/10, Microsoft Office, Adobe Reader
- Υποστήριξη της ανάλυσης ενός αρχείου σε επίπεδο επεξεργαστή.
- Υποστήριξη της εξαγωγής των επισυναπτόμενων αρχείων ή των αρχείων που κατεβάζει ένας χρήστης σε ασφαλή αρχεία σε .pdf απαλλαγμένα από κάθε κακόβουλο κώδικα μηδενικού χρόνου.
- Για κάθε κακόβουλο αρχείο να δημιουργείται αναλυτική αναφορά

➢ Εφεδρικά αντίγραφα

Θα πρέπει να γίνεται τακτική λήψη εφεδρικών αντιγράφων των προσωπικών δεδομένων, να υπάρχουν οι επαρκείς πόροι για τη λήψη αυτών, όπως και να γίνονται τακτικές δοκιμές ώστε να διασφαλίζεται η ικανοποίηση των αναγκών της εταιρείας. Η λήψη των εφεδρικών αντιγράφων των δεδομένων μπορεί να υλοποιηθεί σε τρεις

ανεξάρτητες διαδικασίες: (α) ημερήσια, (β) εβδομαδιαία και (γ) μηνιαία. Κατά τη μηνιαία διαδικασία συνήθως λαμβάνεται εφεδρικό αντίγραφο, επιπλέον των δεδομένων, και του λογισμικού συστήματος (full system back-up).Τα εφεδρικά αντίγραφα πρέπει να φυλάσσονται σε κατάλληλους χώρους που τα προστατεύουν από φυσικούς και κλιματολογικούς παράγοντες ή από μη εξουσιοδοτημένη πρόσβαση.

- **Διαχείριση Τεχνικών Ευπαθειών και patches**

Θα πρέπει να θεσπισθεί ένα σχέδιο για τη διαχείριση των τεχνικών ευπαθειών και των patches. Η διαχείριση τεχνικών ευπαθειών ικανοποιεί τις ακόλουθες απαιτήσεις:

- Ο υπεύθυνος ασφαλείας είναι υπεύθυνος για την διαχείριση των τεχνικών ευπαθειών και ο διευθυντής πληροφορικής για τα patches.
- Παρακολουθούνται οι διαδικτυακοί τόπων των κατασκευαστών του εξοπλισμού και διεθνών οργανισμών ασφάλειας πληροφοριακών συστημάτων (SANS, CERT) για ανακοινώσεις νέων ευπαθειών.
- Υλοποιείται αποτίμηση των επιπτώσεων από την ευπάθεια από τον υπεύθυνο ασφαλείας.
- Καθορίζονται προτεραιότητες αντιμετώπισης των ευπαθειών ανάλογα με την κρισιμότητα της ευπάθειας και χρονοπρογραμματισμός των ενεργειών.

Πυλώνας 8ος : Ασφάλεια Δικτύων και Επικοινωνιών

- **Κρυπτογράφηση**

Κρυπτογράφηση ονομάζεται η διαδικασία κωδικοποίησης της πληροφορίας με τέτοιο τρόπο ώστε να παρεμποδίζεται η ανάγνωσή της από μη εξουσιοδοτημένα μέρη. Οι χρήση μηχανισμών κρυπτογράφησης συντελούν στην διασφάλιση της εμπιστευτικότητας και της ακεραιότητας των προσωπικών δεδομένων. Δύνανται να χρησιμοποιηθούν μόνο διεθνείς και αναγνωρισμένοι μηχανισμοί κρυπτογράφησης. Η κρυπτογράφηση υλοποιείται μέσω του εξουσιοδοτημένου λογισμικού της εταιρείας, η ακριβής καταγραφή του οποίου πραγματοποιείται από τον υπεύθυνο ασφαλείας.

- **Ασύρματα Δίκτυα**

Η εταιρεία για την υλοποίηση του ασύρματου δικτύου θα πρέπει να λάβει μέριμνα για τον περιορισμό των κινδύνων που απορρέουν από τη χρήση του και συγκεκριμένα θα πρέπει να εξασφαλίζεται ότι οι χρήστες που συνδέονται στο ασύρματο δίκτυο σε καμία περίπτωση δεν έχουν πρόσβαση σε κεντρικές υποδομές.

- **Ηλεκτρονικό ταχυδρομείο**

Η χρήση του ηλεκτρονικού ταχυδρομείου, κατά την υπηρεσία επικοινωνίας των χρηστών, θα πρέπει να ακολουθεί συγκεκριμένους κανόνες. Για παράδειγμα, θα πρέπει να αποφευχθεί η διακίνηση των προσωπικών δεδομένων εκτός της εταιρείας μέσω ηλεκτρονικού ταχυδρομείου, χωρίς την χρήση κρυπτογραφικών μεθόδων ή συνθηματικών. Επίσης, πρέπει να απαγορεύεται η χρήση ηλεκτρονικών μηνυμάτων που περιέχουν προσωπικά δεδομένα και ευαίσθητα προσωπικά δεδομένα σε προσωπικές ηλεκτρονικές θυρίδες.

- **Ιστότοποι και κοινωνικά δίκτυα**

Οι πληροφορίες, που αναρτώνται στις προσβάσιμες από το κοινό ιστοσελίδες ή κοινωνικά δίκτυα θα πρέπει να ελέγχονται, ώστε να μη δημοσιοποιούνται προσωπικά δεδομένα χωρίς την προηγούμενη ρητή συγκατάθεση των υποκειμένων των δεδομένων. Επιπλέον, η πρόσβαση σε κοινωνικά δίκτυα θα πρέπει να υλοποιείται από εταιρικούς λογαριασμούς και με τα κατάλληλα μέτρα προστασίας.

