ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

UNIVERSITY OF PIRAEUS

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

Διπλωματική Εργασία:

«Γενικός Κανονισμός Προστασίας Δεδομένων & ISO 27001: η εφαρμογή τους εντός των επιχειρήσεων»

Επιβλέπων Καθηγητής:
Γεώργιος Μποχώρης

Ντόστη Ανθούλα-Μαρία
ΜΔΕ2042
2 Δεκεμβρίου 2022

Παράρτημα Β: Βεβαίωση Εκπόνησης Διπλωματικής Εργασίας

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΣΤΗ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΒΕΒΑΙΩΣΗ ΕΚΠΟΝΗΣΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

(περιλαμβάνεται ως ξεχωριστή (δεύτερη) σελίδα στο σώμα της διπλωματικής εργασίας)

«Δηλώνω υπεύθυνα ότι η διπλωματική εργασία για τη λήψη του μεταπτυχιακού τίτλου σπουδών, του Πανεπιστημίου Πειραιώς, στη Διοίκηση Επιχειρήσεων : MBA» με τίτλο «Γενικός Κανονισμός Προστασίας & ISO 27001: η εφαρμογή τους εντός των επιχειρήσεων» έχει συγγραφεί από εμένα αποκλειστικά και στο σύνολό της. Δεν έχει υποβληθεί ούτε έχει εγκριθεί στο πλαίσιο κάποιου άλλου μεταπτυχιακού προγράμματος ή προπτυχιακού τίτλου σπουδών, στην Ελλάδα ή στο εξωτερικό, ούτε είναι εργασία ή τμήμα εργασίας ακαδημαϊκού ή επαγγελματικού χαρακτήρα.

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

Υπογραφή Μεταπτυχιακού Φοιτητή/ τριας: .....

Ονοματεπώνυμο: Ντόστη Ανθούλα-Μαρία

Ημερομηνία: 23 Ιουλίου 2022

Αφιέρωση

Στην οικέγενειά μου
και σε όσους με στήριξαν.

Ευχαριστίες

Με την εκπόνηση της παρούσας διπλωματικής μελέτης θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου, Γεώργιο Μποχώρη, για τη ευκαιρία που μου έδωσε σε αυτό το μεταπτυχιακό πρόγραμμα να ανοίξω τους ορίζοντές μου με τις πολύτιμες συμβουλές του και με την αμέριστη βοήθειά του.

Επίσης θα ήθελα να ευχαριστήσω όλους τους καθηγητές αυτού του προγράμματος σπουδών που με τις εύστοχες παρατηρήσεις τους και τις προσπάθειες που κατέβαλαν μας βοήθησαν στην κατάκτηση της γνώσης.

Θα ήθελα επίσης να εκφράσω την ευγνωμοσύνη μου και την αγάπη μου στην οικογένειά μου για την υποστήριξη, την υπομονή τους και την αμέριστη συμπαράστασή τους σε κάθε μου βήμα.

Η παρούσα διπλωματική μελέτη πραγματοποιήθηκε για εκπαιδευτικούς σκοπούς – στα πλαίσια απόκτησης μεταπτυχιακού τίτλου σπουδών. Ως εκ τούτου κάποια από τα στοιχεία που περιέχει μπορεί να μην είναι ακριβή.

ΠΕΡΙΛΗΨΗ

Ο Γ.Κ.Π.Δ. δημιουργήθηκε ως ανάγκη προστασίας των πολιτών της Ε.Ε. από την ραγδαία τεχνολογική εξέλιξη αντικαταστώντας προγενέστερους κανονισμούς/ οδηγίες για την προστασία των δεδομένων. Σχεδιάστηκε για να «εναρμονίσει» τους νόμους περί απορρήτου δεδομένων σε όλες τις χώρες μέλη της Ε.Ε., καθώς και για να παρέχει μεγαλύτερη προστασία και περισσότερα δικαιώματα στα άτομα που ανήκουν τα δεδομένα. Ο Γ.Κ.Π.Δ. δημιουργήθηκε επίσης για να αλλάξει τον τρόπο με τον οποίο οι επιχειρήσεις μπορούν να χειριστούν τις πληροφορίες των χρηστών/πελατών που αλληλοεπιδρούν μαζί τους. Η μη συμμόρφωση με τον κανονισμό μπορεί να οδηγήσει σε μεγάλα πρόστιμα και ζημιά στη φήμη για όσους παραβιάζουν τους κανόνες. Η ανάγκη συμμόρφωσης των επιχειρήσεων στον κανονισμό, και πιο συγκεκριμένα στην ασφάλεια των δεδομένων, οδήγησε στη δημιουργία των πιστοποιήσεων ISO/IEC της οικογένειας 27000.

Σε αυτή την διπλωματική εργασία πραγματοποιείται μια εκτενής αναφορά στην ήδη υπάρχουσα, διαθέσιμη στο διαδίκτυο, βιβλιογραφία για τον Γ.Κ.Π.Δ. και τις πιστοποιήσεις ISO/IEC 27001 και ISO/IEC 27701. Στην συνέχεια προσεγγίζονται θεωρητικά οι δύο πιστοποιήσεις και δίνονται οδηγίες για το πώς μπορούν να υλοποιηθούν αλλά και κάποια παραδείγματα υλοποίησης. Έπειτα πραγματοποιείται η συσχέτιση του Γ.Κ.Π.Δ. με την πιστοποίηση ISO/IEC 27001 και του ISO/IEC 27001 με τον ISO/IEC/27701. Σε αυτό το σημείο αναφέρονται οι ομοιότητες και διαφορές μεταξύ τους. Η διπλωματική ολοκληρώνεται με κάποια συμπεράσματα που συνάγονται κατά τη συγγραφή της.

ΑΡΚΤΙΚΟΛΕΞΑ – ΛΕΞΙΚΟ

Αρτικόλεξα	**Μετάφραση**
Γ.Κ.Π.Δ.	Γενικός Κανονισμός Προστασίας Δεδομένων
GDPR	General Data Protection Regulation
Ε.Ε.	Ευρωπαϊκή Ένωση
Ε.Ο.Χ.	Ευρωπαϊκό Οικονομικό Χώρο
Η.Β.	Ηνωμένο Βασίλειο
Δ.Ο.Τ. / ISO	Διεθνής Οργανισμός Τυποποίησης / International Organization for Standardization
Δ.Η.Ε. / IEC	Διεθνής Ηλεκτροτεχνική Επιτροπή / International Electrotechnical Commission
Α.Ε.Π.	Ακαθάριστο Εγχώριο Προϊόν
Η.Π.Α.	Ηνωμένες Πολιτείες Αμερικής
Α.Π.Δ.	Αναλυτική Περιοδική Δήλωση
CCTV	Closed-Circuit TeleVision
IAPP-EY	International Association of Privacy Professionals – Ernst & Young
Σ.Δ.Α.Π.	Σύστημα Διαχείρισης Ασφάλειας Πληφορίων
Η.Α.Ε.	Ηνωμένα Αραβικά Εμιράτα
IoT	Internet of Things
IP	Internet Protocol
UML	Unified Modeling Language
PET	Political, Economical, (Social) and Technological
PbD	Privacy by Design
CSA STAR	Μητρώο Ασφάλειας, Εμπιστοσύνης & Διασφάλισης
ISMS / Σ.Δ.Α.Π.	Information Security Management System / Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών
OSS	Open Source Solution
OSP	Open Source Platform
IT	Information Technology
P.D.C.A.	Plan Do Check Act
S.M.A.R.T.	Specific, Measurable, Attainable, Realistic, Time-bound
USB	Universal Serial Bus
JAVA	Γλώσσα προγραμματισμού
.NET	OSP για την δημιουργία εφαρμογών
VPN	Virtual Private Network
VLAN	Virtual Local Area Work
LAN	Local Area Work
VPN	Virtual Private Network
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention Systems
Σ.Δ.Π.Α.	Συστήματος Διαχείρισης Πληροφοριών Απορρήτου
SLA	(Service Level Agreement

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ 6

ΑΡΚΤΙΚΟΛΕΞΑ – ΛΕΞΙΚΟ 7

1: Η ΑΝΑΓΚΑΙΟΤΗΤΑ ΕΦΑΡΜΟΓΗΣ ΤΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΤΟΥ ΠΡΟΤΥΠΟΥ ISO/IEC 27001 11

2: ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΑΝΑΣΚΟΠΗΣΗ 14

2.1: Η ΕΙΣΑΓΩΓΗ ΤΟΥ Γ.Κ.Π.Δ. 14
2.1.1: ΜΙΑ ΝΕΑ ΕΠΟΧΗ ΣΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ 14
2.1.2: Η ΕΦΑΡΜΟΓΗ ΤΟΥ Γ.Κ.Π.Δ. 15
2.1.3: Η ΕΦΑΡΜΟΓΗ ΤΟΥ Γ.Κ.Π.Δ. ΕΚΤΟΣ ΤΗΣ ΕΥΡΩΠΗΣ 15
2.2: ΟΙ ΑΝΤΙΔΡΑΣΕΙΣ ΣΤΟΝ Γ.Κ.Π.Δ. 16
2.2.1: ΟΙ ΑΝΤΙΔΡΑΣΕΙΣ, ΟΙ ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΑΛΛΑΓΕΣ ΚΑΙ ΟΙ ΟΔΗΓΙΕΣ ΥΙΟΘΕΤΗΣΗΣ ΣΤΟΝ Γ.Κ.Π.Δ. 16
2.3: Η ΕΠΙΔΡΑΣΗ ΤΟΥ Γ.Κ.Π.Δ. 17
2.3.1: Η ΕΠΙΔΡΑΣΗ ΤΟΥ Γ.Κ.Π.Δ. 17
2.3.2: ΕΠΙΡΡΟΗ ΤΟΥ Γ.Κ.Π.Δ. ΠΑΓΚΟΣΜΙΩΣ 18
2.3.3: Η ΕΠΙΡΡΟΗ ΤΟΥ Γ.Κ.Π.Δ. ΣΤΗΝ ΔΙΟΙΚΗΣΗ ΤΗΣ ΕΠΙΧΕΙΡΗΣΗΣ ΚΑΙ ΣΤΗΝ ΧΡΗΣΗ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ 18
2.3.4: ΟΙ ΕΠΙΠΤΩΣΕΙΣ ΤΟΥ Γ.Κ.Π.Δ. ΕΝΑ ΧΡΟΝΟ ΜΕΤΑ ΤΗΝ ΕΦΑΡΜΟΓΗ ΤΟΥ .. 19
2.3.5: ΟΙ ΕΠΙΠΤΩΣΕΙΣ ΤΟΥ Γ.Κ.Π.Δ. ΤΡΙΑ ΧΡΟΝΙΑ ΜΕΤΑ ΤΗΝ ΕΦΑΡΜΟΓΗ ΤΟΥ . 20
2.3.6: ΤΑ ΑΝΤΑΓΩΝΙΣΤΙΚΑ ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΟΥ Γ.Κ.Π.Δ. 20
2.4: ΠΙΣΤΟΠΟΙΗΣΗ ISO 27001 21
2.4.1: Η ΣΥΜΒΟΛΗ ΤΟΥ ISO 27001 ΣΤΗΝ ΣΥΜΜΟΡΦΩΣΗ ΣΤΟΝ Γ.Κ.Π.Δ.. 21
2.4.2: ΕΦΑΡΜΟΓΗ ΤΟΥ Γ.Κ.Π.Δ. ΜΕΣΩ ΤΗΣ ΧΡΗΣΗΣ ΤΩΝ ΠΡΟΤΥΠΩΝ ISO 22
2.4.3: ISO 27001: ΕΛΕΓΧΟΙ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΜΕ ΒΑΣΗ ΤΟΝ Γ.Κ.Π.Δ. 22
2.4.4: ISO 27001: ΑΝΑΛΥΣΗ ΧΑΣΜΑΤΩΝ 23
2.5: Ο Γ.Κ.Π.Δ. ΚΑΙ Η ΠΛΗΡΟΦΟΡΙΚΗ 24
2.5.1: Η ΕΠΙΡΡΟΗ ΤΟΥ Γ.Κ.Π.Δ. ΣΤΑ COOKIES 24
2.5.2: ΜΕΙΩΣΗ ΤΩΝ COOKIES ΜΕΤΑ ΤΗΝ ΕΦΑΡΜΟΓΗ ΤΟΥ Γ.Κ.Π.Δ. 24
2.5.3: ΣΥΝΕΠΕΙΕΣ ΑΠΟΡΡΗΤΟΥ ΤΟΥ Γ.Κ.Π.Δ. ΓΙΑ ΤΟ IOT 25
2.5.4: Η ΔΥΣΚΟΛΙΑ ΥΙΟΘΕΤΗΣΗΣ ΤΟΥ Γ.Κ.Π.Δ. ΑΠΟ ΤΟΥΣ ΠΡΟΓΡΑΜΜΑΤΙΣΤΕΣ 26
2.5.5: ΠΑΙΧΝΙΔΙ ΩΣ ΜΕΣΟ ΕΚΜΑΘΗΣΗΣ ΤΟΥ Γ.Κ.Π.Δ. ΓΙΑ ΤΟΥΣ ΠΡΟΓΡΑΜΜΑΤΙΣΤΕΣ 26
2.5.6: ΕΦΑΡΜΟΓΗ ΤΟΥ Γ.Κ.Π.Δ. ΑΠΟ ΤΟΥΣ ΠΡΟΓΡΑΜΜΑΤΙΣΤΕΣ 27
2.5.7: ΟΙ ΠΡΟΓΡΑΜΜΑΤΙΣΤΕΣ ΣΤΗΝ ΠΡΟΣΠΑΘΕΙΑ ΕΛΑΧΙΣΤΟΠΟΙΗΣΗΣ ΔΕΔΟΜΕΝΩΝ 28
2.5.8: Ο Γ.Κ.Π.Δ. ΣΤΗΝ ΕΠΟΧΗ ΤΩΝ BIG DATA 29
2.5.9: Η ΕΠΙΡΡΟΗ ΤΟΥ Γ.Κ.Π.Δ. ΣΤΑ PRIVACY POLICIES 29
2.6: Γ.Κ.Π.Δ.: ΑΝΑΛΥΤΕΣ, ΕΡΕΥΝΗΤΕΣ ΚΑΙ ΜΗΧΑΝΙΚΟΙ 30
2.6.1: Η ΣΥΜΒΟΛΗ ΤΩΝ ΑΝΑΛΥΤΩΝ ΣΤΗΝ ΣΥΜΜΟΡΦΩΣΗ ΜΕ ΤΟΝ Γ.Κ.Π.Δ. .. 30
2.6.2: ΤΟ ISO 27001 ΣΕ ΕΡΕΥΝΗΤΙΚΟ ΚΕΝΤΡΟ 30
2.6.3: Ο Γ.Κ.Π.Δ. ΣΤΗΝ ΕΡΕΥΝΑ ΤΟΥ ΓΟΝΙΔΙΩΜΑΤΟΣ 31
2.6.4: Η ΕΠΙΡΡΟΗ ΤΟΥ Γ.Κ.Π.Δ. ΓΙΑ ΤΟΥΣ ΕΡΕΥΝΗΤΕΣ 32

2.6.5: Μεθοδοι και εργαλεια για τους μηχανικους για την συμμορφωση στον Γ.Κ.Π.Δ. 32
2.7: Ο Γ.Κ.Π.Δ. και το ISO 27001 στις επιχειρησεις 33
2.7.1: Απο την Οδηγια 95/46/ΕΚ στον Γ.Κ.Π.Δ.: ISO 27001 33
2.7.2: Τι σημαινει ο Γ.Κ.Π.Δ. για τις επιχειρησεις 34
2.7.3: Εφαρμογη του Γ.Κ.Π.Δ. στις εταιρειες 34
2.7.4: Ο Γ.Κ.Π.Δ. αποτελει ευκαιρια για τις επιχειρησεις 35
2.7.5: Η εφαρμογη του ISO 27001 σε εταιρειες 36
2.7.6: Η επιρροη του ISO 27001 σε εταιρειες 36
2.7.7: Ο Γ.Κ.Π.Δ. σε μικρομεσαιες επιχειρησεις μεσω σχεδιου προσαρμογης 37
2.7.8: Συμμορφωση των μικρομεσαιων επιχειρησεων στον Γ.Κ.Π.Δ. 38
2.7.9: Η αποδοση των επιχειρησεων με την χρηση του ISO 27001 39
2.8: Συμπερασματα βιβλιογραφικης ανασκοπησης 39

3: ΟΙ 12 ΒΑΣΙΚΟΙ ΑΞΟΝΕΣ ΤΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ ISO/IEC 27001 ΚΑΙ ΤΡΟΠΟΙ ΥΛΟΠΟΙΗΣΗΣ ΤΟΥΣ 41

3.1: Πολιτικες ασφαλειας πληροφοριων 43
3.2: Οργανωση ασφαλειας πληροφοριων 45
3.2.1: Ρολοι και Ευθυνες 45
3.2.2: Διαχωρισμος καθηκοντων 46
3.2.3: Επαφη με τις αρχες 47
3.2.4: Επαφη με ομαδες ειδικων συμφεροντων 47
3.2.5:Ασφαλεια πληροφοριων στην διαχειριση εργων 47
3.3: Ασφαλεια ανθρωπινου δυναμικου 48
3.3.1: Διαλογη 48
3.3.2: Όροι και προϋποθεσεις απασχολησης 48
3.4: Κρυπτογραφια 49
3.4.1: Πολιτικη σχετικα με τη χρηση κρυπτογραφικων στοιχειων ελεγχου 49
3.4.2: Διαχειριση κλειδιων 50
3.4.3: Εφαρμογη κρυπτογραφησης 50
3.5: Ασφαλεια επικοινωνιων 53
3.5.1: Ασφαλεια δικτυου 53
3.5.2: Ασφαλεια υπηρεσιων δικτυου - Διαχωρισμος σε δικτυα 53
3.5.3: Συνοπτικη αναφορα υλοποιησης 55
3.6: Διαχειριση συμβαντων ασφαλειας πληροφοριων 56
3.6.1: Υπευθυνος διαχειρισης συμβαντων 56
3.6.2: Αποδεικτικα στοιχεια 57
3.6.3: Εργαζομενοι 57
3.6.4: Παραδειγμα 57

4: ΠΙΣΤΟΠΟΙΗΣΗ ISO/IEC 27701 60

4.1: Τομεις υλοποιησης ISO 27701 61
4.1.1: Προστασια και διατηρηση πληροφοριων απορρητου 61
4.1.2: Κοινη χρηση πληροφοριων απορρητου 61
4.1.3: Διεθνεις μεταφορες προσωπικων πληροφοριων 62
4.1.4: Διαδικασια αλλαγης και διαγραφης πληροφοριων απορρητου 62

4.1.5: Διατηρηση προσωπικων δεδομενων 62
4.2: Υλοποιηση ISO 27701 62
4.3: Παραδειγμα «Δηλωσης απορρητου» 63
4.4: Συμπερασματα 66

5: Γ.Κ.Π.Δ., ISO 27001 και ISO 27701: ΣΥΣΧΕΤΙΣΗ 67

5.1: Διαφορα και ομοιοτητα ISO 27001 με Γ.Κ.Π.Δ. 67
5.2: ISO 27001 και ISO 27701 67
5.3: Εταιρειες που ωφελουνται απο τις πιστοποιησεις ISO 27001 & 27701 67
5.4: Συμπερασματικη συσχετιση του Γ.Κ.Π.Δ. με τις πιστοποιησεις ISO/IEC 27001 και 27701 68

6: ΣΥΜΠΕΡΑΣΜΑΤΑ 74

7: ΒΙΒΛΙΟΓΡΑΦΙΑ 76

1 Η ΑΝΑΓΚΑΙΟΤΗΤΑ ΕΦΑΡΜΟΓΗΣ ΤΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΤΟΥ ΠΡΟΤΥΠΟΥ ISO/IEC 27001

Τα τελευταία χρόνια που η τεχνολογία εξελίσσεται ραγδαία και κατέχει πρωταρχικό ρόλο στην καθημερινότητά μας, από μία απλή ηλεκτρονική παραγγελία έως και την κατάθεση της φορολογικής δήλωσης μέσω διαδικτύου, ήταν αναγκαίο να βρεθεί μία λύση έτσι ώστε να προστατευθούν αυτές οι ευαίσθητες πληροφορίες από μη εξουσιοδοτημένους χρήστες. Η ανάγκη αυτή ήταν επιτακτική καθώς η μη νόμιμη πρόσβαση αποτελεί καταπάτηση των προσωπικών δεδομένων και τα αποτελέσματα των πράξεων των μη εξουσιοδοτημένων χρηστών είναι επιζήμια προς τον κάτοχο των στοιχείων αυτών.

