Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Πληροφοριακά και Επικοινωνιακά Συστήματα με εξειδίκευση στην Ασφάλεια*

Μεταπτυχιακή Διατριβή

Επιχειρησιακή Συνέχεια και Ανάκαμψη και συμμόρφωση με ΓΚΠΔ στον τομέα της Πληροφορικής
(BC/DR (Business Continuity / Disaster Recovery) Management and GDPR compliance in IT sector)

Κωνσταντίνα Κούτσικου

Επιβλέπων Καθηγητής
Δρ. Σταύρος Σιαηλής

Μάϊος 2019

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Πληροφοριακά και Επικοινωνιακά Συστήματα με εξειδίκευση στην Ασφάλεια*

Μεταπτυχιακή Διατριβή

Επιχειρησιακή Συνέχεια και Ανάκαμψη και συμμόρφωση με ΓΚΠΔ στον τομέα της Πληροφορικής (BC/DR (Business Continuity / Disaster Recovery) Management and GDPR compliance in IT sector)

Κωνσταντίνα Κούτσικου

Επιβλέπων Καθηγητής
Δρ. Σταύρος Σιαηλής

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στα Πληροφοριακά και Επικοινωνιακά Συστήματα με εξειδίκευση στην Ασφάλεια από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Μάϊος 2019

ΛΕΥΚΗ ΣΕΛΙΔΑ

Περίληψη

Οι συνεχόμενες τεχνολογικές εξελίξεις δημιουργούν όλο και περισσότερες ανάγκες στο κομμάτι της ασφάλειας ενός οργανισμού, τόσο σε τεχνικό επίπεδο όσο και σε οργανωτικό. Με την έναρξη ισχύος του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων πολλές επιχειρήσεις και οργανισμοί αναγκάστηκαν να αναθεωρήσουν τα επίπεδα ασφαλείας τους και τις δομές επιχειρησιακής συνέχειας και ανάκαμψής. Σε κάποιες επιχειρήσεις τα επίπεδα ασφαλείας αλλά και επιχειρησιακής συνέχειας συνεχίζουν να παραμένουν χαμηλά, παρόλα τα αυστηρά πρόστιμα που προβλέπονται από τον κανονισμό, αλλά και τις συνεχόμενες απειλές ασφαλείας που προκύπτουν καθημερινά.

Η διατήρηση της επιχειρησιακής συνέχειας, η οποία προβλέπεται από τον κανονισμό ανάγκασε πολλές επιχειρήσεις να επαναπροσδιορίσουν τα επίπεδα ασφαλείας τους και σε πολλές περιπτώσεις να απευθυνθούν σε εταιρείες που ειδικεύονται σε αυτόν τον τομέα να τις αξιολογήσουν και να τις συμβουλεύσουν. Κάποιες άλλες εταιρείες στα πλαίσια της συμμόρφωσης με τον νέο κανονισμό προχώρησαν ταυτόχρονα σε πιστοποιήσεις, όπως το ISO 27001, οι οποίες δρουν συμπληρωματικά αλλά και ενδυναμώνουν τις δομές της επιχειρησιακής συνέχειας ενός οργανισμού.

Η παρούσα διατριβή αποτελείται από δύο (2) μέρη, τα οποία λειτουργούν συμπληρωματικά μεταξύ τους. Το πρώτο μέρος αποτελείται από δράσεις σε μορφή «προτύπου» που δημιουργήθηκαν βάσει των άρθρων του κανονισμού και το δεύτερο μέρος αποτελείται από μια εφαρμογή σε java η οποία με βήματα και οδηγίες καθοδηγεί τον χρήστη στην δημιουργία ενός πλάνου επιχειρησιακής συνέχειας και ανάκαμψής. Η εφαρμογή αυτή, είτε συνδυαστικά με το κείμενο της εν λόγω μεταπτυχιακής διατριβής, είτε από μόνη της μπορεί να καθοδηγήσει έναν επαγγελματία και να του παρέχει χρήσιμες πληροφορίες για την εφαρμογή ενός επιτυχημένου πλάνου επιχειρησιακής συνέχειας και ανάκαμψης. Θα πρέπει να επισημανθεί επίσης ότι οι περιοχές ελέγχου για την δημιουργία πλάνου επιχειρησιακής συνέχειας και ανάκαμψης δομήθηκαν σύμφωνα με τις αρχές που προβλέπονται από τον κανονισμό (ΓΚΠΔ).

Συνοψίζοντας, στόχος της εν λόγω μεταπτυχιακής διατριβής είναι να δημιουργηθεί ένα πλήρες πλάνο επιχειρησιακής συνέχειας και ανάκαμψης βασισμένο στον γενικό κανονισμό για την προστασία των δεδομένων προσωπικού χαρακτήρα και να παρέχει σε κάθε νέο επαγγελματία τις κατευθυντήριες γραμμές που χρειάζεται.

Summary

The continuous technological progress creates more and more needs both in the security technical and governance part of an organization. With the entry into force of the General Data Protection Regulation (GDPR), many businesses and organizations have been forced to revise their security levels and also Business Continuity and Recovery structures. Despite the severe fines laid down in the GDPR, and ongoing security threats that arise every day, in some businesses / organizations, the security and business continuity levels remain very low.

Business continuity and recovery maintenance, as provided for in regulation (GDPR), has forced many businesses to redefine their security levels. In many cases they have turned to companies specializing in this field to evaluate and advise them. Some other companies due to the regulation (GDPR), certified according to ISO 27001, in order for them to fulfill all the mandatory criteria provided for in GDPR.

This thesis consists of two (2) parts, which are complementary to each other. The first part consists of the creation of "standard" actions created, based on the articles of the GDPR and the second part is a ‘java’ application which guides the user in creating a business continuity and recovery plan (BCP / DRP). This application, combined with the text of the thesis, can guide a practitioner and provide him with useful information for implementing a successful business continuity and recovery plan. It should also be noted that the control areas for the establishment of a business continuity and recovery plan were based and built on the principles laid down in the articles of the GDPR, which is one of the objectives of this thesis.

In summary, the aim of this postgraduate dissertation is to create a complete business continuity and recovery plan based on the GDPR and to provide any new professional with the appropriate guidelines.

Ευχαριστίες

Σε αυτό το σημείο θα ήθελα να ευχαριστήσω τον καθηγητή μου Δρ. Σταύρο Σιαηλή για την καθοδήγηση του, αλλά και την βοήθεια του στην επιλογή του συγκεκριμένου θέματος.

Επίσης θα ήθελα να ευχαριστήσω όλους εκείνους τους φίλους και συναδέλφους που δέχθηκαν να λάβουν μέρος στην αξιολόγηση της εφαρμογής που υλοποιήθηκε στα πλαίσια της εν λόγω μεταπτυχιακής διατριβής.

Περιεχόμενα

Περιεχόμενα Εικόνων

Περιεχόμενα Πινάκων

Κεφάλαιο 1

Εισαγωγή

Στα πλαίσια ενεργοποίησης του νέου Γενικού Κανονισμού (ΕΕ) 2016/679 (25 Μάϊου 2018) για την «προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών», πολλές εταιρείες και οργανισμοί χρειάστηκε να αναδιοργανώσουν τις δομές τους και να επωμιστούν ένα τεράστιο κόστος για την υιοθέτηση δομών ασφάλειας και επιχειρησιακής συνέχειας τις οποίες δεν κατείχαν μέχρι τότε. Η κουλτούρα ασφάλειας και επιχειρησιακής συνέχειας για τις περισσότερες εταιρείες, ειδικά στην ελληνική επικράτεια ήταν μια πολυτέλεια και όχι μια αναγκαιότητα. Εξαίρεση αποτελούσαν μόνο μεγάλοι όμιλοι επιχειρήσεων με δραστηριότητες στο εξωτερικό, οι οποίοι από νωρίς είχαν επενδύσει και μεριμνήσει για την υιοθέτηση όλων εκείνων των μέσων που καθιστούσαν τις εταιρείες τους ασφαλείς και αξιόπιστες, είτε λόγω εσωτερικών οργανωτικών δομών που διέκριναν το ρίσκο ενός μη ασφαλούς εταιρικού οικοσυστήματος, είτε γιατί ήταν μια απαίτηση των αγορών των οποίον και απευθυνόντουσαν.

Ο νέος αυτός κανονισμός κατάφερε να επαγρυπνήσει αρκετές εταιρείες και οργανισμούς, ώστε να ξεκινήσουν να υιοθετούν όλες εκείνες τις δομές που διασφαλίζουν την εμπιστευτικότητα, την αξιοπιστία και διαθεσιμότητα των ‘πόρων’ τους. Η επιχειρησιακή συνέχεια, και ότι την απαρτίζει, είτε λόγω των μεγάλων προστίμων που προβλέπονται από τον κανονισμό, είτε λόγω της έκτασης που έχει πάρει τόσο στην ευρωπαϊκή επικράτεια όσο και στις χώρες εκτός Ε.Ε. (που δραστηριοποιούνται στην Ε.Ε) είναι ένα ζήτημα που απασχολεί όλους τους οργανισμούς την τελευταία τριετία.

1.1 Δομή Διατριβής

Η δομή της παρούσας διατριβής απεικονίζεται σε 6 κεφάλαια τα οποία περιγράφονται παρακάτω:

Στο πρώτο κεφάλαιο περιγράφει κάποιες γενικές έννοιες που εισήχθηκαν με την εφαρμογή του νέου κανονισμού για τα προσωπικά δεδομένα, πως επηρεάζουν και αναμειγνύονται με τον τομέα της πληροφορικής αλλά και τι καινοτομίες εισάγουν με την ενεργοποίηση τους.

Στο δεύτερο κεφάλαιο γίνεται μια ανάλυση του κανονισμού άρθρο προς άρθρο με σχολιασμούς σχετικά με τις επηρροές που επιφέρει στον τομέα της πληροφορικής και ειδικά στο κομμάτι της επιχειρησιακής συνέχειας που μας αφορά. Εδώ θα πρέπει να σημειωθεί ότι δεν γίνεται μια στυγνή απεικόμιση του κανονισμού αλλά μια προσεγμένη ανάλυση απλοποιώντας έννοιες και τονίζοντας επιρροές στον κομμάτι της επιχειρησιακής συνέχειας, όπου εφαρμόζονται ή όπου αναφέρονται ή υπονοούνται μέσω των άρθρων του κανονισμού.

Στο τρίτο κεφάλαιο γίνεται μια περιγραφή των πλάνων επιχειρησιακή (BCP/DRP) συνέχειας και αποκατάστασης, όπως επίσης και των βασικών παραμέτρων και αποτελεσμάτων που συνδράμουν στην δημιουργία τους, όπως η Business Continuity Impact Analysis και η Αξιολόγηση των ρίσκων, όπου και τα αποτελέσματα τους οδηγούν στην λήψη σωστών αποφάσεων σε σχέση με τα μέσα που πρέπει να ληφθούν από τις επιχειρήσεις. Στα πλαίσια αυτού γίνεται μια προσπάθεια δημιουργίας περιοχών ελέγχου (που είτε προβλέπονται από το νέο κανονισμό και απεικονίζονται αυτούσια, είτε υπονοούνται λόγω των περιοχών που επηρεάζουν) σε σχέση είτε με τις αλλαγές που πρέπει να γίνουν σε ένα υπάρχον πλάνο επειχειρησιακής συνέχειας και επανάκαμψης (BCP/DRP), είτε μπορούν να χρησιμοποιηθούν σαν οδηγός για την δημιουργία ενός πλάνου από επιχειρήσεις ή οργανισμούς. Τέλος γίνεται μια αναφορά στο κομμάτι της διαχειρίσης των αλλαγών (Change Management), το οποίο αποτελεί μια σημαντική διαδικασία για οποιαδήποτε οργανισμό, είτε αυτό αφορά την ασφάλεια και την επιχειρησιακή συνέχεια αλλά και γενικότερα.

Στο κεφάλαιο 4 γίνεται μια ανάλυση πρακτικών backup και recovery παρουσιάζοντας πρακτικές που χρησιμοποιούνται συνήθως από τους οργανισμούς και σχολιάζονται τα προτερήματα και τα μειονεκτήματα τους. Επίσης έχει υλοποιηθεί μια έρευνα αγοράς και προτείνονται κάποιες πιστοποιημένες τεχνολογίες αιχμής, οι οποίες καλύπτουν όλες εκείνες τις πιστοποιήσεις, τις τεχνικές απαιτήσεις αλλά διαθέτουν και όλο το νομικό

πλαίσιο που τις καθιστούν σύννομες σύμφωνα με τον κανονισμό περι επεξεργασίας προσωπικών δεδομένων.

Στο κεφάλαιο 5 προσανατολίζεται στην διατήρηση της ομαλής επιχειρησιακής συνέχειας και προβάλλονται όλα εκείνα τα μέσα που συνδράμουν στην διατήρηση τους, όπως τακτικές δοκιμές, αξιολόγηση (άρθρο 32-1δ του κανονισμού), δημιουργία κουλτούρας ασφάλειας σε έναν οργανισμό και προτάσεις υϊοθέτησης πιστοποιημένων εργαλειών / τεχνολογιών αιχμής για την διασφάλισης της ασφάλειας (άρθρο 32-1δ).

Τέλος στο κεφάλαιο 6 γίνεται μια περιγραφή της εφαρμογής που υλοποίηθηκε στα πλαίσια αυτής της διατριβής με χρήση γλώσσας προγραμματισμού Java 8 και χρήση της πλατφόρμας Java FX και λειτουργεί σαν οδηγός για την δημιουργία ενός πλάνου BCP / DRP. Σε αυτό το κεφάλαιο γίνεται μια σύντομη περιγραφή των τεχνολογιών που χρησιμοποιήθηκαν για την δημιουργία αυτής της εφαρμογής, οδηγίες χρήσης, όπως επίσης και τι ανάγκες μπορεί να καλύψει σε μια επιχείρηση.

1.2 Ιστορικό Υπόβαθρο

Στις 25 Μαΐου 2018 ξεκίνησε σε όλα τα Κράτη-Μέλη η εφαρμογή του νέου Γενικού Κανονισμού (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 και για την ελεύθερη κυκλοφορία των δεδομένων αυτών». Ο εν λόγω κανονισμός αντικατέστησε την ισχύουσα Οδηγία 95/46/ΕΚ όπως επίσης και την εθνική νομοθεσία ν. 2472/1997 [1].

Η εφαρμογή του νέου κανονισμού ενεργοποιείται όπως είναι φυσικό για όλα τα κράτη-μέλη της ευρωπαϊκής ένωσης και εφαρμόζεται επίσης και στις περιπτώσεις όπου ο υπεύθυνος ή ο εκτελών την επεξεργασία έχει έδρα ή εγκατάσταση στην Ευρωπαϊκή Ένωση. Εάν η επεξεργασία πραγματοποιείται εντός ή εκτός της ΕΕ δεν επηρεάζει τον κανονισμό εφόσον πληρούνται τα παραπάνω [1].

Συμμόρφωση επίσης επιβάλλεται και στις περιπτώσεις όπου το υποκείμενο βρίσκεται στην Ευρωπαϊκή Ένωση και ο υπεύθυνος επεξεργασίας ή ο εκτελών της επεξεργασίας βρίσκεται εκτός ΕΕ [1].

Ο νέος κανονισμός δομήθηκε με τις γενικές αρχές του υφιστάμενου νομοθετικού πλαισίου προστασίας των προσωπικών δεδομένων αλλά θέτοντας ένα αυστηρότερο πλαίσιο όσον αφορά την επεξεργασία και την προστασία των προσωπικών δεδομένων

από τις επιχειρήσεις αλλά και τους κρατικούς φορείς, όπως επίσης και για τις εταιρείες που έχουν συναλλαγές με τα Κράτη-Μέλη της ευρωπαϊκής ένωσης. Δημιουργείτε λοιπόν ένα εναρμονισμένο νομοθετικό πλαίσιο σε επίπεδο ευρωπαϊκής ένωσης καταργώντας την ανάγκη ύπαρξης νόμων σε εθνικό επίπεδο. Εταιρείες και οργανισμοί που διαθέτουν παραρτήματα σε διάφορες χώρες της ευρωπαϊκής ένωσης πλέον έχουν να κάνουν με ένα ενιαίο κανονισμό που αφορά όλους και απευθύνονται σε μια ενιαία εθνική αρχή προστασίας δεδομένων [1].

Σε σχέση με το παρελθόν, ο νέος κανονισμός δίνει έμφαση στις τεχνικές και οργανωτικές αλλαγές που πρέπει να τηρούν οι εταιρείες αλλά και οι κρατικοί φορείς ώστε να εξασφαλίζουν την πλήρη προστασία των προσωπικών δεδομένων των φυσικών προσώπων. Οι εν λόγω αλλαγές παρουσιάζουν πολλές ομοιότητες με πρότυπα όπως ISO 27001 και ISO 22301 και έχουν άμεση σχέση με την επιχειρησιακή συνέχεια ενός οργανισμού αλλά και την άμεση επανάκαμψη του (BCP/DRP, άρθρο 32, [1]) σε περίπτωση φυσικού ή τεχνικού συμβάντος. Πολλές εταιρείες οι οποίες δεν κατείχαν τις προαναφερθείσες πιστοποιήσεις (ISO 27001, ISO 22301) αφενός, και αφετέρου δεν κάλυπταν τα βασικά επίπεδα ασφάλειας, τεχνικά και οργανωτικά, αντιμετωπίζουν τεράστιες δυσκολίες στην προσαρμογή τους ακόμα και ένα (1) χρόνο μετά την ισχύ του κανονισμού. Ο εν λόγω κανονισμός μέσα από την προστασία της επεξεργασίας των προσωπικών δεδομένων προσπαθεί να εισάγει μια γενικότερη κουλτούρα ασφάλειας στις εταιρείες και στους οργανισμούς (τεχνικές, οργανωτικές και νομικές απαιτήσεις).

Έμφαση επίσης δίνεται στην αρχή της λογοδοσίας (Accountability) που επιφέρει ριζικές αλλαγές στο υφιστάμενο δομικό και οργανωτικό πλαίσιο. Οι ταχύτατοι ρυθμοί της τεχνολογίας δημιούργησαν καινούργιες απαιτήσεις σε οργανωτικό πλαίσιο και έτσι πλέον μέσω του νέου κανονισμού οι εταιρείες / οργανισμοί οφείλουν να είναι ‘συμμορφωμένες’ και έτοιμες σε περίπτωση που γίνει κάποιος έλεγχος, τόσο σε οργανωτικό, τεχνολογικό αλλά και νομικό πλαίσιο [1]. Τα πρόστιμα πλέον είναι βαρύτατα και σε σχέση με το παρελθόν οφείλουν να αποδεικνύουν αυτή την ‘συμμόρφωση’ όποτε τους ζητηθεί σε σχέση με το παρελθόν που το βάρος έπεφτε στην Αρχή Προστασίας Προσωπικών Δεδομένων [1].

Ο ενδιαφερόμενος πολίτης πλέον σε σχέση με το παρελθόν θα πρέπει να συναινεί όταν δεδομένα του δίνονται για οποιοδήποτε σκοπό επεξεργασίας, οι προϋποθέσεις λοιπόν γίνονται πιο αυστηρές και ο εκσυγχρονισμός κάποιον οργανισμών και επιχειρήσεων είναι απαραίτητος [1].

Με την ενεργοποίηση του νέου κανονισμού καταργείται η υποχρέωση γνωστοποίησης προς την αρμόδια εποπτική αρχή και αντικαταστάθηκε με την υποχρέωση τήρησης, από τους υπευθύνους επεξεργασίας, αρχείου των δραστηριοτήτων επεξεργασίας όλων των δεδομένων. Οι δε εκτελούντες την επεξεργασία από την πλευρά τους είναι υποχρεωμένοι να τηρούν αρχεία που αφορούν τις κατηγορίες δραστηριοτήτων επεξεργασίας (άρθρο 30) [1].

Σε ότι αφορά το διαδικαστικό μέρος ενδείκνυται να τηρούνται τα παρακάτω [1]:

I. η κατανόηση του νέου κανονισμού απ' όλους τους εμπλεκόμενους και μη (Awareness),
II. συντήρηση των απαραίτητων αρχείων:
    a. αρχείο καταγραφής δεδομένων (Data Inventory)
    b. διαδικασίες, συστήματα και αρχεία (φυσικών και ψηφιακών) που περιέχουν δεδομένα προσωπικού χαρακτήρα (Data Mapping),
III. Gap Analysis,
IV. ο σχεδιασμός ή επανεξέταση των πολιτικών ροών δεδομένων και των επεξεργασιών που διενεργούνται.

Ο υπεύθυνος επεξεργασίας από εδώ και στο εξής υποχρεούται να διενεργεί εκτίμηση αντικτύπου (Data Protection Impact Assessment - DPIA) σχετικά με την επεξεργασία των δεδομένων. Η διαδικασία αυτή θα πρέπει να διενεργείται όποτε κρίνεται απαραίτητο ή όταν εισάγονται νέες τεχνολογίες μέσω των οποίων επεξεργάζονται δεδομένα προσωπικού χαρακτήρα ή θα μπορούσαν να θέσουν σε κίνδυνο δεδομένα προσωπικού χαρακτήρα. Δεν υπάρχουν ιδιαίτερες απαιτήσεις σε ότι αφορά τα τυπικά προσόντα αυτού του ανθρώπου αλλά και τις πιστοποιήσεις. Θα πρέπει όμως να έχει εμπειρία σε ότι αφορά τα νομικά και τεχνικά ζητήματα που αφορούν το κανονισμό και να δρα συμβουλευτικά [1].

Απαιτείται θέσπιση κωδικών δεοντολογίας από τους φορείς / εταιρείες που εκπροσωπούν κατηγορίες υπευθύνων και εκτελούντων την επεξεργασία προκειμένου να εξασφαλίσουν την εφαρμογή του ΓΚΠΔ σύμφωνα με το άρθρο 40 όπως επίσης και μηχανισμών / διαδικασιών πιστοποίησης προστασίας δεδομένων (άρθρο 42) [1].

Τα κατώτερα πρόστιμα παραβάσεων φτάνουν 10,000,000 € ή το 2% του συνολικού παγκόσμιου κύκλου εργασιών του προηγούμενου έτους (όποιο είναι το υψηλότερο). Πρόστιμα δε μπορούν να επιβληθούν και στην περίπτωση που δεν υπάρξει παράβαση αλλά απουσιάζουν τα οργανωτικά / τεχνικά μέτρα που απαιτούνται για την συμμόρφωση με τον ΓΚΠΔ [1].

Τα δε πιο αυστηρά πρόστιμα ανέρχονται στα 20.000.000 € ή σε περίπτωση επιχειρήσεων, έως το 4% του συνολικού παγκόσμιου κύκλου εργασιών του προηγούμενου έτους (όποιο είναι υψηλότερο). Τα πρόστιμα αυτά επιβάλλονται στις περιπτώσεις παράβασης των κανονισμών που περιγράφονται παρακάτω [1]:

- πλήττονται τα δικαιώματα των υποκειμένων των δεδομένων,
- δεν τηρούνται οι βασικές αρχές που αφορούν την επεξεργασία δεδομένων προσωπικού χαρακτήρα,
- γίνεται διαβίβαση δεδομένων προσωπικού χαρακτήρα με αποδέκτη τρίτη χώρα ή διεθνή οργανισμό,
- Μη συμμόρφωση κατόπιν εντολής, προσωρινό ή οριστικό περιορισμό της επεξεργασίας, αναστολή της κυκλοφορίας προσωπικών δεδομένων που επιβάλλει η εποπτική αρχή ή μη παροχή πρόσβασης.

Ο κάθε πολίτης λοιπόν που θεωρεί ότι παραβιάζονται τα δικαιώματα του μπορεί να απευθυνθεί σε οποιαδήποτε εποπτική αρχή και να υποβάλλει την καταγγελία του (Αρχή της εγγύτητας) [1].

Στα δικαιώματα του υποκειμένου εντάσσεται και το δικαίωμα της λήθης που αφορά την διαγραφή των προσωπικών του δεδομένων και αφορά κυρίως τα ψηφιακά δεδομένα καθώς το παραπάνω δικαίωμα δεν μπορεί να ασκηθεί στον έντυπο τύπο (πχ. εφημερίδες, περιοδικά κτλ) [1].

Μέσω του νέου νόμου πλέον υπεύθυνοι είναι εξίσου ο υπεύθυνος και ο εκτελών την επεξεργασία, εν αντιθέσει με τον προηγούμενο νόμο που η ευθύνη βάραινε εξ ολοκλήρου τον υπεύθυνο επεξεργασίας [1].

Μέσω του άρθρου 80 πλέον υπάρχει συλλογική υποστήριξη των δικαιωμάτων του υποκειμένου που μπορεί να γίνει μέσω κάποιου φορέα που θα υποστηρίξει τα δικαιώματά του μέσω δικαστηρίου αντ' αυτού [1].

1.3 Εμπλεκόμενοι Ρόλοι ΓΚΠΔ (GDPR) και BCP/DRP

Οι εμπλεκόμενοι ρόλοι που αναφέρονται στον κανονισμό παρουσιάζονται παρακάτω, επιπλέον έχουν προστεθεί και κάποιο περαιτέρω ρόλοι οι οποίοι είναι έμμεσα εμπλεκόμενοι και είναι οι επαγγελματίες του IT τομέα.

- **Υποκείμενο των Δεδομένων (Πίνακας 1):** Είναι το φυσικό πρόσωπο όπου αναφέρονται / ανήκουν τα προσωπικά δεδομένα [1]. Παρακάτω παρατίθεται μια ενδεικτική λίστα με όλους εκείνους που θεωρούνται υποκείμενα των δεδομένων.

Α/Α	Υποκείμενο των Δεδομένων
1	Προσωπικό εταιρείας ή οργανισμού (Μόνιμο και Προσωρινό)
2	Δυνητικοί εργαζόμενοι που στέλνουν βιογραφικά σε εταιρείες
3	Εργαζόμενοι που έχουν αποχωρήσει από την εταιρεία
4	Εργολάβοι/Εξωτερικοί Συνεργάτες
5	Σύμβουλοι
6	Μαθητές / Σπουδαστές
7	Εθελοντές
8	Διευθυντές
9	Μέτοχοι
10	Μέλη οικογένειας ενός εργαζομένου
11	Χορηγοί
12	Δημόσιοι υπάλληλοι
13	Καταναλωτές
14	Τελικοί Χρήστες του διαδικτύου
15	Τελικοί Χρήστες Ιστοσελίδων (Website)
16	Τελικοί Χρήστες εφαρμογών
17	Πελάτες
18	Προμηθευτές

Πίνακας 1. Παραδείγματα από υποκείμενα των δεδομένων

- **Υπεύθυνος Επεξεργασίας (Data Controller):** Θεωρείται το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, όπου καθορίζουν τους σκοπούς, τις διαδικασίες και τον τρόπο επεξεργασίας των δεδομένων [1].
- **Εκτελών την Επεξεργασία (Data Processor):** Θεωρείται το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα υπό την καθοδήγηση αλλά και την υπευθυνότητα του υπευθύνου επεξεργασίας [1].
- **Αποδέκτης (Πίνακας 2):** Θεωρείται οποιοδήποτε πρόσωπο (φυσικό ή νομικό), η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, όπου κοινοποιούνται τα δεδομένα. Θα πρέπει να σημειωθεί ότι οι δημόσιες αρχές που θα λάβουν στοιχεία

προσωπικού χαρακτήρα στο πλαίσιο συγκεκριμένης έρευνας δεν θεωρούνται αποδέκτες σύμφωνα με το ευρωπαϊκό δίκαιο [1].

Α/Α	Δυνητικοί Αποδέκτες
1	Διοίκηση
2	Υπάλληλοι (Μόνιμο και Προσωρινό προσωπικό)
3	Υπεργολάβοι
4	Εξωτερικοί Συνεργάτες
5	Δημόσιες Υπηρεσίες
6	Διεθνής Οργανισμοί
7	Παραλήπτες εντός ΕΕ
8	Παραλήπτες εκτός ΕΕ
9	Εταιρείες
10	Εκπαιδευτικά Ιδρύματα (Πανεπιστήμια, Τεχνολογικά Ιδρύματα, Κολέγια κτλ)

Πίνακας 2. Δυνητικοί Αποδέκτες Προσωπικών Δεδομένων

- **Τρίτος:** Θεωρείται οποιοδήποτε άλλος (φυσικό πρόσωπο, νομικό πρόσωπο, δημόσια αρχή, υπηρεσία, φορέας, οργανισμός) 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 [1].
- **SA (Supervisory Authority – Εποπτική Αρχή):** εποπτική αρχή είναι η ανεξάρτητη δημόσια αρχή που είναι υπεύθυνη για την παρακολούθηση της εφαρμογής του κανονισμού [1].
- **DPO (Data Protection Officer - Υπεύθυνος Προστασίας Δεδομένων):** Συμβουλεύει τον υπεύθυνο επεξεργασίας και τον εκτελών την επεξεργασία σύμφωνα με τις διατάξεις που προβλέπει ο ΓΚΠΔ. Ο DPO είναι ένας ρόλος συμβουλευτικός και δεν φέρει καμία προσωπική ευθύνη για την μη συμμόρφωση με τον κανονισμό. Τα καθήκοντα και οι προϋποθέσεις που αφορούν τον συγκεκριμένο ρόλο περιγράφονται αναλυτικά στα άρθρα 37 έως 40 [1].

Παρακάτω παρατίθενται επιπροσθέτως ρόλοι οι οποίοι δεν αναφέρονται στον κανονισμό αλλά στο πλαίσιο των εταιρειών αποτελούν ρόλους κλειδιά τόσο για την ακριβή εφαρμογή του αλλά και την εμπλοκή τους στο κομμάτι του BC/DR. Αρχικά παραθέτουμε τους ρόλους κλειδιά που είναι υπεύθυνοι για την τεχνολογική υποδομή της εταιρείας αλλά και για τις διαδικασίες που την πλαισιώνουν:

- **IT manager:** είναι υπεύθυνος για την υλοποίηση και τη διατήρηση της τεχνολογικής υποδομής ενός οργανισμού. Βασική του αρμοδιότητα είναι να παρακολουθεί τις λειτουργικές απαιτήσεις του οργανισμού, να διερευνά στρατηγικές και τεχνολογικές λύσεις.
- **Security Manager:** είναι υπεύθυνος για την προστασία των υπολογιστών, των δικτύων αλλά και των δεδομένων μιας εταιρείας ή ενός οργανισμού από κινδύνους που αφορούν:
    - ιούς υπολογιστών,
    - παραβιάσεις ασφαλείας
    - και κακόβουλες επιθέσεις.

  Στις αρμοδιότητες του λοιπόν είναι η εφαρμογή κατάλληλων μέτρων ασφαλείας ώστε να διασφαλίσει την προστασία της εταιρείας από κακόβουλες ενέργειες αλλά και από απρόοπτα συμβάντα που μπορεί να εμποδίσουν την επιχειρησιακή συνέχεια ενός οργανισμού.

Σύμφωνα με το ISO 22301 [2], θα πρέπει να υπάρχουν κάποιοι βασικοί ρόλοι που θα πρέπει να είναι υπεύθυνοι για την επιχειρησιακή συνέχεια της εταιρείας και για την αποφυγή ανεπιθύμητων συμβάντων που θα μπορούσαν να κοστίσουν τόσο σε χρήμα αλλά και σε φήμη του ονόματος της. Οι ρόλοι χωρίζονται σε δύο (2) κατηγορίες οι οποίοι περιγράφονται παρακάτω:

i. **Ρόλοι σύστασης/παρακολούθησης των διαδικασιών και της εφαρμογής του:**

- **BC Steering Committee Member:** είναι υπεύθυνος για την διασφάλιση ενός πλήρη προγράμματος επιχειρησιακής συνέχειας σύμφωνα με τις ανάγκες αλλά και την στρατηγική της εταιρείας.
- **Program Sponsor:** υπεύθυνος για την επίβλεψη εφαρμογής του προγράμματος και την καθημερινή ομαλή εφαρμογή του.
- **Program Manager:** υπεύθυνος για την εκτέλεση των καθημερινών δραστηριοτήτων που διασφαλίζουν την εφαρμογή του προγράμματος επιχειρησιακής συνέχειας.
- **Business Continuity Planner:** υπεύθυνος για την ανάπτυξη και διατήρηση διαδικασιών ενός τμήματος για την διασφάλιση της άμεσης ανταπόκρισης, αλλά και επαναφοράς της επιχειρησιακής συνέχειας σε περίπτωση ενός

συμβάντος χρησιμοποιώντας εργαλεία και μεθόδους (συστήματα, φόρμες κτλ.) που παρήχθησαν από τον Program Manager.

ii. **Ρόλοι υπεύθυνοι στην περίπτωση συμβάντων αλλά ανάκτησης της ομαλής λειτουργίας:**

- **Team Leader:** υπεύθυνος της ομάδας άμεσης επέμβασης και επαναφοράς σε περίπτωση ενός συμβάντος, αλλά και αυτός που παίρνει τις αποφάσεις.
- **Team Coordinator:** υπεύθυνος για το συντονισμό της ομάδας.
- **Team Administrator:** λειτουργεί σαν συνδετικός κρίκος των παραπάνω ρόλων και συντονίζει πρακτικά και διαδικαστικά θέματα.

1.4 Στόχοι Διατριβής - Καινοτομία

Οι στόχοι της εν λόγω διατριβής είναι η κατανόηση του κανονισμού περι προστασίας προσωπικών δεδομένων και η 'μετατροπή' του σε έναν οδηγό-πρότυπο για τις επιχειρήσεις, οι οποίες αφενός έχουν σαν στόχο την υϊοθέτηση κουλτούρας ασφάλειας και αφετέρου την ομαλή επιχειρησιακή συνέχεια των πόρων τους. Παρακάτω συνοψίζουμε τα ερευνητικά ερωτήματα της εν λόγω διατριβής:

- Πως επηρρεάζει ο καινούργιος κανονισμός για τα προσωπικά δεδομένα (GDPR) το πλάνο επιχειρησιακής συνέχειας και επανάκαμψης (BCP/DRP);
- Πως μπορούμε να δημιουργήσουμε ένα πλάνο επιχειρησιακής συνέχειας και επανάκαμψης (BCP/DRP) βασιζόμενοι στα άρθρα και στις αρχές που προβλέπονται από τον κανονισμό για τα προσωπικά δεδομένα (GDPR);
- Τι περαιτέρω ενέργειες πρέπει να γίνουν από επιχειρήσεις / οργανισμούς για την επίτευξη της επιχειρησιακής συνέχειας και επανάκαμψης (BCP/DRP) μέσω της συμμόρφωση με το κανονισμό για τα προσωπικά δεδομένα (GDPR);
- Πως μπορεί μια μικρομεσαία επιχείρηση να επιτύχει συμμόρφωση με τον κανονισμό (GDPR) και να δημιουργήσει ταυτόχρονα ένα επιτυχημένο πλάνο επιχειρησιακής συνέχειας και επανάκαμψης (BCP/DRP);
- Τι τεχνολογικές λύσεις πρέπει να υλοποιήσει μια επιχείρηση ώστε να επιτύχει αφενός συμμόρφωση με τον κανονισμό και αφετέρου να υλοποιήσει ένα αποτελεσματικό πλάνο επιχειρησιακής συνέχειας και επανάκαμψης (BCP / DRP);

- Τι πρέπει να περιέχει ένα πλάνο επιχειρησιακής συνέχειας και επανάκαμψης (BCP / DRP) για να θεωρείτε αποτελεσματικό;

Λαμβάνοντας υπόψη τα προαναφερθέντα ερευνητικά ερωτήματα, παρακάτω θα γίνει μια προσπάθεια ανάλυσης των στόχων της εν λόγω διατριβής αλλά και της μεθοδολογίας που ακολουθήθηκε για την επίτευξη τους.

Αρχικά έγινε μια προσπάθεια μετατροπής ενός νομικού εγγράφου (GDPR) σε γλώσσα απλή και κατανοητή εισάγοντας έννοιες γνώριμες στον κόσμο της πληροφορικής (όπως επιχειρησιακή συνέχεια) και δημιουργίας δράσεων που απευθύνονται είτε σε τμήματα πληροφορικής εταιρειών με άλλο αντικείμενο δραστηριότητες, είτε σε εταιρείες πληροφορικής κάθε αυτού. Οι δράσεις αυτές παρουσιάζονται με μορφή εμπεριστατωμένων μεθοδολογιών (ITIL), αλλά και με προτάσεις χρήσης εργαλείων πληροφορικής από πιστοποιημένους προμηθευτές που κατέχουν όλα όσα απαιτούνται από τον κανονισμό.

Σε δεύτερο πλάνο δημιουργήθηκε μια εφαρμογή (τεχνολογία Java 8) , η οποία απευθύνεται σε επαγγελματίες πληροφορικής οι οποίοι θέλουν να έχουν έναν οδηγό ο οποίος θα τους βοηθήσει στην δημιουργία ενός βασικού σχεδίου επιχειρησιακής συνέχειας και επανάκαμψης (BCP /DRP) με οδηγίες και ελάχιστες απαιτούμενες προδιαγραφές. Σε αυτό το σημείο θα πρέπει να τονίσουμε ότι η ασφάλεια δεν είναι μόνο τεχνικά μέσα, αλλά ένα συνονθύλευμα τεχνικών, οργανωτικών αλλά και ηθικών μέσων.

Όπως αναφέρεται και σε επόμενα κεφάλαια, εταιρείες νεοσυσταθείσες αλλά και παλίες παρόλο που επιδεικνύουν αρτιότητα στο αντικείμενο που αντιπροσωπεύουν, στερούνται κουλτούρας ασφάλειας, είτε γιατί δεν υπάρχουν οι πόροι να επενδύσουν, είτε γιατί δεν γνωρίζουν την σπουδαιότητα της μέχρι να συμβεί κάποιο τεχνικό ή φυσικό συμβάν. Ένας επιπλέον σκόπος την εν λόγω μελέτης είναι η δημιουργία ενός οδηγού επαγρύπνησης (awareness) στο κομμάτι της επιχειρησιακής συνέχειας, λαμβάνοντας υπόψη όσα εισήχθηκαν με τον νέο κανονισμό και έγιναν αναγκαιότητα.

Με την χρήση της εφαρμογή “BCP-DRP Generator” και σε συνδιασμό με τις δράσεις που περιγραφονται στην εν λόγω διατριβή μπορεί να δημιουργήσει ένα πλάνο επιχειρησιακής συνέχειας και επανάκαμψης που να καλύπτει τόσο τις ανάγκες της εταιρείας του, αλλά και τις συμβατικές ανάγκες / απαιτήσεις των πελατών που σε κάποιες περιπτώσεις έργων πληροφορικής απαιτείται η ύπαρξη BCP/DRP. Η χρήση του εργαλείου μπορεί να γίνει τόσο από μη-έμπειρους (junior) όσο και από έμπειρους

(senior) επαγγελματίες, οι οποίοι στα πλαίσια των εργασιών τους (πχ.consultants, ελεύθεροι επαγγελματίες κτλ.) χρειάζονται να έχουν ένα πρότυπο (template / οδηγό) για την δημιουργία ενός BCP/DRP. Το αρχείο που εξάγεται από την εφαρμογή είναι 100% παραμετροποιήσιμο και μπορούν να προστεθούν ενότητες ή ακόμα και να αφαιρεθούν κάποιες υπάρχουσες. Επίσης σύμβουλοι εταιρειών που το αντικείμενο τους είναι η ασφάλεια και απευθύνονται σε μεγάλο όγκο εταιρειών μπορούν να το προσαρμόσουν ανά περίπτωση, έχοντας πάντα ένα παραμετροποιήσιμο πρότυπο στην διάθεση του.

1.5 Επίλογος

Στο παρόν κεφάλαιο έγινε μια γενική επισκόπηση της παρούσας διατριβής αλλά και μια ανάλυση στο τι ίσχυε μεχρί την έναρξη της ισχύς του νέου κανονισμού για την προστασία των προσωπικών δεδομένων. Παρουσιάστηκαν επίσης οι στόχοι, όπως επίσης και η καινοτομία της εν λόγω μεταπτυχιακής διατριβής.

Στο κεφάλαιο που θα ακολουθήσει θα αναλυθούν εκτενώς όλα τα άρθρα του νέου κανονισμού και θα παρατεθεί σχολιασμός σε σχέση με τις υλοποιήσεις που πρέπει να εφαρμοστούν τόσο στον τομέα της πληροφορικής όσο και στα διαδικαστικά / διαχειριστικά κομμάτια που επηρρεάζουν τον τομέα αυτό.

Κεφάλαιο 2

GDPR - Γενική Επισκόπηση

Ο καινούργιος κανονισμός αποτελείται από 99 άρθρα από τα οποία τα 39 επηρεάζουν άμεσα τον τομέα του IT και το BCP/DRP σχέδιο τους και γενικότερα το κομμάτι διαχείρισης της επιχειρησιακής συνέχειας και διαχείρισης καταστροφών. Στα πλαίσια τις ορθής κατανόησης του κανονισμού στο συγκεκριμένο κεφάλαιο θα παρατεθεί μια επισκόπηση / ανάλυση όλων των άρθρων του κανονισμού ανά κεφάλαιο και ανά τμήμα αντίστοιχα.

2.1 Γενική Επισκόπηση των Άρθρων του Κανονισμού

Στην εν λόγω ενότητα θα παρουσιασθεί η δομή του κανονισμού ανά κεφάλαιο [1] και άρθρο αντίστοιχα.

Στο κεφάλαιο 1 παρουσιάζονται οι Γενικές Διατάξεις (1-4) του κανονισμού, όπου απαρτίζονται από τα εξής άρθρα: άρθρο 1 – Αντικείμενο και στόχοι, άρθρο 2 – Ουσιαστικό πεδίο εφαρμογής, άρθρο 3 – Εδαφικό πεδίο εφαρμογής και άρθρο 4 – Ορισμοί.

Στο κεφάλαιο 2 παρουσιάζονται οι Αρχές (5-11) που πλαισιώνουν τον εν λόγω κανονισμό και απαρτίζονται από τα εξής άρθρα: άρθρο 5 – Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα, άρθρο 6 – Νομιμότητα της επεξεργασίας, άρθρο 7 – Προϋποθέσεις και συγκατάθεση, άρθρο 8 – Προϋποθέσεις που ισχύουν για την συγκατάθεση παιδιού σε σχέση με τις υπηρεσίες της κοινωνίας των πληροφοριών, άρθρο 9 – Επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, άρθρο 10 – Επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν

ποινικές καταδίκες και αδικήματα και άρθρο 11 - Επεξεργασία η οποία δεν απαιτεί εξακρίβωση ταυτότητας.

Στο Κεφάλαιο 3 παρουσιάζονται τα Δικαιώματα του Υποκειμένου Δεδομένων, τα οποία ομαδοποιούνται σε πέντε (5) τμήματα τα οποία παρουσιάζονται παρακάτω. Στο τμήμα 1 (12) περιγράφονται η Διάφανεια και οι Ρυθμίσεις οι οποίες συμπτύσσονται στο άρθρο 12 - Διαφανής ενημέρωση, ανακοίνωση και ρυθμίσεις για την άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων. Στο τμήμα 2 (13-15) περιγράφονται τα άρθρα που αφορούν την Ενημέρωση και την Πρόσβαση στα Δεδομένα Προσωπικού Χαρακτήρα. Το τμήμα 2 του εν λόγω κεφαλαίου απαρτίζεται από τα εξής άρθρα: άρθρο 13 - Πληροφορίες που παρέχονται εάν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται από το υποκείμενο των δεδομένων, άρθρο 14 - Πληροφορίες που παρέχονται εάν τα δεδομένα προσωπικού χαρακτήρα δεν έχουν συλλεγεί από το υποκείμενο των δεδομένων και άρθρο 15 - Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων. Στο τμήμα 3 (16-20) περιγράφονται δικαιώματα που αφορούν την Διόρθωση και την Διαγραφή και απαρτίζονται από τα παρακάτω άρθρα: άρθρο 16 - Δικαίωμα διόρθωσης, άρθρο 17 – Δικαίωμα διαγραφής («δικαίωμα στη λήθη»), άρθρο 18 – Δικαίωμα περιορισμού της επεξεργασίας, άρθρο 19 – Υποχρέωση γνωστοποίησης όσον αφορά τη διόρθωση ή τη διαγραφή δεδομένων προσωπικού χαρακτήρα ή τον περιορισμό της επεξεργασίας, άρθρο 20 - Δικαίωμα στη φορητότητα των δεδομένων, άρθρο 16 - Δικαίωμα διόρθωσης, άρθρο 17 – Δικαίωμα διαγραφής («δικαίωμα στη λήθη»), άρθρο 18 – Δικαίωμα περιορισμού της επεξεργασίας, άρθρο 19 – Υποχρέωση γνωστοποίησης όσον αφορά τη διόρθωση ή τη διαγραφή δεδομένων προσωπικού χαρακτήρα ή τον περιορισμό της επεξεργασίας και άρθρο 20 - Δικαίωμα στη φορητότητα των δεδομένων. Στο τμήμα 4 (21-22) περιλαμβάνει το άρθρο 21 που αφορά το Δικαίωμα Εναντίωσης και το άρθρο 22 που αφορά την Αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφιλ. Τέλος, το τμήμα 5 περιλαμβάνει το άρθρο 23 που αφορά τους Περιορισμούς.

Στο κεφάλαιο 4 παρουσιάζονται θέματα του αφορούν τον υπεύθυνο επεξεργασίας και τον εκτελών την επεξεργασία και περιγράφονται σε πέντε (5) διαφορετικά τμήματα. Στο τμήμα 1 (24-31) περιέχονται οι Γενικές Υποχρεώσεις και απαρτίζονται από τα παρακάτω άρθρα: άρθρο 24 – Ευθύνη του υπευθύνου επεξεργασίας, άρθρο 25 – Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού, άρθρο 26 – Από κοινού υπεύθυνοι επεξεργασίας, άρθρο 27 – Εκπρόσωποι υπευθύνων επεξεργασίας ή

εκτελούντων την επεξεργασία μη εγκατεστημένων στην Ένωση, άρθρο 28 – Εκτελών την επεξεργασία, άρθρο 29 – Επεξεργασία υπό την εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, άρθρο 30 – Αρχεία των δραστηριοτήτων επεξεργασίας και άρθρο 31 - Συνεργασία με την εποπτική αρχή. Στο τμήμα 2 (32-34) περιγράφονται τα άρθρα σχετικά με την Ασφάλεια των Δεδομένων Προσωπικού Χαρακτήρα, όπως: άρθρο 32 – Ασφάλεια επεξεργασίας, άρθρο 33 - Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή και άρθρο 34 - Ανακοίνωση παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων. Στο τμήμα 3 (35-36) περιγράφονται η Εκτίμηση Αντικτύπου αλλά και η προηγούμενη διαβούλευση: άρθρο 35 - Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων και άρθρο 36 – Προηγούμενη Διαβούλευση. Στο τμήμα 4 (37-39) περιγράφονται οι αρχές και υποχρεώσεις σχετικά με τον Υπεύθυνο Προστασίας Δεδομένων, όπως: άρθρο 37 – Ορισμός του υπευθύνου προστασίας δεδομένων, άρθρο 38 – Θέση του υπευθύνου προστασίας δεδομένων και άρθρο 39 - Καθήκοντα του υπευθύνου προστασίας δεδομένων. Στο τμήμα 5 (40-43) περιγράφονται όλα τα σχετικά που αφορούν τους Κώδικες Δεοντολογίας αλλά και την Πιστοποίηση: άρθρο 40 – Κώδικες δεοντολογίας, άρθρο 41 – Παρακολούθηση των εγκεκριμένων κωδίκων δεοντολογίας, άρθρο 42 – Πιστοποίηση και άρθρο 43 – Φορείς πιστοποίησης.