- **Κινητές Συσκευές (Mobile Devices)**

Η εταιρεία θα πρέπει να αναπτύξει τις κατάλληλες πολιτικές, διαδικασίες και συστήματα διαχείρισης των κινητών συσκευών που χρησιμοποιούνται από τους υπαλλήλους της, προκειμένου να ελαχιστοποιήσει τη πιθανότητα εμφάνισης απειλών, μέσω της χρήσης των εν λόγω συσκευών, για την προστασία των προσωπικών της δεδομένων. Ειδικότερα, προτείνεται η απαγόρευση της πρόσβασης στο εταιρικό δίκτυο από τις προσωπικές κινητές συσκευές των χρηστών. Η πρόσβαση στις υπηρεσίες του εταιρικού δικτύου θα πρέπει να επιτρέπεται αποκλειστικά και μόνο από εταιρικές κινητές συσκευές εγκεκριμένες από την Διεύθυνση Πληροφορικής. Επιπλέον, θα πρέπει να εγκατασταθεί ένα σύστημα διαχείρισης κινητών συσκευών, το οποίο ενδεικτικά θα περιλαμβάνει την δυνατότητα τήρησης μητρώου λογισμικού και υλικού , την υποστήριξη συνθηματικών και κρυπτογράφησης, τον περιορισμό των εφαρμογών που μπορούν να «κατέβουν» στις συσκευές μέσω διαδικτύου και τον εντοπισμό των συσκευών που έχουν χαθεί ή κλαπεί. Ιδανικά, κάθε εταιρική κινητή συσκευή θα πρέπει να διαθέτει προστασία από κακόβουλο λογισμικό μηδενικού χρόνου και μηχανισμούς κρυπτογράφησης για την επικοινωνία και την αποθήκευση των προσωπικών δεδομένων.

Πυλώνας 9ος : Διαχείριση σχέσεων με τρίτα μέρη

Τα τρίτα μέρη αποτελούν πιθανό κίνδυνο για την ασφάλεια των προσωπικών δεδομένων. Ως εκ τούτου, οι κίνδυνοι που προέρχονται από τη συνεργασία της εταιρείας με τρίτα μέρη θα πρέπει να διερευνώνται αναλυτικά και επισταμένα ετησίως μέσω εκπόνησης αποτίμησης της επικινδυνότητας καθώς και αποτίμησης των επιπτώσεων στην ιδιωτικότητα. Ως ελάχιστες απαιτούμενες ενέργειες της εταιρείας για την προστασία των προσωπικών της δεδομένων από τις σχέσεις που αυτή αναπτύσσει με τρίτα μέρη προτείνονται οι ακόλουθες:

- ✓ Απαγόρευση σε τρίτα μέρη της πρόσβασης στους πληροφοριακούς πόρους και στις κτιριακές εγκαταστάσεις επεξεργασίας προσωπικών δεδομένων της εταιρείας, εάν δεν έχει υπογραφεί προηγουμένως σχετική σύμβαση συνεργασίας μεταξύ τους.
- ✓ Τα ζητήματα σχετικά με την προστασία των προσωπικών δεδομένων της εταιρείας θα πρέπει να ρυθμίζονται με ειδικές συμβάσεις, οι οποίες θα διασφαλίζουν ότι οι τρόποι και οι σκοποί της επεξεργασίας τους από τρίτα μέρη είναι συμβατοί τόσο με την πολιτική προστασίας αυτής όσο και με τις απαιτήσεις του Κανονισμού.
- ✓ Για οποιαδήποτε αλλαγή στους όρους παροχής υπηρεσιών από τρίτα μέρη, θα πρέπει να λαμβάνεται υπόψη η κρισιμότητα των προσωπικών δεδομένων και να αποτιμώνται εκ νέου οι κίνδυνοι από την εταιρεία.
- ✓ Τα τρίτα μέρη υποχρεούνται να μεριμνούν για την εφαρμογή των κατάλληλων τεχνικών και οργανωτικών μέτρων για την αποφυγή ενδεχόμενων περιστατικών ασφάλειας των προσωπικών δεδομένων της εταιρείας, τα οποία τυγχάνει να επεξεργάζονται ως εκτελούντες την επεξεργασία για λογαριασμό της εταιρείας
- ✓ Τα τρίτα μέρη οφείλουν να παρέχουν συνδρομή στην εταιρεία οποτεδήποτε χρειαστεί, ώστε να διασφαλίζεται η συμμόρφωση αυτής προς τις υποχρεώσεις που απορρέουν από τη διενέργεια εκτιμήσεων αντικτύπου για την προστασία των δεδομένων ή την προηγούμενη διαβούλευση με την εποπτική αρχή.
- ✓ Καθορισμός της διαδικασίας παρακολούθησης των υπηρεσιών από τρίτα μέρη και κοινοποίηση σε αυτά της προβλεπόμενης από την εταιρεία διαδικασίας αναφοράς των περιστατικών και ευπαθειών ασφάλειας.

Πυλώνας 10ος : Διαχείριση περιστατικών ασφαλείας

- ➢ **Αναφορά περιστατικών ασφαλείας και αδυναμιών**

Τα περιστατικά που σχετίζονται με την ασφάλεια των προσωπικών δεδομένων θα πρέπει να αναφέρονται, το συντομότερο, στον Υπεύθυνο Προστασίας Δεδομένων, ενώ οι ευπάθειες κάθε είδους που σχετίζονται εξίσου με την ασφάλεια των προσωπικών

δεδομένων θα πρέπει να γνωστοποιούνται άμεσα στον Υπεύθυνο Ασφάλειας της εταιρείας. Τόσο για την αναφορά των περιστατικών ασφαλείας όσο και των ευπαθειών, κρίνεται σκόπιμη η ύπαρξη συγκεκριμένης διαδικασίας, για την οποία θα πρέπει να λαμβάνει γνώση τόσο το προσωπικό της επιχείρησης όσο και οι συνεργάτες αυτής. Δεν αποκλείεται μάλιστα η ύπαρξη ειδικών εντύπων για την καλύτερη αποτύπωση και περιγραφή των αδυναμιών και των περιστατικών ασφαλείας.

Επιπλέον, σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, η εταιρεία θα πρέπει να γνωστοποιήσει αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος, την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή, εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Όταν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιείται εντός 72 ωρών, συνοδεύεται από αιτιολόγηση για την καθυστέρηση.

- **Διαχείριση περιστατικών ασφαλείας και ευπαθειών**

Τα συμβάντα που σχετίζονται με την ασφάλεια των προσωπικών δεδομένων θα πρέπει να αντιμετωπίζονται άμεσα ώστε να ελαχιστοποιηθούν οι συνέπειες. Για τον λόγο αυτό η εταιρεία θα πρέπει να θεσπίσει τις κατάλληλες διαδικασίες και ένα ολοκληρωμένο πλαίσιο αντιμετώπισης των απειλών που παραβιάζουν την ασφάλεια των πληροφοριακών συστημάτων.