Η πρώτη ανάγκη για προστασία των προσωπικών δεδομένων δημιουργήθηκε το 1995 που δημοσιεύτηκε και η πρώτη μορφή του Γ.Κ.Π.Δ. με την τότε ονομασία «Οδηγία για την Προστασία Δεδομένων». Η έκδοση αυτή δεν επαρκούσε με το πέρασμα των ετών καθώς είχε συνταχθεί σε μια εποχή που το διαδίκτυο ήταν στα σπάργανα και η χρήση του δεν ήταν αρκετά διαδεδομένη αλλά ούτε προσβάσιμη σε μεγάλο κοινό. Με την ευρεία χρήση των ηλεκτρονικών υπολογιστών, των κινητών αλλά και του ίντερνετ έπρεπε να εφαρμοστούν νέα μέτρα που να συνάδουν με τις τρέχουσες ανάγκες. Το 2016 η Ε.Ε. υιοθέτησε τον Γ.Κ.Π.Δ., ο οποίος αναγνωρίστηκε ως νόμος που πρέπει να ακολουθούν όλα τα κράτη μέλη της και τέθηκε σε πλήρη εφαρμογή από τον Μάιο του 2018.

Ο Γ.Κ.Π.Δ. της Ε.Ε. έχει ως στόχο να διευρύνει την προστασία των δεδομένων στην εποχή των Big Data και του Cloud Computing, εξασφαλίζοντας ότι η προστασία των δεδομένων αποτελεί θεμελιώδες βασικό δικαίωμα, το οποίο θα ρυθμίζεται με συνέπεια σε όλη την Ε.Ε.. Στόχος του είναι να διευκολύνει τη ροή δεδομένων προσωπικού χαρακτήρα σε όλα τα κράτη μέλη της. Κάθε εταιρεία, που εξυπηρετεί Ευρωπαίους πολίτες και συλλέγει τα δεδομένα τους, θα πρέπει να συμμορφώνεται με αυτή την οδηγία, ακόμη και αν η ίδια εδρεύει σε χώρα εκτός Ε.Ε..

Ο Γ.Κ.Π.Δ. προστατεύει τα προσωπικά δεδομένα των χρηστών και εφαρμόζεται κατά την επεξεργασία, αποθήκευση και μεταφορά όλων των δεδομένων που διαχειρίζεται μια εταιρεία. Έτσι, αποδεικνύεται η σημαντικότητα της ροής της ψηφιακής πληροφορίας μέσα στην επιχείρηση. Ένας κλάδος που επηρεάζεται από τον κανονισμό είναι και η Data Analysis που έχει ως πρωταρχικό της στόχο να προσφέρει επιπρόσθετη αξία στην επιχείρηση μέσα από την επεξεργασία, αναζήτηση και μελέτη των εταιρικών δεδομένων με σκοπό να απαντά σε επιχειρηματικές ερωτήσεις, να κάνει πρόβλεψη άγνωστων αποτελεσμάτων και να συμβάλει στην αυτοματοποίηση των αποφάσεων.

Η ασφάλεια δεδομένων είναι η προστασία των ψηφιακών πληροφοριών από τη μη εξουσιοδοτημένη πρόσβαση, διαφθορά ή κλοπή καθ' όλη τη διάρκεια του κύκλου ζωής τους. Όταν η ασφάλεια δεδομένων εφαρμόζεται σωστά, ισχυρές στρατηγικές ασφάλειας δεδομένων προστατεύουν τα περιουσιακά στοιχεία ενός οργανισμού από εγκληματικές δραστηριότητες στον κυβερνοχώρο, προστατεύοντας τα παράλληλα από εσωτερικές απειλές και ανθρώπινα λάθη. Τα ανθρώπινα λάθη, ακόμα και σήμερα που δίνεται μεγάλη έμφαση στην εκπαίδευση του προσωπικού από τους οργανισμούς, παραμένουν μεταξύ των κορυφαίων αιτιών παραβίασης δεδομένων στην εποχή μας.

Τα δεδομένα θα πρέπει να υπόκεινται σε επεξεργασίες προστασίας, όπως κρυπτογράφηση και απόκρυψη δεδομένων, και η επεξεργασία ευαίσθητων αρχείων να γίνεται με αυτοματοποιημένη διαδικασία, που ενισχύει τους ελέγχους και τη συμμόρφωση με τις κανονιστικές απαιτήσεις.

Από τότε που τέθηκε σε ισχύ ο Γ.Κ.Π.Δ., έχουν δοθεί περισσότερα από 900 πρόστιμα σε ολόκληρο τον Ε.Ο.Χ. και τα πρόστιμα του κανονισμού στο Η.Β. έχουν αυξηθεί σημαντικά.

Ο κανονισμός προβλέπει πρόστιμα έως και 20 εκατομμύρια ευρώ ή έως και 4% του συνολικού παγκόσμιου κύκλου εργασιών της εταιρείας κατά το προηγούμενο οικονομικό έτος, όποιο από τα δύο ποσά είναι υψηλότερο. Το μεγαλύτερο πρόστιμο δόθηκε στην Amazon κατά το έτος 2021 και ανερχόταν στα 746 εκατομμύρια ευρώ. Ο λόγος που της αποδόθηκε αυτό το πρόστιμο δεν έχει γίνει ευρέως γνωστός, αλλά οι περισσότερες εικασίες προσδίδουν αυτό το πρόστιμο στην χρήση των cookies. Πολλές ακόμα μεγάλες εταιρείες έχουν δεχτεί μεγάλα πρόστιμα για λόγους όπως:

- Την παραβίαση της αρχής ελαχιστοποίησης των δεδομένων (H&M).
- Την αδιαφανή ειδοποίηση απορρήτου μη παρέχοντας στους χρήστες πληροφορίες απορρήτου σε μια εύκολα προσβάσιμη μορφή χρησιμοποιώντας τη γλώσσα που μπορούσαν να καταλάβουν οι χρήστες της (WhatsApp).
- Την μη «ελεύθερη» συγκατάθεση καθώς η απόρριψη των cookies δεν ήταν το ίδιο εύκολο με την αποδοχή των cookies, δηλαδή μόνο με ένα κλικ (Google).

Για να τονιστεί η σημαντικότητα της συμμόρφωσης με τον Γ.Κ.Π.Δ. είναι σημαντικό να αναφερθούμε και σε ένα άρθρο που γνωστοποιεί τα πλήθος των προστίμων που αποδόθηκαν ανά κλάδο εταιρειών μέχρι και το έτος 2020. Πιο συγκεκριμένα, το άρθρο του Neil Hodge με τίτλο «GDPR fines by industry: Telecoms far outpace Big Tech» που δημοσιεύτηκε στο «Compliance week for the well-informed chief compliance officer audit executive» τον Μάρτιου του 2021 αναφέρει τα ακόλουθα πλήθη προστίμων ανά κλάδο:

- Τηλεπικοινωνίες: 69
- Επιχειρήσεις: 45
- Οικονομικές υπηρεσίες: 28
- Φροντίδα υγείας: 17
- Τεχνολογία: 16

Είναι σημαντικό να αναφερθεί πως 3 από τα 12 συνολικά πρόστιμα που είχαν δοθεί στην Ελλάδα αφορούσαν τις τηλεπικοινωνίες. Οι 2 από αυτές είχαν τιμωρηθεί με πρόστιμο 200.000 ευρώ έκαστη. Τα τρία μεγαλύτερα πρόστιμα της Ιταλίας, μέχρι το έτος 2020, αφορούσαν τις τηλεπικοινωνίες με την TIM να πληρώνει πρόστιμο 27,8 εκατομμυρίων ευρώ, την Wind Tre 16,7 εκατομμυρίων ευρώ και την Vodafone Italia 12,25 εκατομμυρίων ευρώ.

Στην συνέχεια παρουσιάστηκε η ανάγκη να δημιουργηθεί κάποιο νέο πρότυπο, με την εφαρμογή του οποίου οι εταιρείες θα πιστοποιούνται, ώστε να καλύψουν μεγάλο εύρος από τα απαιτούμενα που θέτει ο Γ.Κ.Π.Δ.. Ένα από αυτά τα πρότυπα που εξυπηρέτησε αυτή την ανάγκη είναι το ISO. 27001 και με την βάση πιστοποίησης αυτού οι εταιρείες μπορούν να έχουν ένα ικανοποιητικό επίπεδο ασφαλείας για την διαχείριση των προσωπικών δεδομένων που έχουν στην κατοχή τους.

Ένα ακόμα σημαντικό πρότυπο πιστοποίησης είναι το ISO 27.7001. Το ISO/IEC 27701 είναι μια επέκταση απορρήτου δεδομένων στο ISO. 27001 που βοηθά τους οργανισμούς να δημιουργήσουν συστήματα για την υποστήριξη της συμμόρφωσης με τον Γ.Κ.Π.Δ. και άλλες απαιτήσεις απορρήτου δεδομένων. Το πρότυπο αυτό παρέχει το απαραίτητο πρότυπο για την οικοδόμηση εμπιστοσύνης κατά τη διαχείριση δεδομένων. Οι προμηθευτές, οι καταναλωτές και οι συνεργάτες των

εταιρειών μπορούν να έχουν εμπιστοσύνη στις πολιτικές, τις διαδικασίες και τα πρωτόκολλα της επιχείρησης, όταν αυτή συμμορφώνεται με το διεθνές πρότυπο ISO 27701.

Η κατανόηση από όλα τα μέλη της Ε.Ε. για την επιτακτική ανάγκη εφαρμογής του Γ.Κ.Π.Δ. οδήγησε στην δημιουργία των πιστοποιήσεων ISO., απαραίτητα πλέον στην λειτουργία των εταιρειών. Η παρούσα διπλωματική, λοιπόν, λαμβάνοντας υπόψιν της τη σπουδαιότητα του ανωτέρω κανονισμού και της πιστοποίησης I.SO 27001, θα παραθέσει παραδείγματα εφαρμογής τους στις επιχειρήσεις, εστιάζοντας τόσο στις μεταρρυθμίσεις που φέρουν όσο και στη συνεχή συμβολή τους ως προς την βελτίωση της εκάστοτε εταιρείας.

2 ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΑΝΑΣΚΟΠΗΣΗ

Στο συγκεκριμένο κεφάλαιο θα πραγματοποιηθεί η βιβλιογραφική ανασκόπηση. Πιο αναλυτικά θα αναφερθούν άρθρα που έχουν δημοσιευτεί στο διαδίκτυο τα τελευταία χρόνια γύρω από το θέμα του Γ.Κ.Π.Δ.. Το ISO 27001 είναι πιστοποιητικό που αφορά συστήματα εταιρειών και δηλώνει ότι συμμορφώνονται με τον κανονισμό. Ακολούθως θα γίνει αναφορά σε μερικά άρθρα ως λύση για την υιοθέτηση του κανονισμού από τις επιχειρήσεις.

2.1: Η εισαγωγή του Γ.Κ.Π.Δ.

2.1.1: Μια νέα εποχή στην προστασία δεδομένων

Το άρθρο «A new era in data protection » των Lawrence Ryz & Lauren Grest αναφέρεται στον Γ.Κ.Π.Δ. και στις βασικές του αρχές. Αρχικά τονίζει ότι ο κανονισμός αυτός αντικαθιστά της Οδηγίας για την Προστασία Δεδομένων. Επισημαίνεται πως ενώ παλιά υπήρχε οδηγία για την προστασία των δεδομένων, πλέον θα εφαρμοζόταν κανονισμός για την προστασία των δεδομένων. Αυτό δηλώνει την αναγκαιότητα ακολούθησής του και την ύπαρξη κυρώσεων σε όσους δεν τον τηρούσαν.

Ο κανονισμός αυτός ήταν ενιαίος και έδινε την ευκαιρία στα κράτη μέλη να δημιουργήσουν συμπληρωματική νομοθεσία σε αυτόν. Στην συνέχεια αναφέρεται στον αντίκτυπο που θα επέφερε στο “e-discovery”. Ο αντίκτυπος του στο ηλεκτρικό επιχειρείν και σε άλλες επιχειρηματικές δραστηριότητες που περιλάμβαναν τη μεταφορά δεδομένων θα προέκυπτε από αλλαγές στους ορισμούς των προσωπικών δεδομένων και στην επεξεργασία δεδομένων.

Το τελικό σχέδιο του κανονισμού αναφέρει ότι οι διαβιβάσεις δεδομένων εκτός Ε.Ε. επιτρέπονται μόνο εάν πληρούνται ορισμένες προϋποθέσεις, όπως η ύπαρξη επαρκών κανονισμών προστασίας δεδομένων από τη χώρα προορισμού και εάν η εταιρεία που διαβιβάζει δεδομένα διαθέτει κατάλληλες διασφαλίσεις.

Όπου τα σύνολα δεδομένων ήταν ιδιαίτερα μεγάλα, οι εταιρείες μπορούσαν να επωφεληθούν από την τεχνολογία “e-discovery” για να τα φιλτράρουν επιτόπου και να μειώνουν τον όγκο των δεδομένων που μεταφέρονται. Η χρήση αυτού του είδους τεχνολογίας όχι μόνο βοήθησε στη συμμόρφωση με τον κανονισμό, με την έννοια ότι η επεξεργασία ήταν αναλογική, αλλά και στην εξοικονόμηση κόστους, όσον αφορά την αναθεώρηση μεγάλων συνόλων δεδομένων.

Τέλος, οι αρθρογράφοι αναρωτιούνται αν ο Γ.Κ.Π.Δ. θα αντέξει με το πέρασμα των χρόνων. Αυτό το αναρωτιούνται καθώς ο νόμος αναπτύσσεται και εξελίσσεται πάντα πιο αργά από την τεχνολογία. Αν και ο Γ.Κ.Π.Δ. προσφέρει μια πιο εναρμονισμένη και ευρεία προσέγγιση για την προστασία των δεδομένων τώρα, είναι δύσκολο να προβλεφθεί ποιες νέες τεχνολογίες μπορεί να προκύψουν σε 20 χρόνια και αν θα τις ικανοποιεί.

2.1.2: Η εφαρμογή του Γ.Κ.Π.Δ.

Κατά την συνέντευξη της αρθρογράφου Claire Laybats με τον συνεντευξιαζόμενο John Davies στο άρθρο «GDPR: Implementing the regulations», γίνεται αντιληπτό πώς ο John Davies αντιλαμβάνεται τη σημαντικότητά του Γ.Κ.Π.Δ.. Χαρακτηριστικά αναφέρει πως ο κανονισμός λέει ότι έκαναν ήδη οι ευσυνείδητες επιχειρήσεις και πως το θεωρεί σωστό να θεσπιστεί για όλες τις επιχειρήσεις. Ο ίδιος έχει ήδη εφαρμόσει σχέδιο πλήρους συμμόρφωσης με τον κανονισμό σε όλα τα υποκαταστήματα της επιχείρησής.

Στην συνέχεια, η αρθρογράφος αναφέρεται στο γεγονός πως το Brexit δεν έχει επιφέρει αλλαγές καθώς όλες οι χώρες που έχουν συναλλαγές με την Ε.Ε. πρέπει να συμμορφώνονται με τον Γ.Κ.Π.Δ..

Γίνεται μια μικρή αναφορά για το πώς λειτουργεί το Facebook και το πώς χρησιμοποιεί τα προσωπικά δεδομένα των χρηστών του, κάνοντας μικρές αναφορές σε άλλα άρθρα. Αυτά τα άρθρα χρησιμοποιούνται ως ανακατευθύνσεις για τους αναγνώστες. Σύμφωνα με τον αρθρογράφο, στα άρθρα αυτά φαίνεται ο καταχρηστικός χαρακτήρας του Facebook που κατά το δυνατόν αποφεύγει τον Γ.Κ.Π.Δ., καθώς τα έσοδα του προέρχονται από διαφημίσεις προσωποποιημένες για τους χρήστες του.