Στο κεφάλαιο 5 παρουσιάζονται τα άρθρα που αφορούν τις Διαβιβάσεις Δεδομένων προς 3ες Χώρες ή Διεθνής Οργανισμούς (44-50) και περιέχονται τα εξής άρθρα: άρθρο 44 – Γενικές αρχές για διαβιβάσεις, άρθρο 45 – Διαβιβάσεις βάσει απόφαση επάρκειας, άρθρο 46 – Διαβιβάσεις που υπόκεινται σε κατάλληλες εγγυήσεις, άρθρο 47 – Δεσμευτικοί εταιρικοί κανόνες, άρθρο 48 – Διαβιβάσεις ή κοινοποιήσεις που δεν επιτρέπονται από το δίκαιο της Ένωσης, άρθρο 49 – Παρεκκλίσεις για ειδικές καταστάσεις και άρθρο 50 - Διεθνής συνεργασία για την προστασία δεδομένων προσωπικού χαρακτήρα.

Στο Κεφάλαιο 6 παρουσιάζονται πληροφορίες και αρχές που διέπουν τις Ανεξάρτητες Εποπτικές Αρχές και χωρίζονται σε δύο (2) τμήματα. Το τμήμα 1 (51-54) περιγράφει το ανεξάρτητο καθεστός των αρχών και διέπεται από τα εξής άρθρα: άρθρο 51 – Εποπτική αρχή, άρθρο 52 – Ανεξαρτησία, άρθρο 53 – Γενικές προϋποθέσεις για τα μέλη της εποπτικής αρχής και άρθρο 54 - Κανόνες για τη σύσταση της εποπτικής αρχής. Το τμήμα 2 (55-59) αφορά τις αρμοδιότητες, τα καθήκοντα και τις εξουσίες των

εποπτικών αρχών και απαρτίζεται από τα εξής άρθρα: άρθρο 55 – Αρμοδιότητα, άρθρο 56 – Αρμοδιότητα της επικεφαλής εποπτικής αρχής, άρθρο 57 – Καθήκοντα, άρθρο 58 – Εξουσίες και άρθρο 59 - Εκθέσεις δραστηριοτήτων.

Το Κεφάλαιο 7 αφορά την Συνεργασία και Συνεκτικότητα και απαρτίζεται από τρία (3) τμήματα. Το τμήμα 1 (60-62) αφορά την συνεργασία: άρθρο 60 – Συνεργασία μεταξύ της επικεφαλής εποπτικής αρχής και των άλλων ενδιαφερόμενων εποπτικών αρχών, άρθρο 61 – Αμοιβαία συνδρομή και άρθρο 62 – Κοινές επιχειρήσεις αρχών ελέγχου. Το τμήμα 2 (63-67) αφορά την Συνεκτικότητα: άρθρο 63 – Μηχανισμός συνεκτικότητας, άρθρο 64 – Γνώμη του Συμβουλίου, άρθρο 65 – Επίλυση διαφορών από το Συμβούλιο Προστασίας Δεδομένων, άρθρο 66 – Επείγουσα διαδικασία και άρθρο 67 - Ανταλλαγή πληροφοριών. Το τμήμα 3 (68-76) αφορά το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων και απαρτίζεται από τα εξής άρθρα: άρθρο 68 – Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, άρθρο 69 – Ανεξαρτησία, άρθρο 70 – Καθήκοντα του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων, άρθρο 71 – Εκθέσεις, άρθρο 72 – Διαδικασία, άρθρο 73 – Πρόεδρος, άρθρο 74 – Καθήκοντα του Προέδρου, άρθρο 75 – Γραμματεία και άρθρο 76 – Εμπιστευτικότητα.

Στο Κεφάλαιο 8 περιέχονται θέματα που αφορούν τις Προσφυγές, την Ευθύνη και τις σχετικές κυρώσεις Κυρώσεις (77-84) και αποτελείται από τα εξής άρθρα: άρθρο 77 – Δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή, άρθρο 78 – Δικαίωμα πραγματικής δικαστικής προσφυγής κατά αρχής ελέγχου, άρθρο 79 – Δικαίωμα πραγματικής δικαστικής προσφυγής κατά υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία, άρθρο 80 – Εκπροσώπηση υποκειμένων των δεδομένων, άρθρο 81 – Αναστολή των διαδικασιών, άρθρο 82 – Δικαίωμα αποζημίωσης και ευθύνη, άρθρο 83 – Γενικοί όροι επιβολής διοικητικών προστίμων και άρθρο 84 – Κυρώσεις.

Στο κεφάλαιο 9 παρουσιάζονται οι Διατάξεις που αφορούν Ειδικές Περιπτώσεις Επεξεργασίας (85-91) και περιγράφονται στα παρακάτω άρθρα: άρθρο 85 – Επεξεργασία και ελευθερία έκφρασης και πληροφόρησης, άρθρο 86 – Επεξεργασία και πρόσβαση του κοινού σε επίσημα έγγραφα, άρθρο 87 – Επεξεργασία του εθνικού αριθμού ταυτότητας, άρθρο 88 – Επεξεργασία στο πλαίσιο της απασχόλησης, άρθρο 89 – Διασφαλίσεις και παρεκκλίσεις σχετικά με την επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς, άρθρο 90 – Υποχρεώσεις τήρησης απορρήτου και

άρθρο 91 – Υφιστάμενοι κανόνες προστασίας των δεδομένων εκκλησιών και θρησκευτικών ενώσεων.

Στο Κεφάλαιο 10 περριγράφονται τα θέματα που αφορούν την Κατ' εξουσιοδότηση Πράξεις αλλά και Εκτελεστικές Πράξεις (92-93) και περιγράφονται στα παρακάτω άρθρα: άρθρο 92 – Άσκηση της εξουσιοδότησης και άρθρο 93 – Διαδικασία επιτροπής.

Τέλος στο τελευταίο κεφάλαιο το οποίο είναι το 11 παρουσιάζονται οι Τελικές Διατάξεις (94-99), και περιγράφονται στα παρακάτω άρθρα: άρθρο 94 – Κατάργηση της οδηγίας 95/46/ΕΚ, άρθρο 95 – Σχέση με την οδηγία 2002/58/ΕΚ, άρθρο 96 – Σχέση με συμφωνίες που έχουν συναφθεί παλαιότερα, άρθρο 97 – Εκθέσεις της Επιτροπής, άρθρο 98 – Επισκόπηση άλλων νομικών πράξεων της Ένωσης για την προστασία των δεδομένων και τέλος άρθρο 99 - Έναρξη ισχύος και εφαρμογή.

2.2 Γενικές Διατάξεις (1-4)

Στις γενικές διατάξεις του κανονισμού εντάσσονται τα άρθρα 1-4, όπου και αναλύονται το αντικείμενο του κανονισμού και οι στόχοι, το ουσιαστικό πεδίο εφαρμογής το εδαφικό πεδίο εφαρμογής και οι ορισμοί που πρέπει να γίνουν κατανοητοί στα πλαίσια του κανονισμού [1].

Ο εν λόγω κανονισμός αφορά την προστασία των φυσικών προσώπων σε ότι αφορά την αυτοματοποιημένη και μη επεξεργασία, στην αρχειοθέτηση στα πλαίσια της επεξεργασίας, αλλά και διακίνηση των προσωπικών τους δεδομένων. Εξαίρεση στον κανονισμό αποτελούν τα δεδομένα που επεξεργάζονται αποκλειστικά σε προσωπική ή οικιακή χρήση, όπως και τα δεδομένα τα οποία εξυπηρετούν σκοπούς προστασίας της δημόσια ασφάλειας (πχ. διερεύνηση ποινικών αδικημάτων κτλ.) [1].

Αξίζει να σημειωθεί ότι ο παρόν κανονισμός αφορά τα κράτη μέλη της ευρωπαϊκής ένωσης αλλά και τις χώρες οι οποίες έχουν συναλλαγές με κράτη μέλη της ευρωπαϊκής ένωσης και επεξεργάζονται δεδομένα αυτών. Με λίγα λόγια στα πλαίσια της παγκοσμιοποίησης και της διακίνησης αλλά και ανταλλαγής αγαθών και υπηρεσιών εκτός Ευρωπαϊκής Ένωσης θα μπορούσαμε να πούμε ότι ο εν λόγω κανονισμός έχει ένα παγκόσμιο αντίκτυπο στις εταιρείες και στους οργανισμούς [1].

Στις γενικές διατάξεις του κανονισμού εντάσσονται ή επαναπροσδιορίζονται καινούργιες έννοιες ή ορισμοί, οι οποίες θα πρέπει να κατανοηθούν ώστε να γίνει αντιληπτό το πεδίο επιρροής τους αφενός αλλά και η καλύτερη κατανόηση των άρθρων που πλαισιώνουν τον κανονισμό. Παρακάτω παρατίθεται μια σύντομη αναφορά όλων αυτών των ορισμών που αναλύονται στο άρθρο 4 του κανονισμού:

1. **Δεδομένα προσωπικού χαρακτήρα (Πίνακας 3):** Με τον όρο προσωπικά δεδομένα (**Εικόνα 1**) θεωρούμε οποιαδήποτε πληροφορία αφορά το πρόσωπο ενός ατόμου όπως: το όνομα, η ηλικία, το επάγγελμα, η οικογενειακή κατάσταση, ο τόπος κατοικίας, η ερωτική του ζωή, η φυλετική του προέλευση, τα πολιτικά του φρονήματα, η θρησκεία, οι απόψεις του γενικότερα για κάποιο θέμα, η συνδικαλιστική του δράσει, το ποινικό του μητρώο που αφορούν το συγκεκριμένο πρόσωπο. Στον παρακάτω πίνακα παρατίθεται μια συλλογή στοιχείων που λογίζονται ως προσωπικά δεδομένα [1]:

ΑΑ	**Προσωπικά Δεδομένα**
1	Όνομα / Επώνυμο
2	Διεύθυνση Σπιτιού
3	Προσωπικός Λογαριασμός Email
4	Προσωπικός Αριθμός Τηλεφώνου
5	Αριθμός Τηλεφώνου Εργασίας
6	Γενέθλια / Ηλικία
7	Γλώσσες
8	Τόπος Γέννησης
9	Εθνικότητα
10	Στοιχεία Ταυτότητας
11	Στοιχεία Διαβατηρίου
12	Αντίγραφα Ταυτότητας και Διαβατηρίου
13	Οποιοδήποτε Κωδικός Αριθμός που αφορά φυσικό πρόσωπο (ΑΜΚΑ,ΙΚΑ κτλ.)
14	Στοιχεία Άδεια οδήγησης , όπως και οποιοδήποτε αντίγραφο
15	Πληροφορίες που αφορούν την οικογένεια (σύζυγο, σύντροφο, παιδιά, γονείς κτλ.)
16	Φύλο
17	Θρησκεία
18	Οικογενειακή Κατάσταση
19	Άδεια Εργασίας ή οποιαδήποτε άλλα στοιχεία που αφορούν έναν εργαζόμενο, όπως ο μοναδικός αριθμός που αντιστοιχεί σε έναν εργαζόμενο σε μια εταιρεία ή οργανισμό
20	Ασφάλειες (Δεδομένα που καταχωρούνται σε ασφαλιστικές ή φορείς πχ. αρρώστιες κτλ.)
21	Ημερομίσθιο / Μισθός

22	Αριθμός Τραπέζης
23	Στοιχεία χρεωστικών και πιστωτικών καρτών
24	Πτυχία και Επίπεδο Εκπαίδευσης
25	CV/ Εργασιακή Εμπειρία
26	Η εμπλοκή σε εργατικό κίνημα ή σωματείο
27	Εκπαιδεύσεις που λαμβάνουν χώρα κατά την διάρκεια εργασίας
28	Αξιολογήσεις που αφορούν ένα φυσικό πρόσωπο, όπως αξιολογήσεις που λαμβάνουν χώρα στην εργασία
29	Εργατοώρες
30	Άδεια
31	Άδεια Ασθενείας
32	Υγεία και Ιατρικά δεδομένα
33	Ποινικές Καταδίκες/Αδικήματα
34	Βίντεο από τις κάμερες ασφαλείας
35	Βιομετρικά Δεδομένα (πχ. δακτυλικά αποτυπώματα)
36	Φωτογραφίες
37	Δεδομένα από την χρήση Internet
38	Δεδομένα από την χρήση επαγγελματικού email
39	Δεδομένα από την χρήση προσωπικού email
40	IP Address, log-in data, cookies κτλ.
41	Ηλεκτρονικά δεδομένα εντοπισμού (κινητό τηλέφωνο, GPS κτλ.)
42	Σύνταξη ή δεδομένα που αφορούν την συνταξιοδότηση κάποιου
43	Ημερομηνία έναρξης εργασίας
44	Χώρος εργασίας
45	Εργασιακές συνθήκες
46	Δεδομένα ήχου
47	Εξωτερικά χαρακτηριστικά (ύψος, βάρος, χρώμα ματιών κτλ.)
48	Οικογενειακή Δομή
49	Χόμπι και λοιπές δραστηριότητες
50	Στοιχεία που αποκαλύπτουν τη φυλετική καταγωγή ή την εθνικότητα
51	Πολιτικές πεποιθήσεις
52	Σεξουαλικές προτιμήσεις ή ότι αφορά την σεξουαλική ζωή ενός ατόμου
53	Συμμετοχές σε οποιοδήποτε είδος σωματίου, δραστηριότητας κτλ.

Πίνακας 3. Προσωπικά Δεδομένα

Εικόνα 1. Προσωπικά Δεδομένα

2. **Επεξεργασία:** Ως επεξεργασία προσωπικών δεδομένων ορίζεται η σειρά πράξεων που διενεργείται είτε με την χρήση μηχανικών μέσων ή αυτοματοποιημένων μεθόδων ή χωρίς την χρήση αυτόν (πχ. Έντυπη επεξεργασία). Η πράξη της επεξεργασίας λοιπόν συνοψίζει όλες τις παρακάτω έννοιές [1]: συλλογή, καταχώριση, οργάνωση, διάρθρωση, αποθήκευση, προσαρμογή ή μεταβολή, ανάκτηση, αναζήτηση πληροφοριών, χρήση, κοινοποίηση / δημοσίευση με διαβίβαση, διάδοση ή κάθε άλλη μορφή διάθεσης, συσχέτιση ή συνδυασμός, περιορισμός, διαγραφή ή καταστροφή.

Η πράξη της επεξεργασίας θα πρέπει να τελείται υπό προϋποθέσεις, οι οποίες συμπτύσσονται παρακάτω [1]:

I. το υποκείμενο των δεδομένων θα πρέπει να έχει συναινέσει για την επεξεργασία τους αλλά και για το σκοπό όπου επρόκειτο να επεξεργαστούν,
II. ο υπεύθυνος επεξεργασίας έχει έννομη υποχρέωση για την ασφαλή επεξεργασία των δεδομένων του υποκειμένου,
III. η επεξεργασία είναι απαραίτητη για την διεκπεραίωση καθηκόντων και γίνεται από τον υπεύθυνο επεξεργασίας,

IV. η επεξεργασία είναι απαραίτητη για το συμφέρον του υποκειμένου και δεν αντίκειται στο συμφέρον, τα δικαιώματα ή τις ελευθερίες του υποκειμένου και ιδιαίτερα στις περιπτώσεις των ανηλίκων.

V. η επεξεργασία αφορά όλα τα εν ζωή φυσικά πρόσωπα και όχι τα πρόσωπα που δεν βρίσκονται εν ζωή, στην δεύτερη περίπτωση υπάρχει άλλη νομοθεσία που καλύπτει το συγκεκριμένο κομμάτι.

3. **Περιορισμός της επεξεργασίας:** Θεωρείται η πράξη κατά την οποία περιορίζεται η μελλοντική επεξεργασία για κάποια δεδομένα προσωπικού χαρακτήρα [1].
4. **Κατάρτιση προφίλ:** Θεωρείται κάθε μορφή αυτοματοποιημένης επεξεργασίας, όπου δημιουργείται με αυτοματοποιημένα μέσα δημιουργία συμπερασμάτων που αφορούν ένα φυσικό πρόσωπο. Σε αυτήν την περίπτωση λογίζονται περιπτώσεις όπως ανάλυση συμπεριφοράς χρηστών μέσα από τις επιλογές τους στο internet ή εξαγωγή συμπερασμάτων για ένα φυσικό πρόσωπο βάση τον τόπο καταγωγής του, την εθνικότητα κτλ. [1]
5. **Ψευδωνυμοποίηση:** Θεωρείται η διαδικασία επεξεργασίας προσωπικών δεδομένων κατά την οποία χρησιμοποιούνται τεχνικοί τρόποι (πχ κρυπτογράφηση) όπου το φυσικό πρόσωπο στον οποίο ανήκουν τα δεδομένα δεν μπορεί να ταυτοποιηθεί χωρίς την ύπαρξη συμπληρωματικών πληροφοριών [1].
6. **Σύστημα Αρχειοθέτησης:** Θεωρείται οποιοδήποτε προσβάσιμο σύνολο δεδομένων προσωπικού χαρακτήρα είτε αυτό υπάρχει σε κάποιο σύστημα είτε σε έντυπη μορφή [1].
7. **Υπεύθυνος επεξεργασίας (Data Controller):** Θεωρείται το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, όπου καθορίζουν τους σκοπούς, τις διαδικασίες και τον τρόπο επεξεργασίας των δεδομένων [1].
8. **Εκτελών την επεξεργασία (Data Processor):** Θεωρείται το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα υπό την καθοδήγηση αλλά και την υπευθυνότητα του υπευθύνου επεξεργασίας [1].
9. **Αποδέκτης (Πίνακας 4):** Θεωρείται οποιοδήποτε πρόσωπο (φυσικό ή νομικό), η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, όπου κοινοποιούνται τα δεδομένα. Θα πρέπει να σημειωθεί ότι οι δημόσιες αρχές που θα λάβουν στοιχεία

προσωπικού χαρακτήρα στο πλαίσιο συγκεκριμένης έρευνας δεν θεωρούνται αποδέκτες σύμφωνα με το ευρωπαϊκό δίκαιο.

Στον παρακάτω πίνακα παρατίθενται όλα τα πιθανά πρόσωπα νομικά ή φυσικά που μπορεί να θεωρηθούν αποδέκτες δεδομένων προσωπικού χαρακτήρα [1].

Α/Α	Δυνητικοί Αποδέκτες
1	Διοίκηση
2	Υπάλληλοι (Μόνιμο και Προσωρινό προσωπικό)
3	Υπεργολάβοι
4	Εξωτερικοί Συνεργάτες
5	Δημόσιες Υπηρεσίες
6	Διεθνής Οργανισμοί
7	Παραλήπτες εντός ΕΕ
8	Παραλήπτες εκτός ΕΕ
9	Εταιρείες
10	Εκπαιδευτικά Ιδρύματα (Πανεπιστήμια, Τεχνολογικά Ιδρύματα, Κολέγια κτλ)

Πίνακας 4. Δυνητικοί Αποδέκτες Προσωπικών Δεδομένων

10. **Τρίτος:** Θεωρείται οποιοδήποτε άλλος (φυσικό πρόσωπο, νομικό πρόσωπο, δημόσια αρχή, υπηρεσία, φορέας, οργανισμός) 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 [1].
11. **Συγκατάθεση:** Θεωρείται η σύμφωνη γνώμη του υποκειμένου δεδομένων για την επεξεργασία των προσωπικών του δεδομένων, εφόσον του έχουν περιγραφεί με σαφήνεια οι λόγοι, ο σκοπός αλλά και ο τρόπος επεξεργασίας των δεδομένων αυτών [1].
12. **Παραβίαση δεδομένων προσωπικού χαρακτήρα:** Θεωρείται η παραβίαση ασφαλείας (τυχαία ή παράνομη) δεδομένων προσωπικού χαρακτήρα τα οποία υποβλήθηκαν προς επεξεργασία [1].
13. **Γενετικά δεδομένα:** Θεωρούνται τα γενετικά χαρακτηριστικά που αφορούν την φυσιολογία ή την υγεία του υποκειμένου (πχ. χρώμα δέρματος, ακμή κτλ) [1].
14. **Βιομετρικά δεδομένα:** Ως βιομετρικά δεδομένα ή χαρακτηριστικά λογίζονται τα φυσικά ή γενετικά χαρακτηριστικά ενός ατόμου όπως τα δακτυλικά αποτυπώματα, η γεωμετρία της παλάμης, η ανάλυση της κόρης του ματιού, τα

χαρακτηριστικά του προσώπου, το DNA του όπως επίσης και χαρακτηριστικά που εκπονούνται μέσω τεχνικής επεξεργασίας και αφορούν την ανάλυση της φωνής ενός ατόμου, την συμπεριφορά, την υπογραφή κτλ [1].

15. **Δεδομένα που αφορούν την υγεία:** Θεωρούνται τα δεδομένα τα οποία αφορούν την ψυχική ή την σωματική υγεία του υποκειμένου και γενικότερα οποιοδήποτε στοιχείο αποκαλύπτει την κατάσταση υγείας του ατόμου [1].
16. **Κύρια εγκατάσταση:** Αφορά κυρίως την κύρια εγκατάσταση του υπευθύνου επεξεργασίας και του εκτελούντα την επεξεργασία. Σε ότι αφορά τον υπεύθυνο επεξεργασίας ως κύρια εγκατάσταση εντός ΕΕ θεωρείται αυτή στην οποία λήφθηκαν οι αποφάσεις περί σκοπών και μέσων επεξεργασίας [1].

    Σε ότι αφορά τον εκτελούντα την επεξεργασία ως κύρια εγκατάσταση θεωρείτε το μέρος στο οποίο εκτελούνται οι δραστηριότητες επεξεργασίας ανεξαρτήτως της φυσικής του εγκατάστασης [1].

17. **Εκπρόσωπος:** Θεωρείται ο το φυσικό ή νομικό πρόσωπο που εκπροσωπεί τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία [1].
18. **Επιχείρηση:** Θεωρείται κάθε φυσικό ή νομικό πρόσωπο που ασκεί οικονομική δραστηριότητα [1].
19. **Όμιλος επιχειρήσεων:** Μια επιχείρηση και οι ελεγχόμενες από αυτή επιχειρήσεις [1].
20. **Δεσμευτικοί εταιρικοί κανόνες:** Αφορά τις πολιτικές προστασίας που ασκεί μια εταιρεία ή ένας όμιλος επιχειρήσεων οι οποίες πρέπει να ακολουθούνται από έναν υπεύθυνο επεξεργασίας ή τον εκτελών την επεξεργασία [1].
21. **Εποπτική αρχή:** εποπτική αρχή είναι η ανεξάρτητη δημόσια αρχή που είναι υπεύθυνη για την παρακολούθηση της εφαρμογής του κανονισμού [1].
22. **Ενδιαφερόμενη εποπτική αρχή:** αφορά την εποπτική αρχή στην επάγονται τα υπό επεξεργασία δεδομένα. Αυτό ισχύει όταν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία επάγονται στην συγκεκριμένη εποπτική αρχή.

Σε ότι αφορά το υποκείμενο των δεδομένων αφορά την εποπτική αρχή στην χώρα της ΕΕ που διαμένουν.

Και τέλος την εποπτική αρχή στην οποία έχει υποβληθεί καταγγελία [1].

23. **Διασυνοριακή επεξεργασίας:** Αφορά την επεξεργασία δεδομένων η οποία γίνεται σε πολλαπλές εγκαταστάσεις σε ότι αφορά τα κράτη μέλη της ΕΕ ή στις περιπτώσεις που η επεξεργασία γίνεται σε μια εγκατάσταση του υπευθύνου

επεξεργασίας ή του εκτελούντα την επεξεργασία αλλά επηρεάζει υποκείμενα δεδομένων που βρίσκονται σε περισσότερα του ενός κράτη μέλη της ΕΕ [1].

24. **Σχετική και αιτιολογημένη ένσταση**: αιτιολογημένη ένσταση ως προς την ύπαρξη παράβασης του κανονισμού [1].
25. **Υπηρεσία της κοινωνίας των πληροφοριών[1]:** οποιαδήποτε αμειβόμενη υπηρεσία παρέχεται εξ αποστάσεως με ηλεκτρονικά μέσα και κατόπιν παραγγελίας ενός αποδέκτη υπηρεσιών [3].
26. **Διεθνής οργανισμός:** κάθε οργανισμός ή φορείς αυτού που διέπονται από διεθνής συμφωνίες μεταξύ των χωρών [1].

2.3 Αρχές (5-11)

Σύμφωνα με το άρθρο 5 του κανονισμού ο υπεύθυνος επεξεργασίας θα πρέπει να μπορεί να αποδεικνύει συμμόρφωση στις παρακάτω αρχές [1]:

- να υπάρχει νομιμότητα, αντικειμενικότητα και διαφάνεια σε όλα τα προσωπικά δεδομένα του υποκειμένου συμπεριλαμβανομένου της συγκατάθεσης του,
- σε ότι αφορά την συγκατάθεση θα πρέπει να είναι ξεκάθαρη και κατανοητή γλώσσα,
- να κρατιούνται τα ελάχιστα δεδομένα για το σκοπό που χρειάζονται (Ελαχιστοποίηση Δεδομένων),
- να είναι ακριβή,
- να υπάρχει πολιτική διατήρησης για το χρόνο που κρατούνται τα δεδομένα
- Ακεραιότητα και Εμπιστευτικότητα των δεδομένων (Integrity and Confidentiality).

Πέραν των αρχών που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα σημαντικός παράγοντας είναι να πληρούνται κάποιες προϋποθέσεις που αφορούν την νομιμότητα αυτής. Η επεξεργασία θεωρείται νόμιμη εφόσον πληρείται τουλάχιστον μία από τις παρακάτω προϋποθέσεις [1]:

- η συναίνεση του υποκειμένου για την επεξεργασία των δεδομένων και τον σκοπό της επεξεργασίας αυτής,
- επεξεργασία στα πλαίσια εκτέλεσης συμβάσεων μεταξύ του υποκειμένου και άλλων μερών,

[1] οδηγία 2015/1535 άρθρο 1, παράγραφος 1, στοιχείο β

- η επεξεργασία καθίσταται απαραίτητη βάσει των έννομων υποχρεώσεων του υπευθύνου επεξεργασίας,
- η επεξεργασία είναι απαραίτητη για την διαφύλαξη των συμφερόντων του υποκειμένου,
- η εκτέλεση της επεξεργασία από τον υπεύθυνο επεξεργασίας είναι απαραίτητη στα πλαίσια του δημοσίου συμφέροντος ή εξουσίας,
- τα έννομα συμφέροντα του υπευθύνου επεξεργασίας που απαιτούν την επεξεργασία των δεδομένων του υποκειμένου δεν θα πρέπει να καταπατούν τις ελευθερίες και τις αξίες αυτού.

Σε ότι αφορά την συγκατάθεση επεξεργασίας δεδομένων προσωπικού χαρακτήρα θα πρέπει να σημειωθεί ότι οι σκοποί της επεξεργασίας αυτής θα πρέπει να είναι σε απλή, κατανοητή και προσβάσιμη μορφή όπως επίσης και η ανάκληση της συγκατάθεσης να μπορεί να γίνει με τον ίδιο εύκολο τρόπο χωρίς περαιτέρω διαδικασίες. Η επεξεργασία στην οποία υποβλήθηκαν τα δεδομένα πριν την ανάκληση της συγκατάθεσης δεν θεωρείτε παράνομη.

Στο άρθρο 8 του κανονισμού αφιερώνεται ένα ολόκληρο εδάφιο το οποίο αφορά την επεξεργασία δεδομένων που αφορούν ανήλικα άτομα, κάτι το οποίο αφορά επίσης τις επιχειρήσεις σε περιπτώσεις έγγαμων υπαλλήλων όπου κατατίθενται δεδομένα που αφορούν ανήλικα τέκνα στα πλαίσια της ασφάλισης ή γονικών παροχών.

Η επεξεργασία των δεδομένων που αφορά ποινικά αδικήματα θα πρέπει να διενεργείτε μόνο υπό τον έλεγχο επίσημης αρχής.

Τέλος να σημειωθεί ότι εάν και εφόσον στα πλαίσια της επεξεργασίας των δεδομένων δεν απαιτείται η ταυτοποίηση ή η εξακρίβωση της ταυτότητας των δεδομένων, ο υπεύθυνος επεξεργασίας δεν υποχρεούται να συλλέξει περαιτέρω πληροφορίες για την ταυτοποίηση του ατόμου [1].

2.4 Δικαιώματα του Υποκειμένου Δεδομένων (12-23)

Στην συγκεκριμένη ενότητα θα παρουσιαστούν τα δικαιώματα του υποκειμένου των δεδομένων χωρισμένα σε πέντε (5) τμήματα που αποτελούνται από άρθρα του κανονισμού.

2.4.1 Τμήμα 1 (12) – Διαφάνεια και Ρυθμίσεις

Σύμφωνα με τις οδηγίες του άρθρου 12 θα πρέπει να δίνονται οι πληροφορίες σχετικά με τα δεδομένα του υποκειμένου, εφόσον ζητηθούν και έχει πραγματοποιηθεί η ταυτοποίηση του προσώπου[2] . Η συγκεκριμένη απαίτηση του κανονισμού, δημιουργεί μια σειρά αλλαγών στον τομέα του IT είτε αφορά αιγών εταιρείες πληροφορικής είτε οποιαδήποτε άλλη εταιρεία.

Το άρθρο 12 προβλέπει την διαφανής ενημέρωση του υποκειμένου σε ότι αφορά τα προσωπικά του δεδομένα και θα πρέπει να παρέχονται πληροφορίες σχετικά σε διάστημα ενός μήνα από την στιγμή που θα ζητηθούν. Αυτό μπορεί να γίνει είτε γραπτώς είτε τηλεφωνικώς εφόσον έχει γίνει η ταυτοποίηση του προσώπου. Το εν λόγω άρθρο λοιπόν προϋποθέτει επαρκή τεχνολογική υποδομή ώστε τα δεδομένα να συλλέγονται με τον πιο βέλτιστο τρόπο [1].

2.4.2 Τμήμα 2 (13-15) – Ενημέρωση και Πρόσβαση σε Δεδομένα Προσωπικού Χαρακτήρα

Στο εν λόγω τμήμα συνοψίζονται οι παραχθέντες πληροφορίες που ο υπεύθυνος επεξεργασίας υποχρεούται να έχει διαθέσιμες εφόσον τα δεδομένα συλλεχθούν από το υποκείμενο αυτών. Αυτό προϋποθέτει μια οργανωμένη υποδομή που να διασφαλίζει την ακρίβεια και την ασφαλή κράτηση αυτών των δεδομένων. Οι πληροφορίες αφορούν:

- τα στοιχεία υπευθύνου επεξεργασίας,
- τα στοιχεία υπευθύνου προστασίας δεδομένων,
- σκοπούς επεξεργασίας,
- αποδέκτες των δεδομένων,
- χρονικό διάστημα διατήρησης των δεδομένων αυτών (retention policy),
- δικαίωμα επεξεργασίας ή διόρθωσης των προσωπικών του δεδομένων και άλλα πολλά που δεν αφορούν το πεδίο του IT.

Στην περίπτωση που τα δεδομένα δεν έχουν συλλεχθεί από το υποκείμενο αυτών αλλά μέσω κάποιου συστήματος, ο υπεύθυνος επεξεργασίας οφείλει να παρέχει τις παρακάτω πληροφορίες:

[2] μέσω ταυτότητας ή άλλων νόμιμων διαδικασιών

- ταυτότητα και στοιχεία επικοινωνίας υπευθύνου επεξεργασίας και του υπευθύνου προστασίας δεδομένων,
- σκοπούς επεξεργασίας αλλά και νομική βάση,
- κατηγορίες δεδομένων προσωπικού χαρακτήρα,
- αποδέκτες η κατηγορίες αυτών,
- όλα όσα προβλέπονται στο άρθρο 13, όπως επίσης και άλλα πολλά τα οποία δεν έχουν άμεση σχέση με το αντικείμενο του ΙΤ.

Να σημειωθεί ότι σύμφωνα με το άρθρο 15 του κανονισμού το υποκείμενο των δεδομένων έχει το δικαίωμα πρόσβασης στα δεδομένα που το αφορούν αλλά και να λαμβάνει πληροφορίες σχετικά με όλα τα θέματα που προαναφέρθηκαν παραπάνω (Άρθρο 12 και Άρθρο 13).
Όπως αναφέρεται παραπάνω στο άρθρο 13 το υποκείμενο των δεδομένων έχει το δικαίωμα διόρθωσης των δεδομένων προσωπικού χαρακτήρα (Άρθρο 15) [1].

2.4.3 Τμήμα 3 (16-20) – Διόρθωση και Διαγραφή

Το υποκείμενο των δεδομένων έχει το δικαίωμα Διαγραφής των προσωπικών του δεδομένων. Ο υπεύθυνος επεξεργασίας δε από την πλευρά του θα πρέπει να εκτελέσει το συγκεκριμένο αίτημα χωρίς καθυστέρηση από την πλευρά του εφόσον πληρούνται οι παρακάτω προϋποθέσεις:

- τα δεδομένα δεν είναι πλέον χρήσιμα, στην περίπτωση που τα δεδομένα είναι ακόμα απαραίτητα ο υπεύθυνος επεξεργασίας μπορεί να αρνηθεί την διαγραφή τους,
- ανακαλείται η αρχική συγκατάθεση επεξεργασίας,
- διαφωνεί με την επεξεργασία
- παράνομη επεξεργασία
- αναγκαστική διαγραφή λόγω δικαίου

Ο υπεύθυνος επεξεργασίας έχει το δικαίωμα άρνησης διαγραφής εφόσον νομικές υποχρεώσεις, έννομα συμφέροντα, δεδομένα που αφορούν τον τομέα υγείας, όπως και δεδομένα που αφορούν σκοπούς έρευνας ή ιστορικούς και η διαγραφή τους εμποδίζει ή αλλοιώνει το αποτέλεσμά τους (Άρθρο 17) [1].

Λαμβάνοντας υπόψη συγκεκριμένες παραμέτρους και εφόσον ισχύουν έστω και μια από αυτές, το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει περιορισμό επεξεργασίας των δεδομένων αυτών.

Οι βασικοί παράμετροι συνοψίζονται παρακάτω:

- όταν τα δεδομένα δεν είναι ακριβή και χρειάζονται επαλήθευση απ' τον υπεύθυνο επεξεργασίας,
- παράνομη επεξεργασία,
- η χρήση τους είναι απαραίτητη για την άσκηση νομικών και λοιπών αξιώσεων,
- σε περιπτώσεις αντιρρήσεων του υποκειμένου των δεδομένων για την επεξεργασία των προσωπικών δεδομένων

Σε περιπτώσεις που τα προσωπικά δεδομένα έχουν υποστεί περιορισμό επεξεργασίας θα πρέπει να δοθεί συγκατάθεση του υποκειμένου για οποιαδήποτε επεξεργασία (Άρθρο 18) [1].

Οι ενέργειες που αφορούν την διόρθωση, διαγραφή και τον περιορισμό (άρθρα 16, 17, 18) των προσωπικών δεδομένων θα πρέπει να επικοινωνηθούν σε κάθε αποδέκτη στον οποίο και γνωστοποιήθηκαν και ο υπεύθυνος επεξεργασίας με την σειρά του θα πρέπει να ενημερώσει το υποκείμενο των δεδομένων σχετικά με τους αποδέκτες [1].

Το υποκείμενο στο οποίο ανήκουν τα προσωπικά δεδομένα έχει το δικαίωμα να ζητήσει και να λάβει τα προσωπικά του δεδομένα από τον υπεύθυνο επεξεργασίας σε αρχείο αναγνώσιμο από τα τεχνικά μέσα και να τα διαβιβάσει σε άλλον υπεύθυνο επεξεργασίας. Όλα τα παραπάνω ισχύουν εφόσον η επεξεργασία βασίζεται στην συγκατάθεση (consent) και η επεξεργασία γίνεται από αυτοματοποιημένα μέσα (Άρθρο 19) [1].

Το υποκείμενο στο οποίο ανήκουν τα προσωπικά δεδομένα έχει το δικαίωμα να ζητήσει και να λάβει τα προσωπικά του δεδομένα από τον υπεύθυνο επεξεργασίας σε αρχείο αναγνώσιμο από τα τεχνικά μέσα και να τα διαβιβάσει σε άλλον υπεύθυνο επεξεργασίας. Όλα τα παραπάνω ισχύουν εφόσον η επεξεργασία βασίζεται στην συγκατάθεση (consent) και η επεξεργασία γίνεται από αυτοματοποιημένα μέσα (Άρθρο 20) [1].

2.4.4 Τμήμα 4 (21-22) – Δικαίωμα Εναντίωσης και Αυτοματοποιημένη Λήψη Αποφάσεων

Το συγκεκριμένο άρθρο προσανατολίζεται στο δικαίωμα εναντίωσης του υποκειμένου των δεδομένων ως προς την επεξεργασία των δεδομένων του είτε μέσω αυτοματοποιημένων τεχνικών μέσων (πχ. Viber, Facebook) είτε μέσω απευθείας αίτησης στον υπεύθυνο επεξεργασίας των δεδομένων (Άρθρο 21).

Το Άρθρο 22 προσανατολίζεται στα δικαιώματα το υποκειμένου των δεδομένων που αφορούν τις αποφάσεις που απορρέουν μέσω αυτοματοποιημένης επεξεργασίας και τις κατάρτισης προφίλ. Αυτό πρακτικά σημαίνει ότι αφενός υπάρχει προστασία ως προς το υποκείμενο των προσωπικών δεδομένων, και αφετέρου οποιαδήποτε λήψη απόφασης παρθεί σε σχέση με τα προφίλ που προκύπτει από τα προσωπικά δεδομένα του υποκειμένου θα πρέπει να αποδεικνύεται από τον υπεύθυνο επεξεργασίας η ανθρώπινη παρέμβαση κατά την διάρκεια της λήψης απόφασης. Το συγκεκριμένο άρθρο επηρεάζει σε μεγάλο βαθμό τα αυτοματοποιημένα συστήματα λήψης αποφάσεων που συλλέγουν δεδομένα από διαφορετικά συστήματα και καταρτίζουν προφίλ και εξάγονται συμπεράσματα βάσει των αποτελεσμάτων τους.

Στα πλαίσια του Άρθρου 22 υπάρχουν εξαιρέσεις που επιτρέπουν την κατάρτιση προφίλ εφόσον επιτρέπεται βάσει δικαίου κράτους-μέλους ή εξυπηρετεί έννομα συμφέροντα (Άρθρο 22) [1].

2.4.5 Τμήμα 5 (23) – Περιορισμοί

Το άρθρο 23 επικεντρώνεται στο κομμάτι των περιορισμών και στην τήρηση των απολύτως απαραίτητων δεδομένων που χρειάζονται για την διεκπεραίωση των καθηκόντων μιας εταιρείας ή ενός οργανισμού (κρατικού ή μη). Επίσης η πρόσβαση θα πρέπει να είναι περιορισμένη και συγκεντρωμένη μόνο σε εκείνες της κατηγορίες δεδομένων που είναι απαραίτητο, αλλά και στους χρήστες που χρειάζεται [1].

2.5 Υπεύθυνος Επεξεργασίας και Εκτελών την Επεξεργασία (24-43)

Στην συγκεκριμένη ενότητα θα παρουσιαστούν οι γενικές υποχρεώσεις και τα γενικότερα καθήκοντα και απαιτήσεις, όπου πρέπει να πληρούνται από τον υπεύθυνο επεξεργασίας και τον εκτελών την επεξεργασία. Η εν λόγω ενότητα χωρίζεται σε πέντε

(5) τμήματα, τα οποία απαρτίζονται από αντίστοιχα άρθρα, όπως προβλέπεται από τον κανονισμό.

2.5.1 Τμήμα 1 (24-31) - Γενικές Υποχρεώσεις

Τα άρθρα 24-31 επικεντρώνονται περισσότερα στα καθήκοντα, τις αρμοδιότητες αλλά και τις αρχές που πρέπει να διέπουν έναν υπεύθυνο επεξεργασίας αλλά και έναν εκτελών την επεξεργασία.

Η ευθύνη του υπευθύνου επεξεργασίας επικεντρώνεται στην οργάνωση τόσο των τεχνικών αλλά και των οργανωτικών μέσων που θα αποδεικνύουν με διαφανή τρόπο ότι η επεξεργασία πραγματοποιείται σύμφωνα με τον εν λόγω κανονισμό.

Στο άρθρο 25 εισάγεται η έννοια της προστασίας δεδομένων από το σχεδιασμό (by design) και εξ' ορισμού. Ο υπεύθυνος επεξεργασίας είναι υποχρεωμένος να εφαρμόσει όλα εκείνα τα τεχνικά και διαδικαστικά μέτρα όπως επίσης και πολιτικές οι οποίες καθιστούν την επεξεργασία αλλά και διατήρηση των προσωπικών δεδομένων ασφαλή. Επανέρχεται επίσης η έννοια της 'ελαχιστοποίησης' σε ότι αφορά την συγκέντρωση αλλά και την επεξεργασία των δεδομένων, δηλαδή θα πρέπει να συγκεντρώνονται κατ' ελάχιστο τα δεδομένα που χρειάζονται αν περίπτωση. Επίσης σημαντική είναι και η ψευδονυμοποίηση των δεδομένων ώστε να μην είναι δυνατή η ταυτοποίηση των προσώπων στα οποία ανήκουν.

Σε περιπτώσεις όπου προβλέπονται περισσότεροι από ένας υπεύθυνοι επεξεργασίας το υποκείμενο των δεδομένων μπορεί να προσάψει ευθύνες στον καθένα ξεχωριστά.

Στις περιπτώσεις υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία μη εγκατεστημένων στην Ένωση θα πρέπει να οριστούν γραπτώς εκπρόσωποι στην ένωση και πιο συγκεκριμένα στην χώρα στην οποία τα δεδομένα υποβάλλονται σε επεξεργασία ή προσφέρονται υπηρεσίες ή αγαθά. Στην περίπτωση που η επεξεργασία είναι περιστασιακή ή προσωρινή ή αφορά ποινικές καταδίκες δεν ισχύει η ανωτέρω υποχρέωση.

Σχετικά με τον εκτελών την επεξεργασία είναι σημαντικό η επεξεργασία να γίνεται εφόσον τηρούνται όλες οι τεχνικές, οργανωτικές (άρθρο 32 και άρθρο 40) αλλά και σύννομες απαιτήσεις που απαιτούνται από τον κανονισμό. Επίσης οποιαδήποτε ένταξη επιπλέον εκτελούντος την επεξεργασία θα πρέπει να γίνει κατόπιν άδειας του υπευθύνου επεξεργασίας. Επίσης στην περίπτωση που ανατεθούν καθήκοντα προς εκτέλεση σε άλλον εκτελών την επεξεργασία από τον ίδιο τον εκτελούντα την

επεξεργασία για δραστηριότητες που είναι υπ' ευθύνη του υπευθύνου επεξεργασίας, σε περίπτωση που δεν ακολουθούνται όλοι οι κανόνες τόσο σε τεχνικό αλλά και διαδικαστικό επίπεδο τότε ο αρχικός εκτελών την επεξεργασία είναι πλήρως υπόλογος στον υπεύθυνο επεξεργασίας. Η επεξεργασία των προσωπικών δεδομένων διέπεται από σύμβαση σύμφωνα με το δίκαιο της ευρωπαϊκής ένωσης (αφορά τόσο τον εκτελούντα την επεξεργασία όσο και τον υπεύθυνο επεξεργασίας). Η εν λόγω σύμβαση πρέπει να προβλέπει τις παρακάτω παραμέτρους:

- επεξεργασία δεδομένων βάση καταγεγραμμένων διαδικασιών και πολιτικών,
- τήρηση εμπιστευτικότητας των υπό επεξεργασία προσωπικών δεδομένων,
- καλύπτει όλα τα τεχνικά, διαδικαστικά και νομικά μέτρα που περιγράφονται στο άρθρο 32 και αφορούν την ασφάλεια δεδομένων προσωπικού χαρακτήρα,
- λαμβάνονται υπόψη όλα τα μέτρα που αφορούν την αλλαγή ή πρόσληψη νέου εκτελούντος την επεξεργασία,
- προβλέπεται υποδομή τεχνική και οργανωτική ώστε να εκπληρώνονται όσα προβλέπονται στο κεφάλαιο ΙΙΙ του κανονισμού και αφορούν τα δικαιώματα του υποκειμένου των δεδομένων,
- λαμβάνονται υπόψη τα άρθρα που αφορούν την ασφάλεια δεδομένων προσωπικού χαρακτήρα (άρθρα 32-34) και τα άρθρα που αφορούν την εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων (άρθρα 35-36),
- μετά το πέρας παροχής υπηρεσιών επιστρέφονται τα δεδομένα στον υπεύθυνο επεξεργασία ή διαγράφονται (τα ίδια και τα υφιστάμενα αντίγραφά τους) εκτός και αν απαιτείται η περαιτέρω διατήρηση τους βάσει νόμων (πχ. δεδομένα που αφορούν οικονομικά ή φορολογικά θέματα και απαιτείται η διαχείριση τους για ένα εύλογο χρονικό διάστημα βάση νομοθεσίας),
- οι πληροφορίες σε σχέση με τα προσωπικά δεδομένα είναι διαθέσιμες στον υπεύθυνο επεξεργασίας αλλά και στους ελέγχους που γίνονται κατά διαστήματα,
- ενημέρωση στον υπεύθυνο επεξεργασίας σε περίπτωση που σε κάποιες περιπτώσεις παρατηρούνται κινήσεις ή ενέργειες που καταπατούν τον κανονισμό.

Οι τεχνικές υποδομές, οι διαδικασίες, οι απαραίτητες πιστοποιήσεις αλλά και ο κατάλληλος κώδικας δεοντολογίας αποτελούν διαβεβαιώσεις ότι ακολουθούνται όλοι οι κανόνες που περιγράφονται παραπάνω από τον κανονισμό.

Σε κάθε περίπτωση ο υπεύθυνος επεξεργασίας είναι αυτός ο οποίος ορίζει το πότε θα πρέπει να υποβληθούν τα δεδομένα προσωπικού χαρακτήρα υπό επεξεργασία.