Για την διαχείριση των περιστατικών παραβίασης των προσωπικών δεδομένων προτείνεται η ύπαρξη μίας Υπηρεσίας Διαχείρισης Περιστατικών Ασφάλειας, η οποία θα ως έχει σκοπό την αυτοματοποιημένη συλλογή και την ανάλυση των γεγονότων (logs) που δημιουργούνται από τα διάφορα πληροφοριακά συστήματα της εταιρείας. Η συγκεκριμένη υπηρεσία θα πρέπει να βασίζεται στην δυνατότητα συλλογής και επεξεργασίας σε πραγματικό χρόνο των καταγεγραμμένων περιστατικών ασφαλείας ή άλλων σχετικών με την ασφάλεια γεγονότων από όλα τα κρίσιμα συστήματα και εφαρμογές του δικτύου, καθώς και από όλους τους ενεργούς μηχανισμούς ασφάλειας της υποδομής, ενημερώνοντας έγκαιρα (alert) τους διαχειριστές του συστήματος σε περιπτώσεις σημαντικών απειλών και βοηθώντας σημαντικά στην άμεση αντιμετώπισή τους.

Πυλώνας 11ος : Ανάκαμψη από καταστροφή και σχέδιο συνέχειας διαδικασιών

- **Σχέδιο ανάκαμψης από καταστροφή και συνέχισης διαδικασιών**

- Θα πρέπει να προσδιορισθούν οι κρίσιμες επιχειρηματικές δραστηριότητες της εταιρείας καθώς και τα επιχειρησιακά αγαθά που σχετίζονται με αυτές, ούτως ώστε να εκτιμηθούν οι πιθανές επιπτώσεις ύστερα από κάποια μερική ή ολική καταστροφή.
- Θα πρέπει να προσδιορισθούν τα συμβάντα ασφαλείας που μπορούν να προκαλέσουν διακοπές στις επιχειρηματικές δραστηριότητες της εταιρείας. Επιπροσθέτως να προσδιορισθούν οι επιπτώσεις και οι πιθανότητες εμφάνισής τους.
- Θα πρέπει να καθορισθούν οι αρμοδιότητες και οι ευθύνες όλων των εμπλεκόμενων στο σχέδιο και οι χρόνοι αποκατάστασης της ομαλής λειτουργίας της εταιρείας.
- Θα πρέπει να θεσπισθούν οι διαδικασίες αναφοράς και διαχείρισης των καταστροφών και να εκπαιδευτεί κατάλληλα το προσωπικό για την υλοποίηση του σχεδίου.
- Θα πρέπει να καθορισθούν οι διαδικασίες ελέγχου, δοκιμής και ενημέρωσης του σχεδίου και να συμπεριληφθούν όλοι οι απαραίτητοι πόροι για την υλοποίηση του σχεδίου όπως εξυπηρετητές, δικτυακός εξοπλισμός, θέσεις εργασίας κ.λπ.
- Θα πρέπει να αναφέρονται με σαφήνεια οι περιπτώσεις και οι συνθήκες για τις οποίες ενεργοποιείται το σχέδιο (ή κάποιο μέρος του), καθώς και τους υπεύθυνους για την εκτέλεση του. Όταν υπάρξουν νέες απαιτήσεις από την εταιρεία, το σχέδιο θα πρέπει να συμπληρώνεται κατάλληλα.
- Θα πρέπει να θεσπιστούν οι διαδικασίες προσωρινής αποκατάστασης των λειτουργιών της εταιρείας, έως ότου ολοκληρωθεί η πλήρης αποκατάσταση (εφεδρικός εξοπλισμός ή τοποθεσίες, συνεργασία με τρίτους για την παροχή υπηρεσιών κλπ.).
- Το σχέδιο θα πρέπει να δοκιμάζεται ετησίως σε όλες του τις διαστάσεις, προκειμένου να διασφαλιστεί η εγκυρότητα και η αποτελεσματικότητά του.
- Κατά τη δοκιμή του σχεδίου, θα πρέπει να υπάρχει σαφές χρονοδιάγραμμα για κάθε τμήμα που θα εξεταστεί.
- Οι δοκιμές ελέγχου του σχεδίου θα πρέπει να περιλαμβάνουν:
  - ✓ Τον έλεγχο σε θεωρητικό επίπεδο διάφορων σεναρίων.
  - ✓ Την προσομοίωση διάφορων γεγονότων, ειδικά κατά την εκπαίδευση του προσωπικού.
  - ✓ Τον έλεγχο των δυνατοτήτων του εξοπλισμού να ανταπεξέλθει στις απαιτήσεις του σχεδίου.

- ✓ Τη δοκιμή του σχεδίου σε κάποιες εναλλακτικές εγκαταστάσεις ώστε να μη δημιουργούνται παρεμβολές στις λειτουργίες της εταιρείας.
- ✓ Τις δοκιμές των δυνατοτήτων των εξωτερικών συνεργατών να ανταπεξέλθουν στις απαιτήσεις του σχεδίου.
- ✓ Τη διενέργεια πλήρους υλοποίησης του σχεδίου ώστε να δοκιμαστεί η δυνατότητα όλων να ενεργήσουν όπως προβλέπεται.

Πυλώνας 12ος : Συμμόρφωση με νομικές, κανονιστικές διατάξεις και τεχνικά πρότυπα

➢ Συμμόρφωση με τη σχετική νομοθεσία

Ο σχεδιασμός, η λειτουργία και η διαχείριση των πληροφοριακών συστημάτων είναι πιθανό να υπόκειται σε κάποιας μορφής νόμους ή συμβάσεις. Το νομικό τμήμα τη εταιρείας θα πρέπει να φροντίζει για τη συμμόρφωση με τους διάφορους νόμους και ρυθμίσεις. Στο πλαίσιο αυτό θα πρέπει να καθορισθεί ένας κατάλογος με την σχετική νομοθεσία που πρέπει να συμμορφώνεται κάθε εταιρεία.