Το Facebook δεν είναι η μόνη εταιρεία που αντιτίθεται στη νομοθεσία περί προστασίας δεδομένων. Στο παρελθόν όλοι οι οργανισμοί μπορούσαν να παρακολουθούν, να αποθηκεύουν και να αναλύουν τεράστιες ποσότητες προσωπικών δεδομένων. Το πρόβλημα αυτό υπάρχει και θα υπάρχει ακόμα στις χώρες που δεν υπάγονται στον Γ.Κ.Π.Δ.. Αναφέρεται επίσης ότι μόλις εξετάσουν τις επιπτώσεις για τα προσωπικά τους δεδομένα και την προστασία τους, θα προχωρήσουν άμεσα και αυτές στην σύνταξη του δικού τους κανονισμού.

2.1.3: Η εφαρμογή του Γ.Κ.Π.Δ. εκτός της Ευρώπης

Η εφαρμογή των ευρωπαϊκών κανονισμών για τη προστασία των προσωπικών δεδομένων ισχύει και εκτός της Ε.Ε.. Το άρθρο «European Data Privacy Standards Implemented in Laws Outside Europe» έρχεται σε συνέχεια του άρθρου που είχε γράψειο ίδιος ο Graham Greenleaf το 2012 για τους νόμους περί απορρήτου δεδομένων των είκοσι (20) χωρών με το υψηλότερο Α.Ε.Π. εκτός Ευρώπης που έχουν τέτοιους νόμους. Το αποτέλεσμα είναι ότι αυτές οι χώρες εφαρμόζουν 5,95 από τις 10 διακριτές ευρωπαϊκές αρχές προστασίας της ιδιωτικής ζωής.

Στο άρθρο τονίζεται πως υπήρχε συσχέτιση του Α.Ε.Π. της χώρας με την Ομάδα των είκοσι (ή αλλιώς G-20 που είναι ένα διεθνές forum για τις κυβερνήσεις και τους διοικητές των κεντρικών τραπεζών από τις 20 μεγάλες οικονομίες). Μόνο οκτώ (8) μη ευρωπαϊκές χώρες στη λίστα των κορυφαίων πενήντα τριών (53) χωρών ανά Α.Ε.Π. δεν διέθεταν, κατά το έτος 2018, νόμους για το απόρρητο δεδομένων νόμους. Από τις δέκα τρεις (13) μη ευρωπαϊκές χώρες του G20, μόνο τέσσερεις (4) χώρες δεν είχαν νόμους περί απορρήτου δεδομένων που να πληρούν αυτό το ελάχιστο διεθνές πρότυπο. Με οποιοδήποτε από αυτά τα μέτρα, η πλειοψηφία των σημαντικών χωρών, από οικονομική και πολιτική άποψη, είχαν νόμους περί απορρήτου δεδομένων που πληρούσαν αυτά τα ελάχιστα διεθνή πρότυπα «πρώτης γενιάς».

Στην συνέχεια είχε αξιολογηθεί ο βαθμός στον οποίο τα δέκα ευρωπαϊκά πρότυπα, που αποτελούσαν τη «δεύτερη γενιά» προτύπων απορρήτου δεδομένων, είχαν εφαρμοστεί έως το 2017 στους νόμους των είκοσι κορυφαίων και μη ευρωπαϊκών χωρών. Οι χώρες που είχαν την υψηλότερη εφαρμογή των ευρωπαϊκών αρχών από τις «είκοσι (20) κορυφαίες χώρες του Α.Ε.Π.» ήταν το Περού, η Νότια Αφρική και η Νότια Κορέα. Οι περισσότερες χώρες εκτός Ε.Ε. που είχαν χαμηλή θέση, είχαν υπό

υλοποίηση νέα νομοθετικά μέτρα που θα τις έκαναν να φτάσουν τη μέση εφαρμογή των αρχών στο 6,5/10.

Το άρθρο αυτό συμπεραίνει ότι υπάρχουν ισχυρές ενδείξεις ότι τα ευρωπαϊκά ή αλλιώς «δεύτερης γενιάς» πρότυπα απορρήτου των δεδομένων συνεχίζουν να υιοθετούνται εκτός Ευρώπης σε πολύ σημαντικό βαθμό.

2.2: Οι αντιδράσεις στον Γ.Κ.Π.Δ.

2.2.1: Οι αντιδράσεις, οι προτεινόμενες αλλαγές και οι οδηγίες υιοθέτησης στον Γ.Κ.Π.Δ.

Το άρθρο «One Year and Loads of Data Later, Where Are We? An Update on the Proposed European Union General Data Protection Regulation» του Dla Piper εξετάζει τον Προτεινόμενο Γ.Κ.Π.Δ. της Ε.Ε., ένα χρόνο μετά την πρότασή του από την Ευρωπαϊκή Επιτροπή. Συγκεκριμένα αναλύθηκαν οι αντιδράσεις στον Γ.Κ.Π.Δ. των κρατών μελών της Ε.Ε., της Ομάδας Εργασίας για την Προστασία Δεδομένων του Άρθρου 29, των αρμοδίων επιτροπών του Ευρωπαϊκού Κοινοβουλίου και του Συμβούλιου της Ευρωπαϊκής Ένωσης και εντοπίστηκαν οι μέχρι τότε νομοθετικές ενέργειες για τον Γ.Κ.Π.Δ.. Επιπλέον, οι προτεινόμενες τροποποιήσεις σε αυτόν από την κοινοβουλευτική επιτροπή είναι λεπτομερείς, ιδίως στους τομείς του διευρυμένου πεδίου εφαρμογής του Γ.Κ.Π.Δ., των ειδοποιήσεων παραβίασης προσωπικών δεδομένων, της συναίνεσης και των νόμιμων βάσεων για την επεξεργασία, τη φορητότητα δεδομένων, το δικαίωμα στη λήθη, τους υπευθύνους προστασίας δεδομένων και τις διασυνοριακές διαβιβάσεις δεδομένων, μεταξύ άλλων. Τέλος, παρατίθενται τα βήματα για την προετοιμασία για ενδεχόμενη υιοθέτησή του.

Οι αντιδράσεις στον Γ.Κ.Π.Δ. ήταν μικτές. Υπήρξαν αποκλίνουσες απόψεις των κρατών μελών σχετικά με αρκετές διατάξεις του, συμπεριλαμβανομένης της επιλογής ενός κανονισμού ως του κατάλληλου νομοθετικού μέσου, με ορισμένα κράτη μέλη να δηλώνουν ότι ενδέχεται να ασκήσουν τα δικαιώματά τους σε καταγγελία επικουρικότητας, υποστηρίζοντας ότι ο Γ.Κ.Π.Δ. παραβιάζει αυτήν την αρχή της Ε.Ε.. Ορισμένοι ισχυρίζονται ότι το δικαίωμα στη λήθη και στη διαγραφή των προσωπικών δεδομένων κάποιου είναι ανεφάρμοστο. Πολλοί εξέφραζαν παράπονα για την αυξημένη εδαφική εμβέλεια του κανονισμού και άλλοι καταδίκαζαν το σύντομο χρονικό διάστημα για τους υπεύθυνους επεξεργασίας να εκδίδουν ειδοποιήσεις για παραβιάσεις προσωπικών δεδομένων και το κόστος που επιφέρει στις μικρομεσαίες επιχειρήσεις.

Στο άρθρο σημειώνονται τα σημεία που πρέπει να αλλαχθούν στον Γ.Κ.Π.Δ. και δίνεται κάποιες διευκρινίσεις. Πιο συγκεκριμένα, για παράδειγμα, αναφέρει πως η δήλωση WP29 ενώ υποστηρίζει μια εξαίρεση οικιακής χρήσης, υποδεικνύει ότι υπάρχει ισχυρό επιχείρημα για εφαρμογή του Γ.Κ.Π.Δ. (π.χ. των εξουσιών έρευνας των εποπτικών αρχών) σε όλα τα είδη δραστηριοτήτων επεξεργασίας προσωπικών δεδομένων. Σύμφωνα με το άρθρο, αυτό θα μπορούσε να επιτευχθεί μέσω της τροποποίησης του άρθρου 52 του Γ.Κ.Π.Δ. σχετικά με τα καθήκοντα των εποπτικών αρχών και μέσω των αναλυτικών κριτηρίων για την εφαρμογή της εξαίρεσης οικιακής χρήσης. Κατά τον ίδιο τρόπο αναφέρεται και σε άλλα καίρια σημεία.

Τέλος, αναφέρονται τα επτά κύρια βήματα για την υιοθέτηση του Γ.Κ.Π.Δ.. Το πρώτο βήμα τονίζει πως η τελική μορφή του Γ.Κ.Π.Δ. που θα πρέπει να υιοθετείται από τις εταιρείες δεν ήταν γνωστό εκείνη την χρονική περίοδο, αλλά ήταν σημαντικό να το γνώριζαν. Ως δεύτερο βήμα προτρέπει να προσλάβουν έναν υπεύθυνο προστασίας δεδομένων που θα ενημερώνεται συνέχεια για τον κανονισμό. Στην συνέχεια προτρέπει την εκάστοτε εταιρεία να βεβαιωθεί ότι λαμβάνει την κατάλληλη

συγκατάθεση τεκμηριώνοντάς την σωστά και να έχουν σωστότερα έγγραφα τεκμηρίωσης και συστήματα για την επεξεργασία δεδομένων. Ως πέμπτο βήμα αναφέρει ότι πρέπει να θέτουν υψηλούς στόχους προστασίας δεδομένων πριν από την επίσημη εφαρμογή του Γ.Κ.Π.Δ. για να εξασφαλίσουν την ασφάλεια απορρήτου. Ακολούθως αναφέρεται στην σημαντικότητα του η κάθε εταιρεία να βρει από μόνη της τα κενά ασφαλείας της και να τα διορθώσει, κάτι που θα έχει ως αποτέλεσμα το προσωπικό της να εκπαιδευτεί σε τέτοιες καταστάσεις και να είναι έτοιμο σε μελλοντικές επιθέσεις. Τέλος, προτρέπει τους αναγνώστες του άρθρου να δουν τον κανονισμό σαν μία ευκαιρία όχι μόνο για την υιοθέτησή του αλλά και για την ενημέρωση και τον εξορθολογισμό των οργανισμών και των συστημάτων τεκμηρίωσης και πληροφοριών και ως μια ευκαιρία για την αύξηση εμπιστοσύνης των πελατών στις επιχειρήσεις που επεξεργάζονται τα προσωπικά δεδομένα τους.

2.3: Η επίδραση του Γ.Κ.Π.Δ.

2.3.1: Η επίδραση του Γ.Κ.Π.Δ.

Ο Γ.Κ.Π.Δ. αντιπροσωπεύει την πιο σαρωτική προσπάθεια που έχει γίνει για την επίβλεψη του τρόπου με τον οποίο οι επιχειρήσεις συλλέγουν και διαχειρίζονται τα δεδομένα καταναλωτών. Παρέχει στους ευρωπαίους πολίτες μεγαλύτερο έλεγχο των δεδομένων τους, ενώ επιβάλλει αυστηρές κυρώσεις για τις επιχειρήσεις που δεν συμμορφώνονται.

Ο κανονισμός άλλαξε από τον τρόπο συλλογής δεδομένων έως τον τρόπο που σχεδιάζονται και χρησιμοποιούνται οι εταιρικές βάσεις δεδομένων. Επίσης, άλλαξε δυνητικά τον τρόπο με τον οποίο διεξάγεται η έρευνα και ανάπτυξη επηρεάζοντας τις πρακτικές κυβερνοασφάλειας.

Στην συνέχεια, στο άρθρο «Weighing the impact of GDPR » του Samuel Greengard αναφέρεται πως η ψηφιακή τεχνολογία έχει αλλάξει αναπόφευκτα το πρόσωπο της ιδιωτικής ζωής, καθώς πολλά στοιχεία της υφίστανται επιθέσεις. Η Η.Π.Α. και ορισμένες άλλες χώρες έχουν υιοθετήσει μια προσέγγιση εξαίρεσης στη συλλογή δεδομένων, ενώ η Ευρώπη έχει εφαρμόσει μια πιο περιοριστική προσέγγιση επιλογής. Αυτός ο κανονισμός αποτελεί υποχρέωση για τα άτομα που χειρίζονται τέτοια στοιχεία και προστασία για τους χρήστες.

Από την άλλη πλευρά υπάρχουν πολλές πιθανές παγίδες που ίσως να προκύπτουν από τον Γ.Κ.Π.Δ.. Μία εκ των οποίων αποτελεί η πολυπλοκότητα του Γ.Κ.Π.Δ. και ο τρόπος με τον οποίο οι ρυθμιστικές αρχές και τα δικαστήρια ερμηνεύουν ορισμένες από τις σκόπιμα ασαφείς διατυπώσεις του. Υπάρχει επίσης έντονη αντίθεση στον εταιρικό στίβο, όπου εστιάζουν στο κέρδος από τα δεδομένα και όχι στην αποτροπή των καταχρήσεων και παραβιάσεων.

Οι προσωπικοί βοηθοί όπως οι Siri, Alexa και Cortana εισάγουν πρόσθετες προκλήσεις συμμόρφωσης καθώς όλα αυτά τα συστήματα συλλέγουν και αποθηκεύουν δεδομένα για άτομα. Ακόμη και τα συστήματα ανθρώπινων πόρων, τα συστήματα μισθοδοσίας και παρόμοια αποθετήρια προσωπικών δεδομένων θα μπορούσαν να επηρεαστούν σημαντικά από τον κανονισμό. Επιπλέον, ο Γ.Κ.Π.Δ. προσθέτει ένα επίπεδο πολυπλοκότητας πάνω σε ένα ήδη πολύπλοκο ευρωπαϊκό πλαίσιο απορρήτου. Πολλές εταιρείες δεν διέθεταν τεχνογνωσία στον τρόπο με τον οποίο θα έπρεπε να εφαρμόσουν και να διαχειριστούν δεδομένα βάσει του Γ.Κ.Π.Δ..

Η αντίδραση των καταναλωτών παίζει καταλυτικό ρόλο. Εάν μεγάλος αριθμός ατόμων αμφισβητούσε τον τρόπο με τον οποίο οι εταιρείες χρησιμοποιούσαν τα δεδομένα τους, οι επιχειρήσεις θα μπορούσαν να φτάσουν σε ένα σημείο καμπής όπου θα έπρεπε να επανεξετάσουν τον θεμελιώδη τρόπο με τον οποίο προσεγγίζουν τη

διαχείριση δεδομένων ή να επαναξιολογήσουν τη θεμελιώδη αξία των δεδομένων και τον τρόπο που έχουν έσοδα από αυτά.

2.3.2: Επιρροή του Γ.Κ.Π.Δ. παγκοσμίως

Ο Jan Philip Albrecht στο άρθρο του με τίτλο «How the GDPR will Change the World» κάνει μια εκτενή αναφορά για το πως ο Γ.Κ.Π.Δ. θα επηρεάσει τα παγκόσμια δεδομένα.Πιο συγκεκριμένα, στις 24 Μαΐου του 2018 ο Γ.Κ.Π.Δ. τέθηκε σε ισχύ για δραστηριότητες επεξεργασίας προσωπικών δεδομένων εντός των επιχειρήσεων. Είναι υψίστης σημασίας να γίνει αντιληπτό πώς ο Γ.Κ.Π.Δ. άλλαξε όχι μόνο τα ευρωπαϊκά δεδομένα για την προστασία αλλά και ολόκληρο τον κόσμο. Αυτό φάνηκε από τον Δεκέμβριο του 2015 κατά την συμφωνία που έγινε μεταξύ του Ευρωπαϊκού Κοινοβουλίου και του Ευρωπαϊκού Συμβουλίου.

Ο Γ.Κ.Π.Δ. επέφερε περισσότερη ασφάλεια δικαίου καθώς τώρα 28 διαφορετικά νομικά συστήματα, 28 διαφορετικά δικαστικά αλλά και οι κουλτούρες επιβολής ορίζουν το ρυθμιστικό περιβάλλον. Αυτή η αλλαγή σε ένα ενιαίο νομικό πλαίσιο που περιλαμβάνει ίσους όρους ανταγωνισμού για όλες τις εταιρείες στην ευρωπαϊκή αγορά είναι εξαιρετικά θετικό και για τις επιχειρήσεις αλλά και για τους καταναλωτές. Προκειμένου να τηρηθεί η υποχρέωση του πρωτογενούς δικαίου της Ε.Ε. για την προστασία των δεδομένων, το Δικαστήριο της Ε.Ε. κατέστησε πρόσφατα σαφές ότι δεν υπάρχει τρόπος να ξεπεραστεί το υψηλό επίπεδο προστασίας των προσωπικών δεδομένων στην Ε.Ε.. Η αυστηρή διατύπωση σχετικά με τις διεθνείς μεταφορές δεδομένων είναι αποτελέσματα των υποκείμενων προβλημάτων που εμφανίστηκαν σε όλη την αναπτυσσόμενη οικονομία του Διαδικτύου την τελευταία δεκαετία. Κανένας υπεύθυνος επεξεργασίας δεδομένων δεν μπορεί να το αγνοήσει ενώ κάποιες κυβερνήσεις πιέστηκαν και πιέζονται να αυξήσουν τα πρότυπα προστασίας των δεδομένων τους, προκειμένου να επιτρέψουν στις οικονομίες τους πρόσβαση στην ψηφιακή ενιαία αγορά της Ε.Ε.. Τέλος επισημαίνεται ότι ο Γ.Κ.Π.Δ. χρησιμεύει ως αφετηρία για τα διεθνή πρότυπα και για μια αξιόπιστη ψηφιακή αγορά.

Με αυτό το πλαίσιο, ο Γ.Κ.Π.Δ. χρησίμευσε ως πρότυπο και για άλλους τομείς πολιτικής όπου οι συνέπειες της παγκοσμιοποίησης και της ψηφιοποίησης απαιτούσαν μια νέα ρυθμιστική προσέγγιση προκειμένου να διαφυλαχθούν αποτελεσματικά οι αξίες και τα πρότυπα. Δίνεται έτσι στην Ε.Ε. μία ευκαιρία, καθώς δείχνει ότι είναι δυνατή η επίτευξη κοινής δράσης μέσω μιας δημοκρατικής διαδικασίας στη βάση υψηλών προτύπων για τα δικαιώματα των πολιτών και των καταναλωτών, καθώς η Ε.Ε. αποτελεί μια ανταγωνιστική και καινοτόμα ενιαία αγορά.