Σύμφωνα με το άρθρο 30 κάθε υπεύθυνος επεξεργασίας θα πρέπει να τηρεί αρχείο στο οποίο θα περιγράφονται τα παρακάτω:

- τα στοιχεία του υπευθύνου επεξεργασίας, του εκπροσώπου αλλά και του υπευθύνου προστασίας δεδομένων (όνομα, επώνυμο, στοιχεία επικοινωνίας κτλ),
- περιγραφή του σκοπού επεξεργασίας,
- οι κατηγορίες των δεδομένων (πχ. ατομικά στοιχεία [όνομα, επώνυμο, όνομα πατρός] κτλ), όπως επίσης και οι κατηγορίες των υποκειμένων (πχ. υπάλληλοι κτλ),
- κατηγορίες σε σχέση με τους υφιστάμενους αποδέκτες αλλά και δυνητικούς (πχ. δημόσιες υπηρεσίες, τράπεζες κτλ) τόσο εντός ΕΕ όσο και σε χώρες εκτός ΕΕ,
- προθεσμίες διαγραφής των κατηγοριών των προσωπικών δεδομένων,
- πληροφορίες σχετικά με διαβιβάσεις σε χώρες εκτός ΕΕ,
- περιγραφή των πρακτικών ασφάλειας και των υποδομών όπου είναι δυνατό,

Σε σχέση με τις κατηγορίες επεξεργασίας θα πρέπει να τηρούνται απ' τον εκτελών την επεξεργασίας και τον εκπρόσωπο αναλυτικό αρχείο δραστηριοτήτων με όσα περιγράφονται ανωτέρω. Τα αρχεία αυτά πρέπει να είναι διαθέσιμα στην εποπτική αρχή όποτε ζητηθούν [1].

2.5.2 Τμήμα 2 (32-34) – Ασφάλεια Δεδομένων Προσωπικού Χαρακτήρα

Το άρθρο που αναφέρεται στην ασφάλεια και την επεξεργασία είναι και αυτό που αφορά περισσότερο τον τομέα του IT και επηρεάζει περισσότερο τόσο τα security policies των εταιρειών τα οποία αν δεν υπάρχουν θα πρέπει να ενταχθούν στις πολιτικές της εταιρείας και εάν ήδη υπάρχουν θα πρέπει να επανεξεταστούν. Αλλαγές επίσης επέρχονται και στο θέμα που ερευνούμε και αφορά το BC/DR της εταιρείας όπου αρκετές περιοχές θα πρέπει επίσης να επανεξεταστούν και μα προσαρμοστούν στην ισχύουσα νομοθεσία. Οι τεχνικές αλλά και οι διαδικασίες οι οποίες είτε πρέπει να επανεξεταστούν είτε να επαναπροσδιοριστούν αναφέρονται παρακάτω ανά περίπτωση:

- Ψευδωνυμοποίηση και κρυπτογράφηση δεδομένων προσωπικού χαρακτήρα.
- συνεχή παρακολούθηση και αξιολόγηση των αρχών απορρήτου, ακεραιότητας, διαθεσιμότητας και αξιοπιστίας των συστημάτων που επεξεργάζονται προσωπικά δεδομένα.
- Δυνατότητα άμεσης αποκατάστασης πρόσβασης και διαθεσιμότητας των δεδομένων σε περίπτωση τεχνικού προβλήματος ή οποιαδήποτε άλλου συμβάντος που μπορεί να διακόψει την ομαλή λειτουργία των συστημάτων.
- Συνεχής αξιολόγηση των τεχνικών και οργανωτικών διαδικασιών και εργαλείων μέσω δοκιμών και τακτικών-συνεχόμενων αξιολογήσεων στα πλαίσια διασφάλισης της ασφάλειας των συστημάτων.

Θα πρέπει να σημειωθεί επίσης ότι είναι απαραίτητη η συνεχής αξιολόγηση του επιπέδου ασφαλείας, ώστε συνεχώς να λαμβάνονται υπόψη οι κίνδυνοι που απορρέουν από την χρήση συστημάτων αλλά και δεδομένων που περιέχονται αυτά. Ενδεικτικά, θα πρέπει με κάθε μέσο να αποφεύγεται η επεξεργασία και η προσπέλαση από μη εξουσιοδοτημένα άτομα, η καταστροφή άνευ άδειας των υπευθύνων, απώλεια, αλλοίωση, παράνομη ή άνευ άδειας κοινοποίηση. Ο κάθε οργανισμός ή εταιρεία θα πρέπει να λαμβάνει όλα τα απαραίτητα μέτρα, μέσα αλλά και πιστοποιήσεις που θα λειτουργήσουν βοηθητικά και υποστηρικτικά ώστε να αποφευχθούν απώλειες που αναφέρονται παραπάνω.

Τα άρθρα 33 και 34 αφορούν την γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή αλλά και την ανακοίνωση της παραβίασης αυτής στο υποκείμενο των δεδομένων εντός 72 ωρών από τη στιγμή που γίνει αντιληπτό το συμβάν. Από την πλευρά του ο υπεύθυνος επεξεργασίας θα πρέπει να ενημερώσει τον υπεύθυνο επεξεργασίας όταν λάβει χώρα οποιοδήποτε είδους παραβίαση. Σε ότι αφορά την αρχή θα πρέπει να υπάρξει αναλυτική άμεση ή σταδιακή ενημέρωση με στοιχεία όπου περιγράφονται παρακάτω:

- το είδος της παραβίασης,
- κατηγορίες δεδομένων που επηρεάστηκαν,
- αριθμό επηρεαζόμενων,
- αριθμό των αρχείων ή συστημάτων που επηρεάστηκαν,
- στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων,
- συνέπειες που προήλθαν από την εν λόγω παραβίαση,

- μέτρα που ελήφθησαν στα πλαίσια της παραβίασης,
- μέτρα άμβλυνσης των συνεπειών ή διορθωτικά μέτρα / ενέργειες,

Ταυτόχρονα με την εποπτική αρχή θα πρέπει να σημειωθεί ότι θα πρέπει να ενημερωθεί και το υποκείμενο των δεδομένών για την σχετική παραβίαση εφόσον από την εταιρεία / οργανισμό δεν έχουν εφαρμοστεί όλα τα κατάλληλα μέτρα πχ κρυπτογράφηση των δεδομένων που να απειλεί τις ελευθερίες του υποκειμένου [1].

2.5.3 Τμήμα 3 (35-36) – Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων και προηγούμενη διαβούλευση

Πριν από οποιαδήποτε επεξεργασία των δεδομένων προσωπικού χαρακτήρα, όπου μπορεί να επιφέρει επιπτώσεις στο υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας θα πρέπει να κάνει μια εκτίμηση (ΕΑ – Εκτίμηση Αντικτύπου) κατά πόσο οι πράξεις επεξεργασίας αυτές θα επηρεάσουν τις ελευθερίες και τα δικαιώματα του υποκειμένου των δεδομένων. Η εν λόγω εκτίμηση θα πρέπει να περιέχει τουλάχιστον τις παρακάτω πληροφορίες ώστε να θεωρείτε ολοκληρωμένη και σαφής:

- περιγραφή των πράξεων / ενεργειών επεξεργασίας των δεδομένων,
- σκοπός της επεξεργασίας,
- λόγους επεξεργασίας από τον υπεύθυνο επεξεργασίας,
- αναγκαιότητα των πράξεων αυτών σε σχέση με τους σκοπούς που περιγράφονται παραπάνω,
- εκτίμηση κινδύνου (ενδείκνυται κλίμακα σε αυτό σημείο και διαδικασία σχετική),
- μέτρα προστασίας / ασφάλειας ώστε να μην διακινδυνεύσουν τα συμφέρονται και οι ελευθερίες του υποκειμένου των δεδομένων.

Η εν λόγω εκτίμηση θα πρέπει να επαναπροσδιορίζεται ελέγχεται ως προς την ορθότητα της.

Σύμφωνα με το άρθρο 36 ο υπεύθυνος επεξεργασίας μπορεί να ζητήσει την συμβουλή της εποπτικής αρχής σε σχέση με την εκτίμηση αντικτύπου και εφόσον τα αποτελέσματα αυτής υποδεικνύουν ότι τα δεδομένα προσωπικού χαρακτήρα θα μπορούσαν να εκτεθούν σε κίνδυνο [1].

2.5.4 Τμήμα 4 (37-39) – Υπεύθυνος Προστασίας Δεδομένων (DPO-Data Protection Officer)

Ο υπεύθυνος προστασίας δεδομένων είναι το πρόσωπο το οποίο επιλέγεται από τον υπεύθυνο επεξεργασίας και τον εκτελών την επεξεργασίας. Ο ρόλος του υπευθύνου προστασίας δεδομένων είναι συμβουλευτικός και στις αρμοδιότητες του είναι να επιβλέπει την στρατηγική (διαδικασίες, πολιτικές κτλ) της εταιρείας σε σχέση με τον κανονισμό αλλά και τα μέτρα προστασίας που λαμβάνονται ώστε να διασφαλιστεί αφενός η συμμόρφωση με τον εν λόγω κανονισμό αλλά και η ασφάλεια των δεδομένων προσωπικού χαρακτήρα.

Θα πρέπει να σημειωθεί ότι ο κανονισμός δεν προβλέπει συγκεκριμένα κριτήρια για την πρόσληψη ενός DPO, βασικό κριτήριο αποτελούν η επαγγελματική εμπειρία του και η αντίληψη του σχετικά με εταιρικά θέματα και θέματα ασφάλειας [1].

2.5.5 Τμήμα 5 (40-43) – Κώδικες Δεοντολογίας και Πιστοποίηση

Στα πλαίσια διαφύλαξης της προστασίας των προσωπικών δεδομένων ο κανονισμός ενθαρρύνει την ύπαρξη κώδικα δεοντολογίας, διαδικασιών και πρακτικών. Τέτοιου είδους διαδικασίες μπορεί να είναι οι πολιτικές ασφάλειας μια εταιρείας, οι κώδικες δεοντολογίας (που ορίζει ο κλάδος/τομέας και καταρτίζονται από την ένωση που εκπροσωπεί κάθε κλάδο) , εγγεγραμμένες διαδικασίες και πρακτικές που εξασφαλίζουν την ασφαλή επεξεργασία αλλά και διαφύλαξη των προσωπικών δεδομένων και άλλα πολλά. Σημαντικό παράγοντα αποτελεί η παρακολούθηση αυτών των πολιτικών αλλά και η διαρκής ενημέρωση τους και επαναπροσδιορισμός του ανάλογα με τις ανάγκες που προκύπτουν αλλά και δυνητικούς κινδύνους στα πλαίσια ενός συνεχώς εξελισσόμενου περιβάλλοντος. [1]

Όπως αναφέρεται στο άρθρο 42 ο κανονισμός ενθαρρύνει την ύπαρξη πιστοποίησης μέσω μηχανισμών ή οργανισμών που αποδεικνύουν την συμμόρφωση μιας εταιρείας ή ενός οργανισμού με τον παρόντα κανονισμό. Οι φορείς πιστοποίησής δε, θα πρέπει να διαθέτουν το επίπεδο της εμπειρογνωμοσύνης σύμφωνα πάντα με τις απαιτήσεις που προβλέπονται από τις εποπτικές αρχές αλλά και βάση προτύπων (πχ. EN-ISO /IEC 17065/2012) [1].

2.6 Διαβιβάσεις Δεδομένων προς 3ες Χώρες ή Διεθνής Οργανισμούς (44-50)

Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (ΓΚΠΔ) και οι κανόνες που τον διέπουν ισχύουν και στις περιπτώσεις διαβίβασης των δεδομένων σε χώρες εκτός ΕΕ. Η Ευρωπαϊκή Επιτροπή μπορεί να επιτρέψει την διαβίβαση δεδομένων σε μια τρίτη χώρα εφόσον αυτή έχει χαρακτηριστεί ως "επαρκής" μέσω εμπεριστατωμένων διαδικασιών, έτσι η διαβίβαση δεδομένων μπορεί να γίνει χωρίς περαιτέρω εγγυήσεις.

Σε περιπτώσεις μη ύπαρξης επάρκειας η διαβίβαση μπορεί να γίνει μόνο εφόσον υποβληθούν οι κατάλληλες εγγυήσεις (πχ. ύπαρξη μέτρων και πολιτικών ασφάλειας για την διαβίβαση των δεδομένων) που προβλέπει ο κανονισμός.

Στην περίπτωση δε, που δεν πληρείται καμία από τις παραπάνω προϋποθέσεις η διαβίβαση μπορεί να γίνει μέσω κάποιων προϋποθέσεων, όπως για παράδειγμα η συγκατάθεση του υποκειμένου των δεδομένων στην διαβίβαση των δεδομένων εφόσον του έχουν γνωστοποιηθεί ο σκοπός επεξεργασίας, οι κίνδυνοι που υπάρχουν κτλ [1].

2.7 Ανεξάρτητες Εποπτικές Αρχές (51-59)

Η εν λόγω ενότητα απαρτίζεται από δύο (2) τμήματα τα οποία αποτελούνται από άρθρα, τα οποία αφορούν τις ανεξάρτητες εποπτικές αρχές αλλά και τις αρμοδιότητες, τα καθήκοντα και τις εξουσίες που είναι σε θέση να εκτελούν και να εφαρμόζουν.

2.7.1 Τμήμα 1 (51-54) - Ανεξάρτητο Καθεστώς

Οι εποπτικές αρχές κάθε κράτους-μέλους αποτελούν ένα ανεξάρτητο καθεστώς το οποίο καθορίζεται από χώρα ξεχωριστά με διαφανή τρόπο διασφαλίζοντας τις αρχές του κανονισμού περί προστασίας προσωπικών δεδομένων. Το κάθε κράτος-μέλος προβλέπει δια νόμου τόσο τη σύσταση της εποπτικής αρχής αλλά τις προϋποθέσεις αυτών που θα την πλαισιώνουν [1].

2.7.2 Τμήμα 2 (55-59) – Αρμοδιότητα, Καθήκοντα και Εξουσίες

Το τμήμα 2 όπου συμπεριλαμβάνονται τα άρθρα 55 έως 59 περιγράφει επί της ουσίας τις αρμοδιότητες, τα καθήκοντα αλλά και τις εξουσίες που πρέπει να ασκούνται από τις αρμόδιες εποπτικές αρχές. Αξίζει να σημειωθεί ότι στο άρθρο 57 περιγράφονται με πλήρη ανάλυση τα καθήκοντα τα οποία πρέπει να έχει κάθε εποπτική αρχή με βασικό γνώμονα την επιβολή αλλά και την παρακολούθηση που αφορά την εφαρμογή του εν λόγω κανονισμού. Οι παραβιάσεις δημοσιοποιούνται σε ετήσια κλίμακα, όπως επίσης και τα μέτρα τα οποία ελήφθησαν για την αντιμετώπιση τους ή τον μετριασμό τους [1].

2.8 Συνεργασία και Συνεκτικότητα (60-76)

Στον κανονισμό προβλέπεται συνεργασία μεταξύ των εποπτικών αρχών αλλά και αμοιβαία συνδρομή για την επιτυχή εφαρμογή του κανονισμού αλλά και την αντιμετώπιση καταστάσεων από κοινού, όπως για παράδειγμα ελέγχων, ερευνών κτλ.

Στα πλαίσια της συνεκτικότητας οι εποπτικές αρχές της ΕΕ συνεργάζονται μεταξύ τους ώστε να συμβάλουν στην ενιαία εφαρμογή του παρόντος κανονισμού.

Το συμβούλιο προστασίας δεδομένων δε αποτελεί ένα «νομικό πρόσωπο» της ΕΕ και απαρτίζεται από τον πρόεδρο του, απ' τους προϊσταμένους των εποπτικών αρχών αλλά και τον επόπτη προστασίας δεδομένων. Στα πλαίσια της παρουσίας τους διασφαλίζει την ενιαία εφαρμογή του κανονισμού για όλα τα κράτη μέλη εκδίδοντας κατευθυντήριες γραμμές και προσδιορίζοντας τις απαιτήσεις ανά περίπτωση. Στα πλαίσια των ετήσιων αναφορών εκδίδονται σχετικές εκθέσεις που αφορούν την επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Στα άρθρα 72-76 του κανονισμού διευκρινίζονται διαδικασίες που αφορούν τόσο την εκλογή του προέδρου και τα καθήκοντα του, όσο και τις αρμοδιότητες της σχετικής γραμματείας. Αξίζει να σημειωθεί ότι ο όρος της εμπιστευτικότητας είναι κάτι που αναφέρεται και προβλέπεται στις δράσεις του συμβουλίου προστασίας δεδομένων τόσο σε διαδικαστικό επίπεδο, όσο και σε επίπεδο εσωτερικής πρόσβασης στις πληροφορίες [1].

2.9 Προσφυγές, Ευθύνη και Κυρώσεις (77-84)

Σημαντικό κεφάλαιο του κανονισμού αποτελεί αυτό που αναφέρεται στις προσφυγές, την ευθύνη και τις κυρώσεις και αποτελείται από 8 άρθρα τα οποία επί της ουσίας περιγράφουν τόσο τα δικαιώματα του υποκειμένου όσο και τις νομικές πράξεις/κυρώσεις που επιβάλλονται σε περίπτωση που απειλούνται οι ελευθερίες του ή τα συμφέροντά του.

Το υποκείμενο των δεδομένων έχει το δικαίωμα να υποβάλει καταγγελία σε εποπτική αρχή εφόσον θεωρεί ότι οι πράξεις αυτές εναντιώνονται στον παρόντα κανονισμό. Η δε εποπτική αρχή από την πλευρά της υποχρεούται να ενημερώνει το υποκείμενο των δεδομένων για την πρόοδο της υπόθεσης του. Επίσης το υποκείμενο των δεδομένων έχει το δικαίωμα να προσφύγει νομικά κατά της εποπτικής αρχής εφόσον δεν καλύπτονται τα δικαιώματα του, όπως να μελετηθεί η καταγγελία του ή να λάβει ενημέρωση για την έκβαση της υπόθεσης του εντός 3 μηνών. Επιπροσθέτως, το υποκείμενο των δεδομένων μπορεί να προσφύγει δικαστικά και κατά του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, εφόσον παραβιάστηκαν τα δικαιώματά του στα πλαίσια του εν λόγω κανονισμού. Η εκπροσώπηση (οργάνωση, ένωση κτλ) του υποκειμένου των δεδομένων επίσης είναι εφικτή και προβλέπεται από τον κανονισμό εφόσον από την πλευρά του εκπροσώπου διατίθενται καταστατικοί σκοποί. Σε ότι αφορά τις δικαστικές διαδικασίες πρέπει να αναφερθεί ότι εφόσον υπάρχει εκκρεμότητα σε διαφορετικό κράτος μέλος από αυτό που έγιναν οι νομικές κινήσεις, οι διαδικασίες μπορούν να ανασταλούν. Σε κάθε περίπτωση το υποκείμενο των δεδομένων εφόσον έχει υποστεί ζημιά υλική ή μη έχει το δικαίωμα διεκδίκησης αποζημίωσης, όπως προβλέπεται από τον κανονισμό [1].

Σχετικά με την επιβολή προστίμων παρακάτω παρουσιάζονται αναλυτικά όσα προβλέπονται από τον εν λόγω κανονισμό (άρθρο 83, [1]):

Πρόστιμο: 10.000.000,00 ή 2% του συνολικού παγκόσμιου τζίρου του προηγούμενου έτους (ανάλογα με το πιο είναι μεγαλύτερο)

Παράβαση: Παράβαση σε σχέση με τις υποχρεώσεις του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία, του φορέα πιστοποίησης και του φορέα παρακολούθησης σύμφωνα με τα παρακάτω άρθρα: Άρθρο 8, Άρθρο 11, Άρθρο 25, Άρθρο 39, Άρθρο 42, Άρθρο 41 (παράγραφος 4) και Άρθρο 43.

Πρόστιμο: 20.000.000,00 ή 4% του συνολικού παγκόσμιου τζίρου του προηγούμενου έτους (ανάλογα με το πιο είναι μεγαλύτερο)

Παράβαση:

- Παράβαση των αρχών που αφορούν την επεξεργασία αλλά και την έγκριση που περιλαμβάνονται στα άρθρα: 5, 6, 7 και 9,
- Παράβαση των δικαιωμάτων του υποκειμένου σύμφωνα με τα άρθρα 12 – 22,
- Παράβαση που αφορά την διαβίβαση των προσωπικών δεδομένων σε Τρίτη χώρα, όπως περιγράφεται στα άρθρα 44 έως 49,
- Παράβαση σε σχέση με τις υποχρεώσεις που περιγράφονται στο κεφάλαιο IX – Διατάξεις που αφορούν ειδικές περιπτώσεις επεξεργασίας,
- Η μη συμμόρφωση στις εντολές της εποπτικής αρχής σύμφωνα με το άρθρο 58, παρ.1 και παρ.2.

Σχετικά με τις κυρώσεις που αποτελεί αντικείμενο του άρθρου 84 επισημαίνεται ότι κάθε κράτος μέλος θα πρέπει να θεσπίσει τις σχετικές κυρώσεις άλλων περιπτώσεων πέρα από αυτές που προαναφέρθηκαν στο άρθρο 83 και αφορούν τα διοικητικά πρόστιμα.

2.10 Διατάξεις που αφορούν Ειδικές Περιπτώσεις Επεξεργασίες (85-91)

Η επεξεργασία που αφορά την ελευθερία της έκφρασης και την πληροφόρηση στα πλαίσια δημοσιογραφικών, πανεπιστημιακών σκοπών αλλά και πάσης φύσης καλλιτεχνικής συμπεριλαμβανομένου και λογοτεχνικής έκφρασης, εξαιρείται από κάποια κεφάλαια του κανονισμού για την προστασία των προσωπικών δεδομένων. Τα κεφάλαια αυτά περιγράφονται παρακάτω:

- Κεφάλαιο II – Αρχές,
- Κεφάλαιο III – Δικαιώματα του υποκειμένου δεδομένων,
- Κεφάλαιο IV – Υπεύθυνος επεξεργασίας και εκτελών την επεξεργασία,
- Κεφάλαιο V - Διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες ή διεθνείς οργανισμούς,
- Κεφάλαιο VI – Ανεξάρτητες εποπτικές αρχές,

- Κεφάλαιο VII – Συνεργασία και συνεκτικότητα,
- Κεφάλαιο IX – Ειδικές περιπτώσεις επεξεργασίας δεδομένων

Εξαίρεση επίσης αποτελεί και η πρόσβαση στα επίσημα έγγραφα τα οποία εξυπηρετούν την ενημέρωση αλλά και διαφάνεια στα πλαίσια δημοσίου συμφέροντος.

Στα πλαίσια της επεξεργασίας γίνεται ξεχωριστή αναφορά και στον εθνικό αριθμό ταυτότητας του υποκειμένου, όπου εντάσσεται στα προσωπικά δεδομένα αυτού και η χρήση του για οποιαδήποτε σκοπό από τρίτους θα πρέπει να γίνεται ακολουθώντας και εφαρμόζοντας τις δέουσες εγγυήσεις.

Η προστασία των δικαιωμάτων που αφορά επεξεργασία στα πλαίσια της απασχόλησης που αφορά σκοπούς: πρόσληψης, εκτέλεσης συμβάσεως απασχόλησης, εκτέλεση υποχρεώσεων που προβλέπονται από το νόμο, εκτέλεση υποχρεώσεων που προβλέπονται από συλλογικές συμβάσεις, διαχειριστικούς, προγραμματισμού και οργάνωσης εργασίας, ισότητας, πολυμορφίας, υγείας και ασφάλειας, προστασίας περιουσίας του εργοδότη, προστασίας περιουσίας των πελατών και σκοπούς άσκησης, απόλαυσης ή διασκέδασης,

θεσπίζεται μέσω κανονισμών από τους κρατικούς φορείς των κρατών μελών στα πλαίσια των ατομικών ή συλλογικών συμβάσεων ή άλλης νομοθεσίας. Σε αυτό το σημείο θα πρέπει να επισημανθεί ότι ο εργοδότης από την πλευρά του έχει θεσπίσει όλα εκείνα τα μέτρα (τεχνικά, διαδικαστικά κτλ) που διαφυλάττουν την προστασία των δεδομένων του υποκειμένου των δεδομένων και επίσης τα δεδομένα του δεν χρησιμοποιούνται για σκοπούς που καταπατούν την αξιοπρέπεια, τις ελευθερίες, και τα συμφέρονται του υποκειμένου.

Στα πλαίσια της αρχειοθέτησης προς το δημόσιο συμφέρον θα πρέπει να αναφερθεί ότι θα πρέπει να τηρούνται όλα εκείνα τα τεχνικά, οργανωτικά και διαχειριστικά μέτρα που καθιστούν την επεξεργασία ασφαλή και δεν καταπατούν τις ελευθερίες του υποκειμένου. Και σε αυτό το σημείο εντάσσεται η τήρηση της αρχής της ελαχιστοποίησης των δεδομένων και τις χρήσης ψευδωνύμων στα πλαίσια της ασφάλειας του υποκειμένου. Σχετικά δε, με την επεξεργασία για επιστημονικούς, ιστορικούς ή στατιστικούς σκοπούς υπάρχουν εξαιρέσεις και παρεκκλίσεις από τα άρθρα 15, 16, 18 και 21 του κανονισμού στα πλαίσια πάντα της ασφαλούς επεξεργασίας. Το ίδιο ισχύει και για τους σκοπούς αρχειοθέτησης στα πλαίσια του δημοσίου συμφέροντος.

Στα πλαίσια κάθε είδους επεξεργασίας σημαντικό είναι να τηρείται το επαγγελματικό απόρρητο [1].

2.11 Κατ' εξουσιοδότηση Πράξεις και Εκτελεστικές Πράξεις (92-93)

Στα άρθρα 92 και 93 του παρόντος κανονισμού γίνεται αναφορά στις κατ' εξουσιοδότησή και εκτελεστικές πράξεις οι οποίες λαμβάνονται από την επιτροπή υπο προϋποθέσεις και κοινοποιούνται στο Ευρωπαϊκό Κοινοβούλιο αλλά και το Συμβούλιο. Η αρμόδια επιτροπή δε συνίσταται σύμφωνα με την έννοια που περιγράφεται στον κανονισμό της ΕΕ με αριθμό 182/2011 [1].

2.12 Τελικές Διατάξεις (94-99)

Στις τελικές διατάξεις του κανονισμού εμπεριέχονται η κατάργηση της προηγούμενης οδηγίας 95/46/ΕΚ και η ενεργοποίηση του παρόντος κανονισμού, όπου έγινε στις 25 Μάϊου 2018. Επίσης επισημαίνεται η εγκυρότητα της οδηγίας 2002/58/ΕΚ που αφορά την επεξεργασία των δεδομένων στα πλαίσια των ηλεκτρονικών επικοινωνιών.

Θα πρέπει επίσης να αναφερθεί ότι ο παρόν κανονισμός θα αξιολογείται και θα βελτιστοποιείται συνεχώς λαμβάνοντας υπόψιν τις τεχνολογικές αλλαγές και εξέλιξη, όπως επίσης και την επέκταση προσαρμογή άλλων κανονισμών που έχουν να κάνουν με την επεξεργασία των δεδομένων και αφορούν άλλα όργανα της ΕΕ [1].

2.13 Επίλογος

Η κατανόηση των άρθρων του κανονισμού αλλά και των αναγκών που προκύπτουν επό αυτόν, είναι το πρώτο βήμα ώστε να επιτύχει μια εταιρεία την πλήρη συμμόρφωση με τον κανονισμό, αλλά και για να εφαρμοστούν οι κατάλληλες υλοποίησεις που θα συμβάλλουν στην δημιουργία ενός επιτυχημένου πλάνου επιχειρησιακής συνέχειας και επανάκαμψης (BCP /DRP).

Στο επόμενο κεφάλαιο θα παρουσιαστούν εκτενώς οι δράσεις που πρέπει να εφαρμοστούν, λαμβάνοντας υπόψη τον κανονισμό για την προστασία των προσωπικών δεδομένων (GDPR), ώστε να δημιουργηθεί ένα επιτυχημένο σχέδιο επιχειρησιακής συνέχειας και επανάκαμψης (BCP / DRP). Οι περιοχές ελέγχου δημιουργήθηκαν αποκλειστικά λαμβάνοντας υπόψη τις απαιτήσεις του κανονισμού και διαμορφώθηκαν με τέτοιο τρόπο ώστε μια εταιρεία να μπορεί να δημιουργήσει ένα ολοκληρωμένο πλάνο (BCP / DRP). Επι της ούσίας με την ανάλυση των περιοχών ελέγχου αποδεικνύεται ότι μια εταιρεία μπορεί να επιτύχει την δημιουργία ενός πλάνου επιχειρησιακής συνέχειας και επανάκαμψης στηριζόμενη στα άρθρα του κανονισμού (GDPR).

Κεφάλαιο 3

ΓΚΠΔ και Επιχειρησιακή Συνέχεια

Στο κεφάλαιο αυτό θα αναλυθούν όλα εκείνα τα μέτρα που πρέπει να υλοποιηθούν από μια εταιρεία ή έναν οργανισμό βασισμένοι στους άρθρα και τους ελέγχους που προβλέπονται από τον κανονισμό για την υλοποίηση ενός επιτυχημένου BCP/DRP. Επιπλέον θα γίνουν αναφορές σε άλλα πρότυπα όπως ISO 27001, τα οποία συμπληρωματικά με τον καινούργιο κανονισμό συμβάλλουν στην διαμόρφωση κουλτούρας ασφάλειας σε έναν οργανισμό.

Οι συνεχόμενες τεχνολογικές εξελίξεις αλλά και τα αυξημένα ποσοστά κυβερνοεπιθέσεων καθιστούν από μόνα τους τον τομέα της ασφάλειας σημαντικό για έναν οργανισμό και στα πλαίσια αυτού θα πρέπει να ληφθούν όλα εκείνα τα κατάλληλα μέτρα που θα θωρακίσουν έναν οργανισμό ώστε αφενός να επανέλθει το γρηγορότερο δυνατό σε λειτουργεία αλλά και με το μικρότερο κόστος. Σαφέστατα, η υιοθέτηση κουλτούρας ασφάλειας σε έναν οργανισμό είναι μια χρονοβόρα διαδικασία απαρτιζόμενη από πολλά στάδια, αλλά και από τεχνολογικά αλλά και διοικητικά μέτρα. Σύμφωνα με έρευνες η παραβίαση δεδομένων, η οποία έχει πολλά παρακλάδια και μπορεί να γίνει με ποικίλους τρόπους των οποίων αιτία είναι τόσο η έλλειψη τεχνολογικών υποδομών αλλά και τεχνογνωσίας όσο και έλλειψη ενημερότητας των εμπλεκομένων, αποτελεί σήμερα παράγοντα υψηλού ρίσκου. Ενδεικτικά αναφέρονται παρακάτω πέντε (5) τύποι «ευπαθειών» [4] που μπορεί να αποτελέσουν αίτια

παραβίασης δεδομένων και η έλλειψη λήψης μέτρων μπορεί να αποβεί μοιραία για έναν οργανισμό/εταιρεία :

- Ευπάθειες που αφορούν παλιό λογισμικό που δεν έχουν ληφθεί οι κατάλληλες ενημερώσεις ή τα κατάλληλα μέτρα : Τα τρωτά σημεία χωρίς διορθώσεις (software patches) μπορεί να αποτελέσουν στους 'χάκερ' πέρασμα στις ευαίσθητές πληροφορίες μιας εταιρείας ή ενός οργανισμού.
- Ανθρώπινο λάθος: Το ανθρώπινο λάθος αποτελούσε πάντα μια απ' τις μεγαλύτερες ευπάθειες. Σύμφωνα με στατιστικά στοιχεία μιας μελέτης CompTIA το ανθρώπινο λάθος αντιπροσωπεύει το 52% των βασικών αιτιών των παραβιάσεων της ασφάλειας. Στα πλαίσια των ανθρώπινων σφαλμάτων συγκαταλέγονται : η χρήση αδύναμων κωδικών, η αποστολή ευαίσθητων πληροφοριών σε λάθος παραλήπτες, απάτες διαδικτυακού 'ψαρέματος' (phising) κτλ
- Κακόβουλο λογισμικό: η έλλειψη μέτρων ασφαλείας που αποτρέπουν την εγκατάσταση ή τη λήψη ή την εντόπιση και καταπολέμηση κακόβουλου λογισμικού, εντάσσουν το κακόβουλο λογισμικό (malware) σε μια απειλή που απασχολεί όχι μόνο τα οικιακά δίκτυα αλλά και τα δίκτυα επιχειρήσεων/οργανισμών.
- Κακή χρήση: κακή χρήση θεωρείται η σκόπιμη κατάχρηση των συστημάτων μιας εταιρείας/οργανισμού και κατ' επέκταση προσωπικών δεδομένων ή εμπιστευτικών δεδομένων από έναν εξουσιοδοτημένο χρήστη (πχ. εκτελών την επεξεργασία), συνήθως για προσωπικό όφελος. Η ελεγχόμενη πρόσβαση σε αυτό το σημείο ή η ελαχιστοποίηση των δεδομένων μπορεί να ελαχιστοποιήσει τον κίνδυνο σε τέτοιες περιπτώσεις αλλά σε κάθε περίπτωση η συγκεκριμένη αιτία είναι από αυτές που μπορούν δύσκολα να καταπολεμηθούν.
- Φυσική κλοπή μίας συσκευής μεταφοράς δεδομένων: Η φυσική κλοπή αποτελεί επίσης έναν σημαντικό παράγοντα ειδικά στην σύγχρονη εποχή όπου οι περισσότερες εταιρείες στα πλαίσια της αποτελεσματικότητας αλλά και της εύκολης προσβασιμότητας παρέχουν στους χρήστες τους φορητούς υπολογιστές smart phones, tablets κτλ. Σίγουρα η φυσική κλοπή μπορεί να λάβει χώρα και στις φυσικές εγκαταστάσεις μιας εταιρείας, κάτι όμως που είναι πιο δύσκολο λαμβάνοντας υπόψιν τα μέτρα ασφαλείας όπως κάμερες, συστήματα συναγερμού, προσωπικό φύλαξης κτλ. Οι κινητές συσκευές είναι αυτές έχουν την

μεγαλύτερη επικινδυνότητα. Σε αυτές τις περιπτώσεις μέτρα όπως ισχυροί κωδικοί πρόσβασης (συμπεριλαμβανομένου και bios passwords) αλλά και η κρυπτογράφηση κωδικών και αρχείων.

Όλοι οι παραπάνω παράγοντες αποτελούν αντικείμενο λήψης μέτρων τόσο στα πλαίσια του κανονισμού που αφορά τα προσωπικά δεδομένα (GDPR) αλλά και στα πλαίσια ενός ολοκληρωμένου πλάνου επιχειρησιακής συνέχειας (BCP/DRP).

3.1 Πλάνο Επιχειρησιακής Συνέχειας (Business Continuity Plan)

Η επιχειρησιακή συνέχεια (Business Continuity) [5] και κατ' επέκταση το σχέδιο επιχειρησιακής συνέχειας (Business Continuity Plan - BCP) είναι η διαδικασία σύστασης ενός συστήματος που διασφαλίζει την πρόληψη αλλά και την ανάκτηση το επιχειρησιακών λειτουργιών και δομών από μια πιθανή απειλή ή καταστροφή. Το εν λόγω σχέδιο διασφαλίζει την προστασία τόσο των περιουσιακών στοιχείων μιας επιχείρησης όσο και των φυσικών προσώπων που πλαισιώνουν αυτή.

Στα πλαίσια του BCP συμπεριλαμβάνονται όλοι οι δυνητικοί κίνδυνοι που μπορεί να επηρεάσουν τις δραστηριότητες μιας εταιρείας αλλά και τα μέτρα πρόληψης ή αντιμετώπισης αυτών, καθιστώντας την ύπαρξη του ζωτικής σημασίας για έναν οργανισμό. Το BCP αποτελεί σχέδιο στρατηγικής σημασίας για έναν οργανισμό και αποτελεί αναγκαιότητα για όλες τις επιχειρήσεις και τους οργανισμούς.

Ένα BCP θα πρέπει να περιλαμβάνει κατ' ελάχιστο:

- τον καθορισμό των κινδύνων που μπορεί να προκύψουν, όπως κυβερνοεπιθέσεις, παραβιάσεις δεδομένων, φυσικές καταστροφές, φυσική κλοπή κτλ.,
- τον τρόπο με τον οποίο οι κίνδυνοι αυτοί μπορεί να επηρεάσουν τις λειτουργίες μιας επιχείρησης,
- τις διασφαλίσεις, τις πολιτικές και τις διαδικασίες που πρέπει να εφαρμοστούν για τον μετριασμό των κινδύνων αυτών,
- έλεγχος διαδικασιών (testing) ελέγχου,
- επανέλεγχος των διαδικασιών και συχνές ενημερώσεις.

Το BCP αποτελεί ένα σημαντικό κομμάτι μιας επιχείρησης καθώς οι δυνητικές απειλές μπορεί να σημαίνουν κόστος και κατ' επέκταση πτώση της κερδοφορίας καθώς σε πολλές περιπτώσεις οι ασφαλίσεις δεν καλύπτουν το κόστος αυτό. Επίσης εάν ένας οργανισμός δεν έχει λάβει όλα εκείνα τα μέτρα που διασφαλίζουν την διαφύλαξη της επιχειρησιακής του συνέχειας, η ευθύνη μετατίθεται στον ίδιο τον οργανισμό.

Τα βασικά βήματα που πρέπει να ακολουθήσεις μια επιχείρηση για την υλοποίηση ενός BCP περιγράφονται παρακάτω:

- Ανάλυση Επιχειρηματικών Επιπτώσεων (Business Impact Analysis - BIA): αφορά τον εντοπισμό των λειτουργιών οι οποίες πρέπει να ανακάμψουν σε σύντομο χρονικό διάστημα ώστε η επιχείρησή να είναι πάλι λειτουργική,
- Ανάκτηση: προσδιορισμός των βημάτων για την ανάκτηση των κρίσιμων επιχειρηματικών λειτουργιών,
- Ομάδα Επιχειρησιακής Συνέχειας: αποτελείται από ανθρώπους οι οποίοι είναι υπεύθυνοι για τον σχεδιασμό του εν λόγω πλάνου αλλά και τον συντονισμό των ενεργειών σε περίπτωση οποιουδήποτε συμβάντος,
- Εκπαίδευση: εκπαίδευση της ομάδας και έλεγχος ετοιμότητας του εν λόγω σχεδίου.

Στα πλαίσια της οργάνωσης σημαντικό είναι να συλλεχθούν όλες οι απαραίτητες πληροφορίες επικοινωνίας τόσο των άμεσα εμπλεκόμενων αλλά και των εξωτερικών πόρων εκτός εταιρείας (πχ. προμηθευτές, εξωτερικοί συνεργάτες, πάροχοι κτλ). Επίσης σημαντικό κομμάτι αποτελεί και ο κατάλογος των πόρων της επιχείρησης που χρήζουν παρακολούθηση στα πλαίσια της επιχειρησιακής συνέχειας.

Σημαντικό στάδιο αποτελεί η φάση Testing του BCP, όπου προσομοιώνονται συνθήκες κρίσης και δοκιμάζεται η αποτελεσματικότατά του πλάνου, η ετοιμότητα της επιχείρησης αλλά και τα τρωτά σημεία που έχουν διαφύγει από τον αρχικό σχεδιασμό. Αυτό σημαίνει ότι το εν λόγω πλάνο θα πρέπει να αναθεωρείται και να προσαρμόζεται συνεχώς, λαμβάνοντας υπόψη τόσο της επιχειρησιακές ανάγκες αλλά και τις γενικότερες εξωγενείς συνθήκες, όπως καινούργια είδη επιθέσεων, η ένταξη νέων κανονισμών που επηρεάζουν τον τομέα των επιχειρήσεων, όπως ο γενικός κανονισμός προσωπικών δεδομένων (GDPR).

Το BCP αποτελεί μια επιχειρησιακή διαδικασία από μόνο του και αφορά ολόκληρο τον οργανισμό γι' αυτό είναι σημαντικό να επικοινωνείτε και να υπάρχει επαγρύπνηση και

ενημέρωση όλων των εμπλεκομένων μιας επιχείρησης. Η ενημέρωση του προσωπικού και η συνεχείς εκπαίδευση του συνδράμει σημαντικά στην εδραίωση κουλτούρας επιχειρησιακής συνέχειας σε έναν οργανισμό, στον μετριασμό των κινδύνων αλλά και στην γρήγορη επανάκαμψη των λειτουργιών του. Στα πλαίσια του μετριασμού που προαναφέραμε θα πρέπει να σημειωθεί ότι ένας εκπαιδευμένος υπάλληλος μπορεί να αποφύγει κινδύνους (πχ. phishing emails) που απειλούν την επιχειρησιακή συνέχεια μιας εταιρείας, οπότε το κομμάτι της επαγρύπνησης του προσωπικού θα πρέπει να είναι συνεχές και συγχρονισμένο με τις εξελίξεις που συμβαίνουν σε παγκόσμιο επίπεδο.

3.2 Πλάνο Ανάκτησης σε Περίπτωση Καταστροφής (Disaster Recovery Plan)

Το σχέδιο αποκατάστασης λειτουργίας (Disaster Recovery Plan - DRP) είναι συνδεδεμένο και λειτουργεί σε συνεργασία με το Business Continuity Plan. Επί της ουσίας είναι μια τεκμηριωμένη διαδικασία [6] ή ένα σύνολο από επιμέρους διαδικασίες που πρέπει να ακολουθηθούν στα πλαίσια της επανάκαμψης ενός οργανισμού από μια καταστροφή. Η τεκμηρίωση αυτή είναι γραπτή και συγκεντρώνει όλες τις ενέργειες που πρέπει να λαμβάνονται υπόψη πριν, κατά την διάρκεια και μετά από μια καταστροφή. Με τον όρο καταστροφή εννοούμε όλες εκείνες τις μη-προγραμματισμένες ενέργειες που μπορεί να προκύψουν σε έναν οργανισμό και να επιφέρουν διακοπή των κανονικών επιχειρησιακών διαδικασιών, όπως πληροφοριακά συστήματα, δίκτυα, εξοπλισμό σε επίπεδο Hardware και Software αλλά και θέματα που αφορούν τόσο την απώλεια δεδομένων αλλά και την παραβίαση αυτών κτλ.

Ένα DRP θα πρέπει να περιλαμβάνει τα παρακάτω στοιχεία [6] :

- Χρόνος απόκρισης σε συμβάντα,
- Συνθήκες που θα ενεργοποιούσαν το DRP,
- Διαδικασίες που πρέπει να ακολουθηθούν μέχρι την αποκατάσταση των υποδομών,
- Ρόλους και αρμοδιότητες,
- Διαδικασίας για το backup των δεδομένων αλλά και για την ασφαλή πρόσβαση σε αυτά,
- Διάγραμμα δικτύων και συνδέσεων,

- Λίστα προσωπικού και τις προσβάσεις που έχει ο καθένας τόσο σε φυσικό επίπεδο (πχ κτίριο, computer room κτλ) αλλά και προσβάσεις σε συστήματα,
- Διαδικασία επικοινωνίας και πλήρης λίστα προσωπικού για επικοινωνία σε περιπτώσεις έκτακτης ανάγκης τόσο ανθρώπων μέσα στην εταιρεία αλλά και συνεργατών (πχ. πάροχοι δικτύου, πωλητές, συμβούλων κτλ),
- Λεπτομερής περιγραφές όλων των στοιχείων διαμόρφωσης που απαιτούν τα συστήματα (configuration information),
- Πλάνο ασκήσεων DRP,
- Χρόνοι αποκατάστασης των δεδομένων και των συστημάτων,
- Συχνότητα backup δεδομένων,
- Μέτρα ασφάλειας για την αποθήκευση των backup, των αδειών software, και των πληροφοριών διαμόρφωσης (system configuration),
- Πλήρης λίστα των ανθρώπων που είναι υπεύθυνοι για την εκτέλεση, τη δοκιμή, την αποθήκευση και την αποκατάσταση των αντιγράφων ασφαλείας.

3.3 Ανάλυση Αντικτύπου Επιχειρησιακής Συνέχειας (Business Continuity Impact Analysis)

Η ανάλυση αντίκτυπου επιχειρησιακής συνέχειας (Business Impact Analysis - BIA) είναι ένα σημαντικό [5] μέρος της ανάπτυξης ενός επιτυχημένου Business Continuity Plan και προσδιορίζει τα αποτελέσματα που θα προκύψουν σε περίπτωση διακοπής επιχειρησιακών λειτουργιών και διαδικασιών. Παρέχονται επίσης πληροφορίες σχετικά με την λήψη αποφάσεων σχετικά με τις προτεραιότητες που πρέπει να δοθούν αλλά και τις στρατηγικές ανάκτησης που πρέπει να ακολουθηθούν.

Στα πλαίσια μιας επιτυχημένης ανάλυσης αντικτύπου θα πρέπει να αναλυθούν κατ' ελάχιστο οι παρακάτω μεταβλητές:

- Χρονική Στιγμή: ώρα της ημέρας, εποχή του χρόνου κτλ που μπορεί να προκύψει μια καταστροφή,
- Διάρκεια διακοπής: ορισμός διάρκειας κατά την οποία μπορεί να αρχίζουν να προκύπτουν επιχειρησιακές συνέπειες,
- Λειτουργικό αντίκτυπο: επιχειρησιακό αντίκτυπο που να προκύψει κατά την απώλεια των επιχειρησιακών λειτουργιών και διαδικασιών,

- Οικονομικό αντίκτυπο: οικονομικές επιπτώσεις που μπορεί να προκύψουν κατά την απώλεια των επιχειρησιακών λειτουργιών και διαδικασιών.

Στα πλαίσια της BIA θα μπορούσαμε να εντάξουμε και την εκτίμηση αντικτύπου (Data Protection Impact Assessment - DPIA) που προβλέπεται από το άρθρο 35 του κανονισμού και ειδικότερα όσα προβλέπονται από τη παράγραφο 7α – 7β. Συμπληρωματικά η συγκεκριμένη ανάλυση θα μπορούσε να επεκταθεί και να αποτελέσει έναν πληρέστερο 'οδηγό' καλύπτοντας και άλλα άρθρα του κανονισμού, τα οποία είναι σημαντικά και θα πρέπει να λαμβάνονται υπόψη στα πλαίσια της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, όπως το άρθρο 6, άρθρο 9, άρθρο 14, άρθρο 17 και άρθρο 47 2β-2δ. Θα πρέπει επίσης να σημειωθεί σε αυτό το σημείο ότι σε περίπτωση που δεν ληφθούν τα σχετικά μέτρα αυτό θα μπορούσε να αποτελέσει υψηλό ρίσκο για μια εταιρεία. Στα πλαίσια λοιπόν της εκτίμησης αντικτύπου θα πρέπει να αναλυθούν οι παρακάτω περιοχές:

- Κατηγορίες δεδομένων (πχ. δεδομένα εργαζομένων) (άρθρο 47, παράγραφος 2β) συμπεριλαμβανομένων των ειδικών κατηγοριών που προβλέπονται από τον κανονισμό (πχ. βιομετρικά δεδομένα, δεδομένα υγείας),
- Στοιχεία δεδομένων (πχ. όνομα, επώνυμο, ηλικία κτλ) τηρώντας την αρχή ελαχιστοποίησης ανά σκοπό όπως προβλέπεται από το άρθρο 47 παράγραφος 2δ,
- Πηγή των δεδομένων αυτών (σ.σ. σε περίπτωση που προέρχονται από τρίτους θα πρέπει να καλύπτεται η διαδικασία που αναφέρεται στο άρθρο 14 όπως επίσης και ο υπεύθυνος επεξεργασίας από τον οποίο προήλθαν τα δεδομένων),
- Πράξεις επεξεργασίας,
- Σκοπός επεξεργασίας για κάθε προβλεπόμενη πράξη τηρώντας την αρχή περιορισμού του σκοπού όπως προβλέπεται από το άρθρο 47 παράγραφος 2β και 2δ,
- Νομική βάση σε σχέση με τον σκοπό επεξεργασίας (άρθρο 6 για τις απλές κατηγορίες δεδομένων και άρθρο 9 για τις ειδικές κατηγορίες δεδομένων),
- Περίοδος διατήρησης των δεδομένων [τόσο στα πραγματικά συστήματα όσο και στο backup που διατηρεί μια εταιρεία] (άρθρο 17),
- Εκτίμηση του κινδύνου,
- Μέτρα αντιμετώπισης των κινδύνων.