➢ Συμμόρφωση με τον Κανονισμό

Όλο το προσωπικό, οι διαδικασίες, οι πολιτικές, της εταιρείας για την επεξεργασία των προσωπικών δεδομένων θα πρέπει να ελέγχονται περιοδικά για τη συμμόρφωσή τους με τον Νέο Κανονισμό. Προτείνεται η υλοποίηση ενός συστήματος εσωτερικού και εξωτερικού ελέγχου της συμμόρφωσης με τον Κανονισμό, το οποίο θα πρέπει να περιλαμβάνει το σύνολο των πολιτικών, διαδικασιών και καθηκόντων, τα οποία τίθενται σε εφαρμογή από την εταιρεία και έχει ως στόχο την αποτελεσματική και αποδοτική λειτουργία της, έτσι ώστε να ανταποκρίνεται κατάλληλα στους κινδύνους που σχετίζονται με τα προσωπικά δεδομένα. Η εταιρεία θα πρέπει να ελέγχει σε ετήσια βάση ή όποτε απαιτείται τη συμμόρφωσή της με τον Κανονισμό. Κάθε έλεγχος μπορεί να συνοδεύεται από έκθεση που να περιλαμβάνει την περιγραφή των προβλημάτων που εντοπίστηκαν, την πιθανή επίπτωση από τα προβλήματα που εντοπίστηκαν, τα αίτια αυτών και ο τρόπος αντιμετώπισής τους.

➢ Συμμόρφωση με τεχνικά πρότυπα

Η ασφάλεια της εταιρείας θα πρέπει να ελέγχεται ανεξάρτητα και συστηματικά ώστε να επιβεβαιωθεί ότι οι πρακτικές που έχουν υιοθετηθεί είναι σύμφωνες με τις απαιτήσεις ασφάλειας. Ο έλεγχος αυτός θα πρέπει να γίνεται από κάποιον εξωτερικό σύμβουλο. Προτείνονται οι ακόλουθοι μηχανισμοί ελέγχου:

- **Αποτίμηση τεχνικών ευπαθειών εσωτερικού δικτύου.** Με την αποτίμηση των τεχνικών ευπαθειών θα πρέπει να ανιχνεύονται με αυτοματοποιημένα εργαλεία οι ευπάθειες των πληροφοριακών συστημάτων. Σκοπός της τεχνικής αυτής είναι η ανίχνευση όλων των ευπαθειών των πληροφοριακών συστημάτων της εταιρείας.

- **Δοκιμές Διείσδυσης από εξωτερικά δίκτυα.** Είναι η ελεγχόμενη προσομοίωση μιας επίθεσης προκειμένου να επιτευχθεί ένας προκαθορισμένος στόχος. Σκοπός τους είναι να εντοπιστούν συγκεκριμένες πληροφορίες σχετικές με την ύπαρξη γνωστών ευπαθειών και να διερευνηθεί κατά πόσο είναι δυνατόν ένας τρίτος, κάνοντας χρήση αυτών των πληροφοριών, είναι σε θέση να δημιουργήσει προβλήματα στα πληροφοριακά συστήματα. Δεν έχουν σκοπό να εντοπίσουν όλες τις ευπάθειες, αλλά να αποδείξουν ότι η ασφάλεια του συστήματος μπορεί να διακυβευτεί. Οι δοκιμές θα πρέπει να πραγματοποιηθούν στη βάση μηδενικής γνώσης (zero knowledge) των πληροφοριακών συστημάτων.

- **Επιθεώρηση των μηχανισμών ασφάλειας βάση του ISO/IEC 27001.** Τα πληροφοριακά συστήματα θα πρέπει να ελεγχθούν με βάση ένα σύνολο από λίστες ελέγχου (checklists), οι οποίες διαμορφώνονται με βάση διεθνή πρότυπα σχετικά με την ασφάλεια. Οι ελεγκτές θα εκτελέσουν την εργασία τους μέσα από προσωπικές συνεντεύξεις, εξετάσεις των ρυθμίσεων, αναλύσεις των διαμοιρασμένων πόρων δικτύου και μελέτες των ιστορικών στοιχείων (log files).

Τα ευρήματα θα πρέπει να ταξινομούνται ανάλογα με την κρισιμότητά τους σε ευρήματα critical, high, medium, low και info. Τα ευρήματα υψηλής επικινδυνότητας θα πρέπει να αναφέρονται άμεσα στον υπεύθυνο ασφάλειας. Η Ανάδοχος Εταιρεία/Σύμβουλος που θα αναλάβει να ελέγξει τα πληροφοριακά συστήματα της εταιρείας θα πρέπει να έχει την κατάλληλη αποδεδειγμένη τεχνογνωσία και εμπειρία.

5.4 Προτεινόμενες δράσεις

Οι περισσότερες εταιρείες δεν έχουν πλήρη επίγνωση των κινδύνων των δεδομένων και της ιδιωτικής ζωής, καθώς και για όλους τους άλλους κινδύνους του κυβερνοχώρου που αντιμετωπίζουν τα δεδομένα τους και τα συστήματα των πληροφοριών. Αυτοί οι κίνδυνοι, όπως ήδη αναφέρθηκε, συνήθως προκαλούνται από κακόβουλους εισβολείς, εσωτερικούς ή εξωτερικούς. Και οι δύο τύποι αυτοί εισβολέων έχουν ως στόχο την κλοπή ευαίσθητων πληροφοριών όπως αρχεία πελατών, τα αρχεία υγείας των εργαζομένων, ερευνητικά δεδομένα, οικονομικά αρχεία κ.λπ. επειδή τα δεδομένα αυτά

έχουν πολύ μεγάλη αξία. Τα στοιχεία αυτά (προσωπικά δεδομένα, οικονομικά δεδομένα, κ.λπ.) της εταιρείας είναι σε κίνδυνο λόγω της απρόσεκτης και αμελούς συμπεριφοράς των υπαλλήλων και άλλων έμπιστων χρηστών της εταιρείας με αυξημένα επίπεδα πρόσβασης όπως εξωτερικοί συνεργάτες και προμηθευτές. Ως εκ τούτου, τα θέματα διαχείρισης των κινδύνων καθίστανται υψίστης σημασίας και επιβάλουν στην εταιρεία να αναπτύξει και να εφαρμόσει ένα Μοντέλο Διακυβέρνησης Προστασίας Προσωπικών για την διαχείριση των ανωτέρω κινδύνων.