2.3.3: Η επιρροή του Γ.Κ.Π.Δ. στην διοίκηση της επιχείρησης και στην χρήση των προσωπικών δεδομένων

Στο άρθρο «GDPR Impact on Company Management and Processed Data» των Sabina-Daniela Axinte, Gabriel Petrică και Ioan Bacivarov παρέχει πληροφορίες για τον Γ.Κ.Π.Δ. και αναλύει τον αντίκτυπό του σε νομικά πρόσωπα διαφόρων τάξεων, καθώς και σε φυσικά πρόσωπα. Επιπλέον, παρέχει πλαίσιο και ταξινόμηση για τους τύπους δεδομένων που αποτελούν αντικείμενο του παρόντος κανονισμού, μέτρα που πρέπει να λαμβάνουν οι εταιρείες για την επίτευξη συμμόρφωσης, αποτρεπτικά μέτρα που μπορούν να επιβάλουν οι ρυθμιστικοί φορείς για μη συμμορφούμενη συμπεριφορά και παραβιάσεις δεδομένων, καθώς και συστάσεις ασφαλείας τόσο για εργοδότες όσο και για εργαζομένους.

Οι εταιρείες και οι νομικές οντότητες ελέγχου πρέπει να συνεργάζονται προκειμένου όλα τα μέρη να επωφελούνται από τις κατευθυντήριες γραμμές για την

προστασία δεδομένων, ανεξάρτητα από την παγκόσμια θέση τους και την αντίστοιχη νομοθεσία. Ανάλογα με την τρέχουσα κατάσταση, τα σχέδια δράσης μπορούν να επεκταθούν πολύ πέρα από την αναθεώρηση των υφιστάμενων πολιτικών απορρήτου και να επηρεάσουν όλες τις εταιρείες, ανεξαρτήτως μεγέθους. Επιπλέον αναφέρεται στην συναίνεση για τη χρήση cookies από τους χρήστες και στο ότι πρέπει να δοθεί έμφαση στο συγκεκριμένο, κάτι που στο παρελθόν δεν υπήρχε. Μόνο η θετική απάντηση του χρήστη δηλώνει συναίνεση για την χρήση προσωπικών δεδομένων. Τέλος, κάθε εταιρεία, ανεξάρτητα από το μέγεθός της, πρέπει να έχει έναν Υπεύθυνο Προστασίας Δεδομένων.

2.3.4: Οι επιπτώσεις του Γ.Κ.Π.Δ. ένα χρόνο μετά την εφαρμογή του

Στο άρθρο «The impact of GDPR one year on» του Paul Breitbarth αναφέρονται τα αποτελέσματα που έχει επιφέρει ο Γ.Κ.Π.Δ. ένα χρόνο μόλις μετά την εφαρμογή του. Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων δημοσίευσε την πρώτη του επισκόπηση της εφαρμογής και επιβολής του κανονισμού και τα ευρήματα έδειξαν ότι υπήρχαν 206.326 περιπτώσεις που είχαν αναφερθεί από τις Α.Π.Δ.. Σχεδόν οι μισές από αυτές τις υποθέσεις, δηλαδή 96.622, αφορούσαν καταγγελίες, ενώ πάνω από το ένα τέταρτο, δηλαδή 64.684, αφορούσαν συγκεκριμένες παραβιάσεις δεδομένων.

Η έκθεση της Ευρωπαϊκής Επιτροπής διερεύνησε την ευαισθητοποίηση, τη συμμόρφωση και την επιβολή των κανόνων και αποκάλυψε ότι πάνω από το 67% των Ευρωπαίων είχαν ακούσει για τον Γ.Κ.Π.Δ.. Αυτό το ποσοστό αυξήθηκε στο 73% μέχρι τον Ιούλιο του 2018. Σύμφωνα με την Ευρωπαϊκή Επιτροπή, οι πιο συχνοί τύποι καταγγελιών, που αναφέρθηκαν κατά το πρώτο έτος εφαρμογής του κανονισμού, ήταν για τις τηλεπωλήσεις, τα διαφημιστικά μηνύματα ηλεκτρονικού ταχυδρομείου και τις κάμερες παρακολούθησης (CCTV).

Είχε σημειωθεί πρόοδος σύμφωνα με την Ετήσια Έκθεση Διακυβέρνησης του Ιδιωτικού Απορρήτου της IAPP-EY. Περίπου το 89% των συμμετεχόντων στην έρευνα στην Ε.Ε. δήλωσαν ότι είχαν διορίσει έναν υπεύθυνο προστασίας δεδομένων ως απάντηση στον Γ.Κ.Π.Δ., ενώ η ευαισθητοποίηση σε θέματα προστασίας δεδομένων είχε αυξηθεί όσον αφορά:

- τη συμμόρφωση κατά 83%,
- τις παραβιάσεις δεδομένων κατά 68% και
- τις πρωτοβουλίες προστασίας της ιδιωτικής ζωής κατά 61%.

Η πιο κοινή πτυχή της νομοθεσίας που επαναλαμβάνεται παγκοσμίως είναι η καθοδήγηση σχετικά με τα δικαιώματα των υποκειμένων των δεδομένων, τις απαιτήσεις λογοδοσίας και τις παραβιάσεις δεδομένων, τα οποία έχουν δημιουργήσει εκτεταμένο δημόσιο ενδιαφέρον και ευαισθητοποίηση για τον τρόπο χειρισμού των προσωπικών δεδομένων από οργανισμούς.

Τέλος, το άρθρο αναφέρεται στον αντίκτυπο του Brexit και την αβεβαιότητα που συνέχιζε να επικρατεί σχετικά με την έξοδο του Η.Β. από την Ε.Ε.. Εάν η κυβέρνηση διαπραγματευόταν μια συμφωνία, τότε η ελεύθερη ροή δεδομένων από την οποία το Η.Β. θα επωφελούταν ως μέλος της Ε.Ε. βάσει του Γ.Κ.Π.Δ. θα συνεχιζόταν κατά τη μεταβατική περίοδο πριν από τη σύναψη τελικής συμφωνίας επάρκειας. Ωστόσο, ένα σενάριο «χωρίς συμφωνία» θα είχε αναμφίβολα πιο σοβαρές και εκτεταμένες επιπτώσεις. Ενώ βάση της καθοδήγησης του Επιτρόπου Πληροφοριών, οι διαβιβάσεις δεδομένων μεταξύ του Η.Β. και της Ε.Ε. δεν θα επηρεάζονταν προς το παρόν, θα υπήρχε όμως επείγουσα ανάγκη να εφαρμοστούν συμβατικές ρήτρες για τη

νομιμοποίηση των μεταφορών από την Ε.Ε. στο Η.Β.. Αυτό θα οφειλόταν στο γεγονός ότι το Η.Β. θα θεωρείτο στην πραγματικότητα ως «τρίτη χώρα».

2.3.5: Οι επιπτώσεις του Γ.Κ.Π.Δ. τρία χρόνια μετά την εφαρμογή του

Στο άρθρο «"It may be a pain in the backside but..." Insights into the impact of GDPR on business after three years» των Gerard Buckley, Tristan Caulfield και Ingolf Becker αναφέρονται τα αποτελέσματα που έχει επιφέρει ο Γ.Κ.Π.Δ. τρία χρόνια μετά την εφαρμογή του.

Ο στόχος αυτής της μελέτης είναι να διερευνήσει εάν ο Γ.Κ.Π.Δ. είναι μια επίπονη και δαπανηρή αλλαγή χωρίς κανένα κέρδος για τις επιχειρήσεις. Χρησιμοποιήθηκαν ημι-δομημένες συνεντεύξεις με 14 στελέχη που είναι υπεύθυνα για τις επιχειρήσεις, τα οικονομικά, το μάρκετινγκ, τη νομική και την τεχνολογία και προέρχονται από έξι μικρές, μεσαίες και μεγάλες εταιρείες στο Η.Β. και την Ιρλανδία. Μέσα από τις συνεντεύξεις αποδείχθηκε πως η απειλή των προστίμων κάνει τις επιχειρήσεις να δώσουν περισσότερη σημασία στο απόρρητο.

Έχει δημιουργήσει νέες θέσεις εργασίας για την υποστήριξη του Γ.Κ.Π.Δ.. Έχει αναγκάσει τις εταιρείες, σε διάφορους βαθμούς, να εκσυγχρονίσουν τις πλατφόρμες τους. Αυτό ωφέλησε έμμεσα τις επιχειρήσεις με καλύτερες διαδικασίες διαχείρισης κινδύνου, υποδομές ασφάλειας πληροφοριών και ενημερωμένες βάσεις δεδομένων πελατών. Η συμμόρφωση, για ορισμένους, χρησιμοποιείται ως σήμα αξιοπιστίας για την φήμη της εκάστοτε επιχείρησης. Από την άλλη πλευρά υπάρχουν πολλές προκλήσεις εφαρμογής. Η ενδοεταιρική επικοινωνία είναι πιο περιορισμένη. Ο κανονισμός έχει αυξήσει το κόστος και την εσωτερική γραφειοκρατία. Οι μικρές επιχειρήσεις βλέπουν τον Γ.Κ.Π.Δ. ως υπερβολικό και ότι χρειάζεται πάρα πολλούς πόρους, χρήματα και ενέργειες.

Συμπερασματικά, ο Γ.Κ.Π.Δ. μπορεί να χαρακτηριστεί ως επίπονος κανονισμός από τις επιχειρήσεις, αλλά το έχει κάνει πιο προσεκτικό με τα δεδομένα. Τέλος, προτείνεται μια νέα έκδοση του Γ.Κ.Π.Δ. που θα αφορά μόνο τις μικρο-μεσαίες επιχειρήσεις της Ε.Ε., που θα τροποποιήσει τα μηνύματα ώστε να είναι πιο θετικά, ενώ θα συνεχίζει να ενισχύει την πειθαρχία των εταιρικών δεδομένων.

2.3.6: Τα ανταγωνιστικά πλεονεκτήματα του Γ.Κ.Π.Δ.

Σύμφωνα με το άρθρο «The Competitive Effects of the GDPR» των Michal S Gal και Oshrit Aviv, το τίμημα της προστασίας δεδομένων μέσω της υιοθέτησης Γ.Κ.Π.Δ. είναι υψηλό καθώς δημιουργεί κάποιες επιβλαβείς επιπτώσεις. Μία από αυτές είναι ο περιορισμός του ανταγωνισμού στις αγορές δεδομένων, δημιουργώντας πιο συγκεντρωμένες δομές αγοράς και εδραιώνοντας την ισχύ στην αγορά όσων είναι ήδη ισχυροί. Άλλη μια σημαντική επίπτωση είναι ο περιορισμός στην ανταλλαγή δεδομένων μεταξύ διαφορετικών συλλεκτών δεδομένων, αποτρέποντας έτσι την πραγματοποίηση ορισμένων συνεργειών δεδομένων που μπορεί να οδηγήσουν σε καλύτερη γνώση που βασίζεται σε δεδομένα. Το άρθρο εστιάζει στον τρόπο με τον οποίο επηρεάζει τις επιλογές που έχουν στην διάθεσή τους οι εταιρείες για τη συγκέντρωση των απαραίτητων δεδομένων και τη συνακόλουθη ικανότητά τους να πραγματοποιούν οικονομίες κλίμακας και πεδίου στην ανάλυση δεδομένων. Προσδιορίζει επτά κύριες παράλληλες δυναμικές της αγοράς που ενδέχεται να περιορίσουν τη συλλογή δεδομένων και την κοινή χρήση δεδομένων, μόνο μερικές από τις οποίες έχουν αναγνωριστεί μέχρι στιγμής. Υπό ορισμένες συνθήκες της αγοράς, ο Γ.Κ.Π.Δ. έχει ακούσιες και μέχρι στιγμής μη αναγνωρισμένες επιπτώσεις στον

ανταγωνισμό, την αποτελεσματικότητα, την καινοτομία και την ευημερία. Από την ανάλυση που γίνεται προσδιορίζονται ποιες είναι οι βραχυπρόθεσμες επιπτώσεις και ποιες οι μακροπρόθεσμες.

Δύο σημεία αξίζει να τονιστούν. Πρώτον, ο Γ.Κ.Π.Δ. έχει επιπτώσεις πολύ πέρα από τα γεωγραφικά σύνορα της Ε.Ε. καθώς πολλές διεθνείς εταιρείες, που δραστηριοποιούνται στην Ε.Ε. ή συναλλάσσονται μαζί της, πρέπει να συμμορφώνονται με τους κανόνες της. Μόλις αυτές οι εταιρείες υιοθετήσουν τους εσωτερικούς μηχανισμούς που είναι απαραίτητοι για τη συμμόρφωση με τον κανονισμό, μπορούν να χρησιμοποιηθούν και για δεδομένα εκτός Ε.Ε.. Δεύτερον, οι περισσότερες από τις επιπτώσεις που αναλύονται σε αυτό το άρθρο είναι μακροπρόθεσμες, οι οποίες δεν θα εξαφανιστούν μόλις η αγορά προσαρμοστεί στην ύπαρξη του Γ.Κ.Π.Δ.. Επομένως, αξίζει να επανεκτιμηθούν οι συνολικές επιπτώσεις στην ευημερία του νομικού καθεστώτος δεδομένων που επιλέχθηκε.

Το άρθρο προτείνει ορισμένα μέσα για τη μείωση των επιβλαβών επιπτώσεων στον ανταγωνισμό, ενώ παράλληλα προσπαθεί να προστατεύσει τον ζωτικό στόχο της ιδιωτικής ζωής. Αρχικά, όταν η αβεβαιότητα σχετικά με τον τρόπο εκπλήρωσης των νομικών υποχρεώσεων του Γ.Κ.Π.Δ. συμβάλλει στη συγκέντρωση, μπορεί να είναι χρήσιμο να εξεταστούν τρόποι περιορισμού αυτής της αβεβαιότητας. Η ανάπτυξη τεχνολογικών προτύπων για τη φορητότητα και τη διαλειτουργικότητα δεδομένων μπορεί να συμβάλει στη μείωση της επακόλουθης αβεβαιότητας ως προς το ποια πρότυπα θα μπορούσαν τελικά να εφαρμοστούν και να διατηρούν μεγαλύτερη αξία από τα δεδομένα που συλλέγονται. Ακόμα, θα μπορούσε να δοθεί προτεραιότητα στην ανάπτυξη καλύτερων και ταχύτερων εργαλείων για την επαλήθευση της συμμόρφωσης με τον κανονισμό. Τέλος, η πιστοποίηση των διαδικασιών διαχείρισης δεδομένων και ελέγχου θα μπορούσε να συμβάλλει σημαντικά στη μείωση του κόστους και η κυβέρνηση θα μπορούσε να έχει καθοριστικό ρόλο είτε πιστοποιώντας τέτοια εργαλεία είτε βοηθώντας στη διευκόλυνση αυτής της πιστοποίησης.

Μέσα από αυτό το άρθρο, οι αρθρογράφοι ελπίζουν να αναγνωριστούν τέτοιες επιπτώσεις που θα οδηγήσουν στην επανεκτίμηση της ισορροπίας μεταξύ του απορρήτου και της ευημερίας. Ενώ η μέτρηση των βλαβών στην ιδιωτική ζωή και η σύγκρισή τους με τις επιπτώσεις στον ανταγωνισμού και στην καινοτομία είναι μια εξαιρετικά δύσκολη εργασία, οι λύσεις που προτείνονται σε αυτό το άρθρο αποφεύγουν την ανάγκη για μια τόσο προσεκτική εξισορρόπηση, παρόλο που η προστασία δεδομένων παραμένει ένας ουσιαστικός παράγοντας για την ευημερία.

2.4: Πιστοποίηση ISO 27001

2.4.1: Η συμβολή του ISO 27001 στην συμμόρφωση στον Γ.Κ.Π.Δ..

Ο Γ.Κ.Π.Δ. αλλάζει θεμελιωδώς τον τρόπο με τον οποίο χειρίζονται τα δεδομένα σε κάθε τομέα της επιχείρησης και η εφαρμογή του δεν χαρακτηρίζεται εύκολη από πολλούς συγγραφείς.

Το άρθρο « How ISO 27001 can help achieve GDPR compliance» των Isabel Maria Lopes, Teresa Guarda και Pedro Oliveira εστιάζει στο ερώτημα: «Κατά πόσο η εφαρμογή των προτύπων ISO 27001 μπορεί να αντιπροσωπεύει έναν παράγοντα διευκόλυνσης για τους οργανισμούς κατά την συμμόρφωσή τους με τον Γ.Κ.Π.Δ.». Για να δοθεί απάντηση σε αυτό έχουν αναλυθεί αρκετοί ιστότοποι.

Στο συμπέρασμα που καταλήγει είναι ότι αν και το Γ.Κ.Π.Δ. είναι αναγκαίος πρέπει να τονιστούν τα οφέλη των επιχειρήσεων και το κέρδος που θα έχουν από την εφαρμογή τους. Αν δεν γίνει αυτό τότε θα θεωρηθεί απλά άλλος ένας περιορισμός στο λειτουργικό περιβάλλον και όχι ένα ανταγωνιστικό πλεονέκτημα για την επιχείρηση.

Ο Γ.Κ.Π.Δ. δημιουργεί στρατηγικό πλεονέκτημα στην εταιρεία που τον υιοθετεί και ένας τρόπος για να αποδείξει ότι πιστοποιεί τις προϋποθέσεις του είναι το ISO 27001. Όσες εταιρείες αναλύθηκαν και είχαν ήδη ISO 27001 έδειξαν ότι βρίσκονταν σε εξαιρετική θέση συμμόρφωσης στις νέες απαιτήσεις του Γ.Κ.Π.Δ. καθώς τις βοηθάει να ανταποκρίνονται συνεχώς στις νέες αυτές απαιτήσεις.

2.4.2: εφαρμογή του Γ.Κ.Π.Δ. μέσω της χρήσης των προτύπων ISO

Σύμφωνα με το άρθρο « One Model For Implementation GDPR Based On ISO Standards» του Tzanko Tzolov, θα έπρεπε να δοθεί έμφαση στα οφέλη της εφαρμογής του Γ.Κ.Π.Δ. και στην προστιθέμενη αξία που προσφέρει στην επιχείρηση. Έτσι, τα μοντέλα υλοποίησης επικεντρώνονται στη σκέψη που βασίζεται στον κίνδυνο, λαμβάνοντας υπόψη τις τεχνολογικές καινοτομίες, τους περιβαλλοντικούς παράγοντες, τη διαχείριση πληροφοριών, τη διαχείριση της εφοδιαστικής αλυσίδας και την παγκοσμιοποίηση.