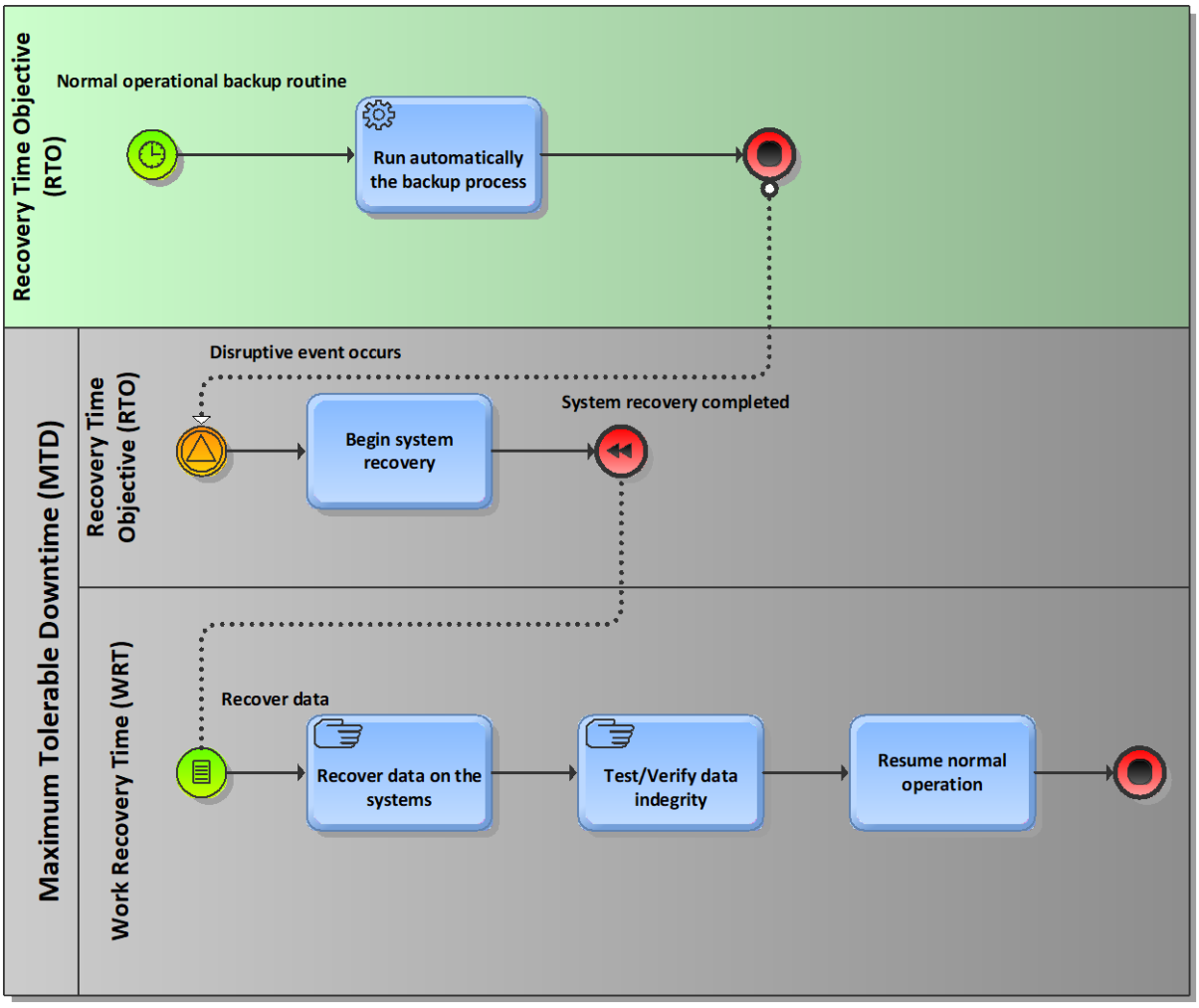
Η Business Impact Analysis και η εκτίμηση αντικτύπου (Data protection impact assessment and prior consultation) που απαιτείται από τον κανονισμό θα μπορούσαν να λειτουργήσουν συνεργατικά και αλληλεξαρτώμενα για την επίτευξη τόσο των σκοπών που πρεσβεύει ο κανονισμός προστασίας των προσωπικών δεδομένων αλλά και για την διασφάλιση τόσο της ασφαλούς επεξεργασίας αλλά και της προστασίας των δεδομένων αυτών από πάσης φύσεως κινδύνους. Η ενημέρωση τους θα πρέπει να είναι συνεχής προσαρμοσμένη πάντα στις απαιτήσεις στις εταιρείες αλλά και στις τεχνολογικές εξελίξεις.

Με την ολοκλήρωση της BIA μπορούν να προκύψουν σημαντικά αποτελέσματα που μπορούν να βοηθήσουν στον καθορισμό των παρακάτω απαιτήσεις που είναι σημαντικές στα πλαίσια αποκατάστασης των επιχειρησιακών διαδικασιών (**Εικόνα 2**) [7]:

- **Recovery Point Objective (RPO):** είναι το εύρος ή το ποσό ή το ποσοστό της απώλειας δεδομένων που μπορεί να γίνει ανεκτό από τα επιχειρησιακά πληροφοριακά συστήματα. Ο συγκεκριμένος δείκτης έγκειται στην στρατηγική αντιγράφων ασφαλείας που έχει μια εταιρεία, ορισμένες εταιρείες εκτελούν αντίγραφα ασφαλείας σε πραγματικό χρόνο, κάποιες άλλες εκτελούν ωριαίες ή καθημερινές αντιγραφές και μερικές εκτελούν εβδομαδιαία αντίγραφα ασφαλείας. Στην περίπτωση των εβδομαδιαίων αντίγραφων ασφαλείας, σημαίνει ότι μια εταιρεία θα μπορούσε να ανεχτεί την απώλεια δεδομένων αξίας μιας εβδομάδας. Εάν τα αντίγραφα ασφαλείας πραγματοποιούνται κάθε Σάββατο βράδυ για παράδειγμα και ένα σύστημα αποτυγχάνει το απόγευμα του Σαββάτου, έχουν χαθεί τα δεδομένα ολόκληρης της εβδομάδας. Το RPO βασίζεται τόσο στις τρέχουσες διαδικασίες λειτουργίας όσο και στις εκτιμήσει για το τι μπορεί να συμβεί σε περίπτωση κάποιου συμβάντος ή μιας καταστροφής. Ο δείκτης RPO διασφαλίζει ότι οι διαδικασίες ανάκτησης σε περίπτωση καταστροφής θα είναι ικανές να επαναφέρουν την επιχείρηση σε ένα σημείο που θα πραγματοποιείτε χωρίς μεταβολές ή μη αναστρέψιμες απώλειες η επιχειρησιακή συνέχεια [8].
- **Recovery Time Objective (RTO):** ορίζεται ο διαθέσιμος χρόνος για την ανάκτηση των συστημάτων και λοιπών πόρων [8].
- **Work Recovery Time (WRT):** είναι ο χρόνος εργασίας για τον έλεγχο των κρίσιμων επιχειρησιακών λειτουργιών (hardware, software, configuration) μετά

την επαναφορά τους. Αυτό μπορεί να είναι κάποιοι έλεγχοι που πραγματοποιούνται απ' τους administrators στις βάσεις δεδομένων, ή στον έλεγχο σωστής λειτουργίας των συστημάτων. Ο συγκεκριμένος δείκτης αποτελεί το δεύτερο μέρος που χρειάζεται για τον υπολογισμό του δείκτη MTD [7] [8].

- **Maximum Tolerable Downtime (MTD):** είναι ο μέγιστος χρόνος που μια επιχείρηση μπορεί να ανεχθεί την απουσία ή τη μη διαθεσιμότητα συγκεκριμένης επιχειρηματικής λειτουργίας. Η κάθε επιχειρηματική λειτουργία έχει και διαφορετικό MTD. Όσο πιο κρίσιμη είναι μια επιχειρηματική λειτουργία τόσο μικρότερης διάρκειας MTD έχει. Η δείκτης MTD αποτελείται από δύο (2) στοιχεία, τον χρόνο ανάκτησης των συστημάτων και τον χρόνο ανάκτησης της εργασίας (MTD = RTO + WRT) [8].



Εικόνα 2. RTO και MTD διαδικασία

Σε αυτό το σημείο θα πρέπει να σημειωθεί ότι με τους δείκτες που προαναφέρθηκαν καλύπτονται όσα αναφέρονται στο άρθρο 32 του κανονισμού και συγκεκριμένα στην παράγραφο 1β – 1δ. Πιο συγκεκριμένα, με τις συγκεκριμένες μετρικές σε συνδυασμό με

όλα τα τεχνικά μέσα, διασφαλίζεται η διαθεσιμότητα και η αξιοπιστία των συστημάτων και των επιχειρησιακών υπηρεσιών που πλαισιώνουν την επεξεργασία των δεδομένων σε συνεχή βάση. Επιπροσθέτως καλύπτονται οι διαδικασίες και οι τεχνικές που απαιτούνται για την αποκατάσταση της διαθεσιμότητας αλλά και της πρόσβασης σε περίπτωση κάποιου συμβάντος. Οι εν λόγω δείκτες επίσης θα πρέπει να σημειωθεί ότι χρησιμεύουν και σαν εργαλεία αξιολόγησης των τεχνικών και των οργανωτικών μέτρων μιας εταιρείας κάτι που επίσης προβλέπεται στο άρθρο 32.

3.4 Διαχείριση / Αξιολόγηση Ρίσκων

Η αξιολόγηση των ρίσκων είναι μια σημαντική διαδικασία για κάθε οργανισμό και δρα συμπληρωματικά και σε ένα ανώτερο επίπεδο από την BIA και DPIA προαναφέραμε. Η διαχείριση των ρίσκων πέραν των μεμονωμένων αξιολογήσεων που μπορεί να γίνονται σε περιστατικά μέσω της BIA και DPIA στα πλαίσια της επιχειρησιακής συνέχειας θα πρέπει να γίνεται σε εταιρικό επίπεδο στα πλαίσια των τεχνολογικών (πχ. Υιοθέτηση νέων συστημάτων που ενδυναμώνουν την ασφάλεια του οργανισμού) αλλά και διαχειριστικών επενδύσεων (πχ. υιοθέτηση νέων προτύπων που προωθούν την κουλτούρα ασφάλειας σε έναν οργανισμό) που γίνονται στα πλαίσια της επιχειρησιακής συνέχειας. Σύμφωνα με το άρθρο 32 παράγραφος 2 του κανονισμού θα πρέπει να λαμβάνονται υπόψη οι κίνδυνοι που έχουν να κάνουν με την επεξεργασία των δεδομένων. Σε αυτό το σημείο θα πρέπει να σημειώσουμε ότι η διαχείριση και αξιολόγηση των ρίσκων θα πρέπει να δρα συμπληρωματικά και λαμβάνοντας υπόψη τα αποτελέσματα που προκύπτουν από την BIA και την DPIA ώστε να μπορούν να λαμβάνονται οι σωστές αποφάσεις, αλλά και να γίνονται οι σωστές επενδύσεις που προάγουν την διασφάλιση της επιχειρησιακής συνέχειας. Απαραίτητη και πρέπει να επισημαίνεται πάντα είναι η διαχείριση ρίσκων για όλες της κατηγορίες επεξεργασίας.

Ρίσκο ειδικά στον τομέα του IT είναι οποιαδήποτε απειλή που μπορεί να καταστήσει μη διαθέσιμα ή να καταστρέψει ολοσχερώς τα δεδομένα μιας επιχείρησης, τα συστήματα και τις επιχειρησιακές διαδικασίες. Είναι ο κίνδυνος που συνδέεται με τη χρήση, την ιδιοκτησία, τη λειτουργία, τη συμμετοχή, την επιρροή και την υιοθέτηση των πληροφοριακών συστημάτων μέσα σε έναν οργανισμό [9]. Στον τομέα της πληροφορικής υπάρχουν διαφορετικοί τύποι ρίσκων, οι οποίοι θα πρέπει να αξιολογούνται διαφορετικά και να λαμβάνονται τα αντίστοιχα μέτρα που

ελαχιστοποιούν την πιθανότητα να συμβούν. Παρακάτω παραθέτουμε μερικές από αυτές τις κατηγορίες [9]:

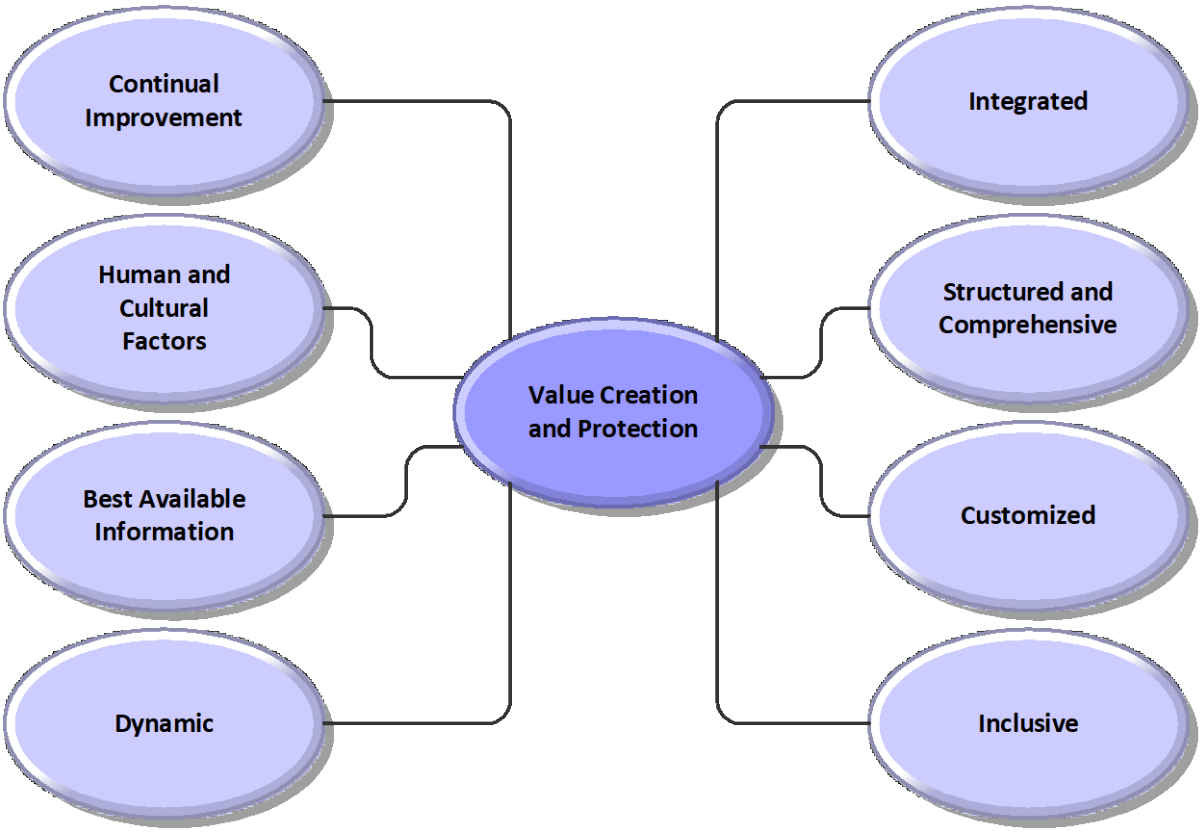
I. Ασφάλεια: για παράδειγμα ελλιπή μέτρα σε σχέση με την εξουσιοδότηση πρόσβασης στα επιχειρησιακά δεδομένα,
II. Διαθεσιμότητα: αδυναμία πρόσβασης στα δεδομένα ή τις υπηρεσίες μιας εταιρείες, είτε λόγω τεχνικών προβλημάτων, είτε λόγω έλλειψης οργανωτικών μέτρων που προάγουν την διαθεσιμότητα αυτών,
III. Παραγωγικότητα: για παράδειγμα μειωμένη παραγωγικότητα λόγω αργού δικτύου ή απαρχαιωμένων συστημάτων,
IV. Μη Συμμόρφωση σε κανονισμούς και νόμους - π.χ. μη τήρηση νόμων και κανονισμών (π.χ. GDPR).

Μια μεθοδολογία εκτίμησης κινδύνου περιλαμβάνει συνήθως [10]:

- την διαδικασία αξιολόγησης κινδύνου,
- καθορισμό των όρων σε σχέση με τους παράγοντες κινδύνου και τις σχέσεις μεταξύ τους,
- τρόπος αξιολόγησης (π.χ. ποσοτικός, ποιοτικός κτλ.), προσδιορίζοντας τους παράγοντες που πρέπει να ληφθούν υπόψη,
- ο τρόπος που θα αναλυθούν τα ρίσκα και σε τι να δοθεί περισσότερη βαρύτητα.

Σύμφωνα με το ISO 31000 – 2018 η διαχείριση των ρίσκων βασίζεται σε 3 παράγοντες στις αρχές (principles), το πλαίσιο (framework) και τις διαδικασίες (processes) [11].

Παρακάτω θα γίνει μια διαγραμματική προσέγγιση των αρχών (principles) (**Εικόνα 3**), οι οποίες συμπίπτουν στο μεγαλύτερο μέρος τους με τις αρχές που προβλέπονται από τον κανονισμό σε σχέση με την προστασία των προσωπικών δεδομένων καθώς υπάρχει άμεση συνάφια για παράδειγμα σε πολλά σημεία με τους κώδικες δεοντολογίας (και ότι πλαισιώνει αυτούς) που περιγράφονται στο άρθρο 40, 41 αλλά και στο κομμάτι της πιστοποίησης στο άρθρο 42:



Εικόνα 3. Αρχές (principles) σύμφωνα με το ISO 31000:2018 [11]

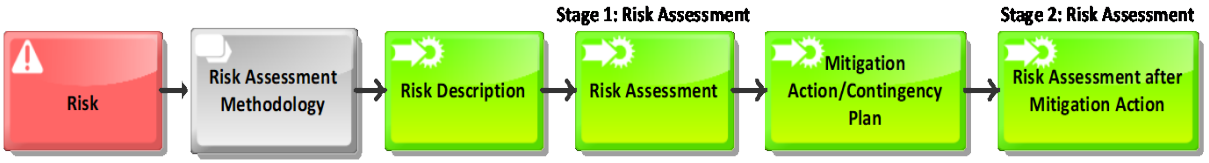
Παρακάτω περιγράφεται μια προτεινόμενη μεθοδολογία (**Πίνακας 5**) ανάλυσης των ρίσκων η οποία όπως αναλύεται διαγραμματικά (**Εικόνα 4**) χωρίζεται σε δύο (2) στάδια αξιολόγησης πριν το σχέδιο μετριασμού αλλά και μετά. Επί της ουσίας σύμφωνα με την προτεινόμενη μέθοδο με την εμφάνιση του ρίσκου ή την δυνητική εμφάνιση του ρίσκου ενεργοποιείται η διαδικασία αξιολόγησής του και ακολουθεί:

V. η περιγραφή και η ανάλυση των επιπτώσεων του ρίσκου,
VI. η αξιολόγηση του ρίσκου πριν ληφθούν τα κατάλληλα μέτρα μετριασμού,
VII. και η επαναξιολόγηση του ρίσκου εφόσον ληφθούν υπόψη τα μέτρα που λήφθηκαν για τον μετριασμό του.

Ένα ρίσκο δεν σταματά ποτέ να υπάρχει ακόμα και αν ληφθούν όλα τα κατάλληλα μέτρα καθώς υπάρχει πάντα η πιθανότητα να προκύψει. Με τα μέτρα μετριασμού ελαχιστοποιούμε την πιθανότητα να συμβεί το ρίσκο αυτό ή μετριάζουμε κατά κάποιο τρόπο τις επιπτώσεις. Στην εν λόγω μεθοδολογία θα μπορούσε να προστεθεί και το κόστος αν προκύψει μια καταστροφή και το κόστος των μέτρων μετριασμού για να έχουμε μια πιο ολοκληρωμένη αξιολόγηση. Σε κάποιες περιπτώσεις το κόστος για την

λήψη μέτρων μετριασμού σε σχέση με το κόστος που θα προκύψει αν επέλθει μια καταστροφή είναι μεγαλύτερο, οπότε ένας οργανισμός αξιολογεί ότι πρέπει να αναλάβει το ρίσκο και να μην προβεί σε ασύμφορες λύσεις μετριασμού.

Στην περίπτωση για παράδειγμα του κανονισμού για τα προσωπικά δεδομένα κάποιες εταιρείες που δεν διέθεταν τα κατάλληλα μέτρα ασφάλειας (πχ. πιστοποίηση ISO 27001, ή ISO 22301) αναγκάστηκαν να επαναξιολογήσουν τις τεχνολογικές υποδομές τους τόσο σε τεχνικό όσο και οργανωτικό επίπεδο, ώστε να διασφαλίσουν την συμμόρφωση τους με τον κανονισμό καθώς τα πρόστιμα τόσο της μη-συμμόρφωσης όσο και της παραβίασης δεδομένων προσωπικού χαρακτήρα είναι ασύμφορα.

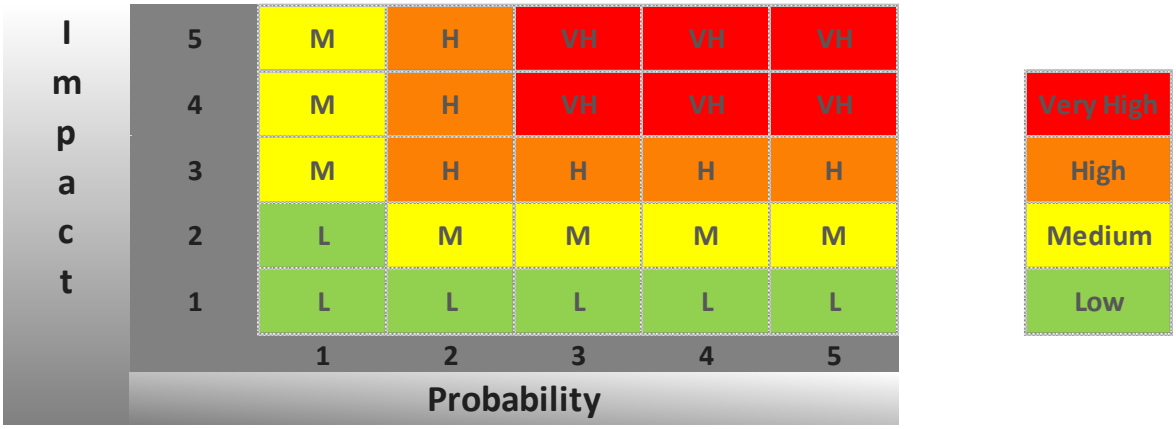


Εικόνα 4. Διαδικασία διαχείρισης ρίσκων

Περιγραφή Τιμής	Επεξήγηση
Κατηγορία Ρίσκου	Κατηγοριοποιούμε τα ρίσκα/κινδύνους/ευπάθειες ανάλογα το είδος τους.
Περιγραφή Ρίσκου	Περιγραφή Ρίσκου
Ημ/νία	Ημ/νία Καταγραφής
Πηγή Ρίσκου	Πηγή απ' όπου προήλθε το ρίσκο.
Κτήτορας (owner)	Τμήμα ή εκπρόσωπος, όπου ανήκει το ρίσκο.
Επιπτώσεις του ρίσκου	Επιπτώσεις
Πιθανότητα	Πιθανότητα (**Εικόνα 5**): • 1. Πολύ Μικρή = Σχεδόν απίθανο . **(0-20%)** • 2. Μικρή = Μικρή πιθανότητα να συμβεί.**(20-40%)** • 3. Μεσαία= Μεσαία πιθανότητα να συμβεί.**(40-60%)** • 4. Υψηλή = Υψηλή πιθανότητα να συμβεί. **(60-80%)** • 5. Πολύ Υψηλή = Πολύ υψηλή πιθανότητα να συμβεί. **(80-100%)**
Επίπτωση	Επίπτωση (**Εικόνα 5**): •1. Πολύ Μικρή = Πολύ μικρή επίπτωση. **(0-20%)** • 2. Μικρή = Μικρή επίπτωση. **(20-40%)** • 3. Μεσαία= Μεσαία επίπτωση. **(40-60%)** • 4. Υψηλή = Υψηλές/Μεγάλες επιπτώσεις. **(60-80%)** • 5. Πολύ Υψηλή = Πολύ υψηλές/Πολύ μεγάλες επιπτώσεις. **(80-100%)**

Προβολή Κινδύνου (Πιθανότητα*Επίπτωση)	Προβολή Κινδύνου (**Εικόνα 5**)
Σχέδιο Μετριασμού	Σχέδιο Μετριασμού
Σχέδιο Έκτακτης Ανάγκης	Σχέδιο Έκτακτης Ανάγκης
Κατάσταση	Open or Discontinued
Πιθανότητα	Πιθανότητα (**Εικόνα 5**): • 1. Πολύ Μικρή = Σχεδόν απίθανο . **(0-20%)** • 2. Μικρή = Μικρή πιθανότητα να συμβεί.**(20-40%)** • 3. Μεσαία= Μεσαία πιθανότητα να συμβεί.**(40-60%)** • 4. Υψηλή = Υψηλή πιθανότητα να συμβεί. **(60-80%)** • 5. Πολύ Υψηλή = Πολύ υψηλή πιθανότητα να συμβεί. **(80-100%)**
Επίπτωση	Επίπτωση (**Εικόνα 5**): •1. Πολυ Μικρή = Πολύ μικρή επίπτωση. **(0-20%)** • 2. Μικρή = Μικρή επίπτωση. **(20-40%)** • 3. Μεσαία= Μεσαία επίπτωση. **(40-60%)** • 4. Υψηλή = Υψηλές/Μεγάλες επιπτώσεις. **(60-80%)** • 5. Πολύ Υψηλή = Πολύ υψηλές/Πολύ μεγάλες επιπτώσεις. **(80-100%)**
Προβολή Κινδύνου (Πιθανότητα*Επίπτωση)μετά τα σχέδια μετριασμού και έκτακτης ανάγκης	Προβολή Κινδύνου (έχοντας ακολουθήσει τα σχέδια Μετριασμού ή το σχέδιο έκτακτης ανάγκης) (**Εικόνα 5**)

Πίνακας 5. Μεθοδολογία ανάλυσης ρίσκων



Εικόνα 5. Risk Matrix [12]

3.5 Περιοχές Ελέγχου ΓΚΠΔ (GDPR)

Παρακάτω παρουσιάζονται επιλεκτικά οι περιοχές / άρθρα του GDPR που είτε επηρεάζουν της περιοχές ενός ήδη υπάρχοντος BCP/DRP είτε μπορούν να

χρησιμοποιηθούν για την δημιουργία / εφαρμογή ενός BCP/DRP από εταιρείες και οργανισμούς:

Περιοχή Ελέγχου 1 (C1)

Εμπλεκόμενα Άρθρα:

-Άρθρο 1 - Αντικείμενο και στόχοι

Δράσεις:

Θα πρέπει να γίνουν κατανοητά το αντικείμενο και οι στόχοι του κανονισμού ώστε να υλοποιηθούν αλλά και να εφαρμοστούν οι κατάλληλες δράσεις.

Περιοχή Ελέγχου 2 (C2)

Εμπλεκόμενα Άρθρα:

-Άρθρο 2 - Ουσιαστικό πεδίο εφαρμογής

Δράσεις:

Το ίδιο ισχύει και για το άρθρο 2 το οποίο θα πρέπει να κατανοηθεί ώστε οι δράσεις που θα υλοποιηθούν θα καλύπτουν τις απαιτήσεις του κανονισμού.

Περιοχή Ελέγχου 3 (C3)

Εμπλεκόμενα Άρθρα:

-Άρθρο 3 - Εδαφικό πεδίο εφαρμογής

Δράσεις:

Θα πρέπει να γίνει κατανοητό και να ληφθούν οι απαραίτητες δράσεις, ειδικά για εταιρείες πολυεθνικές και εταιρείες που έχουν εμπορικές και άλλου είδους συναλλαγές με εταιρείες εκτός Ευρωπαϊκής Ένωσης.

Περιοχή Ελέγχου 4 (C4)

Εμπλεκόμενα Άρθρα:

-Άρθρο 4 - Ορισμοί

Δράσεις:

- Ψευδωνυμοποίηση των δεδομένων: Υλοποίηση Data masking μεθόδων για την προστασία των δεδομένων προσωπικού χαρακτήρα (προτεινόμενη τεχνολογία που θεωρείται 'Best Practice' η χρήση oracle DB [13]).
- Σύστημα Αρχειοθέτησής: Υλοποίηση τεχνολογιών με βαθμίδες εμπιστευτικότητας γνωστές ως 'row level security' (confidentiality levels per data or files) [14].
- Επεξεργασία: Δημιουργία πολιτικών και σεμιναρίων επαγρύπνησης (awareness trainings) σε σχέση με την επεξεργασία των προσωπικών δεδομένων στους χρήστες.
- Δεδομένα Προσωπικού Χαρακτήρα: Δημιουργία πολιτικών σε σχέση με τα δεδομένα προσωπικού χαρακτήρα και την επεξεργασία τους.
- Περιορισμός Επεξεργασίας: Δημιουργία πολιτικών αλλά και τεχνικής υποδομής που υποστηρίζει τα ελάχιστα πεδία που χρειάζονται προς συμπλήρωση για την εφαρμογή οποιασδήποτε επιχειρησιακής διαδικασίας. Για παράδειγμα σε ένα σύστημα μισθοδοσίας θα μπορούσε να υπάρχουν ενδείξεις ανά πεδίο συμπλήρωσης γύρω από τα δεδομένα που χρειάζονται για να διατηρηθούν σε ότι αφορά την πρόσληψη ενός εργαζομένου, το ίδιο ισχύει και για τα πελατειακά συστήματα πχ CRM, ERP κτλ.
- Κατάρτιση Προφίλ: Το υποκείμενο επεξεργασίας θα πρέπει να γνωρίζει με ακρίβεια για ποιο λόγο καταρτίζεται ένα προφίλ και γιατί, θα πρέπει επίσης να έχει την δυνατότητα να επιλέγει αν θέλει να συναινέσει σε αυτό ή όχι.
- Υπεύθυνος Επεξεργασίας: Θα πρέπει να αναφέρεται ο ρόλος του υπευθύνου επεξεργασίας στο BCP / DRP.
- Εκτελών την Επεξεργασία: Θα πρέπει να αναφέρεται ο ρόλος του εκτελούντα την επεξεργασίας στο BCP / DRP.
- Αποδέκτης: Θα πρέπει να αναφέρονται οι αποδέκτες των δεδομένων στο BCP / DRP.
- Τρίτος: Θα πρέπει να αναφέρεται και να διευκρινίζεται στο BCP / DRP.
- Συγκατάθεση: Θα πρέπει να υπάρχει φόρμα συγκατάθεσης για όλα τα είδη προσωπικών δεδομένων και τους λόγους όπου συλλέγονται – επεξεργάζονται, και να συγκεντρώνονται σε σύστημα ποια υποκείμενο έχουν συναινέσει για την επεξεργασία των δεδομένων τους (και ποια όχι) αλλά και σε ποιους όρους έχουν συναινέσει.
- Παραβίαση Δεδομένων Προσωπικού Χαρακτήρα: Στο BCP / DRP θα πρέπει να αναφέρονται όλα τα μέσα και οι διαδικασίες που εξασφαλίζουν την προστασία των προσωπικών δεδομένων σε έναν οργανισμό.

- Γενετικά Δεδομένα: Δημιουργία πολιτικών ως προς την διατήρηση, επεξεργασία και προστασία αυτών των γενετικών δεδομένων, όπως επίσης και υιοθέτηση τεχνικών που διασφαλίζουν την προστασία αυτών.
- Βιομετρικά Δεδομένα: Δημιουργία πολιτικών ως προς την διατήρηση, επεξεργασία και προστασία των βιομετρικών δεδομένων, όπως επίσης και υιοθέτηση τεχνικών που διασφαλίζουν την προστασία αυτών.
- Δεδομένα που αφορούν την Υγεία: Δημιουργία πολιτικών ως προς την διατήρηση, επεξεργασία και προστασία των δεδομένων υγείας, όπως επίσης και υιοθέτηση τεχνικών που διασφαλίζουν την προστασία αυτών.

<u>Περιοχή Ελέγχου 5 (C5)</u>

Εμπλεκόμενα Άρθρα:

-Άρθρο 5 - Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα

Δράσεις:

- Θα πρέπει να γραφτούν πολιτικές εφόσον δεν υπάρχουν.
- Θα πρέπει να γραφτούν διαδικασίες σχετικά με την επεξεργασία των προσωπικών δεδομένων αλλά και την νομιμότητά της επεξεργασίας.
- Θα πρέπει να υλοποιηθούν εφαρμογές στα συστήματα της εταιρείας που προάγουν την προστασία αυτών.
- Φόρμα συγκατάθεσης για επεξεργασία προσωπικών δεδομένων (consent) προς όλα τα υποκείμενα των δεδομένων.
- Ελαχιστοποίηση δεδομένων και υλοποίηση πρακτικών που προάγουν την συγκεκριμένη εφαρμογή.
- Εύκολα προσβάσιμα, ώστε ανά πάσα στιγμή το υποκείμενο των δεδομένων να έχει στην διάθεση του τα προσωπικά δεδομένα που το αφορούν.
- Ακεραιότητα: Η αρχή της ακεραιότητας συνεπάγεται την υιοθέτηση όλων εκείνων των τεχνικών ασφαλείας που εξασφαλίζουν την ακεραιότητα των δεδομένων προσωπικού χαρακτήρα.
- Retention policy: Υιοθέτηση πολιτικών, διαδικασιών αλλά και τεχνικών μέσων που προάγουν τα διαστήματα που θα διατηρούνται τα δεδομένα προσωπικού χαρακτήρα. Πχ. πολιτικές για την διαχείριση των backup, των δεδομένων κάμερας

ασφαλείας, την διατήρηση των προσωπικών δεδομένων ενός υπαλλήλου απ' την στιγμή που αποχωρεί από την εταιρεία.

- Εμπιστευτικότητα: Η εμπιστευτικότητα των δεδομένων προσωπικού χαρακτήρα είναι μια αρχή που αποτελείται από πολιτικές, διαδικασίες αλλά και τεχνικά μέσα που προάγουν την διατήρηση αυτής. Επίσης είναι σημαντικό να σημειωθεί ότι θα πρέπει να τηρούνται και οι απαραίτητοι κώδικες δεοντολογίας.
- Ακρίβεια σε σχέση με τα προσωπικά δεδομένα αλλά και τους όρους που αφορούν την επεξεργασία αυτών.
- Τήρηση των προσωπικών δεδομένων για τους σκοπούς επεξεργασίας για την οποία κρατιούνται, κάτι που πρέπει να αναφέρεται τόσο συστημικά ανα κατηγορία δεδομένων αλλά και σε επίπεδο διαδικασιών.
- Δημιουργία πολιτικών αποκλειστικά για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και όλων των προαναφερθέντων τεχνικών.

<u>Περιοχή Ελέγχου 6 (C6)</u>

Εμπλεκόμενα Άρθρα:

-Άρθρο 6 - Νομιμότητα της επεξεργασίας

Δράσεις:

- Θα πρέπει όπως και στο προηγούμενο άρθρο να υλοποιηθούν πολιτικές, διαδικασίες αλλά και υλοποιήσεις στα συστήματα μιας εταιρείας ώστε να τεκμηριώνεται η νομιμότητα της επεξεργασίας των δεδομένων. Η νομιμότητα θα πρέπει να πλαισιώνεται από τα εξής:
    - Σύννομη συγκατάθεση και να μπορεί να τεκμηριώνεται με χρήση τεχνικών μέσων με τα δεδομένα του υποκειμένου,
    - Ποιος θα λάβει τα δεδομένα και για σκοπούς (πχ. δημοσίου κτλ.),
    - Είδη των δεδομένων και νομιμότητα,
    - Σε ποιους κοινοποιούνται τα δεδομένα αυτά,
    - Ειδικές κατηγορίες δεδομένων.

<u>Περιοχή Ελέγχου 7 (C7)</u>

Εμπλεκόμενα Άρθρα:

-Άρθρο 7 - Προϋποθέσεις και συγκατάθεση,

-Άρθρο 8 - Προϋποθέσεις που ισχύουν για την συγκατάθεση παιδιού σε σχέση με τις υπηρεσίες της κοινωνίας των πληροφοριών.

Δράσεις:

Υιοθέτηση πολιτικών και διαδικασιών που αφορούν τις προϋποθέσεις για συγκατάθεση των δεδομένων.

Περιοχή Ελέγχου 8 (C8)

Εμπλεκόμενα Άρθρα:

-Άρθρο 9 - Επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα

Δράσεις:

Πολιτικές που αφορούν την επεξεργασία των ειδικών κατηγοριών δεδομένων αλλά και εφαρμογή τεχνολογικών πρακτικών που αποσκοπούν στην προστασία τους.

Περιοχή Ελέγχου 9 (C9)

Εμπλεκόμενα Άρθρα:

-Άρθρο 11 - Επεξεργασία η οποία δεν απαιτεί εξακρίβωση ταυτότητας

Δράσεις:

Θα πρέπει να αναφέρεται στις πολιτικές και πρακτικές που αφορούν την επεξεργασία των δεδομένων προσωπικού χαρακτήρα.

Περιοχή Ελέγχου 10 (C10)

Εμπλεκόμενα Άρθρα:

-Άρθρο 12 - Διαφανής ενημέρωση, ανακοίνωση και ρυθμίσεις για την άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων,

-Άρθρο 13 - Πληροφορίες που παρέχονται εάν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται από το υποκείμενο των δεδομένων,

-Άρθρο 14 - Πληροφορίες που παρέχονται εάν τα δεδομένα προσωπικού χαρακτήρα δεν έχουν συλλεγεί από το υποκείμενο των δεδομένων.

Δράσεις:

- Θα πρέπει να υπάρχει διαδικασία που να αναφέρεται αποκλειστικά στα άρθρα 12, 13 και 14 και αφορά την ενημέρωση του υποκειμένου ως προς την επεξεργασία των δεδομένων.
- Εφαρμογή τεχνικών που επιτρέπουν την συλλογή των δεδομένων αυτών ώστε να επιτευχθεί η άμεση, διαφανής και πλήρης ενημέρωση του υποκειμένου καλύπτοντας την διορία κατάθεσης των στοιχείων που προβλέπει ο κανονισμός για το άρθρο 12 (διάστημα ενός (1) μήνα και δικαίωμα παράτασης μέχρι και δύο (2) μήνες εφόσον ενημερωθεί το υποκείμενο των δεδομένων για την εν λόγω παράταση αλλά και τους λόγους αυτής).

<u>Περιοχή Ελέγχου 11 (C11)</u>

Εμπλεκόμενα Άρθρα:

-Άρθρο 15 - Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων,

-Άρθρο 16 - Δικαίωμα διόρθωσης,

-Άρθρο 17 - Δικαίωμα διαγραφής («δικαίωμα στη λήθη»),

-Άρθρο 18 - Δικαίωμα περιορισμού της επεξεργασίας,

-Άρθρο 19 - Υποχρέωση γνωστοποίησης όσον αφορά τη διόρθωση ή τη διαγραφή δεδομένων προσωπικού χαρακτήρα ή τον περιορισμό της επεξεργασίας,

-Άρθρο 20 - Δικαίωμα στη φορητότητα των δεδομένων,

-Άρθρο 21 - Δικαίωμα εναντίωσης.

Δράσεις:

- Υλοποίηση των αναγκαίων προσαρμογών στα συστήματα ώστε να διασφαλιστεί ότι τα προσωπικά δεδομένα μπορούν εύκολα να διαγραφούν κατόπιν αιτήματος.
- Στις περιπτώσεις ανταλλαγής δεδομένων είτε με άλλους υπεύθυνους επεξεργασίας ή οποιοδήποτε άλλο ενδιαφερόμενο μέλος θα πρέπει να υλοποιηθούν διαδικασίες αλλά και τεχνικές μέσω συστημάτων (πχ. σύστημα παρακολούθησης σχετικά με την ανταλλαγή των δεδομένων) ώστε να υλοποιούνται οι πράξεις της διαγραφής όπως προβλέπει ο κανονισμός.

- Οργανωτικές, συμβατικές και διαδικαστικές ρυθμίσεις σε ότι αφορά την επεξεργασία, αποθήκευση και διαγραφή δεδομένων από άλλους εμπλεκόμενους εκτός εταιρείας.

Περιοχή Ελέγχου 12 (C12)

Εμπλεκόμενα Άρθρα:

-Άρθρο 22 - Αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ

Δράσεις:

Δημιουργία διαδικασιών / μέτρων εφόσον η εταιρεία προχωράει σε λήψη αποφάσεων που προέρχονται από αυτοματοποιημένες διαδικασίας συμπεριλαμβανομένης της κατάρτισης προφίλ.

Περιοχή Ελέγχου 13 (C13)

Εμπλεκόμενα Άρθρα:

-Άρθρο 24 - Ευθύνη του υπευθύνου επεξεργασίας

Δράσεις:

- Διαδικασία σχετικά με την ευθύνη του υπευθύνου επεξεργασίας.
- Ένταξη παραγράφου στους κώδικες δεοντολογίας που ορίζει ο κάθε κλάδος/τομέας.

Περιοχή Ελέγχου 14 (C14)

Εμπλεκόμενα Άρθρα:

-Άρθρο 25 - Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού

Δράσεις:

Υιοθέτηση τεχνικών πρακτικών στα συστήματα ώστε να διασφαλίζεται αφενός η προστασία των δεδομένων, αλλά και η περίοδος αποθήκευσης και ποιοι έχουν πρόσβαση σε αυτά.

Περιοχή Ελέγχου 15 (C15)

Εμπλεκόμενα Άρθρα:

-Άρθρο 26 - Από κοινού υπεύθυνοι επεξεργασίας,

-Άρθρο 27 - Εκπρόσωποι υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία μη εγκατεστημένων στην Ένωση.

Δράσεις:

Υλοποίηση διαδικασίας.

<u>Περιοχή Ελέγχου 16 (C16)</u>

Εμπλεκόμενα Άρθρα:

-Άρθρο 28 - Εκτελών την επεξεργασία,

-Άρθρο 29 - Επεξεργασία υπό την εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία.

Δράσεις:

Υλοποίηση διαδικασίας.

<u>Περιοχή Ελέγχου 17 (C17)</u>

Εμπλεκόμενα Άρθρα:

-Άρθρο 30 - Αρχεία των δραστηριοτήτων επεξεργασίας

Δράσεις:

Τήρηση αρχείων επεξεργασίας. Θα ήταν επιθυμητή η υλοποίηση συστήματος όπου είτε αυτοματοποιημένα συλλέγει απ' όλα τα συστήματα τις πράξεις επεξεργασίας των προσωπικών δεδομένων, είτε μεμονωμένου συστήματος όπου καταγράφονται οι πράξεις αυτές. Προ απαιτούμενή η υιοθέτηση πρακτικών data masking αλλά και ύπαρξη μέσων που διασφαλίζουν την ασφάλεια του συστήματος αυτού (πχ. security groups, confidentiality levels κτλ.).

<u>Περιοχή Ελέγχου 18 (C18)</u>

Εμπλεκόμενα Άρθρα:

-Άρθρο 31 - Συνεργασία με την εποπτική αρχή

Δράσεις:

Τα στοιχεία της εποπτικής αρχής θα πρέπει να καταγράφονται στο BCP / DRP.

<u>Περιοχή Ελέγχου 19 (C19)</u>

Εμπλεκόμενα Άρθρα:

-Άρθρο 32 - Ασφάλεια επεξεργασίας

Δράσεις:

- Σχετικά με την ασφάλεια της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και ότι μπορεί να επηρεάσει αυτά θα πρέπει να τηρούνται οι παρακάτω αρχές και πολιτικές:
    - Ψευδωνυμοποίηση των δεδομένων (πχ. υλοποίηση τεχνικών data masking που προαναφέρθηκαν),
    - Διασφάλιση απορρήτου τεχνικά (πχ. υιοθέτηση τεχνικών ασφάλειας – row level security implementations), διαχειριστικά και διαδικαστικά (πχ. υπογραφή τήρησης απορρήτου από τα εμπλεκόμενα μέλη που ασχολούνται με την επεξεργασία των δεδομένων),
    - Ακεραιότητα – η υιοθέτηση πρακτικών ασφαλείας διασφαλίζει την ακεραιότητα των δεδομένων,
    - Διαθεσιμότητα – μέσω του DRP καλύπτεται ένας μέρος της διαθεσιμότητας των δεδομένων. Επίσης η υιοθέτηση τεχνικών αυτοματοποιημένων μέσων που μπορούν να συγκεντρώνουν τόσο τα διαθέσιμα προσωπικά δεδομένα ενός υποκειμένου αλλά και πράξεις επεξεργασίας όπου εφαρμόστηκαν σε αυτά τα δεδομένα,
    - Αξιοπιστία των συστημάτων μέσω υιοθέτηση πολιτικών ασφαλείας αλλά και τεχνολογικών μέσων,
    - Τακτικός έλεγχος αξιοπιστίας – μέσω του testing του BCP/ DRP μπορεί να τεκμηριωθεί η αξιοπιστία τόσο των συστημάτων όσο και των δεδομένων που υπάρχουν σε αυτά,
    - Αποκατάσταση διαθεσιμότητας σε περίπτωση τεχνικού η φυσικού συμβάντος – μέσω του BCP / DRP αλλά και των εδραιωμένων πρακτικών

(διαδικαστικών αλλά και την χρήση τεχνικών μέσω) που αφορούν την άμεση αποκατάσταση,

- Τακτική δοκιμή, εκτίμηση, αξιολόγηση των τεχνικών οργανωτικών μέσων – μέσω του testing του BCP / DRP αλλά και τον έλεγχο των δεδομένων. Επίσης η ύπαρξη τακτικών audits λειτουργεί συμπληρωματικά και διασφαλίζει την συνεχή αξιολόγηση και εκτίμηση των οργανωτικών και τεχνικών μέσων της εταιρείας,
- Διαχείριση ρίσκων – μέσω του BCP/ DRP και την συνεχή ενημέρωση και αξιολόγηση των ρίσκων αλλά και των παραγόντων που απειλούν την επιχειρησιακή συνέχεια μιας εταιρείας (business continuity),
- Διαχείριση ρίσκων για όλες της κατηγορίες επεξεργασίας – μέσω της διαχείριση των ρίσκων που αναφέρονται στο BCP / DRP,
- Ενημέρωση των security policies, processes & procedures της εταιρείας – στα πλαίσια του corrective maintenance και business continuity.