Ο στόχος του μοντέλου είναι η εφαρμογή ενός αποτελεσματικού και αποδοτικού σχεδίου προστασίας των προσωπικών δεδομένων και των πληροφοριακών συστημάτων της εταιρείας που συντηρούν και επεξεργάζονται αυτά τα δεδομένα. Οι πυλώνες στους οποίους βασίζεται το μοντέλο αυτό αναφέρονται στον πίνακα που ακολουθεί:

Α.Α	Πυλώνας	Περιγραφή
1	Οργάνωση	Οργάνωση προστασίας Δεδομένων
2	Μέτρα	Θέσπιση και εφαρμογή μέτρων προστασίας δεδομένων
3	Ανθρώπινο Δυναμικό	Ενημέρωση, εγρήγορσή και αξιοποίηση του ανθρώπινου δυναμικού για την βελτίωση της προστασίας των δεδομένων
4	Τεχνολογία	Χρήση συστημάτων ασφαλείας και πληροφορικής, μεθόδων τεχνικών και άλλων εργαλείων για την υποστήριξη και την βελτίωση της προστασίας των δεδομένων.

Το ανωτέρω μοντέλο υλοποιείται βάση ενός Συστήματος Διαχείρισης της Προστασίας των Προσωπικών Δεδομένων. Το σύστημα αυτό περιλαμβάνει την μεθοδολογία, την στρατηγική και ένα σύνολο από πολιτικές, διαδικασίες και μέτρα προστασίας με σκοπό την προστασία των πληροφοριών και την ιδιωτικότητας των υποκειμένων.

Εναλλακτικά προτείνεται η υλοποίηση ενός συστήματος διαχείρισης της ασφάλειας πληροφοριών και εξειδίκευση του πυλώνα συμμόρφωσης με το νομικό πλαίσιο του Γενικού Κανονισμού Προστασίας Δεδομένων και η πιστοποίηση του σύμφωνα με το πρότυπο ISO/IEC 27001:2013. Το σύστημα διαχείρισης της προστασίας των προσωπικών δεδομένων που προτείνεται, υλοποιείται σε πέντε (5) φάσεις:

- Φάση 1η: Προετοιμασία Προστασίας Δεδομένων
- Φάση 2η: Οργάνωση Προστασίας Δεδομένων
- Φάση 3η: Ανάπτυξη και εφαρμογή μέτρων προστασίας δεδομένων
- Φάση 4η: Διακυβέρνηση της προστασίας δεδομένων
- Φάση 5η: Αξιολόγηση και βελτίωση της προστασίας των δεδομένων

Φάση 1η: Προετοιμασία Προστασίας Δεδομένων

Ο γενικός στόχος της φάσης αυτής είναι η προετοιμασία της εταιρείας για την προστασία των δεδομένων. Πιο συγκεκριμένα:

- Η ανάλυση των απαιτήσεων προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής καθώς και των αναγκών που επηρεάζουν την εταιρεία
- Η συλλογή των σχετικών νόμων, προτύπων και κανονισμών που συσχετίζονται με την προστασία των δεδομένων και της ιδιωτικής ζωής και
- Η κατάρτιση ενός σχεδίου δράσεως με τους απαραίτητους πόρους και πρόγραμμα ώστε να προετοιμάσει την εταιρεία για την διαχείριση των δεδομένων προσωπικού χαρακτήρα στις δραστηριότητες, συναλλαγές, και λειτουργίες της.

Τα βήματα και οι ενέργειες που απαιτούνται για την ολοκλήρωση της φάσης αυτής είναι:

1. Ανάλυση της προστασίας των προσωπικών δεδομένων
2. Συλλογή του νομικού Πλαισίου
3. Ανάλυση επιπτώσεων προστασίας προσωπικών δεδομένων
4. Εκτέλεση αρχικών ελέγχων και αξιολογήσεων
5. Τεκμηρίωση οργάνωσης της διακυβέρνησης των προσωπικών δεδομένων
6. Τεκμηρίωση των δεδομένων
7. Δημιουργία ενός σχεδίου συμμόρφωσης και προστασίας των δεδομένων
8. Πρόγραμμα υλοποίησης του ανωτέρω σχεδίου

Αποτελέσματα: η προετοιμασία της εταιρείας στην αναγνώριση των αποκλίσεων από τον κανονισμό και η αποτίμηση των κινδύνων.

Φάση 2η: Οργάνωση Προστασίας Δεδομένων

Ο γενικός στόχος της φάσης αυτή είναι να καθορισθούν ο οργανωτικές δομές και οι μηχανισμοί για την λειτουργία της προστασίας προσωπικών δεδομένων της εταιρείας. Πιο συγκεκριμένα:

- Η ανάπτυξη του κατάλληλου οργανωτικού σχήματος για το υλοποίηση του σχεδίου συμμόρφωσης και διαχείρισης της επικινδυνότητας με τον πιο αποτελεσματικό τρόπο.
- Ο καθορισμός των υπευθυνοτήτων και ο διορισμός των κατάλληλων στελεχών για την προστασία των δεδομένων.
- Η επιβεβαίωση ότι έχουν κινητοποιηθεί τα απαραίτητα μέρη.
- Η δέσμευση ότι θα εφαρμοσθούν όλα τα μέτρα προστασίας.

Τα βήματα και οι ενέργειες που απαιτούνται για την ολοκλήρωση της φάσης αυτής είναι:

1. Θέσπιση και λειτουργία οργάνωσης διακυβέρνησης δεδομένων.
2. Συμμετοχή ανώτατης διοίκησης στην προστασία δεδομένων.
3. Δέσμευση των εργαζομένων στην προστασία των δεδομένων.
4. Τακτική επικοινωνία για την προστασία των δεδομένων.
5. Υλοποίηση συστήματος διακυβέρνησης, διαχείρισης κινδύνων και συμμόρφωσης
6. Οργάνωση της μέτρησης της απόδοσης μέτρων προστασίας δεδομένων

Τα προϊόντα της φάσης αυτής είναι τα πρακτικά συναντήσεων, καθώς και τα έγγραφα συμφωνίας (δέσμευσης) των εργαζομένων για την εμπιστευτικότητα και την προστασία των προσωπικών δεδομένων, ενώ ως αποτέλεσμα αυτής θωρείται η καλύτερη οργάνωση της εταιρείας σε όλα τα επίπεδα (διοίκηση, ανώτερα στελέχη, προσωπικό κ.λπ.) για την αποτελεσματική λειτουργία της προστασίας των προσωπικών της δεδομένων.