Οι βασικές απαιτήσεις για το μοντέλο είναι η περιγραφή διαδικασιών, ο καθορισμός στόχων, η παρακολούθηση βασικών δεικτών απόδοσης, ο καθορισμός ρόλων και η δημιουργία συνεπών μοντέλων δεδομένων. Οι απαιτήσεις του Γ.Κ.Π.Δ. έχουν οριστεί ως πολιτικές και διαδικασίες που πρέπει να ενσωματωθούν στις επιχειρηματικές διαδικασίες και στους ρόλους των εργαζομένων μέσα στις επιχειρήσεις.

Το ISO 9001:2015 βασίζεται στη διαδικασία προσέγγισης και διαχείρισης κινδύνων, και το οποίο στηρίζει επίσης τον κανονισμό. Η προσέγγιση διαδικασίας που εισήχθη στην αναθεώρηση του προτύπου το 2015 απαιτεί από τους οργανισμούς να διαχειρίζονται τις διαδικασίες τους προκειμένου να επιτύχουν προγραμματισμένα αποτελέσματα σύμφωνα με τους στρατηγικούς στόχους του οργανισμού. Απαιτεί από τους οργανισμούς να αναγνωρίζουν, να καταγράφουν, να εφαρμόζουν, να διατηρούν και να βελτιώνουν συνεχώς τις διαδικασίες και τις αλληλεπιδράσεις τους.

Η κοινή χρήση του Γ.Κ.Π.Δ. και της οικογένειας προτύπων ISO είναι ένας ισχυρός μηχανισμός για την εφαρμογή του Κανονισμού εντός του οργανισμού. Τα πρότυπα μπορούν να χρησιμοποιηθούν στο στάδιο της εφαρμογής ως μεθοδολογία (ISO 9001: 2015), ως μηχανισμοί για την ολοκλήρωση διαφορετικών σταδίων (ISO 31000) ή ως απόδειξη συμμόρφωσης με τον Κανονισμό (ISO 27000 (27001, 27017, 27018)).

2.4.3: ISO 27001: έλεγχοι προστασίας προσωπικών δεδομένων με βάση τον Γ.Κ.Π.Δ.

Το έγγραφο «From ISO/IEC27001:2013 and ISO/IEC27002:2013 to GDPR compliance controls» της Vasiliki Diamantopoulou, Aggeliki Tsohou και της Maria Karyda έχει ως σκοπό να χρησιμοποιείται από τις εταιρείες, οι οποίες συμμορφώνονται με το ISO/IEC 27001:2013, ως βάση για την επέκταση των ήδη υπαρχουσών μονάδων ελέγχου ασφάλειας προς την προστασία δεδομένων και ως καθοδήγηση για την επίτευξη συμμόρφωσης με τον κανονισμό. Για αυτό τον λόγο υποδεικνύει ενέργειες διαχείρισης ασφάλειας που πρέπει να εκτελέσει ένας οργανισμός για να εκπληρώσει τις απαιτήσεις του Γ.Κ.Π.Δ..

Ο Γ.Κ.Π.Δ. προβλέπει πολυάριθμες ρυθμίσεις ελέγχου για την διασφάλιση των προσωπικών δεδομένων. Πολλοί από αυτούς του ελέγχους προβλέπονται και από τον ISO/IEC 27001. Έτσι, οι οργανισμοί που έχουν αναπτύξει ήδη ένα Σ.Δ.Α.Π. είναι πιθανό να ικανοποιούν ήδη πολλές από τις απαιτήσεις του κανονισμού.

Αυτή η μελέτη, αρχικά, εντόπισε τις ομοιότητες μεταξύ του ISO/IEC 27001:2013 και των απαιτήσεων του Γ.Κ.Π.Δ.. Αυτό το κατάφερε μέσα από την ανάλυση των δεκατεσσάρων ενοτήτων ελέγχου του ISO/IEC 27001:2013 και προτείνοντας τις κατάλληλες ενέργειες για την ικανοποίηση των απαιτήσεων προστασίας δεδομένων. Στην συνέχεια, αυτό το έγγραφο προσδιόρισε απαιτήσεις του Γ.Κ.Π.Δ. που δεν καλύπτονται από το ISO/IEC 27001:2013.

Το έγγραφο αποτελεί έναν οδηγό με κατευθυντήριες γραμμές για τους επαγγελματίες του τομέα της ασφάλειας πληροφοριών και της προστασίας της ιδιωτικής ζωής και για την συμμόρφωση με τον κανονισμό. Ως μελλοντική προοπτική του εγγράφου αυτού αναφέρθηκε η απόδειξη της εφαρμογής των προτεινόμενων κατευθυντήριων γραμμών για τη συμμόρφωση με τον κανονισμό μέσω της έρευνας πάνω σε έναν αριθμό πιστοποιημένων κατά ISO 27001 οργανισμών που έχουν συμμορφωθεί στον Γ.Κ.Π.Δ..

2.4.4: ISO 27001: Ανάλυση χασμάτων

Η μελέτη «ISO 27001 Gap Analysis - Case Study» του Ibrahim Al-Mayahi, Sa'ad P. Mansoor περιγράφει τα αρχικά βήματα που έγιναν προς την ανάπτυξη ενός Σ.Δ.Α.Π. για την ηλεκτρονική διακυβέρνηση των Η.Α.Ε.. Για την επίτευξη αυτού του στόχου αποκτήθηκε η πιστοποίηση ISO 27001, του κορυφαίου πρότυπου στην ασφάλεια των πληροφοριών, σε τέσσερις επιλεγμένους οργανισμούς ηλεκτρονικής διακυβέρνησης. Η συγκεκριμένη διαδικασία βοήθησε στον εντοπισμό των αδυναμιών στο υπάρχον σύστημα και να στην ανάδειξη των κινδύνων για την ηλεκτρονική διακυβέρνηση των Η.Α.Ε.. Παρέχει, επίσης, ένα πλαίσιο που είναι πιο ευθυγραμμισμένο με τη δομή και τις ευθύνες του οργανισμού, παρουσιάζοντας τα αποτελέσματα της συγκριτικής αξιολόγησης βάσει του προτύπου ISO27001.

Κατά την ανάλυση βρέθηκαν στοιχεία που έδειξαν ότι ορισμένοι από τους ελέγχους είναι πιο ώριμοι από άλλους. Ένας από τους έντεκα ελέγχους δείχνει 100% μη ωριμότητα και αυτό οφείλεται στην ανυπαρξία εγκεκριμένης πολιτικής ασφαλείας. Άλλοι δύο παρουσιάζουν υψηλό ποσοστό μη συμμόρφωσης και για άλλη μια φορά αυτό οφείλεται στην έλλειψη εφαρμογής αποτελεσματικής πολιτικής ασφάλειας στους συγκεκριμένους ελέγχους. Οι υπόλοιποι έλεγχοι φαίνεται να έχουν υψηλό ποσοστό συμμόρφωσης και αυτό οφείλεται στη διαδικασία εσωτερικής ασφάλειας που εφαρμόζεται από την ομάδα που είναι υπεύθυνη για το εκάστοτε τμήμα. Τέλος, αναφέρεται πως το 56,4% των ελέγχων που εξετάστηκαν διαπίστωσαν ότι συμμορφώνονται με τα πρότυπα ISO 27001, το 18,8% των ελέγχων που εξετάστηκαν διαπιστώθηκε ότι συμμορφώνονται εν μέρει με τα πρότυπα ISO 27001 και το 24,8% των ελέγχων που εξετάστηκαν διαπίστωσαν ότι δεν συμμορφώνονται με τα πρότυπα ISO 27001. Από τα αποτελέσματα φαίνεται ότι υπάρχει μεγάλος αριθμός ελέγχων που πληρούν το απαιτούμενο πρότυπο και λαμβάνοντας υπόψη ότι αυτό είναι η πρώτη προσπάθεια δοκιμής της συμμόρφωσης του οργανισμού, είναι αρκετά ενθαρρυντικό το αποτέλεσμα.

Ένα σύστημα διαχείρισης ασφάλειας πληροφοριών είναι αναπόσπαστο μέρος της διαχείρισης ενός οργανισμού, το οποίο απαιτείται να παρακολουθεί, να επανεξετάζει και να βελτιώνει την ασφάλεια πληροφοριών του οργανισμού. Είναι μια συνεχής διαδικασία που ασχολείται με την ανάπτυξη πολιτικών ασφάλειας και εφαρμόζει διαδικασίες για την αντιμετώπιση απειλών κατά της ασφάλειας. Η ανάλυση χασμάτων χρησιμοποιείται αρχικά για τον εντοπισμό των αδυναμιών στις διαδικασίες του οργανισμού.

Σαν συμπέρασμα, αυτή η έρευνα, τονίζει ότι η ανίχνευση χασμάτων θα πρέπει να είναι μια συνεχής διαδικασία, καθώς ο οργανισμός πρέπει να επανεξετάζει τις

υπάρχουσες δομές για να ενημερώνει την ανάλυση των χασμάτων. Αυτό πραγματοποιείται για να εξασφαλιστεί μακροπρόθεσμη προστασία έναντι των παραβιάσεων ασφάλειας.

2.5: Ο Γ.Κ.Π.Δ. και η πληροφορική

2.5.1: Η επιρροή του Γ.Κ.Π.Δ. στα cookies

Σύμφωνα με τον Γ.Κ.Π.Δ., απαιτείται, κατά την λήψη πληροφοριών στο διαδίκτυο οι οποίες θα μπορούσαν να χρησιμοποιηθούν για ταυτοποίηση ατόμων, η συγκατάθεσή τους.

Μεταξύ άλλων, αυτό επηρεάζει πολλές κοινές μορφές cookies. Το άρθρο «Characterising Third Party Cookie Usage in the EU after GDPR » των Xuehui Hu και Nishanth Sastry εξετάζει την επικράτηση των cookies τρίτων πριν και μετά τον Γ.Κ.Π.Δ. χρησιμοποιώντας δύο σύνολα δεδομένων: προσβάσεις στους 500 κορυφαίους ιστότοπους σύμφωνα με την Alexa.com και εβδομαδιαία δεδομένα cookies που τοποθετούνται στα προγράμματα περιήγησης των χρηστών από ιστότοπους στους οποίους έχουν πρόσβαση 16 χρήστες από το Η.Β. και την Κίνα σε ένα έτος. Διαπιστώθηκε ότι κατά μέσο όρο ο αριθμός των τρίτων μειώθηκε κατά περισσότερο από 10% μετά τον κανονισμό. Όταν εξετάσθηκαν τα ιστορικά περιήγησης των χρηστών σε διάστημα ενός έτους, διαπιστώθηκε ότι δεν υπήρχε σημαντική μείωση στον μακροπρόθεσμο αριθμό των cookies τρίτων, υποδηλώνοντας ότι οι χρήστες δεν κάνουν χρήση των επιλογών που προσφέρει ο Γ.Κ.Π.Δ. για αυξημένο απόρρητο. Οι ιστότοποι που προσφέρουν στους χρήστες τη δυνατότητα επιλογής για το αν επιθυμούν και τον τρόπο παρακολούθησης τους συνήθως καταλήγει στην αποθήκευση περισσότερων cookies κατά μέσο όρο από ό,τι σε ιστότοπους που παρέχουν ειδοποίηση για αποθηκευμένα cookies.

Διαπιστώθηκε ότι οι κορυφαίοι ιστότοποι εκτός Ε.Ε. έχουν λιγότερες ειδοποιήσεις για cookies, γεγονός που υποδηλώνει υψηλότερα επίπεδα παρακολούθησης όταν επισκέπτονται διεθνείς ιστότοπους. Οι ιστότοποι που εδρεύουν στο Η.Β. συμμορφώνονται γενικά στον Γ.Κ.Π.Δ., παρέχουν δηλαδή κάποια μορφή ειδοποίησης cookies.

Οι ακριβείς επιλογές δεν είναι απαραίτητα το «καλύτερο» για τους χρήστες: Πρώτον, οι ιστότοποι του Η.Β. παρουσιάζουν στους χρήστες μια επιλογή που μπορούσε να ήταν λανθασμένη εάν γινόταν αποδεκτή η προεπιλεγμένη επιλογή, καθώς οδηγούσε σε μεγαλύτερο αριθμό cookies τρίτων, από ό,τι πριν. Δεύτερον, αφού μελετήθηκαν οι αριθμοί των cookies τρίτων στα ιστορικά περιήγησης χρηστών, διαπιστώθηκε ότι ο Γ.Κ.Π.Δ. είχε μικρή μακροπρόθεσμη επίδραση στον αριθμό των cookies. Η διαδικασία που απαιτείται από τους χρήστες για να επιλέξουν τις προτιμήσεις απορρήτου τους σε κάθε ιστότοπο που επισκέπτονται ενέχει την πιθανότητα να τους κουράζει με αποτέλεσμα να καταλήγουν να αποδέχονται τις προεπιλεγμένες επιλογές που προσφέρονται από τους ιστότοπους χωρίς να τις ελέγχουν πρώτα.

2.5.2: Μείωση των cookies μετά την εφαρμογή του Γ.Κ.Π.Δ.

Η μελέτη «Changes in Third-Party Content on European News Websites after GDPR» των Timothy Libert, Lucas Graves και Rasmus Kleis Nielsen βασίστηκε σε μια προηγούμενη έρευνα με ονομασία «Περιεχόμενο Ιστού τρίτων σε ιστότοπους ειδήσεων Ε.Ε.: πιθανές προκλήσεις και μονοπάτια για τη βελτίωση του απορρήτου». Τα ευρήματα της έρευνας που βασίστηκε η συγκεκριμένη μελέτη αποκάλυψαν ότι οι

ειδησεογραφικοί ιστότοποι τείνουν να έχουν υψηλότερο όγκο περιεχομένου και cookies τρίτων από άλλους δημοφιλείς ιστότοπους τρίτων που θα μπορούσαν να προκαλέσουν πιθανά προβλήματα με τη συμμόρφωση με τον Γ.Κ.Π.Δ. και γενικότερα να εγείρουν ανησυχίες σχετικά με το απόρρητο. Προτάθηκε η μετεγκατάσταση κάποιου περιεχομένου τρίτων για να λειτουργεί σε βάση πρώτου μέρους για να αντιμετωπίσουν λιγότερες προκλήσεις βάση του Γ.Κ.Π.Δ..

Σε αυτή την μελέτη επιλέχθηκαν επτά μέλη κράτη της Ε.Ε.. Σε κάθε χώρα, συμπεριλήφθη μια επιλογή από ειδησεογραφικούς ιστότοπους, που επιλέχθηκαν με βάση προηγούμενη εργασία που μετρούσε την εμβέλεια και τη σημασία τους. Συγκρίθηκε το περιεχόμενο και τα third-part cookies πριν από τον Γ.Κ.Π.Δ. (Απρίλιος) και μετά από αυτόν (Ιούλιος). Διαπιστώθηκε πως είχαν πραγματοποιηθεί πολλές αλλαγές κατά τη διάρκεια αυτής της χρονικής περιόδου. Πιο συγκεκριμένα, ο συνολικός αριθμός των cookies τρίτων σε ειδησεογραφικούς ιστότοπους μειώθηκε κατά 22%. Αυτό αποκάλυψε πως ορισμένοι ειδησεογραφικοί οργανισμοί ανταποκρίνονταν στον κανονισμό είτε με τη λήψη συναίνεσης για παρακολούθηση τρίτων ή με περιορισμό της χρήσης εξωτερικών cookies γενικά. Εν ολίγοις, διαπιστώθηκε ότι η εισαγωγή του κανονισμού ακολουθήθηκε από σημαντικές μειώσεις στον όγκο των third-part cookies.

2.5.3: Συνέπειες απορρήτου του Γ.Κ.Π.Δ. για το IoT

Οι Daniel Bastos, Fabio Giubilo, Mark Shackleton και Fabi El-Mousa με το άρθρο τους «GDPR Privacy Implications for the Internet of Things» επικεντρώθηκαν στις συνέπειες του Γ.Κ.Π.Δ. στο IoT. Την εποχή που στο διαδίκτυο, το έτος 2018, ήταν συνδεδεμένοι 3,58 δισεκατομμύρια χρήστες, με μόλις 1,36 δισεκατομμύρια 10 χρόνια πριν, με τον καθένα να διαθέτει την δική του ηλεκτρονική ταυτότητα καταλαβαίνουμε ότι υπάρχει μια σημαντική αύξηση στην συνδεσιμότητα. Με την χρήση του IoT γίνεται η επικοινωνία των χρηστών μέσω της χρήση του IP τους. Στο IoT υπάρχουν πολλές πληροφορίες σχετικά με την ζωή των ανθρώπων, που επεξεργάζονται από τα συστήματα αυτά και μπορούν να οδηγηθούν σε πολύ ευαίσθητες πληροφορίες καθώς ο σκοπός τους είναι να παίρνουν αποφάσεις χωρίς την ανάγκη της ανθρώπινης παρέμβασης με παράγοντα πάντα το εξωτερικό περιβάλλον. Εύλογο συμπέρασμα είναι ότι χρειάζεται κάποια προστασία στα συστήματα IoT καθώς ανάλογα με την παραβίαση προσωπικών δεδομένων που θα προβεί το σύστημα θα υπάρχει και το αντίστοιχο αντίκτυπο στην ζωή του ανθρώπου με επόμενο αυτό του οικονομικού κόστους. Αυτό οδηγεί στην απώλεια εμπιστοσύνης από τους χρήστες και σταδιακά επηρεάζει την εικόνα της εταιρείας (Brand) αφού εκπέμπει ένα κλίμα αναξιοπιστίας. Ο Γ.Κ.Π.Δ. τέθηκε σε λειτουργία το 2018 για να προστατεύσει τους χρήστες αλλά και τα προγράμματα από αυτά τα περιστατικά καθώς όλες οι εταιρείες που επεξεργάζονται δεδομένα πρέπει να συμμορφώνονται σε αυτόν.