- Ύπαρξη πιστοποιήσεων ασφάλειας (πχ. ISO 27000 , 27001) οι οποίες λειτουργούν συμπληρωματικά με το BCP / DRP και αποσκοπούν στην υιοθέτηση πρακτικών που αφενός προάγουν την ασφάλεια μιας εταιρείας και αφετέρου συνδράμουν στην επιχειρησιακή συνέχεια μιας εταιρείας.

<u>Περιοχή Ελέγχου 20 (C20)</u>

Εμπλεκόμενα Άρθρα:

-Άρθρο 33 - Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή,

-Άρθρο 34 - Ανακοίνωση παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων.

Δράσεις:

- Δημιουργία πολιτικών και διαδικασιών για την αντιμετώπιση των παραβιάσεων.
- Δημιουργία συστήματος για την καταγραφή των παραβιάσεων δεδομένων.
- Δημιουργία ομάδας αντιμετώπισης παραβιάσεων αλλά και των αντίστοιχων φορέων.
- Δημιουργία templates για την ανακοίνωση των παραβιάσεων αυτών.

- Δημιουργία σεναρίων testing για την υποτιθέμενη ύπαρξη παραβιάσεων αλλά και διαδικασίες εκτέλεσης αυτών.
- Αναθεώρηση όλων των συμβάσεων με εξωτερικά εμπλεκόμενα μέλη για αναθεώρηση των ευθυνών που καλύπτων τις παραβιάσεις δεδομένων.
- Υιοθέτηση συστήματος που διασφαλίζει την ανίχνευση, παρακολούθηση αλλά και μη εξουσιοδοτημένη πρόσβαση σε συστήματα και κατ' επέκταση στα προσωπικά δεδομένα όπως και σύστημα που αποτρέπει τέτοιου είδους πράξεις.
- Υιοθέτηση δικλείδων ασφαλείας σχετικά με την επεξεργασία, διαγραφή και πρόσβαση στα συστήματα.

Περιοχή Ελέγχου 21 (C21)

Εμπλεκόμενα Άρθρα:

-Άρθρο 35 - Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

Δράσεις:

Αναφορά της εκτίμησης αντικτύπου στο BCP / DRP στα πλαίσια των ενεργειών που αποσκοπούν στην διαχείρισης και αντιμετώπιση ρίσκων.

Περιοχή Ελέγχου 22 (C22)

Εμπλεκόμενα Άρθρα:

-Άρθρο 36 - Προηγούμενη διαβούλευση

Δράσεις:

Δημιουργία διαδικασίας για περιπτώσεις όπου η επεξεργασία των δεδομένων θα μπορούσε να προκαλέσει υψηλό κίνδυνο καθώς δεν υπάρχουν μέτρα μετριασμού.

Περιοχή Ελέγχου 23 (C23)

Εμπλεκόμενα Άρθρα:

-Άρθρο 37 - Ορισμός του υπευθύνου προστασίας δεδομένων,

-Άρθρο 38 - Θέση του υπευθύνου προστασίας δεδομένων,

-Άρθρο 39 - Καθήκοντα του υπευθύνου προστασίας δεδομένων.

Δράσεις:

Ύπαρξη πολιτικής σχετικά με το ρόλο του υπευθύνου αλλά και τα καθήκοντα του, όπως επίσης και αναφορά του στο BCP / DRP.

<u>Περιοχή Ελέγχου 24 (C24)</u>

Εμπλεκόμενα Άρθρα:

-Άρθρο 40 - Κώδικες δεοντολογίας,

-Άρθρο 41 - Παρακολούθηση των εγκεκριμένων κωδίκων δεοντολογίας.

Δράσεις:

- Όπως προαναφέρθηκε παραπάνω θα πρέπει να υπάρχουν εγγεγραμμένοι κώδικες δεοντολογίας σε περίπτωση που δεν υπάρχουν και να αναθεωρηθούν οι παλαιότεροι και να εφαρμοστούν όλες οι απαραίτητες αλλαγές που απαιτούνται από τον κανονισμό.
- Στα πλαίσια της επιχειρησιακής συνέχειας οι κώδικες δεοντολογίας της εταιρείας θα πρέπει να αναθεωρούνται τακτικά και να εφαρμόζονται οι απαιτούμενες αλλαγές, όπως προβλέπεται από τον κάθε κλάδο/τομέα.
- Στα πλαίσια των πολιτικών ποιότητας θα πρέπει να διατηρείτε ιστορικών αλλαγών και αναθεωρήσεων αυτών.
- Επίσης οι κώδικες δεοντολογίας θα πρέπει να είναι διαθέσιμοι σε όλα τα εμπλεκόμενα μέλη μιας εταιρείας και στα πλαίσια της διατήρησης των επιπέδων ασφαλείας αυτής.

<u>Περιοχή Ελέγχου 25 (C25)</u>

Εμπλεκόμενα Άρθρα:

-Άρθρο 42 – Πιστοποίηση,

-Άρθρο 43 - Φορείς Πιστοποίησης.

Δράσεις:

Πιστοποιήσεις, όπως πχ. ISO 27001 λειτουργούν βοηθητικά στην εδραίωση πολιτικών, διαδικασιών αλλά και στην υιοθέτηση συστημάτων που προάγουν την ασφάλεια σε έναν οργανισμό.

Περιοχή Ελέγχου 26 (C26)

Εμπλεκόμενα Άρθρα:

-Άρθρο 44 - Γενικές αρχές για διαβιβάσεις,

-Άρθρο 45 - Διαβιβάσεις βάσει απόφαση επάρκειας,

-Άρθρο 46 - Διαβιβάσεις που υπόκεινται σε κατάλληλες εγγυήσεις,

-Άρθρο 47 - Δεσμευτικοί εταιρικοί κανόνες,

-Άρθρο 48 - Διαβιβάσεις ή κοινοποιήσεις που δεν επιτρέπονται από το δίκαιο της Ένωσης,

-Άρθρο 49 - Παρεκκλίσεις για ειδικές καταστάσεις,

-Άρθρο 50 - Διεθνής συνεργασία για την προστασία δεδομένων προσωπικού χαρακτήρα.

Δράσεις:

- Δημιουργία αρχείου διαβιβάσεων σε χώρες εκτός ΕΕ (πχ ποια είδη δεδομένων διαβιβάζονται και για ποιους σκοπούς όπως επίσης και το χρονικό διάστημα).
- Επαναπροσδιορισμό των cloud συστημάτων στην περίπτωση που ο παροχέας βρίσκεται εκτός ΕΕ.
- Αναθεώρηση των συμβάσεων με παροχείς ή συνεργάτες που βρίσκονται σε τρίτες χώρες και διαβιβάζονται σε αυτούς προσωπικά δεδομένα.

Περιοχή Ελέγχου 27 (C27)

Εμπλεκόμενα Άρθρα:

-Άρθρο 82 - Δικαίωμα αποζημίωσης και ευθύνη

Δράσεις:

Δημιουργία διαδικασίας διαχείρισης τέτοιων περιστατικών.

Περιοχή Ελέγχου 28 (C28)

Εμπλεκόμενα Άρθρα:

-Άρθρο 83 - Γενικοί όροι επιβολής διοικητικών προστίμων

Δράσεις:

Τα εν λόγω κόστη θα πρέπει να λαμβάνονται υπόψη στην διαχείριση των ρίσκων της εταιρείας.

<u>Περιοχή Ελέγχου 29 (C29)</u>

Εμπλεκόμενα Άρθρα:

-Άρθρο 87 - Επεξεργασία του εθνικού αριθμού ταυτότητας,

-Άρθρο 88 - Επεξεργασία στο πλαίσιο της απασχόλησης.

Δράσεις:

Θα πρέπει να ληφθούν υπόψη στις πολιτικές, διαδικασίες που αφορούν την ασφάλεια επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, όπως προαναφέρθηκαν παραπάνω.

<u>Περιοχή Ελέγχου 30 (C30)</u>

Εμπλεκόμενα Άρθρα:

-Άρθρο 90 - Υποχρεώσεις τήρησης απορρήτου

Δράσεις:

- Εισαγωγή στους κώδικες δεοντολογίας μιας εταιρείας, όπως προαναφέρθηκε.
- Confidentiality Agreement πρότυπο με όλους τους εμπλεκόμενους μιας εταιρείας αλλά και τήρηση αρχείου αυτών.

Παραπάνω αναλύθηκαν οι περιοχές του κανονισμού που χρειάζονται να μελετηθούν και να κατανοηθούν από μια εταιρεία ώστε να υλοποιηθούν οι κατάλληλες πρακτικές που θα οδηγήσουν στην δημιουργία ή αναθεώρηση των πρακτικών ασφαλείας αλλά και στην υιοθέτηση ενός επιτυχημένου BCP / DRP. Τα παραπάνω άρθρα και κατ' επέκταση οι περιοχές ελέγχου που δημιουργήσαμε επηρεάζουν είτε άμεσα είτε έμμεσα το BCP/DRP μιας εταιρείας. Το IT Governance μιας εταιρείας επηρεάζεται εξ ολοκλήρου από τον κανονισμό και βασιζόμενοι στους δύο κύριους πυλώνες που επαναλαμβάνονται ή νοούνται στα περισσότερα άρθρα ένας οργανισμός θα πρέπει:

- Να αποδεικνύει συμμόρφωση μέσω εμπεριστατωμένων τεχνικών και δράσεων,
- Και να προστατεύει τα δικαιώματα και τις ελευθερίες των υποκειμένων υιοθετώντας πολιτικές, διαδικασίες αλλά και τεχνολογικά μέσα που προάγουν τόσο την ασφάλεια (φυσικό και ψηφιακό επίπεδο) όσο και την επιχειρησιακή συνέχεια.

Παραπάνω λοιπόν παρουσιάζεται ένα πλάνο ενεργειών που μπορεί μια εταιρεία αφενός να χρησιμοποιήσει για να αποδείξει συμμόρφωση στο κομμάτι που αφορά το IT Governance, ακολουθώντας τις δράσεις που προτείνονται, και αφετέρου εφόσον ακολουθηθούν οι ανωτέρω δράσεις να δημιουργηθεί ένα BCP / DRP που να διασφαλίζει την επιχειρησιακή συνέχεια μιας εταιρείας αλλά και την ανάκτηση των επιχειρησιακών δομών της σε περίπτωση οποιαδήποτε κινδύνου.

3.6 Στάδια υλοποίησης επιχειρησιακής συνέχειας (ITSCM ITIL V3)

Σύμφωνα με την ITSCM (ITIL V3) η επιχειρησιακή συνέχεια υλοποιείται και διαχειρίζεται σε τέσσερα στάδια (**Εικόνα 6**) τα οποία και περιγράφονται παρακάτω [15]:

- Initiation: Το αρχικό στάδιο αφορά την δημιουργία/εδραίωση πολιτικών σε έναν οργανισμό, τον καθορισμό του πεδίου εφαρμογής και των στόχων, την κατανομή των πόρων αλλά και γενικότερα τον σχεδιασμό του έργου.
- Requirements and strategy: Το στάδιο αυτό αφορά την ανάλυση των απαιτήσεων, την ανάλυση των επιπτώσεων (BIA) και την εκτίμηση / διαχείριση των ρίσκων.
- Implementation: Στο στάδιο αυτό εφαρμόζονται όλα τα μέτρα μετριασμού που λήφθηκαν παραπάνω, οι δράσεις ανάκτησης και η δοκιμή της αποτελεσματικότητας των σχεδίων.
- Ongoing operation: Το συγκεκριμένο στάδιο αφορά την εκπαίδευση, την ευαισθητοποίηση/επαγρύπνηση (awareness), την διαχείριση των αλλαγών όσον αφορά το BCP/DRP (Change Management) και τις συνεχής δοκιμές αυτών (testing).

Παρακάτω θα προσπαθήσουμε να εντάξουμε τους ελέγχους / δράσεις όπου και αναλύθηκαν στην προηγούμενη ενότητα ανά στάδιο υλοποίησης.

Στάδιο: Initiation

Περιοχές Ελέγχου:

C1, C2, C3, C4, C5, C6, C7, C8, C9, C10, C11, C12, C13, C14, C15, C16, C17, C18, C19, C20, C22, C23, C25, C26, C27, C29, C30 (27 περιοχές ελέγχου)

Εμπλεκόμενα Άρθρα GDPR:

1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 24, 25, 26, 27, 28, 29, 30, 31, 32, 36, 37, 38, 39, 42, 43, 44, 45, 46, 47, 48, 49, 50, 82, 87, 88, 90 (47 εμπλεκόμενα άρθρα)

Σχόλια:

- Ορισμός του σκοπού,
- Ορισμός πεδίου εφαρμογής σε επίπεδο δράσεων,
- Εδαφικό πεδίο εφαρμογής εκτιμώντας τις απαιτήσεις που μπορεί να υπάρχουν ανά χώρας εντός και εκτός ΕΕ,
- Κατανόηση ορισμών και λήψη μέτρων για την επίτευξη των στόχων,
- Εδραίωση πολιτικών / διατάξεων, guidelines και διαδικασιών γύρω από την ασφάλεια λαμβάνοντας υπόψη τις αρχές που διέπουν την επεξεργασία (Δημιουργία πολιτικής επεξεργασίας, εάν δεν υπάρχει),
- Κατανόηση νομικού πλαισίου που διέπει την επεξεργασία,
- Εύρεση προσωπικού κατάλληλου τόσο για την εφαρμογή του κανονισμού όσο και για την υλοποίηση και συντήρηση των μηχανισμών που διασφαλίζουν την ασφάλεια αλλά και την επιχειρησιακή συνέχεια ενός οργανισμού,
- Διαχωρισμός αρμοδιοτήτων του προσωπικού τόσο στα πλαίσια διαχείρισης των πληροφοριών (επεξεργασία) όσο και στην διατήρηση της ασφάλειας αυτών και την αντιμετώπιση / επανάκαμψή σε περίπτωση οποιοδήποτε περιστατικού,
- Καταγραφή των κατηγοριών δεδομένων αλλά και τις κατηγορίες υποκειμένων που επηρεάζουν – Τήρηση αρχείου επεξεργασίας,
- Υιοθέτηση / Εφαρμογή / Εδραίωση κατάλληλων υποδομών (software, hardware, network),

- Καταγραφή του εξοπλισμού και των παρεχόμενων υπηρεσιών,
- Υιοθέτηση / Εφαρμογή / Εδραίωση υποδομών επανάκαμψής (software, hardware, network, sites κτλ.)
- Υιοθέτηση / Εφαρμογή / Εδραίωση όλων εκείνων των μέσων που διασφαλίζουν την Εμπιστευτικότητα (Confidentiality), την Ακεραιότητα (Integrity) και την Διαθεσιμότητα (Availability) τόσο των πληροφορίων όσο και των υπηρεσιών ενός οργανισμού,
- Κατάλληλες πιστοποιήσεις.

<u>Στάδιο: Requirements and Strategy</u>

Περιοχές Ελέγχου:

C19, C21, C28 (3 περιοχές ελέγχου)

Εμπλεκόμενα Άρθρα GDPR:

32, 35, 83 (3 εμπλεκόμενα άρθρα)

Σχόλια:

- Data Protection Impact Assessment,
- Business Continuity Impact Analysis,
- Risk Management / Risk Assessment.

<u>Στάδιο: Implementation</u>

Περιοχές Ελέγχου:

C19, C20, C34 (3 περιοχές ελέγχου)

Εμπλεκόμενα Άρθρα GDPR:

32, 33 (2 εμπλεκόμενα άρθρα)

Σχόλια:

- Εφαρμογή την δράσεων επιχειρησιακής συνέχειας εκτιμώντας τα αποτελέσματα που προκύπτουν από τα παραπάνω στάδια και ειδικά από τα αποτελέσματα που προκύπτουν από τις παρακάτω αναλύσεις:

    - Εκτίμηση Αντικτύπου (DPIA),
    - Business Continuity Impact Analysis,
    - Risk Management / Risk assessment.
- Εφαρμογή πρακτικών που διασφαλίζουν που διασφαλίζουν την Εμπιστευτικότητα (Confidentiality), την Ακεραιότητα (Integrity) και την Διαθεσιμότητα (Availability),
- Δημιουργία του BCP/DRP,
- Δοκιμή των στρατηγικών (αποκατάσταση και αξιοπιστία των επιλεγμένων πρακτικών και αξιολόγηση της αποτελεσματικότητας [άρθρο 32, παράγραφος β-δ]).

<u>Στάδιο: Ongoing Operations</u>

Περιοχές Ελέγχου:

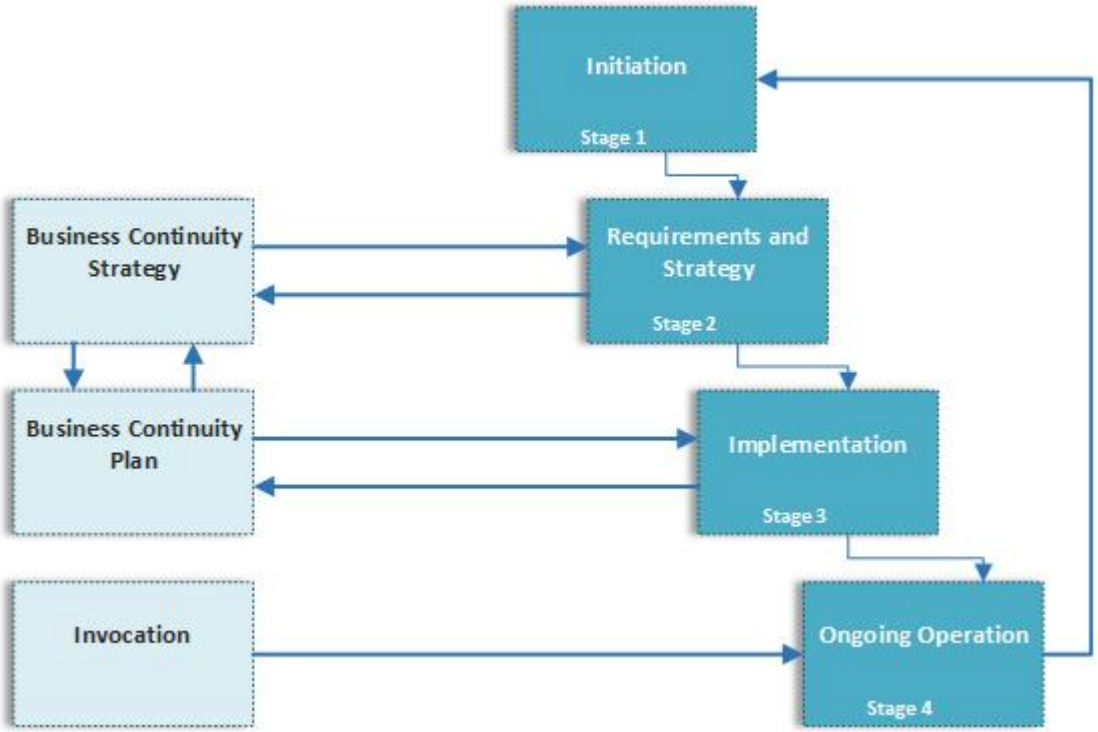
C19, C24 (2 περιοχές ελέγχου)

Εμπλεκόμενα Άρθρα GDPR:

32, 41 (2 εμπλεκόμενα άρθρα)

Σχόλια:

- Συνεχείς δοκιμές,
- Συνεχής αξιολόγηση της αποτελεσματικότητας,
- Επαγρύπνηση (awareness) και εκπαίδευση,
- Ενημερώσεις όπου χρειάζεται και παρακολούθηση των εγκεκριμένων κωδικών δεοντολογίας [άρθρο 41],
- Διαχείριση των αλλαγών στα πλαίσια της ενημέρωσης.



Εικόνα 6. Service Continuity Lifecycle

3.7 Διαχείριση Αλλαγών (Change Management)

Το GDPR από μόνο του αφορά μια μεγάλη αλλαγή της οποίας τα αποτελέσματα επηρεάζουν πολλά πράγματα στον τομέα του IT. Τόσο οι αλλαγές που έχουν επέλθει με τον νέο κανονισμό όσο και οι αλλαγές που προκύπτουν στον κύκλο ζωής και συντήρησης ενός BCP/DRP απαιτούν σωστή διαχείριση και την ύπαρξη των κατάλληλων διαδικασιών που θα πρέπει να ακολουθηθούν για την ομαλή υιοθέτηση τους. Η διαχείριση των αλλαγών υπονοείται σε πολλά άρθρα του κανονισμού και αναφέρεται ενδεικτικά στα παρακάτω:

- Άρθρο 28 – παράγραφος 2: προσθήκη ή αντικατάσταση εκτελούντων την επεξεργασία [1],
- Άρθρο 32: το εν λόγω άρθρο από μόνο του απαιτεί μια διαδικασία διαχείρισης αλλαγών καθώς οι τεχνικές απαιτήσεις, η διατήρηση της αξιοπιστίας των συστημάτων, η διατήρηση και η συντήρηση της διαθεσιμότητας τόσο σε υπηρεσίες όσο και σε πόρους αλλά και γενικότερα η διασφάλιση της ασφάλειας είναι από μόνη της συνεχής διαχείριση και αξιολόγηση αλλαγών [1],

- Άρθρο 35 – παράγραφος 11: μεταβολές που προκύπτουν από την εκτίμηση αντικτύπου [1],
- Άρθρο 47 – παράγραφος 2α: μηχανισμοί αναφοράς, καταχώρισης και διαχείρισης αλλαγών που αναφέρονται στους δεσμευτικούς εταιρικούς κανόνες [1].

Μια αλλαγή στο κύκλο ζωής ενός BCP/DRP και λαμβάνοντας υπόψη το GDPR μπορεί να προκύψει από:

- Αντικατάσταση (ή ακόμα και προσθήκη / πρόσληψη) ανθρώπων κλειδιά στα πλαίσια της επιχειρησιακής συνέχειας κάτι που μπορεί ακόμα και από την αλλαγή ή αντικατάσταση του υφιστάμενων εκτελούντων την επεξεργασία,
- Αλλαγή ενός IT vendor (πχ. backup vendor κτλ) ο οποίος εκτελεί επεξεργασία σε δεδομένα υποκειμένων,
- Αλλαγές ή προσθήκες στο GDPR δεδομένης της συνεχούς εξέλιξης της τεχνολογίας κάτι που έχει σαν συνέχεια την αλλαγή ή την αντικατάσταση τόσο των τεχνικών μέσων προστασίας όσο και των υφιστάμενων διαδικασιών στα πλαίσια της επιχειρησιακής συνέχειας,
- Μεταβολές που προκύπτουν από την εκτίμηση αντικτύπου στα πλαίσια της επεξεργασίας των δεδομένων κάτι που πρέπει να καταχωρηθεί και να αξιολογηθεί σαν αλλαγή και κατ' επέκταση να αξιολογηθεί και σαν ρίσκο,
- Ενδυνάμωση των μέσων κρυπτογράφησης και ψευδωνυμοποίησης στα πλαίσια του άρθρου 32 λόγω συνεχούς εξέλιξης της τεχνολογίας και των απειλών,
- Αλλαγές που προκύπτουν στα πλαίσια συνεχούς αξιολόγησης του BCP / DRP,
- Αλλαγές (τεχνολογικές, διαδικαστικές και νομικές) που προκύπτουν από περιστατικά παραβίασης δεδομένων.

Ανάλογα με την αναγκαιότητα και την σπουδαιότητα μιας αλλαγής θα πρέπει να υπάρχει η ανάλογη κατηγοριοποίηση σε [16] [17]:

- Επείγουσα προτεραιότητας: η αλλαγή θα πρέπει να πραγματοποιηθεί άμεσα καθώς διακυβεύεται η απώλεια της υπηρεσίας ή θα παρουσιαστούν σοβαρά προβλήματα πρόσβασης σε μεγάλο αριθμό χρηστών ή κάποιο άλλο αντίστοιχης σημασίας σοβαρό πρόβλημα. Σε αυτή την περίπτωση θα πρέπει να απαιτηθεί

επείγουσα συνάντηση της CAB/EC [Change Advisory Board / Emergency Board] και πιθανότατα να χρειαστεί να γίνει αναδιανομή πόρων για να πραγματοποιηθούν τέτοιου είδους αλλαγές σε σύντομο χρονικό διάστημα λιγότερο των είκοσι τεσσάρων (24) ωρών.

- Υψηλής προτεραιότητας: η αλλαγή θα πρέπει να υλοποιηθεί σε σαράντα οκτώ (48) ώρες καθώς μπορεί να προκύψουν σοβαρές συνέπειες ή να επηρεάστεί ένας μεγάλος αριθμός χρηστών σε περίπτωση μη υλοποίησης της εν λόγω αλλαγής. Σε αυτού του είδους τις αλλαγές δίνεται μέγιστη προτεραιότητα (αμέσως μετά την επείγουσα) για την απόσπαση πόρων που θα υλοποιήσουν τις αλλαγές και θα κάνουν τις κατάλληλες δοκιμές.
- Μέτρια προτεραιότητας: η αλλαγή αυτή θα πρέπει να υλοποιηθεί σε πέντε (5) ημέρες καθώς δεν υπάρχει κάποια σοβαρή επίπτωση ή άκρως άμεση προτεραιότητα στην υλοποίηση της, αλλά η επιδιόρθωση δεν μπορεί να αναβληθεί για μεγαλύτερο χρονικό διάστημα από αυτών των πέντε (5) ημερών. Σχετικά με την ανακατανομή πόρων υπάρχει μεσαία προτεραιότητα καθώς οι εν λόγω αλλαγές μπορούν να ενταχθούν στο πλάνο υλοποίησης εφόσον συζητηθούν.
- Χαμηλής προτεραιότητας: η αλλαγή θα πρέπει να υλοποιηθεί σε συγκεκριμένη ημερομηνία που θα καθοριστεί στους υπευθύνους. Η αλλαγή κρίνεται αναγκαία και δικαιολογημένη, αλλά μπορεί να καθυστερήσει είτε λόγω χαμηλού ρίσκου, είτε γιατί υπάρχει ένα εύλογο χρονικό διάστημα που θα μπορούσε να υλοποιηθεί. Τέτοιου είδους αλλαγές θα μπορούσαν να είναι προγραμματισμένες αλλαγές σε προγραμματισμένες αναβαθμίσεις των τεχνολογικών πόρων ή αλλαγές που ενδείκνυται να γίνουν στα πλαίσια της ομαλής επιχειρησιακής συνέχειας. Οι πόροι ανακατανέμονται αναλόγως τις ανάγκες καθώς μιλάμε για αλλαγές οι οποίες μπορούν να προγραμματιστούν από πριν.

Θα ήταν εύλογο οι αλλαγές να χωριστούν σε κατηγορίες ώστε αφενός να είναι εμφανές το πεδίο εφαρμογής που επηρεάζουν αλλά και να μπορεί να γίνει σωστός προγραμματισμός τόσο στους ανθρώπινους πόρους που θα πρέπει να συγκεντρωθούν για την υλοποίηση τους αλλά και τεχνολογικούς πόρους (πχ. αναζήτηση vendor για αγορά νέων εργαλείων λογισμικού κτλ). Ο διαχειριστής των αλλαγών (Change Manager) ορίζει την κατηγορία της αλλαγής με βάση τις παρακάτω πληροφορίες [16] [17]:

- Standard Change: η αλλαγή αυτή υλοποιείται με τη χρήση κάποιας υπάρχουσας διαδικασίας (πχ. προγραμματισμένες αναβαθμίσεις συστημάτων ασφαλείας). Δεν χρειάζεται κάποια εξουσιοδότηση για την υλοποίηση τέτοιου είδους αλλαγών.
- IT change model: η αλλαγή αυτή γίνεται με τη χρήση κάποιας διαδικασίας αλλά λόγω των επιρροών που μπορεί να έχει είναι πιθανό να χρειαστεί κάποιο επίπεδο εξουσιοδότησης για την υλοποίηση της. Τέτοιου είδους αλλαγές μπορεί να είναι είτε προγραμματισμένες ενημερώσεις/αναβαθμίσεις συστημάτων μείζονος σημασίας που θα πρέπει να υλοποιούνται σε τακτά χρονικά διαστήματα, είτε κάποια data patches σε συστήματα που ενδείκνυται να υλοποιούνται άμεσα όταν προκύπτουν στα πληροφοριακά συστήματα ενός οργανισμού.
- Minor Change: οι αλλαγές αυτές θα πρέπει να εξουσιοδοτούνται από τον Change Manager και είναι αλλαγές χαμηλού ρίσκου και χαμηλού αντικτύπου, θα ήταν όμως θεμιτό να υλοποιηθούν.
- Significand Change: οι συγκεκριμένες αλλαγές θα πρέπει να εξουσιοδοτούνται από το CAB με όλους τους εμπλεκόμενους παρόντες και αφορούν αλλαγές μετρίου ρίσκου και μετρίου αντικτύπου. Significant Change θα μπορούσε να είναι η βελτιστοποίηση των RTO targets (Recovery Time Object) στα πλαίσια της επανάκαμψής από ένα συμβάν.
- Major Change: οι συγκεκριμένες αλλαγές επίσης θα πρέπει να εξουσιοδοτούνται από το CAB με όλους τους εμπλεκόμενους παρόντες και αφορούν αλλαγές υψηλού ρίσκου και υψηλού αντικτύπου. Τέτοιου είδους αλλαγές θα μπορούσαν να είναι αλλαγές στον backup provider ή η υιοθέτηση νέων IPS/IDS συστημάτων.

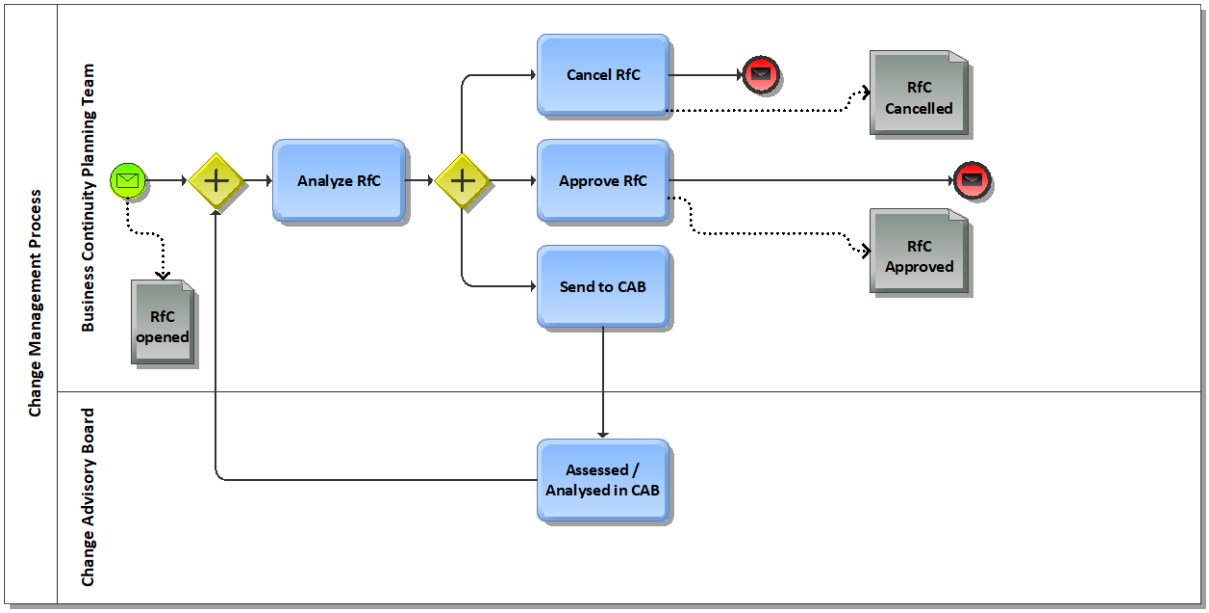
Στα πλαίσια της επιχειρησιακής συνέχειας θα ήταν θεμιτό να υπάρχει σύστημα ή αρχείο καταγραφής των αλλαγών (change management register ή change management system) και όλες οι αλλαγές να συνδέονται με την διαχείριση των αντίστοιχων ρίσκων που θα προκύψουν εφόσον δεν υλοποιηθούν στα πλαίσια μιας πλήρους αξιολόγησης και ανάλυσης. Σημαντικό επίσης στάδιο είναι και η δοκιμή μετά την υλοποίηση αυτών των αλλαγών.

Μια ολοκληρωμένη ανάλυση μιας αλλαγής (RfC) θα πρέπει κατ' ελάχιστον να παρέχει τις παρακάτω πληροφορίες:

- Όνομα του υπευθύνου ο οποίος έκανε την αίτηση της αλλαγής,

- Ημερομηνία καταγραφής,
- Περιγραφή Αλλαγής,
- Λόγος που προτείνεται να γίνει αυτή η αλλαγή,
- Επιπτώσεις που θα προκύψουν αν δεν υλοποιηθεί η εν λόγω αλλαγή,
- Εναλλακτικές λύσεις,
- Σύνδεση με την αξιολόγηση ρίσκων (τα ρίσκα μπορεί να είναι ένα ή περισσότερα) [3.4],
- Κατηγορία αλλαγής,
- Σπουδαιότητα,
- Κόστος,
- Ημερομηνία που πρέπει να υλοποιηθεί,
- και Ημερομηνία υλοποίησης.

Στο παρακάτω διάγραμμα (**Εικόνα 7**) απεικονίζεται η διαδικασία αξιολόγησης (RfC) όπου ξεκινάει με την καταχώρηση του είτε σε σύστημα είτε σε κάποια φόρμα / αρχείο την αξιολόγηση / ανάλυση του από την ομάδα επιχειρησιακής συνέχειας (Business Continuity Management Team). Στην πορεία ένα RfC είτε ακυρώνεται καθώς η υλοποίηση που προτείνεται δεν είναι αναγκαία, είτε εγκρίνεται από την ίδια την ομάδα επιχειρησιακής συνέχειας και προχωράει σε διαδικασία υλοποίησης, είτε λόγω μείζονος σημασίας αλλαγής ('significand', 'major' change category) απαιτείται σύσταση ενός CAB meeting για την λήψη αποφάσεων και την επανεκτίμηση της αλλαγής.



Εικόνα 7. Change Management Process [18]

3.8 Επίλογος

Στο παραπάνω κεφάλαιο αναλύθηκαν οι περιοχές που πλαισιώνουν το πλάνο επιχειρησιακής συνέχειας και ανάκαμψης ενός οργανισμού (BCP / DRP). Επιπροσθέτως δημιουργήθηκαν περιοχές ελέγχου που εκπωνήθηκαν από την μελέτη του κανονισμού για την προστασιά των προσωπικών δεδομένων (GDPR), επαναπροσδιορίστηκαν, αναλύθηκαν και παρουσιάστηκαν σε μορφή προτύπου. Με την χρήση και την εφαρμογή του συγκεκριμένου προτύπου ένας οργανισμός μπορεί να επιτύχει αφενός επιχειρησιακή συνέχεια και αφετέρου επιτυχής επανάκαμψη σε περίπτωση κάποιου συμβάντος.

Στο επόμενο κεφάλαιο θα δοθεί περισσότερη έμφαση στο κομμάτι της επιχειρησιακής ανάκαμψης με προτάσεις σε τεχνολογικές λύσεις, τόσο σε διαδικαστικό όσο και σε τεχνικό επίπεδο, που μπορούν να υϊοθετηθούν από έναν οργανισμό και λειτουργούν συμπληρωματικά με όσα προαναφερθηκαν στις προτεινόμενες δράσεις του παρόντος κεφαλαίου.

Κεφάλαιο 4

Αντίγραφα Ασφαλείας και Ανάκαμψη (Backup&Recovery)

Η ανάκτηση των τεχνολογικών υπηρεσιών μετά από ένα συμβάν ή μια καταστροφή εξαρτάται από τα τεχνολογικά μέσα και τις διαδικασίες που έχει υιοθετήσει ένας οργανισμός, εμπεριεχομένου του RTO των κρίσιμων λειτουργιών του. Στα πλαίσια λοιπόν μιας 'καταστροφής' (φυσικού ή τεχνικού συμβάντος), σημαντικό αφενός ένας οργανισμός να έχει υιοθετήσει όλα εκείνα τα μέσα που διασφαλίζουν την άμεση διαθεσιμότητα των παρεχόμενων υπηρεσιών αλλά να μπορεί να επανακάμψει (άρθρο 32-δ). Ένα σημαντικό βήμα είναι μια εταιρεία να μπορεί σε πρώτη φάση να διαχωρίσει τις παρεχόμενες υπηρεσίες της. Μια εταιρεία πληροφορικής για παράδειγμα :

- Παρέχει τεχνολογικές υπηρεσίες εντός του οργανισμού,
- Παρέχει τεχνολογικές υπηρεσίες σε πελάτες,
- Και δέχεται τεχνολογικές υπηρεσίες από τρίτους (παρόχους, προμηθευτές κτλ.).

Λαμβάνοντας υπόψη τα παραπάνω θα πρέπει να χτιστεί μια στρατηγική αποκατάστασης της επιχειρησιακής συνέχειας προσαρμοσμένη τόσο στις ανάγκες της όσο και στο κόστος υλοποίησης της.

4.1 Αντίγραφα Ασφαλείας (Backup)

Τα αντίγραφα ασφαλείας (backup) αποτελούν ένα βασικό κομμάτι της επιχειρησιακής συνέχειας. Η συχνότητα και ο τύπος των εφεδρικών αντιγράφων πρέπει να καθορίζεται

λαμβάνοντας υπόψη τις απαιτήσεις της διαθεσιμότητας, της ακεραιότητας και της αξιοπιστίας (άρθρο 32-β) των δεδομένων (κατά την διάρκεια καθορισμού των απαιτήσεων). Επίσης θα πρέπει να λαμβάνεται υπόψη το χρονικό διάστημα που θα διατηρούνται τα αντίγραφα ασφαλείας λαμβάνοντας υπόψη τις πολιτικές διατήρησης που προβλέπονται από τον κανονισμό για την προστασία των προσωπικών δεδομένων.
Παρακάτω παρατίθεται πίνακας με όλους τους τύπους των δεδομένων που μπορεί να υπάρχουν σε έναν οργανισμό και κάποιες προτεινόμενες απαιτήσεις που πρέπει να τηρούνται κατ' ελάχιστο από μια εταιρεία σε σχέση με την συχνότητα των αντίγραφων ασφαλείας:

Τύπος Δεδομένων: Δεδομένα Χρηστών (User Data)

Περιγραφή / Σχόλια:

Αρχεία / έγγραφα των χρηστών που υπάρχουν τοπικά στους υπολογιστές τους.

Ελάχιστες απαιτήσεις σχετικά με το backup:

Δεν χρειάζεται να τηρούνται αντίγραφα ασφαλείας. Σε κάθε περίπτωση οι χρήστες θα πρέπει να ενημερώνονται για το που θα πρέπει να τοποθετούνται αρχεία που αφορούν εταιρικά έγγραφα, ώστε να διασφαλίζεται ότι τηρούνται τα αντίγραφα ασφαλείας των εταιρικών δεδομένων (έγγραφα κτλ.).

Τύπος Δεδομένων: Προγράμματα (Programs)

Περιγραφή / Σχόλια:

Ο συγκεκριμένος τύπος δεδομένων αφορά λειτουργικά συστήματα και αρχεία εφαρμογών (εκτελέσιμα αρχεία) που είναι εγκατεστημένα σε αυτά τα συστήματα. Τα συγκεκριμένα δεδομένα αλλάζουν σπάνια.

Ελάχιστες απαιτήσεις σχετικά με το backup:

Θα πρέπει να διατηρείται τουλάχιστον ένα αντίγραφο ασφαλείας λαμβάνοντας υπόψη τα τελευταία updates/configurations που έχουν γίνει στο σύστημα.

Τύπος Δεδομένων: Δεδομένα Παραμετροποίησης (Configuration)

Περιγραφή / Σχόλια:

Ο συγκεκριμένος τύπος περιλαμβάνει δεδομένα διαμόρφωσης λειτουργικών συστημάτων (configuration data), εφαρμογών (πχ. SAP ERP, SharePoint configuration σε περίπτωση που μιλάμε για on premises εγκατάσταση), δεδομένα διαμόρφωσης

συσκευών δικτύου (network devices) κ.λπ. Τα συγκεκριμένα δεδομένα αλλάζουν περιστασιακά ανάλογα με τις ανάγκες.

Ελάχιστες απαιτήσεις σχετικά με το backup:

Θα πρέπει να υπάρχει τουλάχιστον ένα αντίγραφο ασφαλείας με τις τελευταίες ενημερώσεις που έχουν γίνει στα συστήματα. Κάθε φορά που θα γίνονται αλλαγές θα πρέπει να διατηρείται το τελευταίο αντίγραφο.

Τύπος Δεδομένων: Αρχεία Καταγραφής (Log files)

Περιγραφή / Σχόλια:

Ο συγκεκριμένος τύπος δεδομένων αφορά log files συστημάτων όπως λειτουργικά συστήματα, συσκευές δικτύου, εφαρμογές κτλ.

Ελάχιστες απαιτήσεις σχετικά με το backup:

Θα μπορούσαν να μην διατηρούνται. Εξαρτάται πάντα από τις απαιτήσεις κάθε εταιρείας και από τον τύπο των log files.

Τύπος Δεδομένων: Δεδομένα Εφαρμογών (Application Data)

Περιγραφή / Σχόλια:

Σε αυτόν τον τύπο δεδομένων εμπεριέχονται δεδομένα που αποθηκεύονται σε συστήματα εφαρμογών (πχ ERP συστήματα εμπεριεχομένων λογιστικών συστημάτων, συστημάτων μισθοδοσίας κτλ.). Εδώ θα πρέπει να ληφθούν υπόψη οι κατηγορίες προσωπικών δεδομένων που διατηρούνται, όπως επίσης και οι πολιτικές διατήρησης (retention policy) αυτών όπως προβλέπονται από τον κανονισμό αλλά και η διατήρηση μόνο των δεδομένων που χρειάζονται να υποβληθούν σε επεξεργασία και απαιτούνται για την διεκπεραίωσή σύννομων καθηκόντων (πχ. δεδομένα που απαιτούνται για την μισθοδοσία ή την ασφάλιση των εργαζομένων). Εδώ θα πρέπει να σημειωθεί ότι θα πρέπει να τηρηθούν οι διαδικασίες ψευδωνυμοποίησης και κρυπτογράφησης όπως ορίζονται από τον κανονισμό στο άρθρο 32-α.

Ελάχιστες απαιτήσεις σχετικά με το backup:

Θα πρέπει να τηρούνται αντίγραφα ασφαλείας καθημερινά σε προκαθορισμένη ώρα.

Τύπος Δεδομένων: Δεδομένα Δοκιμών (Test Data) [τα οποία χρησιμοποιούνται κατά την διάρκεια του κύκλου ζωής ανάπτυξης λογισμικού]

Περιγραφή / Σχόλια:

Δεδομένα που χρησιμοποιούνται για testing εφαρμογών εάν μιλάμε για εταιρείες πληροφορικής που ασχολούνται με την ανάπτυξη εφαρμογών.

Ελάχιστες απαιτήσεις σχετικά με το backup:

Θα μπορούσε να μην τηρούνται αντίγραφα ασφαλείας. Εξαρτάται πάντα από τα δεδομένα. Αν είναι production data εσωτερικών εφαρμογών δεν χρειάζεται να διατηρούνται. Αν είναι δεδομένα πελάτη και διατηρούνται στις εγκαταστάσεις της εταιρείας θα πρέπει να υπάρχει τουλάχιστον ένα αντίγραφο ασφαλείας στα πλαίσια του testing των εφαρμογών. Εξαρτάται πάντα από τις διαδικασίες μιας εταιρείας αλλά και από τις διαδικασίες που ορίζονται στις συμβάσεις με τους πελάτες.

Τύπος Δεδομένων: Κώδικας (Code)

Περιγραφή / Σχόλια:

Κώδικας εφαρμογών, εφόσον μιλάμε για εταιρείες πληροφορικής που ασχολούνται με την ανάπτυξη εφαρμογών.

Ελάχιστες απαιτήσεις σχετικά με το backup:

Θα πρέπει να τηρούνται αντίγραφα ασφαλείας καθημερινά εφόσον μιλάμε για εσωτερικές εφαρμογές. Το ίδιο και σε ότι αφορά εφαρμογές που αναπτύσσονται για πελάτες εφόσον οι εργασίες γίνονται στις εγκαταστάσεις της εταιρείας. Στην περίπτωση των πελατών θα πρέπει να λαμβάνονται υπόψη οι διαδικασίες που ορίζονται τόσο από τον πελάτη όσο και από τις συμβάσεις μεταξύ των συμβαλλόμενων μερών.

Τύπος Δεδομένων: Emails

Περιγραφή / Σχόλια:

Τα emails τα οποία ανάλογα με την τεχνολογία που έχει μια εταιρεία είτε διατηρούνται σε cloud (πχ. Azure cloud λύσεις), είτε σε κάποιες περιπτώσεις διατηρούνται στον exchange server. Εδώ θα πρέπει να σημειωθεί ότι τα email αποτελούν θέμα μεγάλης κρισιμότητας, υποτιμημένης σε κάποιες περιπτώσεις εταιρειών, καθώς λόγω περιορισμένου storage στον exchange server (καθώς δεν έχει προβλεφθεί ή επενδυθεί κατάλληλο capacity) πολλοί χρήστες δημιουργούν archive files τοπικά και στις περισσότερες περιπτώσεις σε μη κρυπτογραφημένα αρχεία σε laptops που αφενός δεν πληρούν κανόνες ασφαλείας (πχ.bios password, password policy κτλ.) και μεταφέρονται εκτός εταιρείας κάτι που αυξάνει την επικινδυνότητα διαρροής δεδομένων λόγω κλοπής. Από την άλλη μεριά τα συγκεκριμένα δεδομένα σε περίπτωση

ολικής βλάβης ενός laptop δεν μπορούν να ανακτηθούν εφόσον έχουν μεταφερθεί τοπικά στο περιβάλλον εργασίας του χρήστη.

Ελάχιστες απαιτήσεις σχετικά με το backup:

Θα πρέπει να τηρούνται καθημερινά αντίγραφα ασφαλείας. Στις περιπτώσεις που αναφέραμε, όπου τα email διατηρούνται τοπικά από τους χρήστες δεν χρειάζεται να τηρείτε αντίγραφο ασφαλείας. Σε κάθε περίπτωση αν υπάρχει ανάγκη ύπαρξης αντιγράφων ασφαλείας, οι χρήστες θα πρέπει να ενημερώνονται για το που πρέπει να διατηρούν τα archive αρχεία τους ώστε να διασφαλίζεται ότι διατηρούνται τα αντίγραφα ασφαλείας όπως προβλέπεται από την πολιτική της εταιρείας.