Φάση 3η: Ανάπτυξη και εφαρμογή των μέτρων προστασίας δεδομένων

Ο στόχος της φάσης αυτής είναι να αναπτυχθούν και να εφαρμοσθούν τα δέοντα μέτρα προστασίας των δεδομένων για την εταιρεία και ειδικότερα η προτεραιοποίηση των μηχανισμών ελέγχου, ο σχεδιασμός ενός συστήματος ταξινόμησης των δεδομένων και η εφαρμογή των απαιτούμενων σχεδίων συμμόρφωσης και προστασίας των

δεδομένων που είναι αναγκαία για την συμμόρφωση με τον κανονισμό σύμφωνα με τις απαιτήσεις της εταιρείας σας.

Τα αποτελέσματα της φάσης αυτής είναι ο σχεδιασμός της υλοποίησης των σχεδίων συμμόρφωσης και διαχείρισης της επικινδυνότητας, η προμήθεια του κατάλληλου λογισμικού και εξοπλισμού ασφαλείας, η εγκατάσταση τους και η ανάπτυξη των απαραίτητων διαδικασιών και πολιτικών προστασίας των δεδομένων

Η προτεραιοποίηση των κύριων τεχνολογικών μηχανισμών συμμόρφωσης και προστασίας δεδομένων αναφέρονται στον πίνακα που ακολουθεί:

Α.Α	Τεχνολογικά Αντίμετρα	Προτεραιότητα
1	Υπηρεσία Web Application Firewall	Υψηλή
2	Λογισμικό Προστασίας από κακόβουλο λογισμικό μηδενικού χρόνου	Υψηλή
3	Υπηρεσία Διαχείρισης Περιστατικών Ασφαλείας	Υψηλή
4	Κρυπτογράφηση	Υψηλή
5	Σύστημα προστασίας από διαρροή δεδομένων	Μέση

Φάση 4η: Διακυβέρνηση της προστασίας δεδομένων

Στην παρούσα φάση στόχο αποτελεί η καλύτερη ανάπτυξη και εφαρμογή των απαραίτητων μηχανισμών ελέγχου και διακυβέρνησης της προστασίας των δεδομένων προσωπικού χαρακτήρα. Πιο συγκεκριμένα:

- Η διαβεβαίωση της αποτελεσματικής εφαρμογής των απαραίτητων δομών διακυβέρνησης της προστασίας των προσωπικών δεδομένων.
- Η διαβεβαίωση της αποτελεσματικής εφαρμογής των διαδικασιών ποιότητας δεδομένων για την αποτελεσματική προστασία των προσωπικών δεδομένων
- Η διασφάλιση της υποβολής των εκθέσεων για όλα τα ζητήματα προστασίας των προσωπικών δεδομένων σε συνεχή βάση.

Τα βήματα και οι ενέργειες που απαιτούνται για την ολοκλήρωση της φάσης αυτής είναι:

1. Εφαρμογή πρακτικών διαχείρισης και χρήση των προσωπικών δεδομένων
2. Εφαρμογή πρακτικών ποιότητας προσωπικών δεδομένων
3. Εφαρμογή πρακτικών ελαχιστοποίησης των προσωπικών δεδομένων
4. Εφαρμογή πρακτικών αποθήκευσης και καταστροφής των προσωπικών δεδομένων

5. Εφαρμογή διαδικασιών διαχείρισης των αιτήσεων των υποκειμένων
6. Εκτέλεση διαδικασιών εκτίμησης κινδύνων προστασίας των προσωπικών δεδομένων
7. Αναφορές προστασίας προσωπικών δεδομένων
8. Εφαρμογή του σχεδίου διαχείρισης των παραβιάσεων των προσωπικών δεδομένων

Τα προϊόντα της φάσης αυτής είναι η εφαρμογή απαραίτητων σχεδίων και πολιτικών προστασίας των προσωπικών δεδομένων, όπως η εφαρμογή του συστήματος ταξινόμησης των προσωπικών δεδομένων και η εφαρμογή της πολιτικής συγκατάθεσης των υποκειμένων.

Αποτελέσματα: η καλύτερη ποιότητα και διακυβέρνηση των δεδομένων για την πιο αποτελεσματική λειτουργία της προστασίας των προσωπικών δεδομένων της εταιρείας και της μετρίασης των κινδύνων επίθεσης στα δεδομένα της εταιρείας.

Φάση 5η: Αξιολόγηση και βελτίωση της προστασίας των δεδομένων

Ο στόχος της φάση αυτής είναι η αξιολόγηση και η βελτίωση όλων των ειδικών πτυχών της προστασίας των δεδομένων του εταιρικού περιβάλλοντος όπως έλεγχοι, μέτρα, πολιτικές, διαδικασίες, πρακτικές κ.λπ. Πιο συγκεκριμένα:

- Η παρακολούθηση της λειτουργίας και της επίλυσης όλων των θεμάτων που αφορούν την προστασία των δεδομένων
- Η τακτική αξιολόγηση της συμμόρφωσης της εταιρείας με τις εσωτερικές πολιτικές προστασίας προσωπικών δεδομένων και τις επιχειρησιακές διαδικασίες
- Η βελτίωση της προστασίας των δεδομένων με βάση τους ελέγχους και την αξιολόγηση των εσωτερικών και των εξωτερικών ελέγχων.

Τα βήματα και οι ενέργειες που απαιτούνται για την ολοκλήρωσή της είναι:

- Εκτέλεση εσωτερικών ελέγχων προστασίας προσωπικών δεδομένων
- Εκτέλεση εξωτερικών ελέγχων προστασίας προσωπικών δεδομένων
- Εκτέλεση ειδικών αξιολογήσεων και μελετών (δοκιμές διείσδυσης, αποτίμησης ευπαθειών, εποπτεία ελέγχου των μηχανισμών ελέγχου)
- Αξιολόγηση των επιπτώσεων προστασίας προσωπικών δεδομένων
- Επίλυση κινδύνων προστασίας των προσωπικών δεδομένων

- Έκθεση αξιολόγησης κινδύνων και αποτελεσμάτων προστασίας των προσωπικών δεδομένων
- Παρακολούθηση νόμων και κανονισμών προστασίας προσωπικών δεδομένων
- Παρακολούθηση των αποφάσεων της εποπτικής αρχής

Τα προϊόντα της φάσης αυτής είναι η εφαρμογή των απαραίτητων διαδικασιών παρακολούθησης και αξιολόγησης των μηχανισμών ελέγχου όπως η διαδικασία εκτέλεσης εσωτερικών ελέγχων προστασίας προσωπικών δεδομένων και η διαδικασία παρακολούθησης των νόμων και των κανονισμών συμμόρφωσης.