Ως μία πολύ σημαντική πρόκληση του Γ.Κ.Π.Δ. προς τους παρόχους των IoT αναφέρει, το άρθρο, ότι είναι η έλλειψη της καθιερωμένης στρατηγικής για την ασφάλεια, διαχείριση και ενημέρωση των συσκευών IoT. Το δημοσίευμα αυτό έχει εστιάσει στις ανησυχίες και τις απαιτήσεις απορρήτου που δημιουργούνται από τον Γ.Κ.Π.Δ. για τις υπηρεσίες IoT αλλά και έχουν περιγραφεί σε αυτό κάποιες πιθανές κατευθύνσεις για να αντιμετωπιστούν αυτές οι ανησυχίες στο μέλλον. Η σημαντικότητα της έρευνας αυτής, αλλά και παρόμοιων με αυτήν, είναι μεγάλη καθώς οι τεχνικές απορρήτου θα διαδραματίσουν σημαντικό ρόλο στο μέλλον των IoT που θα οδηγήσουν στην υιοθέτησή τους.

2.5.4: Η δυσκολία υιοθέτησης του Γ.Κ.Π.Δ. από τους προγραμματιστές

Οι προγραμματιστές λογισμικού δυσκολεύονται να ενσωματώσουν το απόρρητο που αναφέρεται στον Γ.Κ.Π.Δ. στις εφαρμογές λογισμικού που αναπτύσσουν. Αυτό μπορεί να τους οδηγήσει στην ανάπτυξη εφαρμογών λογισμικού που πραγματοποιούν παραβιάσεις απορρήτου.

Στο έγγραφο «Why are Developers Struggling to Put GDPR into Practice when Developing Privacy-Preserving Software Systems?» των Abdulrahman Alhazmi και Nalin Asanka Gamagedara Arachchilage έγινε μελέτη που διερεύνησε γιατί οι προγραμματιστές δεν μπορούν να ενσωματώσουν το απόρρητο, σύμφωνα με τον Γ.Κ.Π.Δ., σε εφαρμογές λογισμικού. Ως πρώτο βήμα, πραγματοποιήθηκε μια μελέτη συνέντευξης σε προγραμματιστές σχετικά με τις προκλήσεις που αντιμετωπίζουν κατά την ενσωμάτωση του απορρήτου σε εφαρμογές λογισμικού, λαμβάνοντας υπόψη τις αρχές του Γ.Κ.Π.Δ..

Κατά την έρευνα αυτή, δόθηκαν στους συμμετέχοντες το σενάριο και τα διαγράμματα UML του σεναρίου, τα οποία αναπτύχθηκαν αντανακλώντας τις αρχές του κανονισμού. Στην συνέχεια συλλέχθηκαν και αναλύθηκαν οι περιγραφικές απαντήσεις των ερωτηθέντων. Τα ευρήματα της μελέτης αποκάλυψαν πως υπήρχε έλλειψη καλών τεχνικών για την εφαρμογή των αρχών του κανονισμού και πως οι προγραμματιστές δεν ήταν εξοικειωμένοι με τον νόμο και δεν διέθεταν κατάλληλες οδηγίες για την εφαρμογή του.

Ως τρόπους διευκόλυνσης για την εφαρμογή του κανονισμού από τους προγραμματιστές προτείνει τους ακόλουθους:

- Το καθολικό πρότυπο του Γ.Κ.Π.Δ. θα πρέπει να είναι διαθέσιμο, ώστε οι δημιουργοί λογισμικού να μπορούν να το ακολουθούν διατηρώντας τη συνέπεια.
- Ο Γ.Κ.Π.Δ. θα πρέπει να συνοδεύεται από κατευθυντήριες τεχνικές για κάθε αρχή, ώστε να διασφαλίζεται η αποτελεσματική εφαρμογή των αρχών και να αποτρέπεται η χρήση υποτυπωδών τεχνικών από τους προγραμματιστές.
- Οι προγραμματιστές θα πρέπει να έχουν γνώση του Γ.Κ.Π.Δ., των διαδικασιών και των τεχνικών για την εφαρμογή του κατά την ανάπτυξη συστημάτων λογισμικού που διατηρούν το απόρρητο.

2.5.5: Παιχνίδι ως μέσο εκμάθησης του Γ.Κ.Π.Δ. για τους προγραμματιστές

Οι τεχνολογίες και το διαδίκτυο είχαν και έχουν ραγδαία ανάπτυξη κατά την τελευταία δεκαετία. Αυτό είχε οδηγήσει στην αύξηση των παραβιάσεων των δεδομένων και την αναγκαιότητα της υιοθέτησης του Γ.Κ.Π.Δ..

Σύμφωνα με το άρθρο «A Serious Game Design Framework for Software Developers to Put GDPR» των Abdulrahman Alhazmi και Nalin A G Arachchilage, οι προγραμματιστές λογισμικού απέτυχαν να εφαρμόσουν το απόρρητο σε συστήματα λογισμικού σύμφωνα με τις κατευθυντήριες γραμμές του Γ.Κ.Π.Δ.. Ο λόγος που είχε συμβεί αυτό ήταν ότι οι οδηγίες είχαν αναπτυχθεί με γνώμονα τους δικηγόρους και όχι τους προγραμματιστές λογισμικού με αποτέλεσμα οι προγραμματιστές να μην μπορούν να τους εφαρμόσουν. Έτσι, μέσα από το άρθρο αυτό προτάθηκε ένα πλαίσιο σχεδίασης παιχνιδιών για να διδαχθούν οι προγραμματιστές λογισμικού την εφαρμογή του Γ.Κ.Π.Δ. στα συστήματα λογισμικού.

Ο μηχανισμός των πλαισίων κατέγραφε τον τρόπο με τον οποίο οι παίκτες, δηλαδή οι προγραμματιστές, αντιλαμβάνονταν τις απειλές για το απόρρητο των δεδομένων. Όσο περισσότερο κατανοούσε ένας προγραμματιστής τις απειλές δεδομένων που υπήρχαν, τόσο μεγαλύτερη ήταν η πιθανότητα ενσωμάτωσης του απορρήτου. Ο στόχος του παίκτη του παιχνιδιού ήταν να αντιμετωπίσει τα προβλήματα που προκάλεσαν παραβιάσεις δεδομένων αναδεικνύοντας την αξία της χρήσης των αρχών του Γ.Κ.Π.Δ. κατά την ανάπτυξη λογισμικού που θα προστάτευε το απόρρητο. Τα βήματα ταξινόμησης του Bloom χρησιμοποιήθηκαν για την παρουσίαση του διδακτικού περιεχομένου στον παίκτη του παιχνιδιού ως διαδραστικό μέσο.

Ως μελλοντική συνέχεια του άρθρου αυτού θα αποτελούσαν οι εμπειρικές μελέτες για την διερεύνηση για το πόσο το πλαίσιο επηρεάζει τη συμπεριφορά των προγραμματιστών κατά την κατασκευή λογισμικού ως προς το απόρρητο.

2.5.6: Εφαρμογή του Γ.Κ.Π.Δ. από τους προγραμματιστές

Υπάρχουν πολλές διαθέσιμες έρευνες στο διαδίκτυο που εντοπίζουν τα εμπόδια που αντιμετωπίζουν οι προγραμματιστές κατά την ενσωμάτωση των πρωτοκόλλων απορρήτου σε εφαρμογές λογισμικού, αλλά δεν υπάρχουν πολλές έρευνες που διαπιστώνουν γιατί οι προγραμματιστές δεν είναι σε θέση να αναπτύξουν συστήματα που διαφυλάσσουν το απόρρητο, λαμβάνοντας υπόψη τις αρχές του Γ.Κ.Π.Δ.. Η συγκεκριμένη έρευνα έχει ως σκοπό να εξετάσει τα ζητήματα που εμποδίζουν τους προγραμματιστές να δημιουργήσουν εφαρμογές που συμμορφώνονται στον κανονισμό.

Η έρευνα «I'm all ears! Listening to software developers on putting GDPR principles into software development practice» των Abdulrahman Alhazmi και Nalin Asanka Gamagedara Arachchilage περιελάμβανε προγραμματιστές από όλο τον κόσμο που είχαν διαφορετικά χρόνια εμπειρίας (αρχάριοι και έμπειροι). Οι αρχάριοι προγραμματιστές αποδείχτηκε πως ανέπτυξαν εν αγνοία τους ώριμες εφαρμογές με τρωτά σημεία ασφαλείας που έθεταν σε κίνδυνο την ακεραιότητα της εφαρμογής. Ούτε ένας αρχάριος ούτε ένας έμπειρος προγραμματιστής ήξερε απαραίτητα πώς γράφεται ο κώδικας με ασφάλεια. Η υποχρέωση κάθε συμμετέχοντα σε αυτή την έρευνα ήταν να πραγματοποιήσει ο ίδιος και τον σχεδιασμό και την υλοποίηση του λογισμικού.

Αυτή η έρευνα ακολούθησε μια ποιοτική ερευνητική προσέγγιση, η οποία βοήθησε στη σαφή κατανόηση των ζητημάτων που αντιμετώπιζαν οι προγραμματιστές. Για τον εντοπισμό των ζητημάτων αυτών, συλλέχθηκαν και αργότερα αναλύθηκαν τα ποιοτικά δεδομένα που συγκεντρώθηκαν από τους προγραμματιστές. Από αυτά τα δεδομένα βγήκαν τα ακόλουθα συμπεράσματα:

- Οι συμμετέχοντες δεν είχαν καλές τεχνικές για να εφαρμόσουν τις αρχές του Γ.Κ.Π.Δ.. Πιο συγκεκριμένα, πολλοί δεν ήξεραν καν πως να εφαρμόσουν τις αρχές του Γ.Κ.Π.Δ. και άλλοι δεν μπορούσαν να διαφοροποιήσουν τις τεχνικές για τις αρχές του Γ.Κ.Π.Δ.. Παρατηρήθηκε ότι υπήρχαν αρχές, ο Περιορισμός του Σκοπού και η Νομιμότητα, η Δικαιοσύνη και η Διαφάνεια, που έφεραν σύγχυση στους συμμετέχοντες.
- Οι συμμετέχοντες δεν ήταν εξοικειωμένοι με τις αρχές του Γ.Κ.Π.Δ.. Κάποιοι από τους προγραμματιστές δεν είχαν ιδέα για τον κανονισμό, άλλοι γνώριζαν διαφορετικούς νόμους περί απορρήτου δεδομένων (σύμφωνα με την χώρα που ήταν) και άλλοι ήταν εξοικειωμένοι με τον κανονισμό αλλά εξακολουθούσαν να αντιμετωπίζουν δυσκολίες στην εφαρμογή ορισμένων αρχών του. Η μελέτη αυτή διαπίστωσε πως αυτό ήταν το κύριο πρόβλημα, καθώς οι άνθρωποι δεν μπορούν να εφαρμόσουν έννοιες ή αρχές με τις οποίες δεν είναι εξοικειωμένοι.

- Οι συμμετέχοντες ανησυχούσαν περισσότερο για τις λειτουργικές απαιτήσεις. Οι περισσότεροι προγραμματιστές ισχυρίστηκαν πως η εφαρμογή του απορρήτου των δεδομένων λογισμικού δεν είναι ο ρόλος τους καθώς υπάρχουν ειδικές ομάδες για τον σκοπό αυτό.
- Οι συμμετέχοντες δεν είχαν πόρους και διαδικτυακό υλικό για αναφορά και καθοδήγηση κατά την εφαρμογή του απορρήτου των δεδομένων. Αυτό το ζήτημα εντοπίστηκε σε όλες σχεδόν τις αρχές του Γ.Κ.Π.Δ.. Αυτό το ζήτημα οδηγεί τους προγραμματιστές να χρησιμοποιούν τεχνικές, οι οποίες είναι ξεπερασμένες, επομένως δεν εφαρμόζουν αποτελεσματικά το απόρρητο δεδομένων
- Η εφαρμογή του απορρήτου εξαρτάται επίσης από τον πελάτη. Η έρευνα αποκάλυψε ότι οι οργανισμοί διαδραματίζουν κρίσιμο ρόλο στη διασφάλιση ότι οι προγραμματιστές εφαρμόζουν αποτελεσματικά όλες τις αρχές του Γ.Κ.Π.Δ..

2.5.7: Οι προγραμματιστές στην προσπάθεια ελαχιστοποίησης δεδομένων

Η ελαχιστοποίηση δεδομένων αποτελεί μια πρακτική απορρήτου ελαχιστοποίησης της χρήσης των δεδομένων των χρηστών στα λογισμικά των εταιρειών. Το άρθρο τονίζει το πόσο σημαντικό είναι να γίνει αντιληπτό και κατανοητό το προβλήματα που αντιμετωπίζουν οι προγραμματιστές λογισμικού όταν προσπαθούν να εφαρμόσουν την ελαχιστοποίηση των δεδομένων σε συστήματα λογισμικού. Για να αναδειχτεί αυτό το πρόβλημα, έγινε μελέτη για το πως είκοσι τέσσερεις (24) προγραμματιστές λογισμικού εφαρμόζουν την ελαχιστοποίηση δεδομένων σε ένα σχεδιασμό συστήματος λογισμικού όταν τους ζητηθεί.

Κατά την έρευνα «Understanding Software Developers' Approach towards Implementing Data Minimization» των Awanthika Senarath και Nalin Asanka Gamagedara Arachchilage δόθηκε σε όλους τους προγραμματιστές το ίδιο σενάριο δημιουργίας μιας διαδικτυακής εφαρμογής υγειονομικής περίθαλψης που επιτρέπει την εξ αποστάσεως συμβουλευτική με επαγγελματίες ιατρούς και την πληρωμή. Ο κάθε συμμετέχοντας αφιέρωσε δυόμισι ώρες στον σχεδιασμό της υλοποίησης και στην συνέχεια αυτός εγκρίθηκε από την επιτροπή δεοντολογίας του Πανεπιστημίου της Νέας Νότιας Ουαλίας. Κατά τον σχεδιασμό, την υλοποίηση και έπειτα από την ολοκλήρωση στους προγραμματιστές τέθηκαν διάφορες ερωτήσεις. Μέσα από τις απαντήσεις που έδωσαν, οι ερευνητές στόχευαν να παρατηρήσουν πώς ένας προγραμματιστής θα ασκούσε την ελαχιστοποίηση των δεδομένων σε ένα σχεδιασμό συστήματος και τα προβλήματα που είχε κατά την εφαρμογή του.

Τα αποτελέσματα της έρευνας αυτής έδειξαν ότι οι προγραμματιστές δυσκολεύονταν να το εφαρμόσουν όταν δεν γνώριζαν τις δυνατότητες των δεδομένων που θα μπορούσαν να συλλέξουν στη φάση του σχεδιασμού των συστημάτων. Είκοσι (20) από τους είκοσι τέσσερεις (24) προγραμματιστές υποστήριξαν ότι εφάρμοσαν την ελαχιστοποίηση των δεδομένων. Οκτώ (8) από τους είκοσι (20) είπαν ότι δεν ήξεραν αν θα ήταν αποτελεσματική η ελαχιστοποίηση δεδομένων ή εάν εφαρμόστηκε σωστά. Οι περισσότεροι από αυτούς που την εφάρμοσαν εστίασαν στην ελαχιστοποίηση της αποθήκευσης δεδομένων αντί στην ελαχιστοποίηση της συλλογής ή της κοινής χρήσης δεδομένων. Μόνο δύο (2) προγραμματιστές πραγματοποίησαν και τα δύο (2) προαναφερθέντα. Τέλος, οι προγραμματιστές ήταν ασυνεπείς ως προς τον τρόπο με τον οποίο εφάρμοσαν την ελαχιστοποίηση δεδομένων στα σχέδια υλοποίησης του λογισμικού τους.

Ως συμπεράσματα αυτής της έρευνας θεωρήθηκαν τα ακόλουθα:

- Οι προγραμματιστές αντιμετωπίζουν δυσκολίες στην ικανοποίηση των απαιτήσεων ελαχιστοποίησης δεδομένων όταν δεν μπορούν να προκαθορίσουν τα οφέλη που θα προσφέρει στο σύστημα.
- Οι προγραμματιστές προσπαθούν να πραγματοποιήσουν σε ολόκληρη την αλυσίδα επεξεργασίας δεδομένων εντός της εφαρμογής την ελαχιστοποίηση των δεδομένων (συλλογή, αποθήκευση και κοινή χρήση).
- Οι προγραμματιστές είναι ασυνεπείς στους τομείς στους οποίους εστιάζουν (συλλογή, αποθήκευση δεδομένων) και στις τεχνικές που χρησιμοποιούν (κρυπτογράφηση, συνάθροιση) για να εφαρμόσουν την ελαχιστοποίηση δεδομένων στα σχέδια των συστημάτων τους.

2.5.8: Ο Γ.Κ.Π.Δ. στην εποχή των Big Data

Ο Γ.Κ.Π.Δ. τέθηκε σε ισχύ σε μια κρίσιμη στιγμή για την ψηφιακή οικονομία και το οικοσύστημα. Την στιγμή στην οποία αναδύονταν σημαντικοί κίνδυνοι για τα δικαιώματα και τις ελευθερίες, ενώ ταυτόχρονα ξεδιπλώνονταν τεράστιες ευκαιρίες για τη δημιουργία αξίας, την προώθηση της ευημερίας και την ενίσχυση διαφόρων κοινωνικών στόχων. Η θέσπιση πολύπλοκων ρυθμίσεων που σχετίζονται με ένα ταχέως μεταβαλλόμενο περιβάλλον αποτελεί πάντα ένα δύσκολο έργο και το πλαίσιο προστασίας δεδομένων είναι σίγουρα ένα πλαίσιο που βρίσκεται σε συνεχή ροή και, επομένως, δεν αποτελεί εξαίρεση.

Δυστυχώς, ο Γ.Κ.Π.Δ. αποτυγχάνει να αντιμετωπίσει σωστά την αύξηση των πρακτικών των Big Data. Η θέσπιση του Γ.Κ.Π.Δ. θα μπορούσε να αλλάξει ουσιαστικά τον τρόπο διεξαγωγής της ανάλυσης Μεγάλων Δεδομένων, μεταφέροντας τον σε έναν που δεν είναι βέλτιστος και αναποτελεσματικός σταματώντας την καινοτομία στην Ευρώπη και περιορίζοντας τη χρησιμότητα στους ευρωπαίους πολίτες, ενώ δεν θα παρέχει απαραίτητα μεγαλύτερη προστασία της ιδιωτικής ζωής στους πολίτες.