4.2 Τοποθεσίες Αποκατάστασης (Recovery Sites)

Παρακάτω θα γίνει μια προσπάθεια να ορίσουμε την στρατηγική επαναφοράς των παρεχόμενων υπηρεσιών εντός του οργανισμού, οι οποίες απαρτίζονται από τρία (3) βασικά πράγματα:

- Δεδομένα,
- Πληροφοριακά συστήματα, hardware, δίκτυα και επικοινωνίες,
- Συστήματα ή υπηρεσίες που παρέχονται από τρίτους και από αυτά εξαρτάται η λειτουργία άλλων συστημάτων (σε αυτή την περίπτωση θα πρέπει να υπάρχει σύνδεση με το RTO των πρωτευόντων συστημάτων στα οποία υπάρχει εξάρτηση).

Η ανάκτηση των παραπάνω οντοτήτων απαιτούν μια προσεκτική ανάλυση ώστε να γίνει η σωστή επιλογή στρατηγικής και επίσης να αξιολογηθούν και τα ρίσκα [3.4] τα οποία θα προκύψουν σε περίπτωση που δεν ληφθούν τα κατάλληλα μέτρα (εργαλεία και διαδικασίες) λαμβάνοντας υπόψη το κόστος υλοποίησης τους αλλά και το κόστος που θα προκύψει σε περίπτωση που δεν υιοθετηθούν οι κατάλληλες τεχνικές.

Επίσης κατά την εκτίμηση και τον σχεδιασμό θα πρέπει να ληφθούν υπόψη οι παρακάτω παράμετροι:

- η άμεση διαθεσιμότητα πόρων για την επανάκαμψή των υπηρεσιών,
- προτεραιότητα ως προς την επανάκαμψη, δηλαδή ποιες υπηρεσίες / συστήματα πρέπει να αποκατασταθούν πρώτα,
- το κόστος που χρειάζεται για την αποκατάσταση αυτών, καθώς όσο ταχύτερη θέλουμε να είναι η επανάκαμψη τόσο μεγαλώνει και το κόστος.

Όσον αφορά την τοποθεσία επανάκαμψής θα πρέπει να σημειωθεί ότι θα πρέπει να είναι μακριά από το σημείο στο οποίο έγινε η καταστροφή:

- Σε άλλη τοποθεσία μέσα στον οργανισμό όπου είναι προγραμματισμένες να γι' αυτούς τους σκοπούς,
- Συμφωνίες με άλλους οργανισμούς,
- σε μισθωμένες εγκαταστάσεις που εξυπηρετούν αυτούς τους σκοπούς.

Παρακάτω παραθέτουμε εναλλακτικές λύσεις σε ότι αφορά το κομμάτι της επανάκαμψης:

- **Mirrored Sites**

Οι συγκεκριμένες εγκαταστάσεις κάνουν πλήρη αναπαραγωγή των πληροφοριών σε πραγματικό χρόνο και αποτελούν επί της ουσίας ένα αντίγραφο της πρωτεύουσας τοποθεσίας. Από άποψη διαθεσιμότητας έχουν άμεσο αποτέλεσμα και είναι μια από τις βέλτιστες λύσεις σε αυτό το επίπεδο. Σε σχέση με τις διεργασίες τα δεδομένα επεξεργάζονται και αποθηκεύονται ταυτόχρονα από την μία τοποθεσία στην άλλη. Οι συγκεκριμένοι χώροι μπορούν να λειτουργούν μέσα στον ίδιο οργανισμό προστατευμένοι και αποτελούν μια ακριβή λύση και αφορά συνήθως εταιρείες / οργανισμούς οι οποίοι απαιτούν άμεση διαθεσιμότητα των υπηρεσιών τους και το RTO των υπηρεσιών τους θα πρέπει να είναι **άμεσο ή λιγότερο από μια μέρα.**

- **Hot sites**

Οι εγκαταστάσεις αυτές αποτελούν ένα πλήρες αντίγραφο των αρχικών εγκαταστάσεων. Για να γίνει όμως λειτουργικό υπάρχει ανάγκη προσωπικού υποστήριξης το οποίο θα προετοιμάσει τις εγκαταστάσεις για να γίνουν λειτουργικές κάτι που χρειάζεται χρόνο. Αποτελούν μια σχετικά οικονομική λύση σε σχέση με άλλες, και αφορούν εταιρείες / οργανισμούς οι οποίοι μπορούν να αντέξουν την μη-διαθεσιμότητα για ένα λογικό χρονικό διάστημα, δεν εξυπηρετεί όμως εταιρείες οι οποίες έχουν ένα RTO με άμεσους δείκτες επανάκαμψής καθώς απαιτούνται κάποιες εργασίες για να γίνει λειτουργική η υποδομή.

- **Cold Sites**

Τα cold sites διαθέτουν την τεχνική υποδομή για να γίνει μια εγκατάσταση αλλά δεν διαθέτουν τον εξοπλισμό που σημαίνει ότι οι χρήστες θα πρέπει να έχουν μαζί τους laptops, εκτυπωτές κτλ. αλλά και άλλου είδους εξοπλισμό, όπως routers κτλ.. Η συγκεκριμένη λύση απαιτεί αρκετό χρόνο ανάκτησης και υλικό εξοπλισμό που είτε

πρέπει να υπάρχει σε απόθεμα για περίπτωση ανάγκης είτε να υπάρχει σύμβαση με εταιρείες που θα τον παρέχει σε περιπτώσεις που θα συμβεί κάποιο περιστατικό. Σε κάθε περίπτωση η συγκέντρωση αποθέματος εξοπλισμού αποτελεί και αυτή κόστος το οποίο πρέπει να επωμιστεί μια επιχείρηση, και επίσης πρέπει να λάβουμε υπόψη ότι ο χρόνος ανάκτησης αυξάνεται οπότε μιλάμε για μία λύση όπου ένας οργανισμός ή μια εταιρεία δεν έχουν από άμεση ανάκτηση της διαθεσιμότητας. Πολλές εταιρείες σε τέτοιες περιπτώσεις μοιράζονται τέτοιους χώρους με άλλες εταιρείες για μείωση κόστους, αρκεί βέβαια να μην συμβεί περιστατικό την ίδια στιγμή κάτι που καθιστά την ικανότητα (capacity) τέτοιων χώρων ανεπαρκές.

- **Warm sites**

Τα warm sites είναι ένας συνδυασμός hot και cold sites, ο χρόνος ανάκτησης είναι μεταξύ των δύο προαναφερθέντων, δηλαδή θα χρειαστεί περισσότερο χρόνο ανάκτησης από ένα hot site και λιγότερο από ένα cold site, οπότε καταλαβαίνουμε ότι πρόκειται για μια ενδιάμεση επιλογή. Περιλαμβάνει την κατάλληλη υποδομή, όπως επίσης και κάποιο βασικό εξοπλισμό όπως και λειτουργικά συστήματα. Συνήθως εταιρείες για μείωση κόστους 'μοιράζονται' τέτοιου είδους τοποθεσίες με άλλες εταιρείες όπως συμβαίνει και στα cold sites. Ο χρόνος ανάκτησης είναι αρκετός (1 ή 2 εβδομάδες) για να επανέλθει η πλήρης λειτουργικότητα των υπηρεσιών, όποτε η συγκεκριμένη λύση δεν αφορά εταιρείες που έχουν ένα RTO άμεσο.

- **Συμφωνίες μεταξύ εταιρειών**

Μια συνηθισμένη τακτική είναι εταιρείες ή οργανισμοί που είτε βρίσκονται στον ίδιο όμιλο είτε έχουν συνεργασίες ή συμφωνίες μεταξύ τους (για παράδειγμα λόγω κοινοπραξιών σε έργα έχουν κοινά συμφέροντα) για την υποστήριξη σε περίπτωση καταστροφής ή σε περίπτωση κάποιου συμβάντος που διακόπτει την επιχειρησιακή συνέχεια. Σε περίπτωση φυσικής καταστροφής είναι θεμιτό να είναι σε διαφορετικές περιοχές.

Σε κάθε περίπτωση, πριν επιλέξει μια εταιρεία ή ένας οργανισμός κάποια στρατηγική αποκατάστασης θα πρέπει να λάβει σοβαρά υπόψη το κόστος αλλά και τα RTO και RPO targets που έχει θέσει.

Η επιλογή mirrored και hot sites θεωρούνται αυτές που διασφαλίζουν ένα βέλτιστο επίπεδο επανάκαμψής και διασφαλίζουν άμεσα την επιχειρησιακή συνέχεια μιας εταιρείας / οργανισμού. Ενδεικτικά παρακάτω αναφέρουμε κάποιες παραμέτρους που

θα πρέπει να τηρούνται ώστε να διασφαλιστεί η ασφάλεια της συγκεκριμένης τοποθεσίας:

- Να τηρούνται οι αποστάσεις εγκατάστασης των rack στο data center για να την εξασφάλιση ιδανικών συνθηκών λειτουργίας.
- Να υπάρχει φυσική φύλαξη του χώρου ή του κτιρίου γενικότερα,
- Να τηρούνται οι απαιτήσεις που προβλέπονται στα πρότυπα ISO 9001 και ISO 27001.
- Προτείνεται η τοποθεσία όπου υπάρχει το disaster recovery site να είναι μια περιοχή με μικρό ιστορικό φυσικών καταστροφών (σεισμοί, πλημμύρες κτλ) όπως επίσης να είναι και σε απόσταση από πηγές ηλεκτρομαγνητικών παρεμβολών ή χημικής μόλυνσης (πχ. δίπλα από πρατήρια βενζίνης ή εργοστάσια).
- Να υπάρχει φωτισμός λειτουργίας ασφαλείας στις κτιριακές εγκαταστάσεις,
- Οι εγκαταστάσεις να διαθέτουν κατάλληλο σύστημα ανίχνευσης υγρασίας και υδάτων.
- Η τοποθεσία θα πρέπει να εξυπηρετείται μέσω ενσύρματων δικτύων (χαλκού, οπτικών ινών και 4G) από διαφορετικούς τηλεπικοινωνιακούς παρόχους με διπλές οδεύσεις, ώστε σε περίπτωση μεγάλης φυσικής καταστροφής να διασφαλιστεί η διαθεσιμότητα του δικτύου.
- Θα πρέπει να υπάρχει κλιματισμός με μονάδες κλειστού συστήματος με λειτουργία ψύξης, ύγρανσης και αφύγρανσης σε διάταξη τουλάχιστον N+1 (ύπαρξη παραπάνω κλιματιστικών).
- Να υπάρχει πλεονασμός κάλυψης των κλιματιστικών μονάδων στους χώρους φιλοξενίας του εξοπλισμού με πρόβλεψη υπερκάλυψης των αναγκών.
- Πρόβλεψη για UPS και γεννήτριες με συνδυασμένη διαθεσιμότητα 24 ωρών. Επίσης θα πρέπει να υπάρχουν ενεργητικά φίλτρα καταπολέμησης των αρμονικών για την ορθή λειτουργία των υπολογιστικών μονάδων του data center.
- Ύπαρξη αντικεραυνικής προστασίας και σύστημα προστασίας από υπερτάσεις / υποτάσεις. Επίσης θα πρέπει να υπάρχει πρόβλεψη διπλής όδευσης για το ηλεκτρολογικό δίκτυο διανομής, καθώς και ύπαρξη κατάλληλης γείωσης.
- Σε σχέση με την φυσική ασφάλεια θα πρέπει να υπάρχει :
    - έλεγχος πρόσβασης,

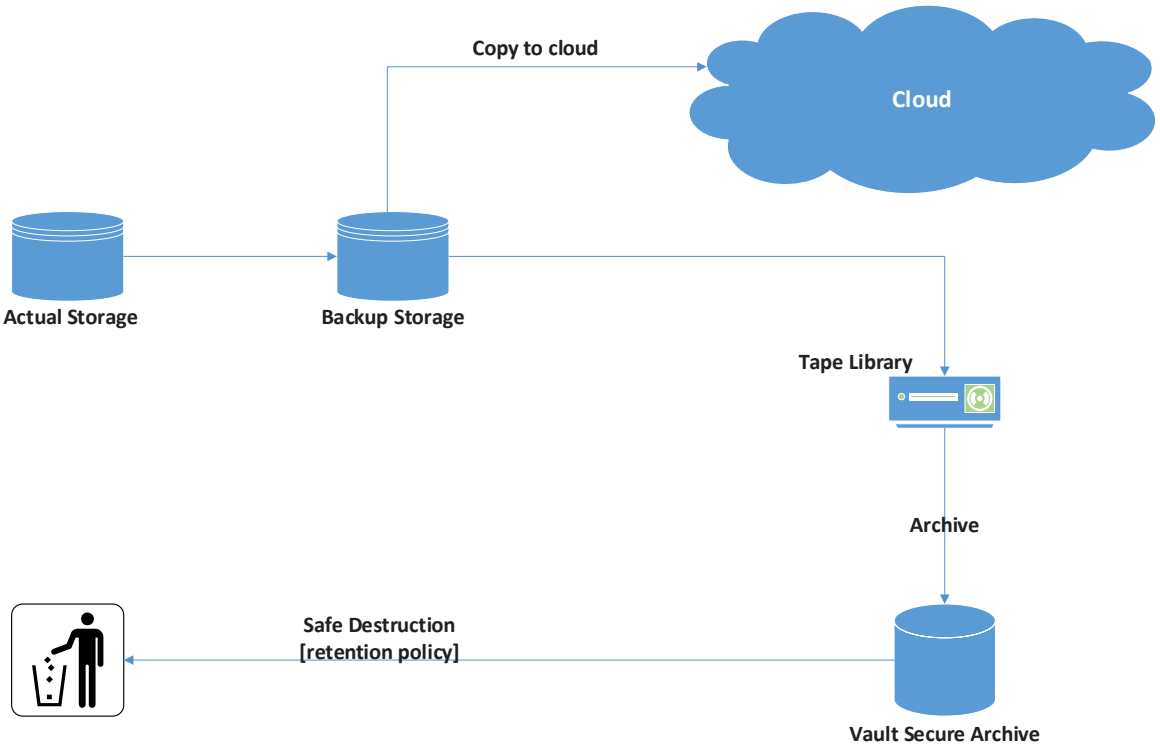
- ύπαρξη συστήματος παρακολούθησης και καταγραφής (CCTV), σε διάστημα αποδεκτό από τον κανονισμό προστασίας των προσωπικών δεδομένων (GDPR) (σε ότι αφορά τα καταγεγραμμένα video),
- ύπαρξη συστήματος συναγερμού με ηχητικό σήμα και διασύνδεση σε κέντρο λήψης σημάτων για την κάλυψη όλων των κτιριακών εγκαταστάσεων,
- ύπαρξη συστήματος ανίχνευσης πυρκαγιάς με σειρήνες συναγερμού, και πρόβλεψη χειροκίνητης ενεργοποίησης,
- ύπαρξη συστήματος κατάσβεσης ειδικό για χρήση σε data center,
- σχεδίαση του computer room ώστε να υπάρχει πυραντοχή για τουλάχιστον 30 λεπτά.

4.3 Τεχνολογικές Προτάσεις

Στις συγκεκριμένη ενότητα θα προταθούν κάποιες τεχνολογικές λύσεις (**Εικόνα 8**) λαμβάνοντας υπ' όψη τόσο την υψηλή διαθεσιμότητα (άρθρο 32-β) [1] και απόδοση, όσο και τις πιστοποιήσεις (άρθρο 42) [1] τους στον τομέα αυτό. Για την υψηλή, ασφαλή και εγγυημένη απόδοση επιλέχτηκαν εμπορικά προϊόντα (Commercial Off The Shelf) τα οποία πιστοποιούνται, ελέγχονται και βελτιώνονται συνεχώς σε πολύ μεγαλύτερο βαθμό από τα λογισμικά ελεύθερου κώδικα τα οποία σε πολλές περιπτώσεις δεν είναι αξιόπιστα. Για την επιλογή τους επίσης έγινε χρήση η αξιολόγηση της αναφοράς της εταιρείας αξιολογήσεων και συμβούλων Gartner [19] όπου κάθε έτος δημοσιεύει ανά τομέα την έκθεση «Gartner Magic Quadrant» στην οποία απεικονίζονται οι εταιρείες και τα προϊόντα τους στις εξής κατηγορίες Niche Players, Challengers, Visionaries και Leaders. Η επιλογή ενός προϊόντος από την κατηγορία Leaders εξασφαλίζει τη μέγιστη δυνατή απόδοση, ασφάλεια και ακεραιότητα σε ένα πληροφοριακό σύστημα.

Για την εξασφάλιση της λειτουργίας ενός κρίσιμου πληροφοριακού συστήματος πρέπει να μην υπάρχει κανένα μοναδικό σημείο αποτυχίας , ακόμα και σε επίπεδο data center. Ακολουθώντας αυτήν την οδηγία ακόμα και το σύστημα αντιγράφων ασφαλείας (backup) πρέπει να είναι πολυεπίπεδο. Έτσι η διαδικασία θα πραγματοποιείται αρχικά σε storage (backup to disk) και σε δεύτερο χρόνο θα γίνεται αντιγραφή στο cloud, ενώ για τη τήρηση ιστορικών αρχείων θα γίνεται μεταφορά σε tape libraries (λαμβάνοντας υπόψη τις πολιτικές διατήρησης των δεδομένων όπως προβλέπονται από τον κανονισμό). Επίσης το Backup Software παράλληλα παρέχει τη δυνατότητα

δημιουργίας διαφορετικών χρηστών και ομάδων χρηστών με διαφορετικές αρμοδιότητες και δικαιώματα εξασφαλίζοντας τα μέγιστα δυνατά επίπεδα ασφαλείας (άρθρο 23-2δ). Σε αυτούς τους χρήστες και ομάδες χρηστών αποδίδονται διαφορετικά δικαιώματα σε διαφορετικά file συστήματα και κόμβους καθώς και διαφορετικές δυνατότητες εκτέλεσης εντολών. Για την εξασφάλιση της ελάχιστης απώλειας δεδομένων προτείνεται σε τακτά χρονικά διαστήματα η λήψη στιγμιότυπων (snapshots) των δεδομένων σε ένα παράλληλο storage ίδιο με το παραγωγικό. Με αυτό τον τρόπο διασφαλίζουμε την διαθεσιμότητα αλλά και την άμεση αποκατάσταση όπως προβλέπεται από το άρθρο 32-1γ του κανονισμού.



Εικόνα 8. Backup & Recovery

4.3.1 Storage

Μια προτεινόμενη λύση, συνίστανται στη χρήση συστημάτων κορυφαίας τεχνολογίας συστημάτων storage που αξιοποιούν τεχνολογία tiering και software defined storage και παρέχουν μοναδικά τεχνολογικά πλεονεκτήματα και προσφέρουν σημαντικά οφέλη, όπως την αυτόματη μεταφορά των δεδομένων σε δίσκους με διαφορετικές τεχνολογίες και αποδόσεις εξασφαλίζοντας κατά αυτόν τον τρόπο την αποδοτικότερη χρήση, την διαθεσιμότητα των δεδομένων και τη μεγάλη αξιοπιστία καθώς δίδεται η δυνατότητα αυτόματου replication των δεδομένων σε disaster recovery site (άρθρο 32 1β-1γ). Επίσης η παραμετροποίηση τους επιτρέπει προκαθορισμένη πρόσβαση (άρθρο 23-2δ)

σε δεδομένα ικανοποιώντας πλήρως όσα προβλέπονται από τον κανονισμό προστασίας προσωπικών δεδομένων (GDPR). Τέτοιες λύσεις προσφέρουν σχεδόν όλοι οι μεγάλοι κατασκευαστές και αναφορικά μερικοί οι εξής, DELL/EMC, IBM, HPe , NetAPP, Hitachi [20], [21], [22], [23], [24].

4.3.1.1 Τεχνολογικά Χαρακτηριστικά

Οι τεχνολογίες που περιγράφηκαν στην προηγούμενη ενότητα παρουσιάζουν κάποια σημαντικά χαρακτηριστικά και παρουσιάζονται παρακάτω [20], [21], [22], [23], [24]:

- **Thin provisioning**

Με το thin provisioning είναι δυνατόν να καταναλώνεται σε ένα σύστημα αποθήκευσης μόνο η χωρητικότητα που πραγματικά χρησιμοποιείται, κατανέμοντας αυτόματα τον διαθέσιμο αποθηκευτικό χώρο σε πολλούς χρήστες, ανάλογα με τον ελάχιστο χώρο που χρειάζεται ο κάθε χρήστης σε ένα δεδομένο συγκεκριμένο χρονικό διάστημα (άρθρο 32-1β – διασφάλιση της διαθεσιμότητα [1]).

- **External Virtualization**

Με το External Virtualization μπορεί να χρησιμοποιηθεί αποθηκευτικός χώρος από πολλαπλά μέσα αποθήκευσης διαφορετικών κατασκευαστών (π.χ. EMC, HP, Sun, Fujitsu, NEC, κτλ.) και με αυτό τον τρόπο η συνολική προσφερόμενη χωρητικότητα μπορεί να φτάσει μέχρι μερικές δεκάδες Petabytes (άρθρο 32-1β – διασφάλιση της διαθεσιμότητα [1]). Όταν κάνουμε virtualize εξωτερικά (external) storage arrays (παρατάξεις), το IBM Storwize V7000 Gen2 για παράδειγμα μπορεί να παρέχει μέχρι 32PB χρήσιμης (usable) χωρητικότητας.

- **Tiering**

Το Tiering είναι μια λειτουργία βελτιστοποίησης της απόδοσης (performance) που αυτόματα μεταφέρει μέρος των δεδομένων ενός volume προς/από, SSD (Solid State Drives) αποθηκευτικά μέσα, από/σε HDD (μηχανικά) αποθηκευτικά μέσα αλλά και μεταξύ SAS και NL SAS δίσκων. Το Easy Tier παρακολουθεί τις αποδόσεις των δίσκων σε μια περίοδο 24 ωρών. Μετά μετακινεί δυναμικά τα υψηλής δραστηριότητας δεδομένα σε ένα υψηλότερο disk tier (SSDs) μέσα στο storage pool. Επίσης θα μετακινήσει τα δεδομένα των οποίων η δραστηριότητα (activity) έχει πέσει χαμηλά από το high tier (SSDs) πίσω στο lower tier (spinning HDDs).

- **Real time compression**

Το Real-time Compression είναι σχεδιασμένο για την αύξηση του αποθηκευτικού χώρου έως και 5 φόρες συμπιέζοντας τα δεδομένα έως και 80%. Σε αντίθεση με άλλες εφαρμογές, το RTC μπορεί να χρησιμοποιηθεί σε παραγωγικό περιβάλλον καθώς λειτουργεί ταυτόχρονα με την εγγραφή των δεδομένων στον δίσκο χωρίς να επηρεάζεται η απόδοση του συστήματος, ενώ δεν υπάρχει αχρησιμοποίητος χώρος στον δίσκο για την αποθήκευση μη συμπιεσμένων δεδομένων που περιμένουν να συμπιεστούν. Τα πλεονεκτήματα του Real-time Compression είναι πολύ σημαντικά και περιλαμβάνουν το χαμηλότερο κόστος κτήσης, λιγότερο χώρο στο rack, χαμηλότερη κατανάλωση κτλ.

- **Κρυπτογράφηση (Encryption)**

Το storage πρέπει υποστηρίζει encryption σε όλους τους δίσκους (άρθρο 32-1α, [1]). Έτσι εξασφαλίζεται ότι σε περίπτωση κακόβουλης αφαίρεσης δίσκων τα δεδομένα δεν θα είναι προσβάσιμα από μη εξουσιοδοτημένα άτομα (άρθρο 32-1β και 2, [1]).

4.3.2 Cloud

Η πρόταση σε cloud είναι το Microsoft Azure, η οποία είναι η cloud πλατφόρμα της Microsoft που φιλοδοξεί να μεταμορφώσει το παραδοσιακό data center προσφέροντας την δυνατότητα παροχής ευέλικτων υπηρεσιών καθώς και την εξυπηρέτηση χρηστών που θέλουν να συνεχίσουν να εργάζονται από οπουδήποτε, με οποιαδήποτε συσκευή με ένα συγκροτημένο και ασφαλή τρόπο (άρθρο 32-1β, [1]-διασφάλιση διαθεσιμότητας). Από τις μεγάλες πολυεθνικές που εκτείνονται σε διαφορετικές ηπείρους και έχουν την ανάγκη να διαμοιράζουν αντιστοίχως μεγάλα υπολογιστικά φορτία, μέχρι και την μικρή εταιρεία που αναζητά την γρήγορη δημιουργία ενός web site με παγκόσμια παρουσία, το Microsoft Azure αποτελεί μία πλατφόρμα που μπορεί να μετατρέψει το cloud σε εργαλείο εξυπηρέτησης των εκάστοτε επιχειρησιακών αναγκών [25].
Οι παρεχόμενες υπηρεσίες του Microsoft Azure κατανέμονται σε 4 βασικές κατηγορίες:

- **Compute Services:** Virtual machines, web sites, cloud services και mobile services.
- **Network services:** Virtual network ως προέκταση του τοπικού data center και Traffic Manager.

- **Data services:** Data management, Business analytics, HDInsight, Cache, Backup και Recovery Manager.
- **Application Services:** Media Services, Messaging, Notification Hubs, BizTalk Services, Active directory, ID management και Multifactor Authentication.

4.3.2.1 Αποθήκευση στο Cloud

Μέσα από την κατηγορία Data services προσφέρεται η δυνατότητα για ασφαλή και αξιόπιστη αποθήκευση στο Azure. Η δυνατότητα για Geolocation Hosting μέσα από 17 διαφορετικά data centers διάσπαρτα ανά την υφήλιο, διατηρεί τα δεδομένα ασφαλή και προσβάσιμα ακόμα και σε περίπτωση καταστροφής. Επίσης έτσι διασφαλίζεται η εφαρμογή του κανονισμού προστασίας προσωπικών δεδομένων, καθώς μπορεί να γίνει επιλογή του datacenter από πριν και να είναι εντός Ε.Ε διασφαλίζοντας όσα προβλέπονται από τον κανονισμό και ειδικά από το άρθρο 32 α-δ [1].

4.3.2.2 Backup

Το Azure προσφέρει έναν εύκολο τρόπο για να καλύψει την συγκεκριμένη ανάγκη είτε με δικά του εργαλεία είτε σε συνδυασμό με λύσεις άλλων κατασκευαστών, δημιουργώντας αντίγραφα με πλήθος πολιτικών τόσο από το τοπικό datacenter όσο και από άλλες συνεργαζόμενες υπηρεσίες cloud. Η διαδικασία Backup προσφέρει πλήρη κρυπτογράφηση των δεδομένων (άρθρο 32 1α [1]) για την εξασφάλιση της ασφαλούς πρόσβασης των δεδομένων.

4.3.2.3 Site Recovery

Το Azure site recovery βοηθάει στην προστασία κρίσιμων εφαρμογών ρυθμίζοντας την αντιγραφή και ανάκτηση εικονικών μηχανών ανάμεσα σε διαφορετικά sites προσφέροντας διέξοδο στην πολυπλοκότητα που εμπεριέχει μία υλοποίηση ενός DR site (άρθρο 32 1γ, [1]). Επίσης η επικοινωνία μεταξύ των διαφόρων sites είναι κρυπτογραφημένη (άρθρο 32 1α, [1]). Τέλος υπάρχει συνεχής έλεγχος της κατάστασης των διαφόρων υπηρεσιών και γίνεται αυτόματη μεταγωγή στο DR site σε περιπτώσεις διακοπής τους από το πρωτεύον Site, εξυπηρετώντας ακόμη και τα πλέον πολυεπίπεδα περιβάλλοντα (άρθρο 32 1β-1γ, [1]).

4.4 Επίλογος

Στην ανωτέρω ενότητα παρουσιάστηκαν τεχνολογικές λύσεις που οδηγούν στην επιτυχημένη ανάκαμψη ενός οργανισμού έπειτα από μια καταστροφή. Μια επιτυχημένη ανάκαμψη όμως δεν αποδεικνύεται εφόσον δεν υπάρξουν οι κατάλληλες δοκιμές που επικυρώνουν την ομαλή έκβαση της. Στο επόμενο κεφάλαιο θα παρουσιαστούν διαδικασίες που αφορούν τις δοκιμές αλλά και οι τακτικές , οι οποίες συμβάλουν στην επιχειρησιακή συνεχεια.

Θα δοθει επίσης έμφαση στην εκπαίδευση, την ενημέρωση και γενικότερα στην επαγρύπνηση (awareness) σε ότι αφορά την επιχειρησιακή συνέχεια, όπως προβλέπεται από το άρθρο 39-β του κανονισμού.

Τέλος στα πλαίσια της ‘άμυνας’ και μετριασμού της πιθανότητας κάποιου συμβάντος που θα απειλήσει την ασφάλεια ενός οργανισμού, θα προταθούν τεχνολογικές λύσεις που θωρακίζουν την ασφάλεια του και ελαχιστοποιούν τις πιθανότητες ενός συμβάντος ασφαλείας.

Κεφάλαιο 5

Διατήρηση της Επιχειρησιακής Συνέχειας

Η διατήρηση της επιχειρησιακής συνέχειας είναι μια συνεχής διαδικασία που περιλαμβάνει την συμμετοχή όλων, τόσο της ομάδας επιχειρησιακής συνέχειας όσο και του ίδιου του προσωπικού το οποίο θα πρέπει να είναι άρτια καταρτισμένο και εκπαιδευμένο τόσο για την διατήρηση αυτής όσο και στην αντίδραση του σε περίπτωση οποιαδήποτε περιστατικού.

Κάθε εταιρεία / οργανισμός πρέπει να έχει ένα συνεχές πρόγραμμα εκπαίδευσης και ενημέρωσης (πχ. Newsletters με ενημερώσεις κτλ.) αλλά και τακτικής άσκησης όπου θα προσομοιώνει τεχνητές συνθήκες 'καταστροφής' (πχ. έναρξη συναγερμού και εκκένωση κτιρίου, ή ψεύτικα phishing emails για την επαγρύπνηση των μελών ώστε να αναγνωρίζουν τέτοιες καταστάσεις και να μη προκύψει οποιαδήποτε διαρροή δεδομένων).

5.1 Πλάνο Δοκιμών

Μια εταιρεία στα πλαίσια της διατήρησης της επιχειρησιακής του συνέχειας θα πρέπει να τηρεί ένα πλάνο δοκιμών (**Πίνακας 6**) και ενημερώσεων ανάλογα της ανάγκες του και να τις καταγράφει στα πλαίσια των αποδείξεων που προβλέπονται από τον κανονισμό.

Έλεγχος	Περιγραφή	Περιοδικότητα
Ενημέρωση πλάνων (updates)	Έλεγχος των πλάνων (BCP / DRP) και ενημέρωση όπου χρειάζεται σε περίπτωση που υπάρχουν αλλαγές ή κρίνεται απαραίτητο να επαναπροσδιοριστούν διαδικασίες. Θα πρέπει να γίνει επίσης έλεγχος και ενημέρωση, όπου χρειάζεται στις διαδικασίες και στις πολιτικές που εμπλέκονται στο BCP/DRP. Σε αυτή την ενημέρωση βοηθάει η διαδικασία διαχείρισης των αλλαγών που περιγράψαμε σε προηγούμενο κεφάλαιο καθώς [3.7].	Ετησίως (ή συντομότερα σε περίπτωση που υπάρχουν αλλαγές)
Έλεγχος πλάνου ως προς την ετοιμότητα και την αλληλεπίδραση των εμπλεκομένων	Διαδικαστικός έλεγχος σε ότι αφορά την αλληλεπίδραση και συνεργασία των ατόμων που εμπλέκονται σε περίπτωση κάποιου συμβάντος ή μιας καταστροφής. Για παράδειγμα σε περίπτωση ενός data breach τι διαδικασίες πρέπει να ακολουθηθούν, ποιοι πρέπει να ενημερωθούν κτλ	Ετησίως (ή συντομότερα σε περίπτωση αλλαγών στις θέσεις των εμπλεκομένων)
Τεχνητή Προσομοίωση	Τεχνητή προσομοίωση μιας κατάστασης. Για παράδειγμα σήμανση συναγερμού και εκκένωση κτιρίου. Σε αυτή την περίπτωση θα πρέπει να ελεγχθούν αν τα πλάνα των κτιρίων είναι σε ετοιμότητα, εάν οι επικοινωνίες είναι ενημερωμένες, εάν οι άνθρωποι είναι εκπαιδευμένοι για τις εξόδους κινδύνου σε περίπτωση κάποιου	Τουλάχιστον 1 φορά το χρόνο

	συμβάντος κτλ.	
Δοκιμή των λειτουργιών	Σε αυτή την περίπτωση θα πρέπει να γίνει δοκιμή όλων των λειτουργιών και διαδικασιών στο disaster recovery site. Θα πρέπει να προσομοιωθεί μια κατάσταση και όλοι οι εμπλεκόμενοι να μεταβούν στο recovery site και να ελεγχθούν όλες οι λειτουργικότητες, όπως επίσης και οι εκτέλεση των διαδικασιών όπως προβλέπεται από το πλάνο. Εδώ θα πρέπει να σημειωθεί ότι αυτή η άσκηση θα πρέπει να γίνει σε κάποια προγραμματισμένη μη-εργάσιμη ώρα ώστε να μην διακοπούν οι εργασίες των εμπλεκομένων και οι υπηρεσίες που παρέχει ο οργανισμός.	2 φορές το χρόνο
Δοκιμή πεδίου	Η δοκιμή πεδίου αφορά την δοκιμή μιας συγκεκριμένη λειτουργικότητας, όπως για παράδειγμα την επαναφορά / ανάκτηση ενός συστήματος. Στην δοκιμή πεδίου θα μπορούσαν να ενταχθούν και οι έλεγχοι ασφάλειας (πχ. penetration testing ενός συστήματος) ή η δοκιμή των αντιγράφων ασφαλείας (backup) δειγματοληπτικά σε κάποια συστήματα.	4 φορές το χρόνο ή και περισσότερες εφόσον υπάρχουν αλλαγές σε κάποια συστήματα ή όποτε κρίνεται απαραίτητο
Πλήρης Δοκιμή	Η πλήρης δοκιμή είναι και αυτό που περιγράφει η λέξη, δοκιμή όλων των λειτουργιών της επιχείρησης, όπως επίσης και του recovery site εμπεριεχόμενης της μετεγκατάστασης σε αυτό. Αποτελεί μια πολύπλοκη διαδικασία η οποία θα πρέπει να είναι προσεκτικά	Ετησίως

	συντονισμένη καθώς δοκιμάζονται όλες οι διαδικασίες που πρέπει να ακολουθηθούν βήμα προς βήμα σε περίπτωση κάποιας καταστροφής.	
Audit	Το audit μπορεί να γίνεται είτε από εσωτερική ομάδα καταρτισμένη ειδικά στην επιχειρησιακή συνέχεια (εμπεριεχομένων των ISO 9001, ISO 27001, GDPR κτλ), είτε από εξωτερικούς ανεξάρτητους φορείς. Σε αυτό σημείο θα πρέπει να σημειωθεί ότι θα πρέπει να υπάρχει ένα πλήρες audit plan που θα περιλαμβάνει όλους τους ελέγχους που θα πρέπει να γίνουν από τον auditor. Τα ευρήματα που θα καταγραφούν θα πρέπει να αξιολογηθούν και να επιλυθούν ώστε να επαναξιολογηθούν τα μέτρα που ελήφθησαν στο επόμενο audit.	Τουλάχιστον μια φορά το χρόνο

Πίνακας 6. Πλάνο Δοκιμών

5.1.1 Δοκιμή Backup

Τα δεδομένα που αφορούν το backup θα πρέπει να ελέγχονται τακτικά ώστε να διασφαλίζεται η εγκυρότητα τους και ότι μπορούν να χρησιμοποιηθούν όταν αυτό είναι απαραίτητο. Όπως αναφέρουμε παραπάνω στην δοκιμή πεδίου (**Πίνακας 6**) θα πρέπει τακτικά, είτε γιατί έχουν γίνει κάποιες αλλαγές στα συστήματα, είτε για λόγους εγκυρότητας θα πρέπει να δοκιμάζονται τα αντίγραφα ασφαλείας ότι είναι λειτουργικά. Πέραν αυτού μπορούν να γίνονται δοκιμές και στις προγραμματισμένες περιόδους αλλά και στα πλαίσια άλλων δοκιμών που περιγράφηκαν σε προηγούμενη ενότητα (**Πίνακας 6**).

Κατά την διαδικασία της δοκιμής θα πρέπει να ελέγχονται κάποιοι παράμετροι όπως:

- τα δεδομένα μπορούν να αποκατασταθούν πλήρως,
- ότι η διαδικασία γίνεται στα πλαίσια του καθορισμένου RTO,

- τα δεδομένα μπορούν να εγκατασταθούν στο σύστημα του recovery site ή στο σύστημα που υπάρχει στα πλαίσια των εν λόγω δοκιμών,
- η επάρκεια του προσωπικού τόσο σε επίπεδο διαδικασιών όσο και τεχνικών γνώσεων στα πλαίσια της αποκατάστασης.

Η συγκεκριμένη δοκιμή όπως και κάθε άλλη θα πρέπει να καταχωρείτε και να σχολιάζονται τα αποτελέσματα αυτής όπως και κάλυψη των παραμέτρων που προαναφέραμε. Σε περίπτωση ανεπιτυχών δοκιμών τα αποτελέσματα θα πρέπει να διερευνώνται και να καταγράφονται, όπως επίσης να εντοπίζεται η πηγή του προβλήματος και να αποκαθίσταται οποιαδήποτε πρόβλημα ή βλάβη. Όταν γίνει αυτή η αποκατάσταση θα πρέπει να επαναληφθούν οι δοκιμές για να εξακριβωθεί ότι έγινε η πλήρη αποκατάσταση. Επίσης απαιτείται και χειροκίνητος δειγματοληπτικός έλεγχος ή χρήση τεχνικών functional testing στα δεδομένα που αποκαταστάθηκαν για να εξακριβωθεί η αξιοπιστία τους.

Σε περιπτώσεις δεδομένων όπου υπάρχουν αρχεία χρόνων τα οποία μια εταιρεία τα κρατάει για λόγους αρχειοθέτησης (εξαιρούμε από αυτή την περίπτωση τα προσωπικά δεδομένα), όπως περιπτώσεις τεχνικών προδιαγραφών συστημάτων που υλοποιήθηκαν χρόνια πριν αλλά διατηρούνται στα αρχεία της εταιρείας, δεδομένης της τεχνολογικής προόδου και της συνεχόμενης αλλαγή των τεχνολογιών θα πρέπει να γίνεται ένας τακτικός έλεγχος επίσης ώστε να εξασφαλιστεί ότι τα συγκεκριμένα δεδομένα / αρχεία μπορούν να αποκατασταθούν πλήρως.

5.2 Εκπαίδευση και Ενημέρωση

Όπως προβλέπεται από το άρθρο 39-β του κανονισμού ο υπεύθυνος προστασία των δεδομένων θα πρέπει να ενημερώνει και να ευαισθητοποιεί τους ανθρώπους (τόσο αυτούς που εμπλέκονται στις πράξεις επεξεργασίας όσο και τους υπόλοιπους) μιας εταιρείας / οργανισμού για θέματα που έχουν να κάνουν με την προστασία των προσωπικών δεδομένων. Πέραν αυτού του άρθρου η κουλτούρα ασφάλειας υπονοείται σε πολλά άρθρα καθώς για να είναι ένας οργανισμός 'ασφαλής' είναι ευθύνη όλων των εμπλεκομένων. Η εδραίωση μιας κουλτούρας ασφάλειας είναι απαραίτητη στις σύγχρονες επιχειρήσεις, και κάθε σύγχρονος οργανισμός πέρα από του μηχανισμούς και τις διαδικασίες ασφάλειας που πρέπει να έχει, πρέπει να ενημερώνει και να εκπαιδεύει το προσωπικό κατάλληλα ώστε να ελαχιστοποιεί τον κίνδυνο οποιασδήποτε

‘καταστροφής’ και να διασφαλίζει με αυτό τον τρόπο την ομαλή επιχειρησιακή συνέχεια. Παρακάτω αναφέρουμε κάποιους μεθόδους επαγρύπνησης του προσωπικού μιας εταιρείας σχετικά με θέματα ασφάλειας:

- Ύπαρξη πολιτικών ασφαλείας οι οποίες επικοινωνούνται σε όλους τους υπαλλήλους, όπως επικοινωνείτε και οποιαδήποτε ενημέρωση (update) / αλλαγή μπορεί να γίνει σε αυτές τις πολιτικές. Για παράδειγμα, password policy, κώδικες δεοντολογίας, κώδικες τήρησης απορρήτου και εμπιστευτικότητας, κώδικες που αφορούν την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, access control policy κτλ.
- Awareness Trainings τουλάχιστον δύο (2) φορές το χρόνο με ανανεωμένο περιεχόμενο σε σχέση τόσο με τις ευπάθειες που μπορεί να προκύψουν αλλά και με παραδείγματα περιστατικών που έχουν συμβεί σε άλλες εταιρείες και έχουν δημοσιευθεί.
- Newsletters με ενημερώσεις ασφαλείας.
- Induction training για θέματα ασφαλείας στους νέοπροσληφθέντες.
- Χρήση gamification μεθόδων που αφορούν το security awareness τόσο σε επίπεδο ασφάλειας προσωπικού υπολογιστή όσο και σε επίπεδο training.

5.3 Ασφάλεια Πληροφοριακών Συστημάτων

Ένα μοντέρνο πληροφοριακό σύστημα καλείται να παρέχει ασφάλεια σε πολλαπλά επίπεδα έτσι ώστε να διασφαλίσει την ακεραιότητα, την διαθεσιμότητα καθώς και την εμπιστευτικότητα των δεδομένων (άρθρο 32 1 και 2). Για να επιτευχθεί αυτό απαιτείται ο προσεχτικός σχεδιασμός ασφαλών πολιτικών περιλαμβάνοντας τεχνικές, διαδικασίες και διοικητικά μέτρα, προφυλάσσοντας από κάθε είδους απειλή τυχαία ή σκόπιμη. Πρέπει επίσης να εξασφαλίζουν την απρόσκοπτη λειτουργία των συστημάτων που προστατεύουν. Για τη διαμόρφωση της πολιτικής προστασίας απαιτείται πρώτα να εντοπιστούν οι πιθανοί παράγοντες και ρίσκα που μπορεί να υπάρχουν μετά να αξιολογηθούν ως προς την πιθανότητα και στη συνέχεια να υλοποιηθεί η διαμόρφωση του πλαισίου για τον σχεδιασμό πολιτικών σχεδιασμού ασφαλείας.

Στο σχεδιασμό της πολιτικής ασφαλείας πρέπει να περιλαμβάνονται όλοι οι παράγοντες που εμπλέκονται με την λειτουργία του πληροφοριακού συστήματος, τόσο εσωτερικά όσο και εξωτερικά και θα πρέπει να καλύπτονται οι ακόλουθες κατηγορίες:

- Ασφάλεια Δικτύου (εσωτερικά / εξωτερικά),

- Ασφάλεια Συστημάτων,
- Ασφάλεια και πρόσβαση προσωπικού,
- Φυσική ασφάλεια,
- Έλεγχος πρόσβασης στο πληροφοριακό σύστημα
- Κεντρική Διαχείριση υλικών και λογισμικών
- Νομικές υποχρεώσεις
- Υλοποίηση Προτύπων ασφαλείας
- Διαχείριση της πολιτικής ασφάλειας
- Συνεχής ενημέρωση του δοκιμή του BCP/DRP

5.3.1 Ασφάλεια Δικτύου

Για την ορθή και απρόσκοπτη λειτουργία του δικτύου απαιτείται η χρήση Next Generation Firewalls σε διάταξη υψηλής διαθεσιμότητας. Η επιλογή της εταιρείας Fortinet που κατέχει θέση leader στο Gartner Reports. [26]

Προτείνεται η σειρά 1500 μέσω του λειτουργικού συστήματος FortiOS της Fortinet το FortiGate υποστηρίζει τα εξής χαρακτηριστικά ενοποιημένης ασφαλείας [27]:

- Stateful inspection,
- Anti-virus,
- Web filtering,
- Application control,
- Intrusion protection,
- Anti-spam,
- Data leak prevention,
- Web application firewall,
- VPN (IPsec, SSL),
- Denial of Service protection.

Το FortiGate 1500D [27] εξασφαλίζει υψηλές δικτυακές επιδόσεις με ενεργοποιημένες τις υπηρεσίες ασφαλείας, μέσω εξειδικευμένων ψηφιακών επεξεργαστών (FortiASIC), τους οποίους έχει αναπτύξει η ίδια η Fortinet.

Το FortiGate 1500D [27] διαθέτει τους εξής επεξεργαστές FortiASIC:

- Network Processor NP-6. Ενισχύει με υλικό (Hardware Acceleration) την λειτουργία του stateful inspection σε IPv4, IPv6 και multicast, την λειτουργία VPN, το Intrusion Prevention και traffic shaping/priority queueing.
- Content Processor CP-8. Ενισχύει με υλικό λειτουργίες που βρίσκονται εκτός της ροής πληροφορίας, όπως κρυπτογράφηση/αποκρυπτογράφησή και εποπτεία περιεχομένου βασισμένου σε υπογραφές (signature based content inspection).

Μέσω αυτών των εξειδικευμένων ψηφιακών επεξεργαστών, το FortiGate 1500D επιτυγχάνει εξαιρετικά υψηλές επιδόσεις. Αναφέρονται ενδεικτικά:

- Firewall throughput 80/80/55Gbps (για πακέτα IPv4 και IPv6 1518/512/64/84 byte),
- Firewall latency 3μs (64 byte UDP),
- Packet forwarding (stateful inspection) 82.5Mpps,
- NGFW throughput (IPS + Application Control) 7Gbps,
- Threat protection throughput (IPS + Application Control + Malware protection) 5Gbps,
- Ενσωματωμένος αποθηκευτικός χώρος 480GB,
- Ενσωματωμένο λογισμικό διαχείρισης και εποπτείας (Web GUI & CLI),
- Για την συλλογή αρχείων καταγραφής (log), διαχείριση, επεξεργασία και ανάλυσή τους, δημιουργία αναφορών και διαχείριση συμβάντων, προσφέρεται το λογισμικό FortiAnalyzer της Fortinet σε μορφή VM,
- Λειτουργία σε διάταξη υψηλής διαθεσιμότητας active/active, active/passive cluster,
- Υποστηρίζει την δημιουργία 10 Virtual Domain (VDOM) για δημιουργία ισάριθμων εικονικών firewall. Η δυνατότητα αυτή μπορεί να επεκταθεί μέχρι τα 250 VDOM με προσθήκη αντίστοιχης άδειας επέκτασης,
- Λειτουργία σε 3ο επίπεδο (route mode) ή 2ο επίπεδο (transparent mode). Οι λειτουργίες αυτές ενεργοποιούνται σε επίπεδο εικονικού firewall, άρα μπορούν να συνυπάρχουν στο FortiGate,
- Υποστήριξη όλων των ανοικτών πρωτοκόλλων δρομολόγησης για IPv4 και IPv6 (RIPv1, RIPv2, RIPng, OSPFv2, OSPFv3, BGP, BGP-4+, integrated IS-IS) και φυσικά στατική δρομολόγηση.