Τα αποτελέσματα της φάσης αυτής είναι ο έλεγχος και η αξιολόγηση των μέτρων προστασίας των προσωπικών δεδομένων με κύριο σκοπό:

- την επιβεβαίωση της βέλτιστης συμμόρφωσης με τον Κανονισμό,
- την ποιότητα και την διακυβέρνηση των δεδομένων για την πιο αποτελεσματική λειτουργία των μηχανισμών προστασίας των προσωπικών δεδομένων και
- την μετρίασης των κίνδυνων επίθεσης στα δεδομένα της εταιρείας.

Κρίσιμοι παράγοντες επιτυχίας

Οι κρίσιμοι παράγοντες για την επιτυχή υλοποίηση του προτεινόμενου μοντέλου διακυβέρνησης της προστασίας των προσωπικών δεδομένων είναι οι ακόλουθοι:

- **Έμπρακτη Υποστήριξη από την Διοίκηση:** Η Διοίκηση θα πρέπει να λάβει τις κατάλληλες αποφάσεις για την προστασία των προσωπικών δεδομένων και την συμμόρφωση με τον Κανονισμό, όπως η δημιουργία και η αποστολή σε όλο το προσωπικό, τους πελάτες και τους συνεργάτες της των πολιτικών για την προστασία των προσωπικών δεδομένων, η έγκριση του Σχεδίου Συμμόρφωσης και Διαχείρισης της Επικινδυνότητας κ.λπ.

- **Υλοποίηση των απαραίτητων ρόλων:** Για την οργάνωση της συμμόρφωσης με τον Κανονισμό και την προστασία των προσωπικών δεδομένων είναι απαραίτητη η θέσπιση του κατάλληλου οργανωτικού πλαισίου, ήτοι ο καθορισμός Υπεύθυνου Προστασίας Δεδομένων, Υπεύθυνου Ασφάλειας Πληροφοριών και Επιτροπής Ελέγχου της Συμμόρφωσης

- **Εφαρμογή του συνόλου του Σχεδίου Συμμόρφωσης και Διαχείρισης της Επικινδυνότητας:** Θα πρέπει να γίνει κατανοητό ότι δεν αρκεί μόνο η υλοποίηση

μέρους ή των κυριότερων μηχανισμών προστασίας των προσωπικών δεδομένων αλλά η προτεραιοποίηση τους και η υλοποίηση στο σύνολο τους.

- **Ενημέρωση, Εκπαίδευση και Συμμετοχή του Προσωπικού στην προστασία των προσωπικών δεδομένων:** Η εταιρεία θα πρέπει να δημιουργήσει και να υλοποιήσει μία στρατηγική ευαισθητοποίησης, εγρήγορσης, συμμετοχής και δέσμευσης όλου του προσωπικού της στην προστασία των προσωπικών δεδομένων.

- **Αξιοποίηση της τεχνολογίας στην Προστασία των Προσωπικών Δεδομένων:** Η εταιρεία θα πρέπει να υλοποιήσει τους απαραίτητους τεχνολογικούς μηχανισμούς στο σύνολο τους για την διαχείριση της προστασίας των προσωπικών δεδομένων όπως σύστημα πρόληψης από διαρροή δεδομένων, σύστημα προστασίας αυτών και σύστημα διαχείρισης περιστατικών ασφαλείας.

ΚΕΦΑΛΑΙΟ 6

ΣΥΜΠΕΡΑΣΜΑΤΑ

Εν κατακλείδι, κατόπιν ολοκλήρωσης της παρούσας έρευνας και με βάση τα αποτελέσματα που πρόεκυψαν κατά την διεξαγωγή της παραπάνω μελέτης περίπτωσης, γίνεται αντιληπτό ότι οι περισσότερες επιχειρήσεις δεν είναι ακόμα πλήρως έτοιμες, σε λειτουργικό και τεχνολογικό επίπεδο, να συμμορφωθούν με τις επιταγές του Γενικού Κανονισμού (ΕΕ) 2016/679, καθώς προηγουμένως απαιτείται η σαφής οριοθέτηση των επαπειλούμενων κινδύνων για την προστασία των προσωπικών δεδομένων και κατόπιν, η εσωτερική τους ανασυγκρότηση σε όλα τα επίπεδα των δραστηριοτήτων τους για την αποτελεσματική διαχείριση αυτών μέσω ενός γενικότερου πλαισίου κανονιστικής συμμόρφωσης.

Ωστόσο, η προσπάθεια συμμόρφωσης της σύγχρονης επιχείρησης με τις επιταγές του Κανονισμού καθίσταται ένα σύνθετο και δύσκολα επιτεύξιμο εγχείρημα, καθώς αυτή παρακωλύεται αισθητά από τους διαρκώς αυξανόμενους κινδύνους που επιφυλάσσουν οι τεχνολογικές εξελίξεις, την ευρεία δημοσιοποίηση προσωπικών δεδομένων και την έκθεση του υποκειμένου τους στο διαδίκτυο, την αυξημένη διαφάνεια των εσωτερικών της διαδικασιών και το αυστηρότερο πλαίσιο υποχρεώσεων αυτής τόσο απέναντι στην αρμόδια εποπτική αρχή όσο και στα υποκείμενα των δεδομένων, καθώς και την επιβολή υψηλών διοικητικών προστίμων και άλλων σχετικών κυρώσεων σε περίπτωση παραβίασης των διατάξεων του Κανονισμού και προσβολής των θεμελιωδών δικαιωμάτων των φυσικών προσώπων.