Το άρθρο « Incompatible: The GDPR in the age of Big Data» του Tal Z. Zarsky καταλήγει στο συμπέρασμα ότι είναι πολύ δύσκολο να προβλεφθεί ποιο θα είναι το πραγματικό αντίκτυπο του Γ.Κ.Π.Δ. στα Big Data analytics και το αντίστροφο. Πολλοί παράγοντες, όπως η αποτελεσματικότητα της επιβολής της Ε.Ε., οι μηχανισμοί πρόστιμου και τα οφέλη που θα επιφέρουν οι τεχνολογίες Big Data, εξακολουθούν να είναι ασαφείς. Ενώ, η ισχυρή θέση της Ε.Ε., όσον αφορά την προστασία των δικαιωμάτων της ιδιωτικής ζωής, είναι αξιοθαύμαστη, είναι πιθανό ότι οι επιπτώσεις που θα έχει ο Γ.Κ.Π.Δ. στις σημαντικές πρακτικές Big Data και τα οφέλη τους να μην έχουν εξεταστεί πλήρως και σωστά και, όπως επισημάνει το άρθρο, να εξεταστούν καλύτερα στον νεότερο κανονισμό που κινείται προς τη θέσπιση και εφαρμογή.

2.5.9: Η επιρροή του Γ.Κ.Π.Δ. στα Privacy Policies

Ο Γ.Κ.Π.Δ. θεωρείται η σημαντικότερη αλλαγή στον κανονισμό απορρήτου των δεδομένων.

Στο άρθρο « The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise» των Razieh Nokhbeh Zaeem και K. Suzanne Barber υπάρχει μια ποσοτική προσέγγιση για την πρόοδο που έχει σημειώσει ο Γ.Κ.Π.Δ. στη βελτίωση των πολιτικών απορρήτου σε όλο τον κόσμο. Αυτό επιτεύχθηκε μέσω ενός εργαλείου εξαγωγής δεδομένων που χρησιμοποιήθηκε έτσι ώστε να συγκρίνει αυτόματα 3 εταιρείες, μαζί με τις 550 πολιτικές απορρήτου τους που έχει η κάθε μία από αυτές, πριν και μετά τον Γ.Κ.Π.Δ.. Για να αξιολογηθεί ποιοτικά το επίπεδο συμμόρφωσης των εταιρειών με τον Γ.Κ.Π.Δ. έγινε και χειροκίνητη μελέτη στις πολιτικές δύο εταιρειών με 450 πολιτικές έκαστη. Το συμπέρασμα ήταν ότι ο Γ.Κ.Π.Δ. έχει σημειώσει πρόοδο

στην προστασία των δεδομένων των χρηστών, αλλά απαιτείται περισσότερη εξέλιξη με το πέρασμα του χρόνου. Ένα καίριο σημείο που χρειάζεται περισσότερη προσοχή και στην συνέχεια παροχή προστασίας στους χρήστες, έτσι ώστε να εκπληρώσει πλήρως την υπόσχεση του Γ.Κ.Π.Δ., είναι ο τομέας της παροχής του δικαιώματός τους να έχουν την δυνατότητα επεξεργασίας καθώς και διαγραφής των στοιχείων και πληροφοριών τους.

Τέλος, εστιάζει στην περίπτωση αποτυχίας εφαρμογής του Γ.Κ.Π.Δ. και στις επιπτώσεις του. Όταν υπάρχει μη συμμόρφωση σε αυτόν, τότε υποδηλώνεται η έλλειψη διαφάνειας του οργανισμού σχετικά με την επεξεργασία και την προστασία των προσωπικών τους πληροφοριών. Η ύπαρξη των ανωτέρω επιβάλλουν τη λήψη πρόσθετων νέων μέτρων για την προστασία και ασφάλεια των περιουσιακών στοιχείων του PII.

2.6: Γ.Κ.Π.Δ.: αναλυτές, ερευνητές και μηχανικοί

2.6.1: Η συμβολή των αναλυτών στην συμμόρφωση με τον Γ.Κ.Π.Δ.

Τα πληροφοριακά συστήματα έχουν πρόσβαση, διαχειρίζονται και καταγράφουν ευαίσθητα δεδομένα για τους πολίτες. Η διεισδυτικότητα αυτών των συστημάτων αυξάνεται δραματικά εξαιτίας της ραγδαίας εξέλιξης της κινητής τηλεφωνίας και του IoT. Ο κύριος στόχος του Γ.Κ.Π.Δ. είναι η προστασία της ιδιωτικής ζωής των πολιτών όσον αφορά την επεξεργασία των προσωπικών τους δεδομένων. Επιβάλλει μια προσέγγιση «Privacy by Design» και «by Default», όπου τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία μόνο όταν απαιτείται από τις λειτουργίες του πληροφοριακού συστήματος.

Το έγγραφο «Static Analysis for GDPR Compliance» των Pietro Ferrara και Fausto Spoto συζητά τον ρόλο που θα μπορούσε να παίξει η στατική ανάλυση στον Γ.Κ.Π.Δ.. Συγκεκριμένα, εισάγει τον Γ.Κ.Π.Δ. και τη στατική ανάλυση και, στη συνέχεια, προτείνει τον τρόπο με τον οποίο οι υπάρχουσες αναλύσεις κηλίδων και οι αλγόριθμοι κοπής προς τα πίσω μπορούν να συνδυαστούν για να παράγουν αναφορές χρήσιμες για τη συμμόρφωση με αυτόν. Εντοπίζει τέσσερις κύριους παράγοντες στη διαδικασία συμμόρφωσης με τον Γ.Κ.Π.Δ. (υπεύθυνους προστασίας δεδομένων, υπεύθυνους ασφαλείας πληροφοριών, διαχειριστές έργων και προγραμματιστές) και προτείνει ένα συγκεκριμένο επίπεδο αναφοράς για καθέναν από αυτούς.

Για να συμμορφωθούν με τη λογοδοσία της πρακτικής, οι υπεύθυνοι επεξεργασίας δεδομένων θα έπρεπε να είναι σε θέση να αποδείξουν ότι ο πραγματικός χειρισμός δεδομένων τους συμμορφώνεται με τις υποχρεώσεις τους. Ωστόσο, ο τύπος της πρόβλεψης ελέγχου περιοριζόταν στον έλεγχο αρχείων καταγραφής. Έτσι, το άρθρο οραματίζεται την εφαρμογή στατικής ανάλυσης PET, για τον έλεγχο των συμπεριφορών του προγράμματος προς τις ευαίσθητες πληροφορίες στα διάφορα στάδια του κύκλου ζωής του λογισμικού.

Το συμπέρασμα του άρθρου αυτού είναι ότι οι στατικοί αναλυτές μπορούν να βοηθήσουν στη συμμόρφωση με τον Γ.Κ.Π.Δ. χρησιμοποιώντας υπάρχουσες στατικές αναλύσεις όπως ανάλυση λεκέδων (taint analysis) και τεμαχισμό προς τα πίσω (backward slicing) αλλά και παρέχοντας πληροφορίες σχετικά με την πηγή και τα στοιχεία λογισμικού.

2.6.2: Το ISO 27001 σε ερευνητικό κέντρο

Η έρευνα «ISO 27001:2013 for Laboratory Management Information System at School of Applied Science Telkom University» του Alit Yuniargan Eskaluspita αυτή

πραγματοποιήθηκε στη Σχολή Εφαρμοσμένων Επιστημών του Πανεπιστήμιο Telkom. Για τις αυξημένες ανάγκες της σχολής, για τα δεδομένα που χρησιμοποιούσαν, χρησιμοποιήθηκε ένα σύστημα οργάνωσης και διαχείρισης όλων των εργαστηριακών δεδομένων και των πρακτικών αναγκών, που ονομαζόταν SIMLAB. Η έρευνα διεξήχθη προσδιορίζοντας το επίπεδο ασφάλειας πληροφοριών σύμφωνα με το ISO 27001:2013 ως πλαίσιο συμμόρφωσης στον Γ.Κ.Π.Δ..

Σε αυτήν την έρευνα, τα δεδομένα συλλέχθηκαν με παρατήρηση και συνέντευξη. Με βάση το ISO 27001:2013, καθορίστηκαν πεδία και επιλέχθηκαν ρήτρες που ήταν κατάλληλες για ερευνητικό υπόβαθρο για τη μέτρηση του επιπέδου ωριμότητας σε κάθε πτυχή του αντικειμένου.

Με το πρότυπο ISO 27001:2013, η αξιολόγηση και η μέτρηση της ασφάλειας των πληροφοριακών συστημάτων ήταν ευκολότερο να πραγματοποιηθεί με την υποστήριξη ειδικών ελέγχων ασφαλείας. Τα αποτελέσματα της έρευνας ήταν τα ακόλουθα:

- Μετά από ανάλυση και αξιολόγηση της ασφάλειας στο SIMLAB, το πληροφοριακό σύστημα έλαβε το επίπεδο 2 σε επίπεδο ωριμότητας.
- Η ρήτρα για την Ασφάλεια Ανθρώπινου Δυναμικού έφτασε το επίπεδο 3 του επιπέδου ωριμότητας (Καλά καθορισμένο).
- Η διαχείριση περιουσιακών στοιχείων έφτασε στο επίπεδο 2 του επιπέδου ωριμότητας.
- Ο Έλεγχος πρόσβασης έφτασε στο επίπεδο 3 του επιπέδου ωριμότητας (Καλά καθορισμένο).
- Η ρήτρα για την Φυσική και Περιβαλλοντική Ασφάλεια έφτασε το επίπεδο 3 του επιπέδου ωριμότητας (Καλά Καθορισμένο).
- Ωστόσο, σε ορισμένους ελέγχους εξακολούθησαν να χρειάζονται τεκμηρίωση και διαδικασίες υποστήριξης.

Από την αξιολόγηση διαπιστώθηκε επίσης ότι οι διαδικασίες και η τεκμηρίωση δεν ήταν στο ίδιο πρότυπο και μορφή. Σε γενικές γραμμές υποδήλωνε πως η SIMLAB χρειαζόταν επιπλέον σχεδιασμούς για την πλήρη συμμόρφωση σε όλα τα πρότυπα ISO 27001:2013.

2.6.3: Ο Γ.Κ.Π.Δ. στην έρευνα του γονιδιώματος

Ο Γ.Κ.Π.Δ. τέθηκε σε εφαρμογή τον Μάρτιο του 2018 ως έγκυρος νόμος σχετικά με την προστασία των δεδομένων στην Ε.Ε. και πλέον κατέχει κυρίαρχη θέση στο νομικό τοπίο. Η θέση του κανονισμού σχετικά με την ευρεία συναίνεση υπήρξε πρόσφατα αιτία ανησυχίας στην ερευνητική κοινότητα του γονιδιώματος.

Η συναίνεση στον Γ.Κ.Π.Δ. επιδιώκει να παρέχει στα άτομα τον έλεγχο των προσωπικών τους δεδομένων, ενώ η ευρεία συναίνεση επιτρέπει στα υποκείμενα της έρευνας να ελέγχουν αν θέλουν τα βιολογικά τους δείγματα και τα σχετικά δεδομένα να χρησιμοποιηθούν σε μελλοντική απροσδιόριστη γονιδιωματική έρευνα. Άρα υπάρχει μια σαφής διαφορά μεταξύ της λογικής πίσω από τη συναίνεση στον κανονισμό και της λογικής πίσω από την συναίνεση στη γονιδιωματική έρευνα.

Το άρθρο «Broad consent under the GDPR: an optimistic perspective on a bright future» του Dara Hallinan εξετάζει σε βάθος την κατάσταση σχετικά με την ευρεία συναίνεση βάσει του Γ.Κ.Π.Δ. και, παρά την ανησυχία που απορρέει από την πρόσφατη νομολογία, προσφέρει μια θετική προοπτική. Αυτή η θετική προοπτική υποστηρίζεται από τρεις οπτικές γωνίες. Η γενική καθοδήγηση της ομάδας εργασίας του άρθρου 29 σχετικά με τη συναίνεση στην επιστημονική έρευνα θα μπορούσε

νόμιμα να παραμεριστεί εάν αποδειχθεί ακατάλληλη και παρεμποδιστική σε σχέση με τις μοναδικές πρακτικές της γονιδιωματικής έρευνας.

2.6.4: Η επιρροή του Γ.Κ.Π.Δ. για τους ερευνητές

Το άρθρο «General Data Protection Regulation (GDPR) and implications for research» Marc Cornock του μιλάει για τον τομέα την έρευνας και το πως θα την επηρεάσει ο Γ.Κ.Π.Δ.. Αναφέρει πως το κλίμα συζήτησης, γύρω από τον κανονισμό, ήταν αρνητικό και γεμάτο άγχος. Στην συνέχεια αναφέρει τους τρεις κύριους στόχους του Γ.Κ.Π.Δ.. Τονίζεται πως τα περισσότερα άρθρα του αφορούν εταιρείες και οργανισμούς και τον τρόπο με τον οποίο χειρίζονται προσωπικά δεδομένα και πως θα έχουν μικρή επίδραση σε μεμονωμένους ερευνητές. Ωστόσο, υπάρχουν ορισμένες διατάξεις εντός του Γ.Κ.Π.Δ. που θα επηρεάσουν άμεσα τους ερευνητές. Οι τομείς που επηρεάζονται είναι οι ακόλουθοι:

- Αλλαγές στη συναίνεση,
- Νέα δικαιώματα για τα άτομα,
- Κοινή χρήση δεδομένων,
- Προστασία των παιδιών και
- Παραβιάσεις δεδομένων και αναφορά

Όσον αφορά τη συγκατάθεση, απαιτείται να αποδεικνύεται ότι το άτομο συναίνει στη χρήση των δεδομένων του, ότι η συγκατάθεση λαμβάνεται με τρόπο κατανοητό και προσβάσιμο από το υποκείμενο και ότι υπάρχει η ευκαιρία για το άτομο να αποχωρήσει από τη μελέτη ανά πάσα στιγμή.

Άλλο ένα δικαίωμα τους που δεν ισχύει απαραίτητα είναι εάν τα δεδομένα ελήφθησαν νόμιμα και εξακολουθούν να είναι απαραίτητα για τον σκοπό για τον οποίο ελήφθησαν. Γεγονός που υπογραμμίζει την ανάγκη να διασφαλιστεί ότι η συγκατάθεση είναι επαρκής για τους σκοπούς της έρευνας.

Ακόμα, υπάρχουν ειδικοί κανόνες σχετικά με τη μεταφορά δεδομένων εκτός Ε.Ε.. που διασφαλίζουν ότι τα δικαιώματα του ατόμου δεν περιορίζονται από τους νόμους της χώρας που λαμβάνει τα δεδομένα. Υπάρχει επίσης η απαίτηση ότι τα δεδομένα είναι φορητά, πράγμα που σημαίνει ότι το άτομο έχει δικαίωμα να τα λάβει με τρόπο που να μπορεί να διαβαστεί από αυτόν. Αυτό μπορεί να σημαίνει ότι οι ερευνητές πρέπει να επανεξετάσουν τον τρόπο με τον οποίο αποθηκεύουν τα δεδομένα του θέματος.

Όσον αφορά τα παιδιά, οι διατάξεις αφορούν τη διασφάλιση ότι κατανοούν κάθε πληροφορία που τους παρέχεται.

Τέλος, το άρθρο τονίζει την ύπαρξη κυρώσεων σε τυχόν μη συμμόρφωση στον κανονισμό αλλά και το άγχος που επικρατούσε καθώς τότε υπήρχαν ελάχιστες επίσημες οδηγίες στις οποίες έπρεπε να βασιστούν για να υλοποιήσουν την υιοθέτηση του.

2.6.5: Μέθοδοι και εργαλεία για τους μηχανικούς για την συμμόρφωση στον Γ.Κ.Π.Δ.

Σύμφωνα με αυτό το άρθρο «Methods and Tools for GDPR Compliance through Privacy and Data Protection Engineering» των Yod-Samuel Martín & Antonio Kung προωθούνται οι αρχές του PbD, που υιοθετεί τις αρχές του Γ.Κ.Π.Δ.. Το PbD απαιτεί την προληπτική εξέταση του απορρήτου από την έναρξη ενός έργου, σε όλες τις δραστηριότητες που εμπλέκονται κατά τη διάρκεια του σχεδιασμού και της ανάπτυξης προϊόντων, υπηρεσιών και συστημάτων, και όχι ως εκ των υστέρων σκέψη. Για να είναι βιώσιμο το PbD, οι μηχανικοί πρέπει να συμμετέχουν αποτελεσματικά

στον βρόχο, καθώς είναι τελικά υπεύθυνοι για τη δημιουργία των προϊόντων τους. Κατά το έτος που είχε γραφτεί το άρθρο, αυτή η μέθοδος δεν ήταν ευρέως διαδεδομένη και υιοθετημένη στην πρακτική της μηχανικής.

Οι συγγραφείς προσπάθησαν να υποστηρίξουν αυτήν τη θέση μέσω της υλοποίησης του έργου PDP4E, το οποίο θα παρείχε στους μηχανικούς μεθόδους και εργαλεία για να εφαρμόζουν συστηματικά τις αρχές προστασίας δεδομένων στα έργα που εκτελούν, ώστε να συμμορφώνονται με τον Γ.Κ.Π.Δ. και να εφαρμόζουν τις αρχές του PbD. Σε αυτό το έργο το απόρρητο είχε εισαχθεί στα υπάρχοντα εργαλεία και μεθόδους μηχανικής λογισμικού γενικής χρήσης. Εγγυήθηκε η εισαγωγή του απορρήτου και της προστασίας δεδομένων σε συγκεκριμένους κλάδους μηχανικής λογισμικού και συστημάτων (διαχείριση κινδύνου, μηχανική απαιτήσεων, σχεδιασμός βάσει μοντέλων, διασφάλιση λογισμικού/συστημάτων), λόγω της συνάφειάς τους με το κανονιστικό πλαίσιο και της ωριμότητας των ισχυόντων σχετικών μεθόδων απορρήτου.