Οι προαναφερθείσες υπηρεσίες ενοποιημένης ασφαλείας υποστηρίζονται από την Fortinet σε πραγματικό χρόνο και σε εικοσιτετράωρη (24) βάση μέσω της υπηρεσίας FortiGuard. Η υπηρεσία FortiGuard εξασφαλίζει αυτόματη ενημέρωση για κάθε καινούρια ευπάθεια/ψηφιακή υπογραφή κακόβουλης κίνησης, η οποία ανιχνεύεται σε παγκόσμια βάση από τα FortiGuard Labs και διατηρεί κάθε FortiGate ενημερωμένο και προστατευμένο. Επίσης θα πρέπει να αναφέρουμε ότι με την ανωτέρω τεχνολογία διασφαλίζουμε στα πλαίσια της ασφάλειας του δικτύου ότι προβλέπεται από το άρθρο 32-1β του κανονισμού και αφορά την διασφάλιση του απορρήτου, της ακεραιότητας και της αξιοπιστίας των συστημάτων [1]. Επιπλέον πέραν των δυνατοτήτων του firewall σε intrusion detection και antivirus προτείνονται επιπλέον εξειδικευμένα λογισμικά με τις παραπάνω λειτουργίες για μέγιστη διασφάλιση της ακεραιότητας και αξιοπιστίας των δεδομένων ενός οργανισμού.

5.3.2 Antivirus

Σαν τεχνολογική πρόταση για antivirus προστασία προτείνεται το «Kaspersky Endpoint Security for Business – Advanced» [28] το οποίο περιλαμβάνει σάρωση τρωτότητας και τεχνολογίες patch διαχείρισης ώστε να συμβάλει στην εξάλειψη τρωτών σημείων στα λειτουργικά συστήματα και στο λογισμικό εφαρμογών. Επιπλέον, προσφέρει ευέλικτες λειτουργίες κρυπτογράφησης που συμβάλλουν στην προστασία των εταιρικών δεδομένων σε περίπτωση που χαθεί ή κλαπεί ένας φορητός υπολογιστής ή μια αφαιρούμενη συσκευή αποθήκευσης . Σε αυτό το σημείο θα πρέπει να αναφέρουμε ότι καλύπτουμε το άρθρο 32-1α και 1β του κανονισμού, όπου απαιτεί κρυπτογράφηση των δεδομένων και διασφάλιση του απορρήτου, της ακεραιότητας και της αξιοπιστίας σε συνεχή βάση [1].

Το εν λόγω εργαλείο περιλαμβάνει τις εξής λειτουργικότητες: Antivirus, Antispyware, Firewall, Application / Device / Web Control, Mobile Security, Data Encryption, Systems Management και Κονσόλα κεντρικής διαχείρισης.

5.3.3 Radar Incident Response Management (Διαχείριση Απόκρισης Περιστατικών)

Το RADAR Incident Response Management (Διαχείριση Απόκρισης Περιστατικών) [29] (**Εικόνα 9**) είναι ένα βραβευμένο λογισμικό διαχείρισης και απόκρισης περιστατικών

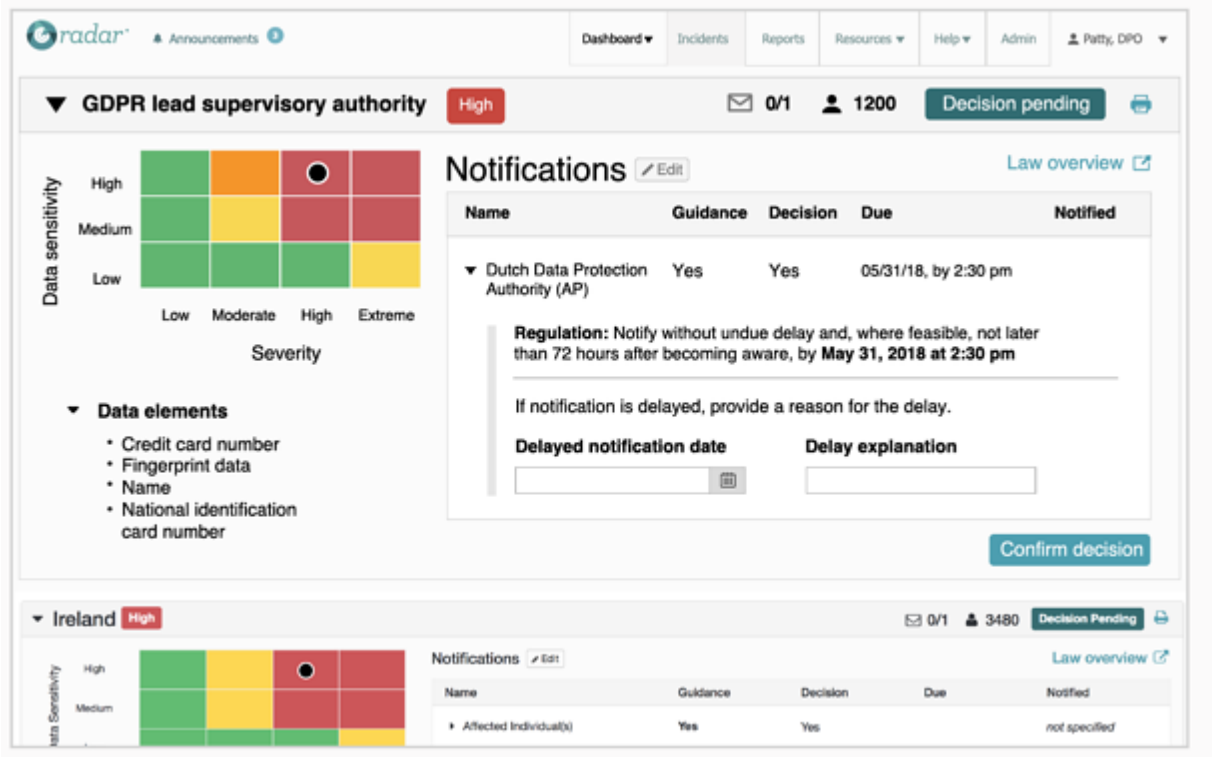
που εμπιστεύονται μεγάλοι οργανισμοί και βιομηχανίες που υπόκεινται στον γενικό κανονισμό για την προστασία των δεδομένων. Με τη χρήση του συγκεκριμένου εργαλείου έχουμε μια αυτοματοποιημένη ανταπόκριση σε περιστατικά που υπόκεινται στους ισχύοντες κανονισμούς (GDPR), συμπεριλαμβανομένης της απαιτούμενης διαδικασίας αξιολόγησης των κινδύνων πολλαπλών παραγόντων, και βοηθάει στην εξασφάλιση συνεκτικών και αξιόπιστων αποφάσεων. Οι δυνατότητες αναφοράς βοηθούν στον προσδιορισμό πού και πώς συμβαίνουν τα επεισόδια/συμβάντα σε έναν οργανισμό.

Το RADAR καθοδηγεί τους χρήστες μέσω διαδικασίας καθορισμού και αξιολογεί εάν ένα περιστατικό συγκαταλέγεται στην κατηγορία απορρήτου ή αφορά συμβάν ασφάλειας. Μέσω διεργασιών δημιουργείτε ένα σχέδιο αντιμετώπισης περιστατικών και δίνονται κατευθυντήριες οδηγίες σύμφωνα με όσα προβλέπονται από τον κανονισμό προστασίας προσωπικών δεδομένων. Το RADAR παρέχει όλα τα απαιτούμενα δικαιολογητικά για να υποστηρίξει την υποχρέωση βάρους αποδείξεως του οργανισμού βάσει των νόμων περί παραβίασης [29] (άρθρο 32, άρθρο 33 και άρθρο 34).

Παρακάτω παρατίθενται κάποια από τα χαρακτηριστικά του:

- Incident Risk Assessment: Αυτοματοποιημένη αξιολόγηση κινδύνου και καθοδήγηση σχετικά με τις παραβιάσεις δεδομένων προσωπικού χαρακτήρα εξασφαλίζοντας την συμμόρφωση ενός οργανισμού με τους κανόνες / νόμους περί παραβίασης που προβλέπονται από τον κανονισμό (GDPR).
- Notifications Letters Module: Παρακολούθηση των απαιτήσεων κοινοποίησης προβλέπονται από τον κανονισμό (ενδεικτικά αναφέρουμε το άρθρο 33 και άρθρο 40), συμπεριλαμβανομένου του ποιος θα πρέπει να ειδοποιηθεί, με ποιον τρόπο και σε ποια ημερομηνία. Κάθε ειδοποίηση παραμένει αποθηκευμένη στο σύστημα διατηρώντας ένα ολοκληρωμένο αρχείο συμβάντων.
- Incident Management Dashboard: Δυνατότητες σάρωσης ελέγχου για την διαχείριση περιστατικών, τον εντοπισμό των γενικότερων τάσεων, το μετριασμό του κινδύνου και την παρακολούθηση της κατάστασης των περιστατικών.
- Reports: Δημιουργία αναφορών μέσω δυναμικών φίλτρων, καλύπτοντας ανάγκες περί ανάλυσης δεδομένων μέσα από την ίδια την εφαρμογή.

- Central Repository: Αποθήκευση συμβάντων, εγγράφων, σημειώσεων, αναφορών και λιστών ελέγχου τα οποία μπορούν να χρησιμοποιηθούν στα πλαίσια εσωτερικών δοκιμών ή ελέγχων (testing / internal audits) αλλά και εξωτερικών (external audits).
- Administration & Policy: 'Role based access control' – και δυνατότητες παραμετροποίησης στην αξιολόγηση πολιτικών συμβάντων.
- Web Submission Forms: οι χρήστες έχουν την δυνατότητα να υποβάλλουν εσωτερικά στην εταιρεία στους αρμοδίους περιστατικά για περαιτέρω αξιολόγηση/έρευνα μέσω αυτή της λειτουργικότητας.
- Contractual Obligations Workflow: Ροή εργασιών (workflow) για επέκταση λειτουργικότητας, η οποία μπορεί να παραμετροποιηθεί με τέτοιον τρόπο ώστε να διασφαλιστεί η συμμόρφωση ενός οργανισμού με οποιοδήποτε κανονισμό (GDPR) ή συμβατική υποχρέωση (εδώ ισχύει σε περιπτώσεις πελατών μιας εταιρείας που έχουν αυστηρά security conventions καθορισμένα στα πλαίσια των συμβολαίων), αλλά και δυνατότητες κοινοποίησης σε περίπτωση ενός συμβάντος.



Εικόνα 9. RADAR incident response and decision-support platform [30]

5.4 Επίλογος

Στην ανωτέρω ενότητα παρουσιάστηκαν τεχνικές που αφορούν την εκτέλεση των δοκιμών αλλά και επαγρύπνησης του προσωπικού σε σχέση με θέματα ασφάλειας και επιχειρησιακής συνέχειας. Παρέχονται τεχνολογικές προτάσεις και λύσεις που διασφαλίζουν την ασφάλεια σε έναν οργανισμό και κατ' επέκταση την επιχειρησιακή συνέχεια.

Στο επόμενο κεφάλαιο, όπου είναι και το τελευταίο της εν' λόγω μεταπτυχιακής διατριβής ακολουθεί μια εφαρμογή η οποία αποτελεί τεχνική πρόταση για την δημιουργία ενός πλήρους πλάνου επιχειρησιακής συνέχειας και ανάκαμψής (BCP / DRP). Στις ενότητες αυτής της εφαρμογής μπορούν να εισαχθούν / εφαρμοστούν όσα προαναφέρθηκαν στις παραπάνω ενότητες. Ο χρήστης έχει πλήρη υποστήριξη μέσω των οδηγιών / κατευθύνσεων που παρέχονται μέσα από την εφαρμογή και μπορεί να οργανώσει αποτελεσματικά το πλάνο του.

Κεφάλαιο 6

Εφαρμογή BCP/DRP

Οι συνεχείς και αυξανόμενες απαιτήσεις στον τομέα της πληροφορικής δημιουργούν συνεχώς ανάγκες στον τομέα της ασφάλειας ακόμη και στις πιο μικρές εταιρείες πληροφορικής. Η ύπαρξη ενός BCP / DRP είναι απαραίτητη πλέον σε όλους καθώς με την έναρξη ισχύος του νέου κανονισμού για τα προσωπικά δεδομένα ακόμα και η πιο μικρή εταιρεία θα πρέπει να αποδεικνύει ότι διαθέτει αφενός όλα τα τεχνικά μέσα (άρθρο 32 1α και 1β) που καθιστούν την οντότητα της ασφαλή και αφετέρου να υπάρχουν γραπτώς όλες εκείνες οι πολιτικές και οι διαδικασίες (άρθρο 32 1γ-1δ και άρθρο 40) που διασφαλίζουν την επιχειρησιακή της συνέχεια αλλά και συνδράμουν στην ομαλή αποκατάσταση της σε περίπτωση οποιαδήποτε συμβάντος.

Πέραν της υιοθέτησης τεχνικών μέσων και μεθόδων, σημαντική επίσης είναι και ο προσεκτικός σχεδιασμό ενός πλάνου επιχειρησιακής συνέχειας και επανάκαμψής, Σε αυτό το σημείο κάθε επαγγελματίας πληροφορικής θα πρέπει να είναι σε θέση να μπορεί να έχει εικόνα των πόρων της επιχείρησης του αλλά και των διαδικασιών που χρειάζονται για να διασφαλίσει την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα τόσο των πληροφοριών που επεξεργάζεται (εμπεριεχομένου των προσωπικών δεδομένων) όσο και των πόρων που χρησιμοποιεί για να έχει πρόσβαση σε αυτές.

6.1 Εφαρμογή «BCP / DRP Guidelines»

Η εφαρμογή 'BCP-DRP Generator' λειτουργεί σαν οδηγός για την δημιουργία ενός πλάνου επιχειρησιακής συνέχειας και ανάκτησης (Business Continuity Plan/Disaster Recovery Plan) για μια επιχείρηση, καθώς επίσης και σαν πρότυπο (template), δίνοντας τη δυνατότητα στον χρήστη να παραμετροποιήσει το εν λόγω πλάνο σύμφωνα με τις ανάγκες του. Στις ενότητες της εφαρμογής εμπεριέχονται οι βασικές μεταβλητές / παράμετροι που πρέπει να κατέχει ένας χρήστης για την δημιουργία ενός BCP / DRP. Στα πλαίσια της παραμετροποίησης μπορεί να αφαιρέσει ή να εισάγει όσες πληροφορίες κρίνονται απαραίτητες σύμφωνα με τις ανάγκες του.

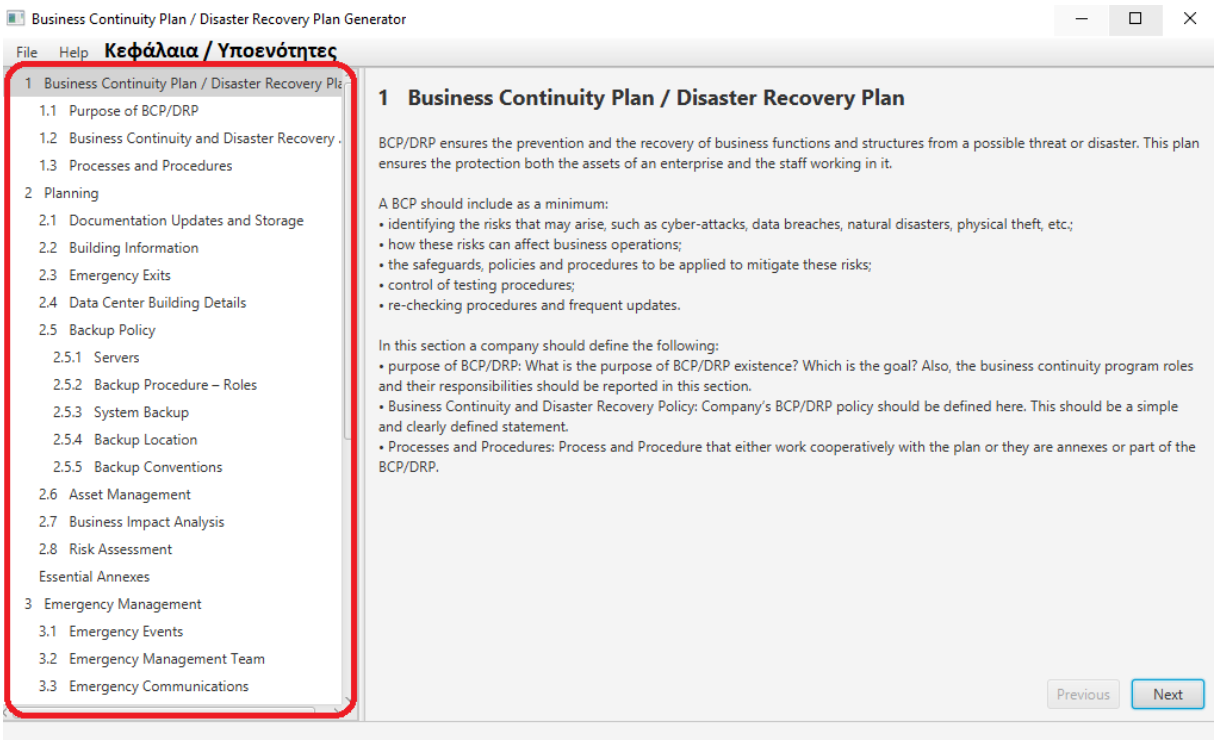
Η εφαρμογή αυτή μπορεί να χρησιμοποιηθεί από νέους επαγγελματίες πληροφορικής ή ακόμα και από ανθρώπους που διαχειρίζονται νεοσυσταθείσες εταιρείες τόσο στον τομέα πληροφορικής αλλά και σε οποιοδήποτε τομέα, που πλέον είναι αναγκαιότητα, διαχειρίζεται πληροφοριακά συστήματα.

Την τελευταία διετία παρατηρείται στην ελληνική επικράτεια μια εξωστρέφεια και όλο και περισσότερες εταιρείες start-up ιδρύονται στην Ελλάδα με βασικό πελατολόγιο τόσο στην Ελλάδα όσο και στο εξωτερικό (Κράτη-Μέλη και Τρίτες Χώρες). Αυτού του είδους οι εταιρίες παρόλο που επιδεικνύουν επάρκεια στο αντικείμενο που αντιπροσωπεύουν (πχ. εταιρείες game development, mobile marketing, software development κτλ.), έχουν αρκετές ελλείψεις στο κομμάτι της ασφάλειας και στο κομμάτι των γραπτών διαδικασιών που πλαισιώνουν αυτή. Σε αυτό το σημείο μια τέτοια εφαρμογή σε συνδυασμό με την εν λόγω μελέτη / διατριβή θα μπορούσε να λειτουργήσει σαν ένας οδηγός στην κατανόηση αλλά και στην εφαρμογή μεθόδων που συνδράμουν στην επιχειρησιακή συνέχεια και οργανωσιακή κουλτούρα. Σε αυτό το σημείο θα πρέπει να σημειωθεί ότι πέραν της αναγκαιότητας και των γενικότερων εξελισσόμενων απαιτήσεων που υπάρχουν γύρω από την ασφάλεια και την επιχειρησιακή συνέχεια, πολλοί πελάτες εταιρειών πλέον εισάγουν σαν απαίτηση στα συμβόλαια τους μεταξύ εταιρειών την ύπαρξη BCP/DRP και την υποβολή του στα πλαίσια υλοποίησης έργων πληροφορικής. Η εφαρμογή BCP/DRP generator καλύπτει όλες εκείνες τις απαιτήσεις που μπορεί να έχει ένας πελάτης από μια μικρή εταιρεία πληροφορικής, η οποία αφενός έχει υιοθετήσει όλα εκείνα τα σύγχρονα μέσα που διασφαλίζουν την ασφάλεια αλλά και την επιχειρησιακή της συνέχεια (πχ. λύσεις cloud storage, μεθόδους κρυπτογράφησης κτλ) αλλά υστερεί στο διαδικαστικό και διαχειριστικό κομμάτι.

6.1.1 Βασική Λειτουργία Εφαρμογής

Σε αυτή την ενότητα θα περιγράψουμε τις βασικές λειτουργικότητες της εφαρμογής σε επίπεδο χρήστη. Η εφαρμογή παρέχει στον χρήστη ένα προκαθορισμένο template / σκελετό πλάνου, το οποίο όμως είναι πλήρως παραμετροποιήσιμο σε επίπεδο τιμών των μεταβλητών στα πλαίσια της εφαρμογής , αλλά και σε επίπεδο δομής όταν γίνει export σε .docx αρχείο.

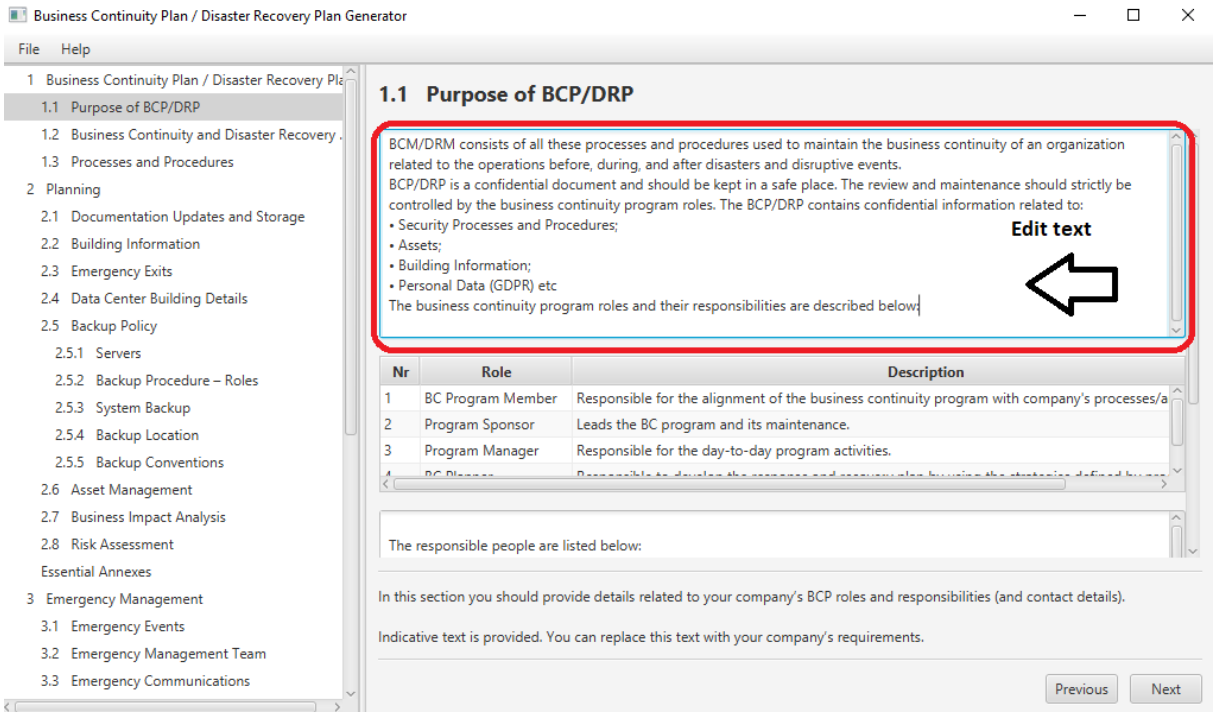
Στην στήλη αριστερά φαίνονται όλα τα κεφάλαια και υποενότητες του BCP/DRP βάσει του προκαθορισμένου template (**Εικόνα 10**). Ο χρήστης επιλέγοντας ένα από τα κεφάλαια, μπορεί να δει στο δεξιό τμήμα της εφαρμογής κάποια βασικές οδηγίες για την υλοποίηση του πλάνου του, καθώς επίσης και να επεξεργαστεί λεπτομέρειες για το επιλεγμένο κεφάλαιο.



Εικόνα 10. BCP/DRP Generator - Κεφάλαια/Υποενότητες

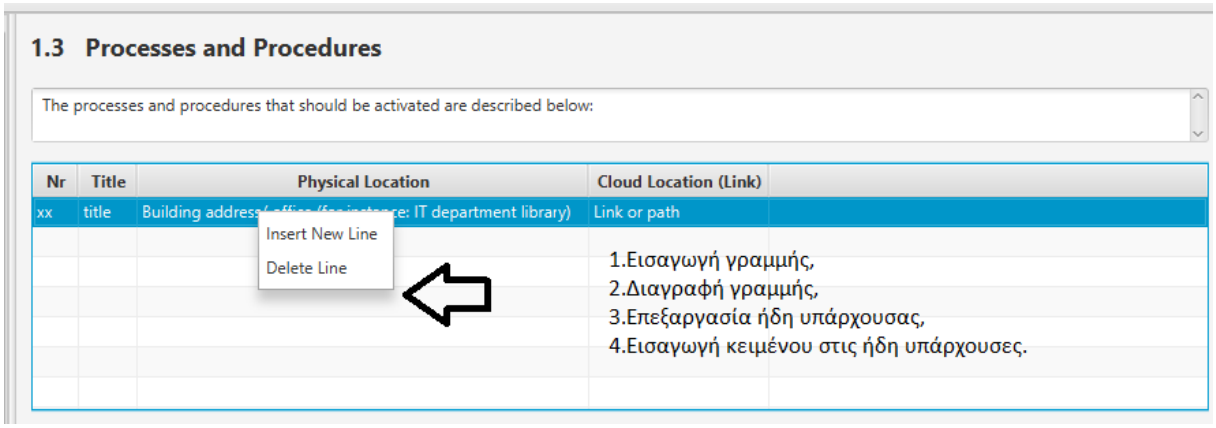
Η επεξεργασία (**Εικόνα 11**) μιας υποενότητας κεφαλαίου και η εισαγωγή κειμένου από τον χρήστη γίνεται με 2 τρόπους μέσα από την εφαρμογή:

- Με τη χρήση ενός πλαισίου κειμένου (text area), όπου ο χρήστης μπορεί να προσθέσει κείμενο ή να αλλάξει το ήδη υπάρχον.



Εικόνα 11. Επεξεργασία υπάρχοντος κειμένου / Δημιουργία καινούργιου περιεχομένου

- Με τη χρήση πίνακα (**Εικόνα 12**), στον οποίο μπορεί ο χρήστης να προσθέσει νέες γραμμές (Insert New Line) ή να αφαιρέσει τυχόν υπάρχουσες (Delete Line), ή να επεξεργαστεί τις ήδη υπάρχουσες καθώς υπάρχει κείμενο με οδηγίες για το τι πρέπει να εισάγει ο χρήστης.



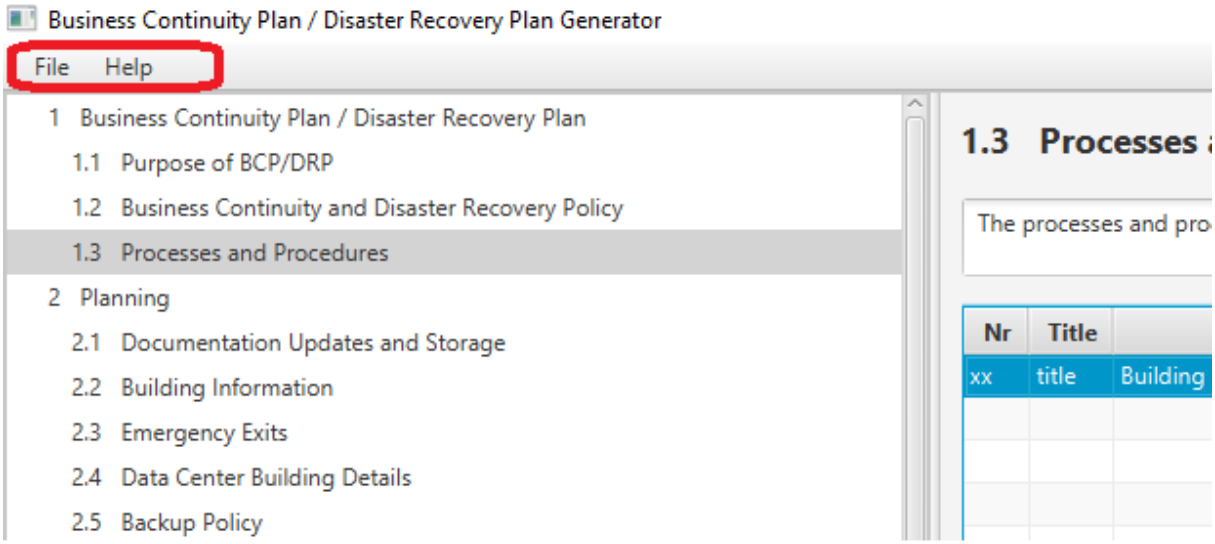
Εικόνα 12. Επεξεργασία περιεχομένου σε πίνακες

Τέλος, μετά την επεξεργασία, ο χρήστης μπορεί να εξάγει το τελικό πλάνο του σε ένα αρχείο Word (αρχείο μορφής .docx) και να το επεξεργαστεί όπως ο ίδιος θέλει. Μπορούν να διαγραφούν ενότητες που δεν χρειάζονται, όπως επίσης και να προστεθούν νέες. Εφόσον εξαχθεί σε αρχείο .docx, το πλάνο είναι πλήρως επεξεργάσιμο με όλες τις λειτουργικότητες των αρχείων Word. Ο χρήστης μετά την πρώτη επεξεργασία μέσα από

την εφαρμογή και εφόσον εξαχθεί το αρχείο σε μορφή .docx μπορεί να συντηρεί το πλάνο του και προσθέτει τις ενημερώσεις όπως γίνεται με όλα τα αρχεία .docx μορφής. Η εφαρμογή μετά από αυτό το στάδιο έχει ολοκληρώσει τον σκοπό της.

Τα menu (**Εικόνα 13**) που βρίσκονται στο πάνω μέρος της οθόνης προσφέρουν τις εξής λειτουργικότητες / επιλογές :

- File:
  - Export to word: εξαγωγή του αρχείου σε .docx όταν ο χρήστης ολοκληρώσει την συμπλήρωση του πλάνου του και θελήσει να εξάγει το αρχείο σε μορφή .docx.
  - Exit: έξοδος από την εφαρμογή.
- Help:
  - Help: Απλές οδηγίες για την εφαρμογή και τις λειτουργικότητες που προσφέρει.
  - About: Πληροφορίες σε σχέση με τα πλαίσια υλοποίησης της εφαρμογής.



Εικόνα 13. Menu File & Help

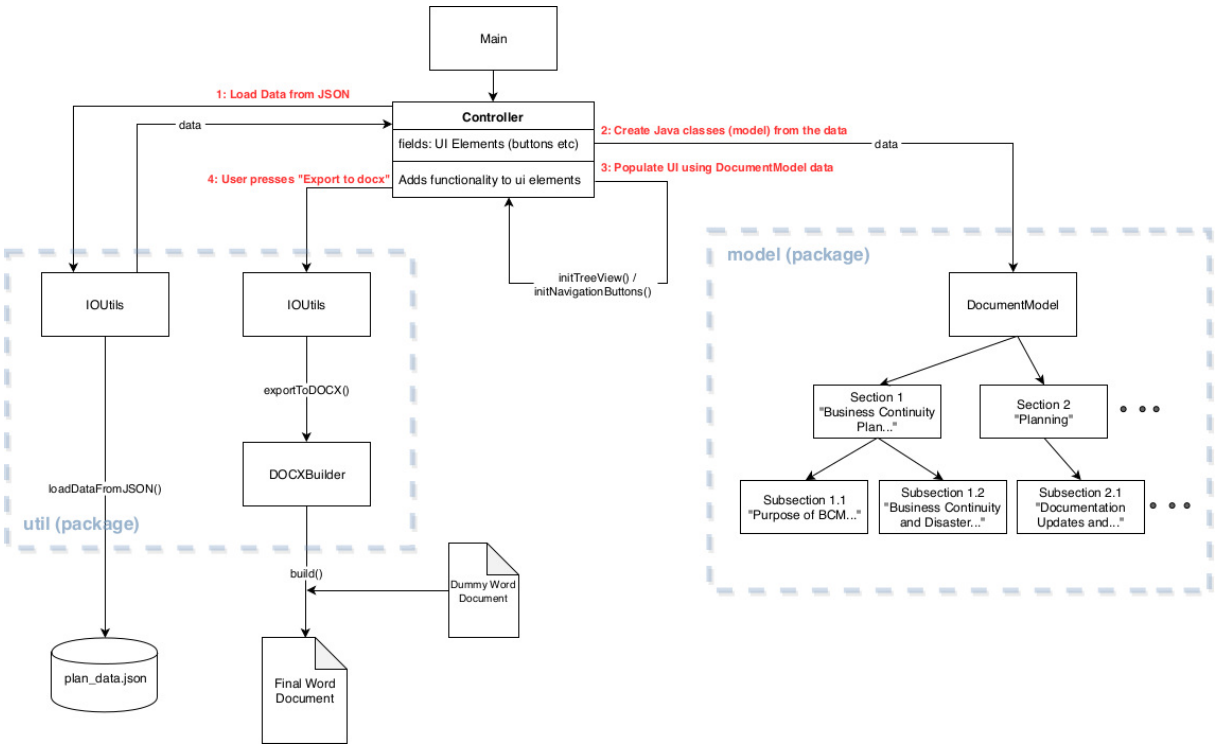
6.1.2 Τεχνικά Χαρακτηριστικά και Λειτουργία

Η εφαρμογή είναι υλοποιημένη σε Java 8, χρησιμοποιώντας τη βιβλιοθήκη ανοικτού κώδικα (ASLv2) docx4j version 6.1.2, η οποία χρησιμοποιείται για την εξαγωγή των δεδομένων του πλάνου σε αρχείο .docx.

Για τη δημιουργία του User Interface χρησιμοποιήθηκε η πλατφόρμα Java FX, η οποία είναι μέρος της Java. Η μορφή της εφαρμογής είναι ένα εκτελέσιμο αρχείο .jar. Εσωτερικά, η εφαρμογή έχει αποθηκευμένα όλα τα δεδομένα του BCP/DRP template σε ένα αρχείο .json.

- Με το άνοιγμα της εφαρμογής, φορτώνονται όλα τα παραπάνω δεδομένα από το αρχείο .json και απεικονίζονται στο χρήστη.
    - Για τη φόρτωση των δεδομένων χρησιμοποιείται η βιβλιοθήκη ανοικτού κώδικα **Jackson**, η οποία είναι μέρος της docx4j.
    - Η απεικόνιση γίνεται είτε με Text Area, είτε με Table (εξαρτάται από τον τύπο των δεδομένων, το οποίο καθορίζεται μέσα στο .json αρχείο).
- Ο χρήστης στη συνέχεια μπορεί να επεξεργαστεί τα δεδομένα μέσω του UI (user interface).
    - Στο αριστερό τμήμα της εφαρμογής απεικονίζονται όλα τα κεφάλαια/υποενότητες του πλάνου, μέσω ενός Tree View.
    - Ο χρήστης κάνοντας κλικ πάνω σε ένα οποιοδήποτε κεφάλαιο, μπορεί να δει στο δεξιό τμήμα της εφαρμογής (edit view), όλα τα δεδομένα του επιλεγμένου κεφαλαίου.
    - Στο δεξιό τμήμα της εφαρμογής επίσης, απεικονίζονται και κάποιες οδηγίες/guidelines για το επιλεγμένο κεφάλαιο σε ένα Label. Το κείμενο των guidelines φορτώνεται επίσης από το αρχείο .json.
- Τέλος αφού ο χρήστης επεξεργαστεί το πλάνο, μπορεί να εξάγει το πλάνο σε μορφή **.docx**, επιλέγοντας το "File → Export to docx" Menu Item.
    - Για αυτή τη λειτουργία η εφαρμογή χρησιμοποιεί ένα (εσωτερικά αποθηκευμένο) κενό dummy αρχείο "template.docx" με κάποια προκαθορισμένα styles, τα οποία χρησιμοποιούνται για τη μορφοποίηση του τελικού αρχείου .docx.
    - Όλα τα περιεχόμενα του τελικού αρχείου .docx δημιουργούνται εξολοκλήρου από την εφαρμογή με κώδικα, με τη χρήση της βιβλιοθήκης docx4j, και προστίθενται στο dummy .docx αρχείο.

Παρακάτω, παρατίθεται ένα διάγραμμα (**Εικόνα 14)** στο οποίο φαίνεται οι γενική ροή του κώδικα και μία γενική εικόνα των σχέσεων μεταξύ των διαφόρων τμημάτων της εφαρμογής:



Εικόνα 14. Class Diagram

6.1.3 Δομή Αρχείου .json

Το αρχείο .json (**Εικόνα 15**) περιέχει όλα τα δεδομένα του πλάνου, λειτουργεί δηλαδή σαν template αυτού. Ο τρόπος δόμησης των δεδομένων μέσα στο αρχείο αυτό γίνεται όπως φαίνεται στην παρακάτω εικόνα:

```
[ {
  "title" : "Purpose of BCP/DRP",
  "index" : "1.1",
  "guidelines" : "Lorem ipsum dolor sit amet...",
  "subsections" : null,
  "contents" : [ {
    "type" : "paragraph",
    "text" : "BCM/DRM consist of all these processes and procedures..."
  }, {
    "type" : "table",
    "columns" : [ {
      "header" : "Role",
      "width" : 1352
    }, {
      "header" : "Description",
      "width" : 3360
    } ],
    "records" : [ {
      "values" : [ "BC Program Member", "Responsible for the alignment of the business..." ]
    }, {
      "values" : [ "Program Sponsor", "Leads the BC program and its maintenance." ]
    }],
    "caption" : "Business Continuity Program Roles"
    }
  ]
},
{
  "title" : "Business Continuity and Disaster Recovery Policy",
  "index" : "1.2",
  "guidelines" : "Lorem ipsum dolor sit amet...",
  "subsections" : [{"..."}],
  "contents" : [{"..."}]
} ]
```

Εικόνα 15. Δομή Αρχείου .Json

Στην παραπάνω εικόνα φαίνεται ένα παράδειγμα 2 κεφαλαίων.

- Το κάθε κεφάλαιο είναι ένα αντικείμενο Json (περικλείεται από **{}**).
- Το κάθε κεφάλαιο περιέχει τα πεδία:
    - Title: ο τίτλος του κεφαλαίου,
    - Index: η αρίθμηση του κεφαλαίου,
    - Guidelines: κείμενο που λειτουργεί σαν οδηγός προς το χρήστη για το παρόν κεφάλαιο,
    - Subsections: είναι Json Array (πίνακας) ο οποίος περιέχει τυχόν υποενότητες του παρόντος κεφαλαίου,
    - Contents: Json Array που περιέχει τα περιεχόμενα του κεφαλαίου. Αυτά μπορεί να είναι:
        - Παράγραφος (type: paragraph),
        - Table (type: table).

6.1.4 Αξιολόγηση Εφαρμογής

Η εφαρμογή "BCP/DRP Guidelines" δόθηκε προς αξιολόγηση σε ένα στοχευμένο δείγμα επαγγελματιών της πληροφορικής και της ασφάλειας συστημάτων. Στους εν λόγω επαγγελματίες δόθηκε η εφαρμογή προς μελέτη και αξιολόγηση, όπως επίσης και ένα ερωτηματολόγιο που απαρτιζεται από δεκαπέντε (15) ερωτήσεις. Οι επαγγελματίες επιλέχτηκαν προσεκτικά και στοχευμένα από εταιρείες πληροφορικής και από βιομηχανίες στην Ελλάδα, αλλά και στο εξωτερικό. Για την διεξαγωγή της έρευνας χρησιμοποιήθηκε το on line εργαλείο "Survey Monkey". Οι ερωτήσεις αλλά και οι πολλαπλές επιλογές στις οποίες υποβλήθηκαν οι επαγγελματίες παρατίθενται παρακάτω:

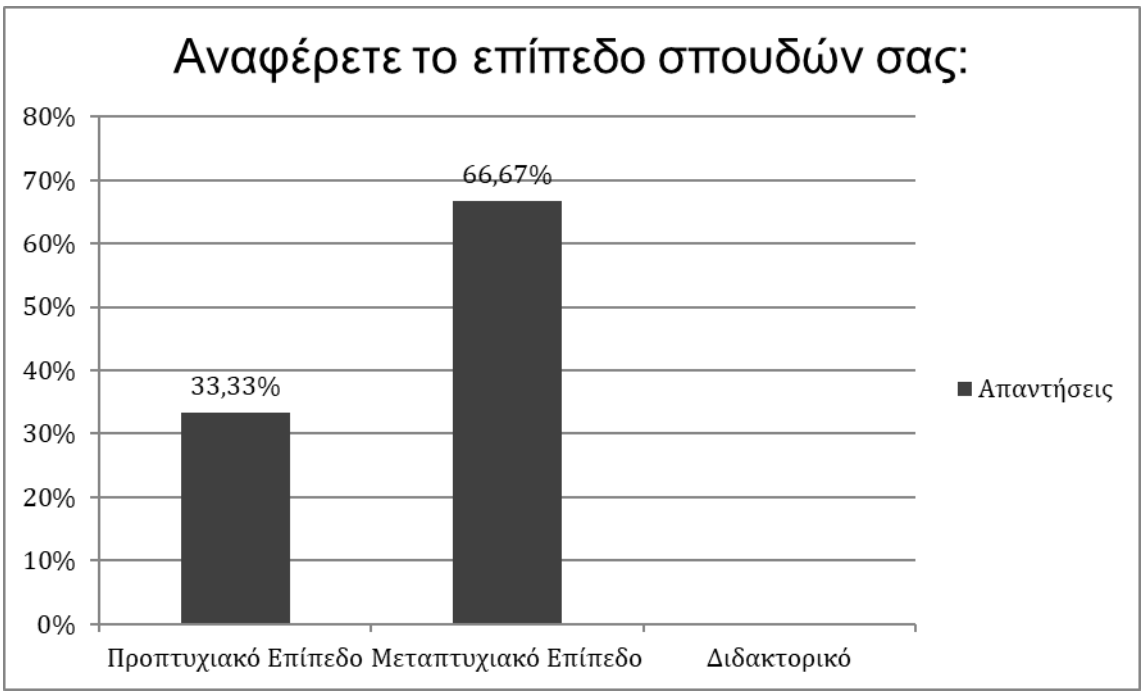
1. **Αναφέρετε το επίπεδο σπουδών σας:** [Προπτυχιακό επίπεδο, Μεταπτυχιακό επίπεδο, Διδακτορικό]
2. **Αναφέρετε την ειδικότητα σας:** [IT, Software Development / Engineer, IT Security, QHSE, Other]
3. **Αναφέρετε την επαγγελματική σας ιδιότητα:** [Ιδιωτικός Υπάλληλος, Δημόσιος Υπάλληλος, Επιχειρηματίας, Ελεύθερος Επαγγελματίας]
4. **Αναφέρετε την ιδιότητα της εταιρείας/οργανισμού που εργάζεστε:** [Εταιρεία Πληροφορικής, Βιομηχανία, Δημόσιος Φορέας / οργανισμός εντός εθνικών ορίων (Ελλάδα), Δημόσιος Φορέας / οργανισμός εντός ευρωπαϊκής ένωσης, Άλλο]
5. **Αναφέρετε τα χρόνια προϋπηρεσίας σας:** [1-5, 5-10, 10 και άνω]
6. Έχετε BCP/DRP στην εταιρεία / οργανισμό που εργάζεστε; [NAI, OXI, Προς άμεση υλοποίηση]
7. **Πόσο πιθανό θα ήταν να χρησιμοποιήσετε την προτεινόμενη εφαρμογή για την υλοποίηση του BCP / DRP πλάνου της εταιρείας / οργανισμού σας;** [Πολύ πιθανό, Πιθανό, Ούτε πιθανό ούτε απίθανο, Απίθανο, Πολύ πιθανό]
8. **Θεωρείτε την εφαρμογή φιλική προς το χρήστη;** [Πάρα πολύ φιλική, Πολύ φιλική, Σχετικά φιλική, Όχι και τόσο φιλική, Καθόλου φιλική]
9. **Θεωρείτε επαρκείς / αποτελεσματικές τις πληροφορίες που παρέχονται για βοήθεια στον χρήστη;** [Πολύ αποτελεσματικές, Αποτελεσματικές, Σχετικά αποτελεσματικές, Όχι και τόσο αποτελεσματικές]

10. **Θεωρείτε επαρκείς / αποτελεσματικές τις οδηγίες συμπλήρωσης του πλάνου, που παρέχονται στον χρήστη;** [Πολύ αποτελεσματικές, Αποτελεσματικές, Σχετικά αποτελεσματικές, Όχι και τόσο αποτελεσματικές]
11. **Πόσο ευχαριστημένοι είστε με την εμφάνιση αυτής της εφαρμογής;** [Πολύ ευχαριστημένος, Ευχαριστημένος, Ούτε ευχαριστημένος ούτε δυσαρεστημένος, Δυσαρεστημένος, Πολύ δυσαρεστημένος]
12. **Το περιεχόμενο της εφαρμογής (ενότητες BCP / DRP) ικανοποιεί τις απαιτήσεις σας;** [Πολύ ικανοποιητικό, Ικανοποιητικό, Ούτε ικανοποιητικό ούτε μη ικανοποιητικό, Όχι και τόσο ικανοποιητικό, Καθόλου ικανοποιητικό]
13. **Τι θα προτείνατε για να βελτιωθεί το περιεχόμενο της συγκεκριμένης εφαρμογής;** [Ελεύθερο κείμενο]
14. **Τι θα προτείνατε για να βελτιωθεί η εφαρμογή σε τεχνικό επίπεδο;** [Ελεύθερο κείμενο]
15. **Θα προτείνατε την εφαρμογή σε κάποιο συνάδελφό σας;** [Πολύ πιθανό να πρότεινα, Πιθανό να πρότεινα, Ούτε πιθανό ούτε απίθανο να πρότεινα, Απίθανο να πρότεινα, Πολύ απίθανο να την πρότεινα]

6.1.4.1 Συγκεντρωτικά Γραφήματα Αξιολόγησης

Από το δείγμα των δέκα (10) επαγγελματιών που εστάλει η εφαρμογή προς αξιολόγηση ανταποκρίθηκαν οι έξι (6) και απήντησαν στο ερωτηματολόγιο που παρατέθηκε παραπάνω. Παρακάτω παρατίθενται διαγραμματικά τα αποτελέσματα που προέκυψαν ανα ερώτημα.

Στο πρώτο γράφημα (**Εικόνα 16**) βλέπουμε ότι το 33,33% των ερωτηθέντων έχουν επίπεδο σπουδών προπτυχιακού επιπέδου και το 66,67%, όπου αποτελεί και την πλειοψηφία, είναι κάτοχοι μεταπτυχιακού τίτλου σπουδών.