Κρίσιμοι παράγοντες ικανοί να οδηγήσουν στην επιτυχή υλοποίηση της συμμόρφωσης των επιχειρήσεων με τις κανονιστικές διατάξεις και κατ' επέκταση στην αποτελεσματική προστασία των προσωπικών δεδομένων που αυτές συλλέγουν, αποθηκεύουν, επεξεργάζονται και διαβιβάζουν, θεωρούνται η ενεργή συμμετοχή των διοικητικών στελεχών στην εφαρμογή του σχεδίου συμμόρφωσης και διαχείρισης της επικινδυνότητας, η σαφής οριοθέτηση των ρόλων και των αρμοδιοτήτων του ανθρώπινου δυναμικού, η πλήρης κατάρτιση και εκπαίδευση αυτού σε θέματα προστασίας των προσωπικών δεδομένων, καθώς και η επικαιροποίηση των πληροφοριακών συστημάτων με τους πλέον κατάλληλους μηχανισμούς για την αντιμετώπιση περιστατικών ασφάλειας των δεδομένων και διαρροής εμπιστευτικών πληροφοριών.

Βιβλιογραφία

1) Αρτίκης Παναγιώτης, «Διαχείριση Αξίας και Κινδύνου», εκδόσεις Φαίδιμος, 2014
2) Κάτσικας Σωκράτης, «Διαχείριση της Ασφάλειας Πληροφοριών», Εκδόσεις Πεδίο,2014
3) Κοτσαλής Λεωνίδας- Μενουδάκος Κωνσταντίνος «Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων», Νομική Βιβλιοθήκη, 2018
4) Μήτρου Λίλιαν, «Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων», Εκδόσεις Σάκκουλα, 2017
5) Μιλτιάδης Νεκτάριος, «Μεθοδολογία Διαχείρισης Κινδύνων Επιχειρήσεων», Εκδόσεις Παπαζήση, 2016

Νομοθεσία

1) Νόμος 2472/1997, «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα»
2) Νόμος 3471/2006, «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν. 2472/97»
3) Νόμος 4070/2012, «Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις»
4) Νόμος 4624/2019, «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις.»
5) Οδηγία 95/46/ΕΚ (1995), Προστασία των φυσικών προσώπων έναντι της επεξεργασία δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.
6) Οδηγία 2002/58/ΕΚ (2002), Επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.
7) Οδηγία (ΕΕ) 2016/680, Προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή

της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου

8) Ομάδα εργασίας του άρθρου 29 (2017) - Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα , Guidelines on Personal data breach notification under Regulation 2016/679, (WP250) 03/10/2017.

9) Ομάδα εργασίας του άρθρου 29 (2017) - Εκτίμηση επιπτώσεων στην προστασία δεδομένων. Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679, έκδοση:01 (WP248 αναθ.01) 04/04/2017, αναθεωρήθηκε 4/10/2017.

10) Ομάδα εργασίας του άρθρου 29 (2017) - Εφαρμογή και καθορισμός διοικητικών προστίμων Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, (WP253) 03/10/2017.

Άλλες Πηγές

1) https://www.wikipedia.org/

2) https://www.euretirio.com/

3) «Check Point's Cyber Security Predictions for 2017», https://blog.checkpoint.com/2016/10/25/check-points-cyber-security-predictions-2017/

4) «The Current State of Ransomware», https://www.sophos.com/ja-jp/medialibrary/PDFs/technical%20papers/sophos-current-state-of-ransomware.pdf

5)https://www.dpa.gr/portal/page?_pageid=33,15048&_dad=portal&_schema=PORTAL

6) https://popaganda.gr/newstrack/to-internet-of-things-chrisimopiite-olo-ke-perissotero-stis-epithesis-apo-kivernoegklimaties/

7) Key Operational Risks for Firms Implementing GDPR», https://www.chasecooper.com/articles/6-key-operational-risks-firms-implementing-gdpr

8) «Κυβερνοασφάλεια. Η Ελλάδα θωρακίζει τις κρίσιμες υποδομές της.», https://emvolos.gr/kyvernoasfaleia-i-ellada-thorakizei-tis-krisimes-ypodomes-tis-toy-stelioy-ralli/

9) «Ασφάλεια στο GSM και τα κινητά τηλέφωνα», https://www.itsecuritypro.gr/asfalia-sto-gsm-ke-ta-kinita-tilefona/

10) https://www.eset.com/gr/ransomware/

11) https://www.ey.com/Publication/vwLUAssets/ey-l-4624-2019-protection-of-personal-data-and-measures-for-the-implementation-of-the-gdpr-gr/$FILE/ey-l-4624-

2019-protection-of-personal-data-and-measures-for-the-implementation-of-the-gdpr-gr.pdf

12) Κουνάδης Γεράσιμος, Senior Manager, Risk Advisory, Deloitte Ελλάδας «Κανονιστική συμμόρφωση: Τα λάθη των Διοικητικών Συμβουλίων», Περιοδικό "Accountancy Greece" (Τεύχος 31): https://www.accountancygreece.gr/%CE%BA%CE%B1%CE%BD%CE%BF%CE%BD%CE%B9%CF%83%CF%84%CE%B9%CE%BA%CE%AE-%CF%83%CF%85%CE%BC%CE%BC%CF%8C%CF%81%CF%86%CF%89%CF%83%CE%B7-t%CE%B1-%CE%BB%CE%AC%CE%B8%CE%B7-%CF%84%CF%89%CE%BD-%CE%B4%CE%B9%CE%BF/

13)«Η εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων στον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR)», https://www.lawspot.gr/nomika-nea/i-ektimisi-toy-antiktypoy-shetika-me-tin-prostasia-dedomenon-ston-geniko-kanonismo

14) «Οι επιπτώσεις του ν. 4624/2019 στις επιχειρήσεις», https://www.kathimerini.gr/1040406/opinion/epikairothta/politikh/oi-epiptwseis-toy-n-46242019-stis-epixeirhseis»

15) «Ολιστική Προστασία Κρίσιμων Υποδομών: Ανθεκτικότητα και Προστασία Διασυνδέσεων», https://www.dianeosis.org/2016/06/critical_infrastructure_synopsis/

16) «How will the GDPR affect human resources professionals», https://tresorit.com/blog/how-will-the-gdpr-affect-human-resources-professionals/

17) «Το Cyber Insurance ως εργαλείο διαχείρισης κινδύνου», https://insuranceworld.gr/27720/apopseis/27720/

18)«Ενοποίηση κυβερνοασφάλειας και προστασίας δεδομένων» https://www.grant-thornton.gr/insights/article/digital-risk-article-2/