Εικόνα 16. Αποτελέσματα 'Ερώτημα 1'

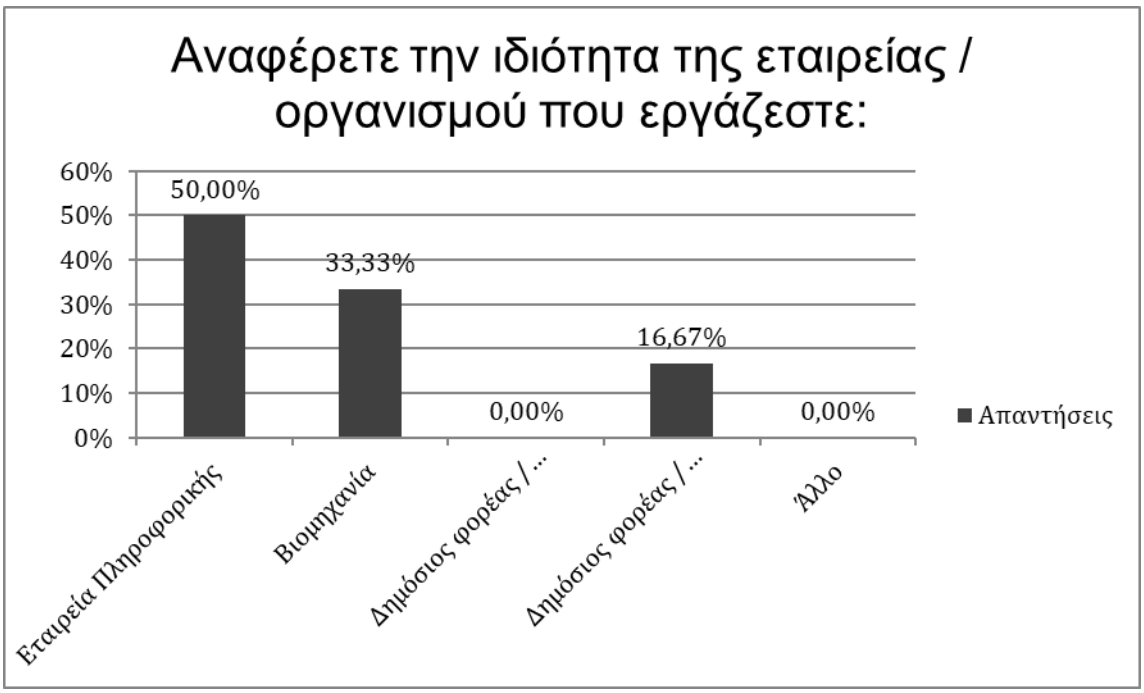
Στο ερώτημα 2 (**Εικόνα 17**) βλέπουμε ότι η πλειοψηφία των ερωτηθέντων προέρχεται από τον τομέα του IT με ποσοστό 50%, και ακολουθούν ειδικότητες όπου προέρχονται από τον τομέα του Software Development/Engineering (16,67%), IT Security (16,67%) και QHSE (16,67%).

Εικόνα 17. Αποτελέσματα 'Ερώτημα 2'

Στο ερώτημα 3 (**Εικόνα 18**) βλεπουμε μια σχετική διασπορά των επαγγελματικών ιδιοτήτων των ερωτηθέντων καθώς το 66,67%, που αποτελεί και την πλειοψηφία, προέρχεται από τον ιδιωτικό τομέα και ακολουθούν επαγγελματίες που προέρχονται από τον δημόσιο τομέα (16,67%) αλλά και το επιχειρείν (16,67%).

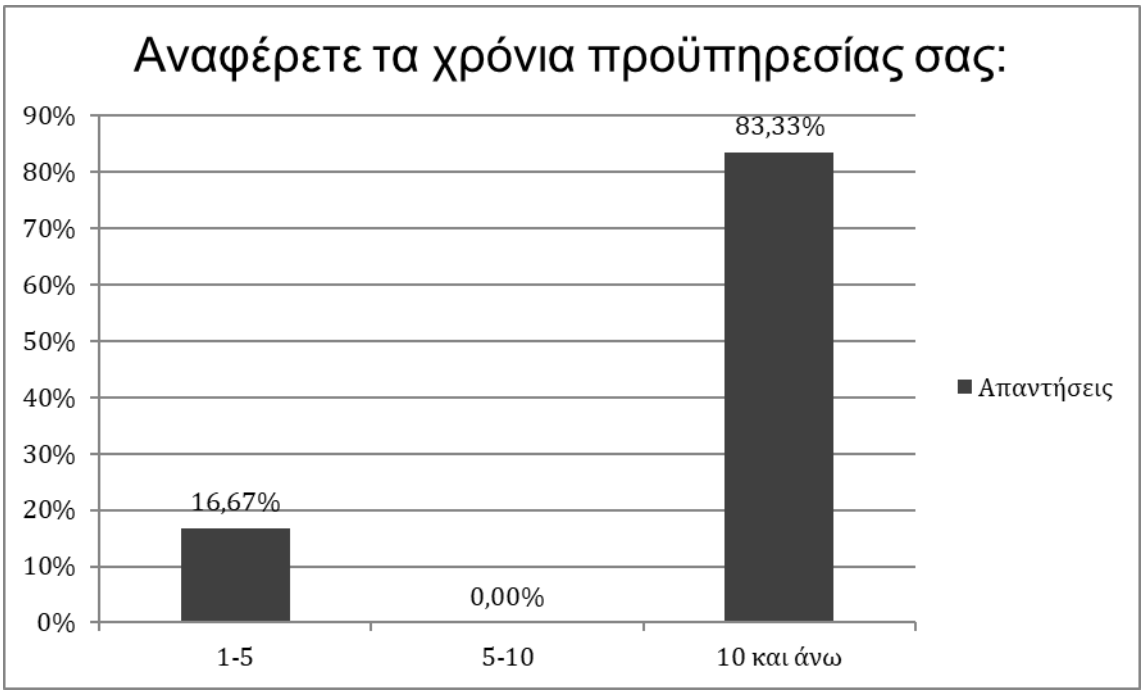
Εικόνα 18. Αποτελέσματα 'Ερώτημα 3'

Παρεμφερή αποτελέσματα παρατηρούμε και στο ερώτημα 4 (**Εικόνα 19**), όπου το 50% των ερωτηθέντων προέρχεται από εταιρείες πληροφορικής, 33,33% από τον τομέα της βιομηχανίας και ένα 16,67% από τον δημόσιο τομέα.



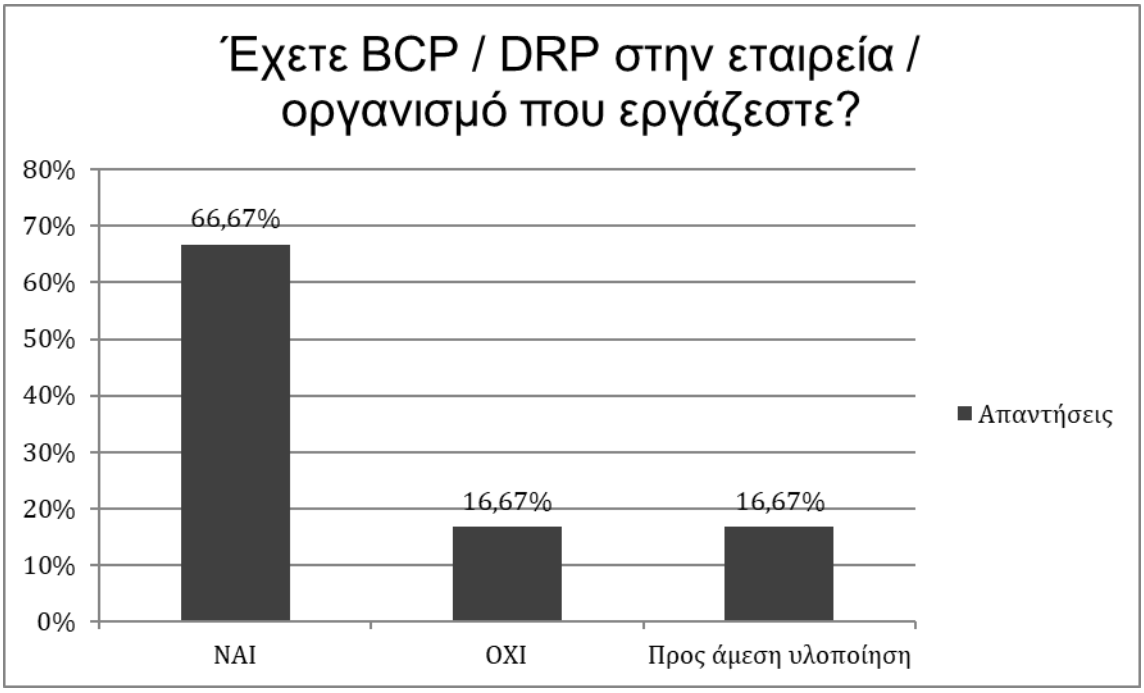
Εικόνα 19. Αποτελέσματα 'Ερώτημα 4'

Στο ερώτημα 5 (**Εικόνα 20**) παρατηρούμε ότι οι περισσότεροι επαγγελματίες που αξιολόγησαν την εφαρμογή έχουν πάνω από 10 χρόνια προϋπηρεσίας (83,33%), κάτι που κάνει την εν λόγω αξιολόγηση πιο εμπεριστατωμένη. Επίσης, ένα 16,67% των ερωτηθέντων κυμαίνεται στα 1-5 χρόνια προϋπηρεσίας.



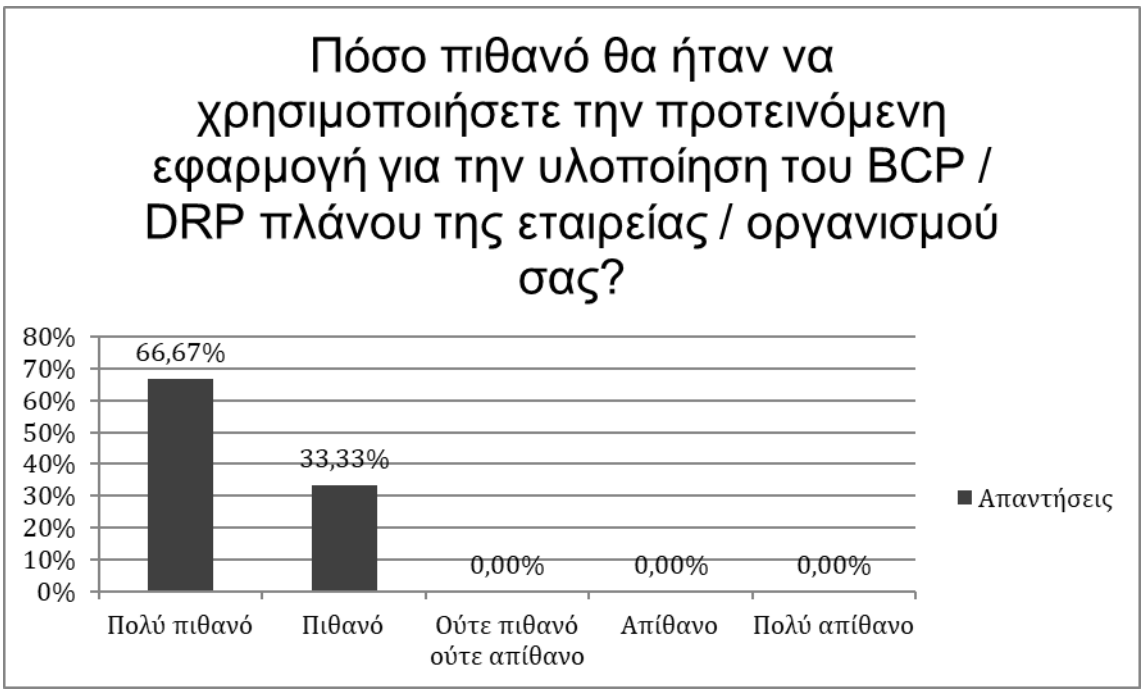
Εικόνα 20. Αποτελέσματα 'Ερώτημα 5'

Στο ερώτημα 6 (**Εικόνα 21**) βλέπουμε ότι το 66,67% των ερωτηθέντων επαγγελματιών έχουν BCP / DRP στον οργανισμό που εργάζονται. Ένα ποσοστό 16,67% απάντησε ότι η εταιρεία στην οποία εργάζεται δεν έχει BCP / DRP και τέλος ένα 16,67% απάντησε ότι η εταιρεία του είναι σε στάδιο άμεσης υλοποίησης ενός BCP / DRP.



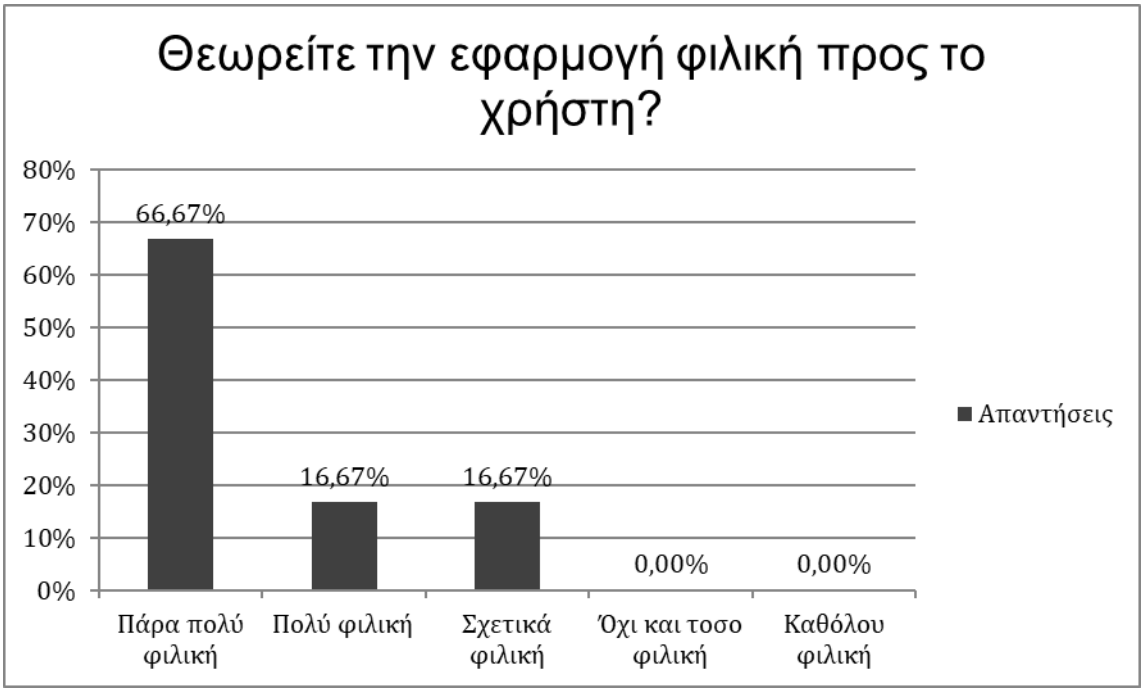
Εικόνα 21. Αποτελέσματα 'Ερώτημα 6'

Στο ερώτημα 7 (**Εικόνα 22**) βλέπουμε ότι το 66,67% των ερωτηθέντων απάντησε ότι είναι 'πολύ πιθανό' να χρησιμοποιήσουν την εν λόγω εφαρμογή για την υλοποίηση του BCP / DRP της εταιρείας τους, όπως επίσης και το 33,33% των ερωτηθέντων απάντησε θετικά και θεωρεί ότι είναι επίσης 'πιθανό' να χρησιμοποιήσει την εν λόγω εφαρμογή.



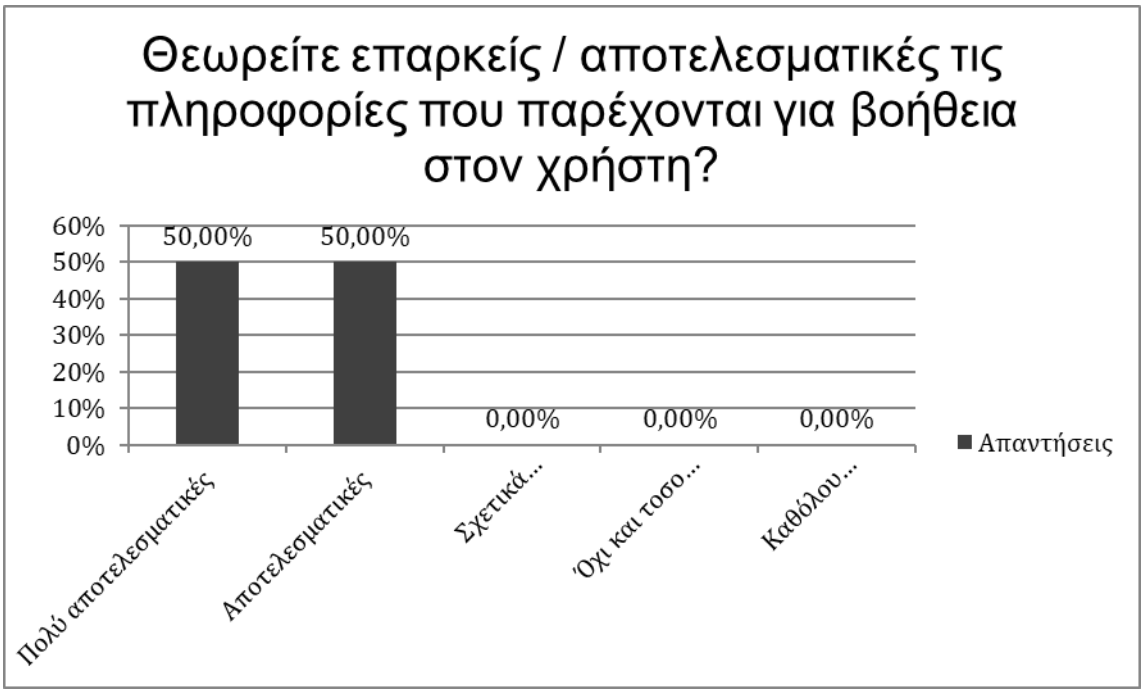
Εικόνα 22. Αποτελέσματα 'Ερώτημα 7'

Στο ερώτημα 8 (**Εικόνα 23**) βλέπουμε ότι η πλειοψηφία (66,67%) θεωρεί την εφαρμογή 'πάρα πολύ φιλική' προς το χρήστη, ένα ποσοστό 16,67% την θεωρεί επίσης 'πολύ φιλική' και ένα ποσοστό 16,67% την θεωρεί 'σχετικά φιλική'.



Εικόνα 23. Αποτελέσματα 'Ερώτημα 8'

Στο ερώτημα 9 (**Εικόνα 24**) βλεπουμε ότι οι πληροφορίες που παρέχονται για βοήθεια των χρηστών χαρακτηρίζονται ‘πολύ αποτελεσματικές’ με ποσοστό 50% και απλά ‘αποτελεσματικές’ με ποσοστό επίσης 50%.

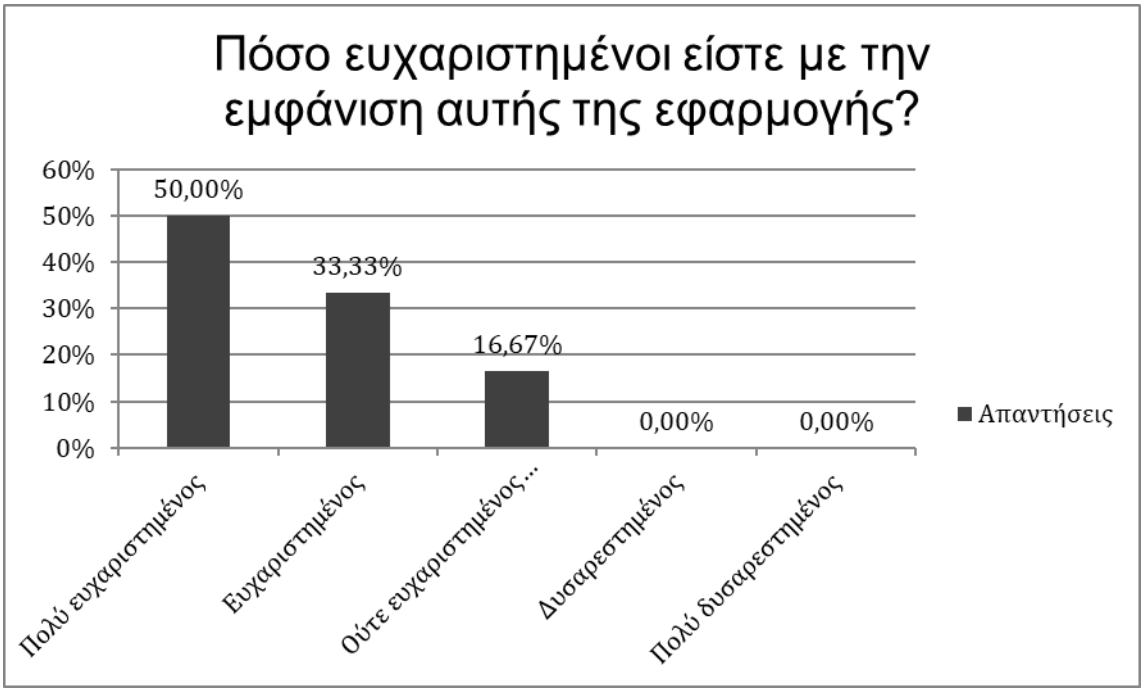


Εικόνα 24. Αποτελέσματα ‘Ερώτημα 9’

Στο ερώτημα 10 (**Εικόνα 25**) παρατηρούμε τα ίδια αποτελέσματα με την προηγούμενη απεικόνιση. Το 50% των ερωτηθέντων θεωρούν ‘πολύ αποτελεσματικές’ τις οδηγίες συμπλήρωσης (guidelines) του πλάνου που παρέχονται στο χρήστη, και το υπόλοιπο 50% χαρακτηρίζει τις οδηγίες ως ‘αποτελεσματικές’.

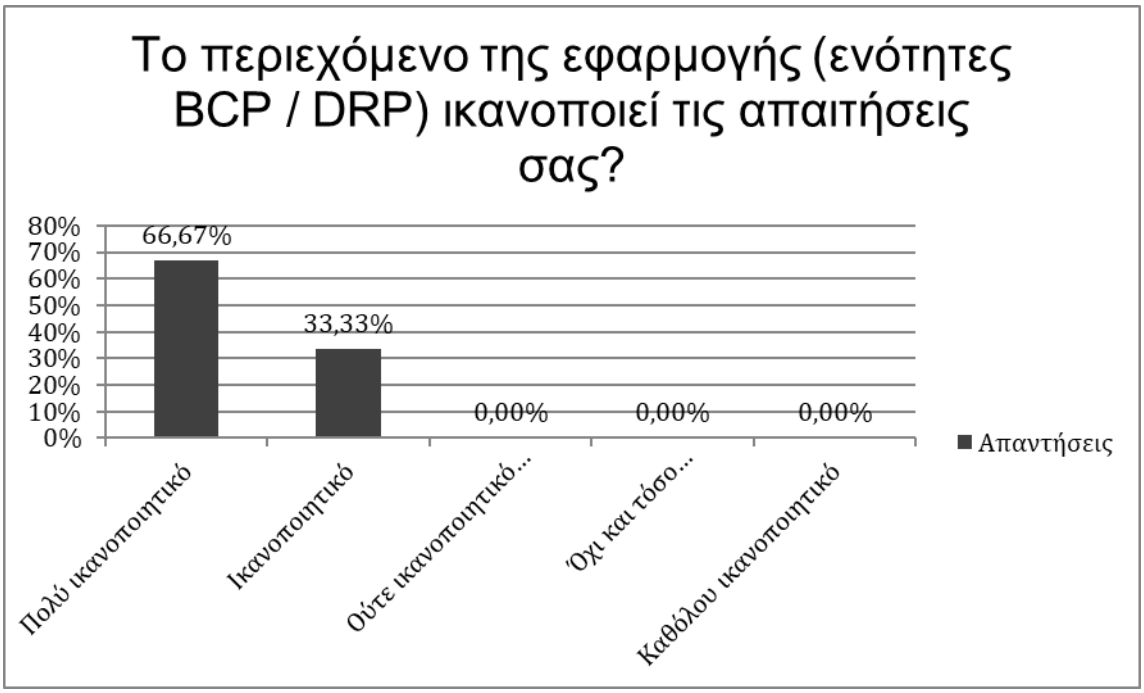
Εικόνα 25. Αποτελέσματα 'Ερώτημα 10'

Στο ερώτημα 11 (**Εικόνα 26**) βλέπουμε ότι το 50% των ερωτηθέντων, όπου αποτελεί και την πλειοψηφία είναι 'πολύ ευχαριστημένο' με την εμφάνιση της εφαρμογής, το 33,33% είναι απλά 'ευχαριστημένο' και ένα 16,67% δηλώνει ουδετερότητα.



Εικόνα 26. Αποτελέσματα 'Ερώτημα 11'

Στο ερώτημα 12 (**Εικόνα 27**) βλέπουμε ότι το 66,67% των ερωτηθέντων δηλώνει ότι το περιεχόμενο της εφαρμογής είναι ‘πολύ ικανοποιητικό’ και το 33,33% χαρακτηρίζει το περιεχόμενο απλά ‘ικανοποιητικό’.



Εικόνα 27. Αποτελέσματα ‘Ερώτημα 12’

Το ερώτημα 13 (**Εικόνα 28**) δίνει την δυνατότητα στους ερωτηθέντες να προτείνουν προσθήκες ή αλλαγές για το περιεχόμενο της συγκεκριμένης εφαρμογής.

Τι θα προτείνατε για να βελτιωθεί το περιεχόμενο της συγκεκριμένης εφαρμογής?		
Ερωτηθέντες	**Ημ/νία Απάντησης**	**Απαντήσεις**
1	May 07 2019 10:41 PM	1. Αναφορά/καθορισμός των stakeholders π.χ. πελάτες, συνεργαζόμενες εταιρίες π.χ. σε Jont Ventures και τα δικά τους expectation από το BCP. 2. Αναφορά στον εξοπλισμό περιορισμού των επιπτώσεων μιας κατάστασης εκτάκτου ανάγκης π.χ. σύστημα πυρόσβεσης (φορητό/μόνιμο), συστήμαα ελέγχου θερμοκρασίας, access control sytsems, etc. 3. Το Impact, να περιλαμβάνει και κατηγορία Reputation και Potential Escalation 4. Εκτός από την ποιοτική ανάλυση του Ρίσκου, να συμπεριλάβει και ποσοτική ανάλυση π.χ. Δεντρου σφαλμάτων, Monte Carlo.
2	May 06 2019 10:15 AM	Το περιεχόμενο της συγκεκριμένης εφαρμογής είναι πλήρες
3	Apr 27 2019 06:17 PM	Πιο domain specific εφαρμογές

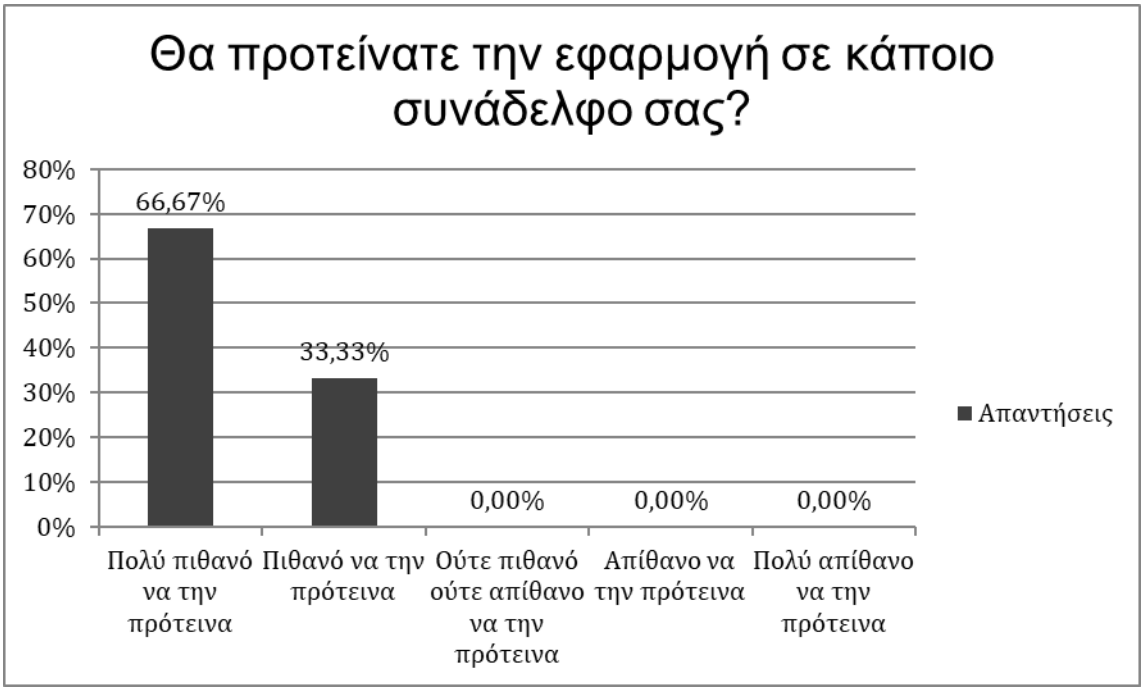
Εικόνα 28. Αποτελέσματα ‘Ερώτημα 13’

Στο ερώτημα 14 (**Εικόνα 29**), το οποίο επίσης είναι πεδίο σχολιασμού από τους ερωτηθέντες , βλέπουμε ότι η επικρατέστερη βελτίωση σε τεχνικό επίπεδο που επικρατεί είναι η μετάβαση της εφαρμογής σε web based.

Τι θα προτείνατε για να βελτιωθεί η εφαρμογή σε τεχνικό επίπεδο?		
Ερωτηθέντες	**Ημ/νία Απάντησης**	**Απαντήσεις**
1	May 07 2019 10:41 PM	-
2	May 06 2019 10:15 AM	Θεωρώ ότι μια καλή προσθήκη θα ήταν να γίνει και εφαρμογή Web
3	Apr 27 2019 06:17 PM	Μεταβαση σε web based

Εικόνα 29. Αποτελέσματα 'Ερώτημα 14'

Στο τελευταίο ερώτημα (**Εικόνα 30**) βλέπουμε ότι οι ερωτηθέντες θα πρότειναν την εφαρμογή σε κάποιο συναδερφό τους. Τα ποσοστά διαμορφώνονται ως εξής: το 66,67% θεωρεί 'πολύ πιθανό' να πρότεινε την εφαρμογή σε κάποιο στνάδελφο του και το 33,33% το θεωρεί επίσης 'πιθανό'.



Εικόνα 30. Αποτελέσματα 'Ερώτημα 15'

Τα αποτελέσματα του ερωτηματολογίου που δόθηκε στους επαγγελματίες για την αξιολόγηση της εφαρμογής σε γενικές γραμμές μπορούν να θεωρηθούν αρκετά θετικά. Η εφαρμογή θεωρείτε χρήσιμη και πέραν των απαντήσεων του ερωτηματολογίου. Οι επαγγελματίες που την αξιολόγησαν θεώρησαν ότι είναι ένα εργαλείο που θα μπορούσε να βοηθήσει αρκετά στα πλαίσια της επιχειρησιακής συνέχειας , τόσο τις εταιρείες που δεν έχουν υλοποιήσει ένα πλάνο επιχειρησιακής συνέχειας και ανάκαμψης, όσο και αυτές που βρίσκονται σε στάδιο επαναξιολόγησης των δομών τους.

Βιβλιογραφία

[1] C. O. T. E. U. EUROPEAN PARLIAMENT, *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC(GDPR),* EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 2016.

[2] A. Team, "https://avalution.com," 28 April 2014. [Online]. Available: https://avalution.com/program-roles-responsibilities-in-a-business-continuity-management-system/.

[3] Ε. Κ. κ. Συμβούλιο, «ΟΔΗΓΙΑ (ΕΕ) 2015/1535 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προδιαγραφών και των κανόνων σχετικά με τις υπηρεσίες της κοινωνίας των πληροφοριών (κωδικοποιημένο κείμενο),» Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, 2015.

[4] «https://www.whoa.com,» https://www.whoa.com, [Ηλεκτρονικό]. Available: https://www.whoa.com/data-breach-101-top-5-reasons-it-happens/.

[5] W. Kenton, «https://www.investopedia.com,» 7 3 2019. [Ηλεκτρονικό]. Available: https://www.investopedia.com/terms/b/business-continuity-planning.asp.

[6] V. P. S. L. M. A. A. H. Keith Stouffer, «https://nvlpubs.nist.gov,» 05 2015. [Ηλεκτρονικό]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

[7] Marek.Z, «https://defaultreasoning.com,» 10 12 2013. [Ηλεκτρονικό]. Available: https://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/.

[8] S. Snedaker, «https://searchitchannel.techtarget.com,» https://searchitchannel.techtarget.com, 01 2008. [Ηλεκτρονικό]. Available: https://searchitchannel.techtarget.com/feature/Business-impact-analysis-for-

business-continuity-Recovery-time-requirements.

[9] «https://www.nibusinessinfo.co.uk,» https://www.nibusinessinfo.co.uk, [Ηλεκτρονικό]. Available: https://www.nibusinessinfo.co.uk/content/what-it-risk.

[10] P. D. G. Rebecca M. Blank, «Guide for Conducting Risk Assessments,» NIST, 2012.

[11] ISO, «https://www.iso.org,» ISO, [Ηλεκτρονικό]. Available: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en.

[12] G. G. Marianthi Theocharidou, «Risk assessment methodologies for critical infrastructure protection. Part II: A new approach,» 2015. [Ηλεκτρονικό]. Available: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC96623/lbna27332enn.pdf.

[13] Waleed Ahmed, Jagan Athreya, Oracle Corporation World Headquarters, «http://www.oracle.com,» 2013. [Ηλεκτρονικό]. Available: http://www.oracle.com/us/products/database/data-masking-best-practices-161213.pdf.

[14] Oracle, «https://docs.oracle.com,» Oracle, [Ηλεκτρονικό]. Available: https://docs.oracle.com/database/121/TDPSG/GUID-72D524FF-5A86-495A-9D12-14CB13819D42.htm#TDPSG90066.

[15] TSO (The Stationery Office), «The Official Introduction to the ITIL Service Lifecycle,» σε *The Official Introduction to the ITIL Service Lifecycle*, TSO (The Stationery Office), 2007, p. 230.

[16] S. Kempter, «IT process maps, 2014. Change Management.,» [Ηλεκτρονικό]. Available: http://wiki.en.it-processmaps.com/index.php/Change_Management.

[17] n. UCISA, «https://www.ucisa.ac.uk,» [Ηλεκτρονικό]. Available: https://www.ucisa.ac.uk/~/media/Files/members/activities/ITIL/servicetransition/chanage_management/ITIL_an%20example%20change%20management%20procedure%20pdf.ashx.

[18] A. &. R. M. &. D. T. A. &. R.-C. A. del-Río-Ortega, «Defining Process Performance Indicators by Using Templates and Patterns.,» 2012.

[19] «https://www.gartner.com/en,» [Ηλεκτρονικό]. Available: https://www.gartner.com/en.

[20] IBM, «https://www.ibm.com,» [Ηλεκτρονικό]. Available: https://www.ibm.com/it-infrastructure/storage .

[21] DELL, «https://www.dell.com,» DELL, [Ηλεκτρονικό]. Available: https://www.dell.com/en-us/work/shop/dell-emc-data-storage-and-backup/sc/storage-products.

[22] HPE, «https://www.hpe.com,» HPE, [Ηλεκτρονικό]. Available: https://www.hpe.com/us/en/storage.html .

[23] NETAPP, «https://www.netapp.com,» NETAPP, [Ηλεκτρονικό]. Available: https://www.netapp.com/us/products/storage-systems/index.aspx .

[24] HITACHI, «https://www.hitachivantara.com,» HITACHI, [Ηλεκτρονικό]. Available: https://www.hitachivantara.com/en-us/products/storage.html.

[25] Microsoft, «https://azure.microsoft.com/en-us/,» Microsoft, [Ηλεκτρονικό]. Available: https://azure.microsoft.com/en-us/.

[26] «https://www.fortinet.com,» https://www.fortinet.com, [Ηλεκτρονικό]. Available: https://www.fortinet.com/solutions/gartner-enterprise-firewalls-mq.html.

[27] «https://www.fortinet.com,» https://www.fortinet.com, [Ηλεκτρονικό]. Available: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_1500D.pdf .

[28] «https://www.gartner.com,» [Ηλεκτρονικό]. Available: https://www.gartner.com/reviews/customers-choice/endpoint-protection-platforms/Nov-2018 .

[29] «https://www.radarfirst.com,» [Ηλεκτρονικό]. Available:

https://www.radarfirst.com/hubfs/PDFs/Product_Info/RADAR_Datasheet.pdf .

[30] radarfirst, «https://www.radarfirst.com,» radarfirst, [Ηλεκτρονικό]. Available: https://www.radarfirst.com/gdpr.

[31] «https://www.ready.gov,» https://www.ready.gov, [Ηλεκτρονικό]. Available: https://www.ready.gov/business/implementation/IT.

[32] «https://www.ibm.com,» IBM, [Ηλεκτρονικό]. Available: https://www.ibm.com/it-infrastructure/storage .

Παράρτημα Α

Γλωσσάριο, συντομογραφίες και επεξηγήσεις

CAB: Change Advisory Board - Συμβουλευτική Επιτροπή Αλλαγών

RfC: Request for Change – Αίτημα για Αλλαγή

BCP: Business Continuity Plan – Πλάνο Επιχειρησιακή Συνέχειας

DRP: Disaster Recovery Plan – Πλάνο Ανάκτησης σε περίπτωση Καταστροφής

GDPR: General Data Protection Regulation - Γενικός Κανονισμός Προστασίας Δεδομένων

RPO: Recovery Point Objective – Στόχος ανάκαμψης

RTO: Recovery Time Objective – Χρόνος ανάκτησης

WTR: Work Recovery Time – Χρόνος εργασίας που χρειάζεται μέχρι την αποκατάσταση

MWR: Maximum Tolerable Downtime – Μέγιστος ανεκτός χρόνος διακοπής

ERP: Enterprise Resource Planning – Είναι τα συστήματα επιχειρησιακού προγραμματισμού πόρων

ΓΚΠΔ: Γενικός Κανονισμός Προστασίας Δεδομένων

Change Management: Διαχείριση αλλαγής

EE: Ευρωπαϊκή Ένωση

ISO: International Organization for Standardization – Διεθνής οργανισμός τυποποίησης

Accountability: Λογοδοσια

Awareness: Επαγρύπνηση

Data Inventory: Αρχείο καταγραφής δεδομένων

Data Mapping: Χαρτογράφηση Δεδομένων

Gap Analysis: Ανάλυση των διαφορών

DPIA: Data Protection Impact Assessment - Εκτίμηση αντικτύπου προστασίας δεδομένων

IT: Information Technology – Τεχνολογία της πληροφορίας

Website: Ιστότοπος

Data Controller: Υπεύθυνος Επεξεργασίας

Data Processor: Εκτελών την Επεξεργασία

SA: Supervisory Authority – Εποπτική Αρχή

DPO: Data Protection Officer - Υπεύθυνος Προστασίας Δεδομένων

IT manager: Information Technology Manager – Διευθυντής/Διαχειριστής πληροφοριακών συστημάτων

Security Manager: Διευθυντής/Διαχειριστής Ασφάλειας

BC Steering Committee Member: Business Continuity Steering Committee Member - Μέλος της Διευθύνουσας Επιτροπής Επιχειρησιακής Συνέχειας

Program Sponsor: Χορηγός προγράμματος

Program Manager: Διαχειριστής προγράμματος

Business Continuity Planner: Σχεδιαστής της επιχειρησιακής συνέχειας

Team Leader: Αρχηγός ομάδας

Team Coordinator: Συντονιστής ομάδας

Team Administrator: Διοικητής / Διαχειριστής ομάδας

Junior: μη έμπειρος (αναφέρεται στα μη έμπειρα στελέχη)

CV: Curiculum Vitae – Βιογραφικό σημείωμα

Internet: Διαδίκτυο

Email: Μήνυμα ηλεκτρονικού ταχυδρομείου

IP Address: Internet Protocol Address - Διεύθυνση διαδικτυακού πρωτοκόλλου

Log-in data: Στοιχεία σύνδεσης

Cookies: μικρά αρχεία κειμένου τα οποία αποθηκεύονται στον φυλλομετρητή (browser) κατά την πλοήγησή στο διαδίκτυο

GPS: Global Positioning System) - Παγκόσμιο Σύστημα Θεσιθεσίας

DNA: Deoxyribonucleic Acid - Νουκλεϊκό οξύ που περιέχει γενετικές πληροφορίες

Confidentiality: Εμπιστευτικότητα

Integrity: Ακεραιότητα

Availability: Διαθεσιμότητα

Retention policy: Πολιτική που καθορίζει το χρονικό διάστημα διατήρησης των δεδομένων

Viber, Facebook: Εφαρμογές μέσων κοινωνικής δικτύωσης

ΕΑ: Εκτίμηση Αντικτύπου

DPO: Data Protection Officer - Υπεύθυνος Προστασίας Δεδομένων

Software patches: Διορθωσεις λογισμικου

Phising: Απάτες διαδικτυακού 'ψαρέματος'

Testing: Έλεγχος διαδικασιών / Δοικιμές

BIA: Business Impact Analysis - Ανάλυση Επιχειρηματικών Επιπτώσεων

Software: Λογισμικό

Hardware: Εξαρτήματα πληροφορικής

System configuration: Πληροφοριές διαμόρφωσης συστημάτων

Principles: Αρχές

Framework: Πλαίσιο

Processes: Διαδικασίες

Procedures: Διαδικασίες (πιο αναλυτικές)

Impact: Επίπτωση

Probability: Πιθανότητα

Risk: Κίνδυνος / Ρίσκο

Risk assessment methodology: Μεθοδολογία αξιολόγησης κινδύνου

Risk description: Περιγραφή κινδύνου/ρίσκου

Risk assessment: Αξιολόγηση κινδύνου

Mitigation action: Μέτρα μετριασμού

Contigency plan: Εναλλακτικό σχέδιο

Risk assessment after mitigation action: Αξιολόγηση του κινδύνου μετά από τη λήψη μέτρων μετριασμού

Very high: Πολύ υψηλο

High: Υψηλό

Medium: Μεσαίο

Low: Χαμηλό

Oracle: εταιρεία λογισμικού

Data masking: μέθοδοι κάλυψης δεδομένων για την προστασία τους

DB: Database – Βάση δεδομένων

Row level security: Ασφάλεια σε επίπεδο γραμμής

Confidentiality levels per data or files: Επίπεδα εμπιστευτικότητας ανά γραμμή δεδομένων ή αρχείων

Awareness trainings: Σεμιναρίων επαγρύπνησης

CRM: Customer Relationship Management - Διαχείριση Πελατειακών Σχέσεων

Consent: Συγκατάθεση

Security policies, processes & procedures: Πολιτικές, διεργασίες και διαδικασίες ασφαλείας μιας εταιρείας

Corrective maintenance: Διορθωτική συντήρηση

Confidentiality Agreement: Συμφωνία εμπιστευτικότητας

IT Governance: Information Technology Governance – Διακυβέρνηση της τεχνολογίας της πληροφορίας

ITSCM ITIL V3: IT Service Continuity Management - Information Technology Infrastructure Library – version 3 - Διαχειριση πληροφοριών επιχειρησιακής συνέχειας - Οδηγός παροχής υπηρεσιών τεχνολογίας πληροφοριών

Initiation: 'Εναρξη

Requirements and strategy: Απαιτήσεις και στρατηγική

Implementation: Εκτέλεση

Ongoing operation: Τρέχουσες λειτουργίες

Guidelines: Κατευθυντήριες γραμμές

Network: Δίκτυο

Sites: Τοποθεσία αλλά και ιστοσελίδα (εξαρτάται την χρήση του όρου)

Data Protection Impact Assessment: Εκτίμηση αντικτύπου προστασίας δεδομένων

Business Continuity Impact Analysis: Ανάλυση αντίκτυπου επιχειρησιακής συνέχειας

Risk Management / Risk Assessment: Διαχείριση κινδύνων / Αξιολόγηση κινδύνου

Business continuity strategy: Στρατηγική επιχειρησιακής συνέχειας

Invocation: Εναρξη ενεργειών

Stage: Σταδιο

EC: Emergency Board – Ομάδα για έκτακτα περιστατικά

Standard Change: Τυπική αλλαγή

Minor Change: Μικρή αλλαγή

Significand Change: Σημαντική αλλαγή

Targets: Στόχοι

Major Change: Μεγάλη / Πολύ σημαντική αλλαγή

IDS / IPS: Intrusion Detection Systems / Intrusion Prevention Systems - Συστήματα ανίχνευσης εισβολών / Συστήματα πρόληψης εισβολών

Change management register / change management system: σύστημα ή αρχείο καταγραφής των αλλαγών

Recovery: Ανάκτηση

SAP: Σύστημα διαχείρισης επιχειρησιακών πόρων

Sharepoint: Σύστημα της Microsoft

On premises: Χρήση του όρου όταν μιλάμε για συστήματα εγκατεστημένα στις εγκαταστάσεις της εταιρείας

User Data: Δεδομένα Χρηστών

Programs: Προγράμματα

Configuration: Δεδομένα Παραμετροποίησης

Log files: Αρχεία Καταγραφής

Application Data: Δεδομένα Εφαρμογών

Test Data: Δεδομένα Δοκιμών

Code: Κώδικας

Azure cloud: Cloud (υπολογιστικοί πόροι) της εταιρείας Microsoft

Capacity: Χωρητικότητα

Bios password, password policy: Πολιτικές μιας εταιρείας που αφορούν την διαχείριση αλλά και αλλαγή των κωδικών των συστημάτων

Recovery Sites: Τοποθεσίες Αποκατάστασης

Storage arrays: παρατάξεις

Tiering και software defined storage: Χωρητικότητα και αποθήκευση που έχει καθοριστεί από το λογισμικό

External Virtualization: Εξωτερική εικονοποίηση

SSD: Solid State Drives - Μονάδες στερεάς κατάστασης

Encryption: Κρυπτογράφηση

Real-time Compression: Συμπίεση σε πραγματικό χρόνο

Compute Services: Υπολογιστικές υπηρεσίες

Network services: Υπηρεσίες δικτύου

Data services: Υπηρεσίες δεδομένων

Application Services: Υπηρεσίες Εφαρμογών

Audit: Έλεγχος

FortiOS: Λειτουργικό σύστημα της εταιρείας FortiGate

Content Processor: Επεξεργαστής περιεχομένου

Throughput: Διακίνηση

Application Control: Έλεγχος εφαρμογών

Malware protection: Προστασία από κακόβουλα προγράμματα

GUI: Graphical User Interface - Γραφικό περιβάλλον χρήστη

Virtual Domain: Εικονικός τομέας

Incident Response Management: Διαχείριση απόκρισης περιστατικών

Incident Risk Assessment: Εκτίμηση κινδύνου συμβάντων

Notifications Letters Module: Μονάδα ειδοποιήσεων

Incident Management Dashboard: Πίνακας ελέγχου περιστατικών

Reports: Αναφορές

Central Repository: Κεντρικό αποθετήριο

Administration & Policy: 'Role based access control' - Διαχείριση & Πολιτική: ''Έλεγχος πρόσβασης βάσει ρόλου'

Web Submission Forms: Φόρμες Υποβολής

Contractual Obligations Workflow: Ροή εργασιών συμβατικών υποχρεώσεων

Template: Πρότυπο