Ως συμπέρασμα υποστηρίζεται πως τα υπάρχοντα εργαλεία μηχανικής λογισμικού γενικής χρήσης έχουν αποδείξει με επιτυχία την εφαρμογή στην ασφάλεια που προσέφεραν. Για αυτό τον λόγο, το έργο PDP4E θα ενσωμάτωνε λειτουργίες μηχανικής προστασίας της ιδιωτικής ζωής και δεδομένων που υπήρχαν ήδη και δεν θα έφτιαχνε νέα εργαλεία από την αρχή. Ακόμα, θα ενσωμάτωνε μεθόδους προστασίας δεδομένων που θα εξειδικεύονταν στην λειτουργία με τη συμμόρφωση στον Γ.Κ.Π.Δ. και θα ενσωμάτωναν τρέχουσες εργασίες σχετικά με πρότυπα και μεθόδους προστασίας (π.χ. ISO 29134 ή ISO 27550). Το έργο αυτό είχε και έχει ως μακροπρόθεσμο σκοπό να δημιουργήσει ένα οικοσύστημα έρευνας και πρακτικής για να ενισχύσει την υιοθέτηση πρακτικών προστασίας δεδομένων στη μηχανική λογισμικού και συστημάτων. Συνολικά, η εφαρμογή των μεθόδων και εργαλείων PDP4E θα διευκολύνει τη μηχανική των προϊόντων που συμμορφώνονται με το Γ.Κ.Π.Δ., γεγονός που θα οδηγήσει σε ευρεία δημιουργία προϊόντων, συστημάτων και υπηρεσιών που προστατεύουν καλύτερα το απόρρητο και τα προσωπικά δεδομένα των πολιτών της Ε.Ε..

2.7: Ο Γ.Κ.Π.Δ. και το ISO 27001 στις επιχειρήσεις

2.7.1: Από την Οδηγία 95/46/ΕΚ στον Γ.Κ.Π.Δ.: ISO 27001

Η προστασία των προσωπικών δεδομένων γνώρισε μεγάλη αναταραχή καθώς υπήρξε αυξανόμενη υιοθέτηση υπηρεσιών που βασίζονται στις υπηρεσίες νέφους (cloud) και στην εστίαση στα προσωπικά δεδομένα ως βασικό στοιχείο στα σύγχρονα επιχειρηματικά μοντέλα. Η κύρια νομική πράξη της Ε.Ε. που όριζε τους γενικούς κανόνες για την επεξεργασία δεδομένων προσωπικού χαρακτήρα ήταν η Οδηγία 95/46/ΕΚ κατά το έτος 2015. Η ταχεία εξέλιξη της τεχνολογίας είχε αναδείξει τις αδυναμίες της Οδηγίας, απαιτώντας προσαρμογή της νομοθεσίας δημιουργώντας τον Γ.Κ.Π.Δ.. Ο κανονισμός στόχευε στην ενίσχυση των δικαιωμάτων των χρηστών, τόνιζε την ευθύνη των υπευθύνων επεξεργασίας και επεξεργασίας δεδομένων και αύξανε τις κυρώσεις για παραβάσεις των διατάξεών του. Ο κανονισμός επιβάρυνε σημαντικά τις επιχειρήσεις που εμπλέκονταν στην επεξεργασία δεδομένων προσωπικού χαρακτήρα προκειμένου να συμμορφωθούν σε αυτόν.

Στο άρθρο «Assessing IT Security Standards Against the Upcoming GDPR for Cloud Systems» των Cesare Bartolini, Gabriela Gheorghe, Andra Giurgiu, Mehrdad Sabetzadeh και Nicolas Sannier τονίζεται πως, κατά την γνώμη των αρθρογράφων, έπρεπε η ακαδημαϊκή κοινότητα να ανακαλύψει τα αλληλοεπικαλυπτόμενα θέματα, όπου οι νομικές απαιτήσεις πληρούσαν τις επιχειρηματικές πρακτικές στην παροχή

υπηρεσιών νέφους. Δηλαδή, ήταν αναγκαία η εντόπιση κενών μεταξύ του τι όριζαν οι κανονισμοί προστασίας δεδομένων και του τί ήταν τεχνικά εφικτό, όσον αφορά τη συμμόρφωση. Προτάθηκαν τα πρότυπα ISO/IEC 27000 που παρείχαν ένα πλαίσιο χειρισμού εννοιών, όπως η πολιτική και οι στόχοι ασφάλειας, οι ορισμοί και η αξιολόγηση κινδύνου, η δέσμευση για συνεχή αξιολόγηση και τεκμηρίωση. Αναφέρεται πως το πρότυπο ISO/IEC 27001-2005 και η αναθεώρηση του 2013, θεωρούνταν ευρέως αποδεκτή από τον χώρο της πληροφορικής. Η πιστοποίηση χαρακτηριζόταν όχι μόνο ως ανταγωνιστικό πλεονέκτημα της επιχείρησης, αλλά και ως απαραίτητη τυπική πιστοποίηση για τις επιχειρήσεις, που σταδιακά είχε μετατραπεί σε απαίτηση των πελατών. Προτείνεται επίσης εκπαίδευση, με βάση το ανοιχτό πλαίσιο πιστοποίησης CSA STAR, που αξιοποιούσε τις απαιτήσεις και τα σημεία ελέγχου του ISO/IEC 27001.

2.7.2: Τι σημαίνει ο Γ.Κ.Π.Δ. για τις επιχειρήσεις

Ο Γ.Κ.Π.Δ. διευρύνει το πεδίο προστασίας δεδομένων, έτσι ώστε όλοι οι οργανισμοί που συλλέγουν και επεξεργάζονται πληροφορίες πελατών να συμμορφώνεται σε αυτόν, ανεξάρτητα από το πού βασίζονται ή πού αποθηκεύονται τα δεδομένα με την cloud αποθήκευση να μην αποτελεί εξαίρεση.

Το άρθρο «What the GDPR means for businesses» των Colin Tankard και Elsevier Ltd, καθώς είναι γραμμένο το 2016, προσπαθεί να παροτρύνει τους οργανισμούς να ενεργοποιηθούν έγκαιρα για τις μεταρρυθμίσεις που θα φέρει ο Γ.Κ.Π.Δ. με την υποχρεωτική εφαρμογή του το 2018. Αναφέρει ποιες αλλαγές θα επέλθουν στην επιχείρηση ως προς την δομή της και εστιάζει στο γεγονός ότι αυτό θα επιφέρει θετικά αποτελέσματα στην επιχείρηση.

Αναφέρεται και στα πρότυπο ISO 27001 και 27002 που έχουν δημιουργηθεί για να βοηθήσουν τους οργανισμούς να διασφαλίσουν ότι διαθέτουν αποτελεσματικά προγράμματα ασφάλειας πληροφοριών. Το ISO 27001 δημιουργήθηκε αρχικά με σκοπό να βοηθήσει στη διαχείριση της ασφάλειας των κρατικών υπηρεσιών και των δεδομένων των πολιτών στα χέρια των παρόχων υπηρεσιών των εταιρειών και συμβάλει στη διασφάλιση της αρχής που κατοχυρώνεται στον Γ.Κ.Π.Δ., ότι υπάρχουν κατάλληλα τεχνολογικά και οργανωτικά μέτρα για την προστασία των πληροφοριών. Βοηθάει τους οργανισμούς να καθορίσουν ευθύνες, όπως ποιο άτομο είναι υπεύθυνο για ορισμένα στοιχεία πληροφοριών και ποιο μπορεί να εξουσιοδοτήσει την πρόσβαση σε δεδομένα.

Αναφέρεται επίσης ότι ο χρόνος υλοποίησης του Γ.Κ.Π.Δ. διαφέρει από εταιρεία σε εταιρεία αλλά αυτό δεν πρέπει να είναι παράγοντας αποφυγής καθώς θα είναι προς όφελος τους. Οι οργανισμοί αφενός πρέπει να διασφαλίσουν ότι δεν θα έχουν οποιοδήποτε επιπλέον κόστος και αφετέρου να γνωρίζουν ότι θα αντιμετωπίσουν κυρώσεις για μη συμμόρφωση σε αυτόν, είτε μερική είτε πλήρη. Αυτό θεωρείται πρακτικά εύκολο αν ληφθούν κατάλληλες προφυλάξεις.

2.7.3: Εφαρμογή του Γ.Κ.Π.Δ. στις εταιρείες

Πριν από τον Γ.Κ.Π.Δ. δεν υπήρχε κάποια ενιαία νομοθεσία σχετικά με την ειδοποίηση παραβίασης προσωπικών δεδομένων εκτός από τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, όπως αναφερόταν στην οδηγία για την προστασία της ιδιωτικής ζωής ηλεκτρονικών επικοινωνιών.

Αρχικά, στο κείμενο «What the GDPR means for businesses» του Colin Tankard αναφέρεται ότι οι οργανισμοί που υφίστανται παραβίαση δεδομένων έχουν το περιθώριο να ενημερώσουν τις αρχές προστασίας δεδομένων εντός 72 ωρών. Οι

κυρώσεις για μη συμμόρφωση με τον κανονισμό είναι τόσο μεγάλες που μπορεί να φτάσουν και τα 20.000.000 ευρώ. Οι οργανισμοί με σημαντικές δραστηριότητες επεξεργασίας δεδομένων υποχρεούνται να ορίσουν έναν υπεύθυνο προστασίας δεδομένων, ο οποίος πρέπει να λειτουργεί ανεξάρτητα από την επιχείρηση.

Σύμφωνα με το Ovum, το 52% των οργανισμών πίστευε ότι ο Γ.Κ.Π.Δ. θα επέφερε πρόστιμα για την επιχείρησή τους και το 68% ότι θα αύξανε δραματικά το κόστος της επιχειρηματικής δραστηριότητας στην Ευρώπη.

Στην συνέχεια του άρθρου αναφέρονται διάφοροι τομείς που θα έκαναν είτε δυσκολότερη είτε ευκολότερη τη συμμόρφωση. Ένα από αυτά αποτελούσε το γεγονός ότι διευρύνθηκαν τα δικαιώματα των μεμονωμένων υποκειμένων των δεδομένων, από την επιλογή μέχρι και το δικαίωμα της λήθης. Από την άλλη πλευρά, ένα πράγμα που διευκόλυνε τους υπευθύνους επεξεργασίας και τους επεξεργαστές δεδομένων είναι η εισαγωγή της έννοιας του one-stop-shop καθώς αφαιρεί μια χρονοβόρα και συχνά δαπανηρή προκάτοχη διαδικασία.

Ο Γ.Κ.Π.Δ. δηλώνει ότι οι οργανισμοί πρέπει να εφαρμόζουν κατάλληλες τεχνολογικές και λειτουργικές διασφαλίσεις για την ασφάλεια των δεδομένων, συμπεριλαμβανομένης της εφαρμογής ισχυρών ελέγχων απορρήτου. Αναφέρει ότι οι οργανισμοί θα πρέπει να υιοθετούν εσωτερικά μέτρα που πληρούν τις αρχές της προστασίας δεδομένων από το σχεδιασμό μέχρι και την υλοποίηση.

Αναφέρεται πως η κρυπτογράφηση θα έπρεπε να ήταν η προεπιλεγμένη επιλογή για την προστασία όλων των δεδομένων, τόσο όταν τα δεδομένα μεταδίδονταν όσο και όταν βρίσκονταν σε αποθήκευση. Αν και τα δεδομένα κρυπτογραφούνταν, θα έπρεπε να περιορίζεται ο όγκος τους για μειώσει του φόρτου προστασίας τεράστιων συνόλων δεδομένων. Ακόμα, τα στοιχεία ελέγχου θα έπρεπε να συνδέονται με βάσεις δεδομένων υποστήριξης, οι οποίες θα βοηθούσαν στον καθορισμό των αναλυτικών δικαιωμάτων και έτσι θα διασφαλιζόταν ότι διατηρούνται ενημερωμένα τα δεδομένα καθώς τα πράγματα εξελίσσονταν.

Η χρήση ισχυρού ελέγχου ταυτότητας θα διασφαλίζε ότι τα άτομα που έχουν πρόσβαση στα δεδομένα είναι όντως αυτά, έτσι ώστε ένας χρήστης με δικαιώματα πρόσβασης σε δεδομένα να μην είχε τη δυνατότητα να μεταβιβάσει αυτά τα δικαιώματα σε κάποιον άλλο. Η χρήση βιομηχανικών προτύπων και πλαισίων βέλτιστων πρακτικών θα μπορούσε να βοηθήσει τους οργανισμούς στο να διαχειρίζονται τους κινδύνους που αντιμετώπιζαν, προσθέτοντας παράλληλα μεγαλύτερη αποτελεσματικότητα και βιωσιμότητα στις δραστηριότητές τους.

2.7.4: Ο Γ.Κ.Π.Δ. αποτελεί ευκαιρία για τις επιχειρήσεις

Το άρθρο «GDPR compliance: your tech department's next big opportunity» του Phil Beckett ξεκινάει μιλώντας για το «τι είναι ο Γ.Κ.Π.Δ.» και στη συνέχεια για το «πώς λειτουργεί» επισημαίνοντας ότι πρόκειται για έναν κανονισμό που είναι αναγκαίος. Στην συνέχεια αναφέρεται στο γεγονός πως κάθε οργανισμός πρέπει να ικανοποιεί κάποιο standard προς τον Γ.Κ.Π.Δ.. Εάν επιλεγεί η καλή άσκηση διακυβέρνησης πληροφοριών, τότε όχι μόνο θα ληφθούν μέτρα για τη συμμόρφωση με τον Γ.Κ.Π.Δ. μέσω αυτής της πρακτικής, αλλά θα μπορούν να ελέγχουν και να έχουν πρόσβαση στα δεδομένα με τρόπο που να τους παρέχει ένα ευρύ φάσμα πλεονεκτημάτων.

Ένα σημαντικό πλεονέκτημα του κανονισμού είναι ότι μειώνει το κόστος στην αποθήκευση δεδομένων καθώς συγκεντρώνονταν μόνο τα απαραίτητα δεδομένα. Το δεύτερο όφελος που επισημαίνεται είναι η δυνατότητα άντλησης γνώσης από την ανάλυση των δεδομένων. Καμία στατιστική ανάλυση δεν προήλθε από αποδιοργανωμένα σύνολα πληροφοριών, αλλά από προσεκτικά κατηγοριοποιημένα

δεδομένα που επιτρέπουν την έξυπνη οργάνωση και την εύκολη εισαγωγή των αποτελεσμάτων σε προγράμματα όπως το Excel. Ένα επιπλέον πλεονέκτημα του Γ.Κ.Π.Δ. είναι το γεγονός ότι η συμμόρφωση δεν αποτελεί απλώς πλεονέκτημα για την επιχείρηση, αλλά και για την ευημερία όλων όσων τα δεδομένα καταγράφονται ή αποθηκεύονται. Αυτό βοηθάει στη διατήρηση του απορρήτου και της ψυχικής ηρεμίας των ανθρώπων και διασφαλίζει ότι τυχόν πληροφορίες που παραδίδονται στις εταιρείες δεν δέχονται κατάχρηση ή αποκάλυψη με τρόπο που δεν θα ήθελαν. Τέλος, το μεγαλύτερο όφελος από τη συμμόρφωση με τον Γ.Κ.Π.Δ., όπως αναφέρεται στο κείμενο, είναι οι πιο εκτεταμένες επιδράσεις που φιλτράρονται σε διαφορετικές και πιο ασυνήθιστες πτυχές της επιχείρησης.

Το κείμενο καταλήγει στο γεγονός πως ο καλύτερος τρόπος για να προσεγγίσει μια επιχείρηση μια τέτοια αλλαγή είναι να την αποδεχτεί πλήρως. Μετατρέποντας τη συμμόρφωση με τον Γ.Κ.Π.Δ. σε μια συναρπαστική ευκαιρία, μπορούν οι εταιρείες να κερδίσουν πραγματικά οφέλη για να ενισχυθούν και τελικά να αξιοποιηθεί μια απαιτούμενη αλλαγή προς όφελός.

2.7.5: Η εφαρμογή του ISO 27001 σε εταιρείες

Σύμφωνα με το άρθρο «Is ISO 27001 worth it?» του Cath Everett, ο μεγαλύτερος υποστηρικτής του ISO 27001 είναι η Ιαπωνία, που αντιπροσωπεύει περισσότερο από το ήμισυ του συνόλου των διαπιστευμένων εταιρειών παγκοσμίως, ακολουθούμενη από την Ινδία και την Κίνα. Γενικότερα, οι επιχειρήσεις επέλεγαν άλλου είδους πιστοποιήσεις όπως το SAS 70 που περιλάμβαναν λιγότερες επίσημες απαιτήσεις ασφάλειας από το πιο εστιασμένο ISO και έδιναν τη δυνατότητα στους οργανισμούς να επιλέγουν τους τομείς στους οποίους επιθυμούσαν να ελεγχθούν. Άλλος ένας λόγος που αναφέρεται ως υπαίτιος για την μη υιοθέτησή του είναι ότι η συμμόρφωση σε αυτόν απαιτούσε τεράστια ποσά χρήματος, προσπάθειας και χρόνου.

Ήταν δύσκολο να γίνει αντιληπτό από τους κατόχους προϋπολογισμού η αξία και τα λειτουργικά οφέλη μιας τέτοιας κίνησης και έτσι δεν την προωθούσαν αρκετά ψηλά στις προτεραιότητες από τα ανώτερα στελέχη ώστε να ληφθεί σοβαρά υπόψη. Για αυτό τον λόγο, το κείμενο προσεγγίζει το θέμα αυτό με τις αναλύσεις κόστους-οφέλους. Επίσης, περιλαμβάνει τον υπολογισμό του πόσο θα κόστιζε σε έναν οργανισμό τόσο οικονομικά όσο και από άποψη χρόνου η ανάληψη μιας πρωτοβουλίας συμμόρφωσης έναντι του πιθανού οικονομικού αντίκτυπου αν δεν την υιοθετούσε (π.χ. βλάβης στη φήμη, πρόστιμα κ.τ.λ.).

Το μεγάλο ζήτημα που τονίζεται στο άρθρο είναι ότι, παρόλο που οι περισσότεροι οργανισμοί αντιλαμβάνονταν την ασφάλεια των πληροφοριών ως πρόβλημα πληροφορικής, στην πραγματικότητα είναι θέμα επιχειρηματικής διακυβέρνησης και πρέπει να αντιμετωπιστεί μέσω της διαχείρισης διαδικασιών, πολιτικών και ανθρώπων.

Οι επαγγελματίες ασφάλειας πληροφοριών πρέπει να αναφέρουν στο διοικητικό συμβούλιο τη λειτουργία της εταιρικής διακυβέρνησης ή της διαχείρισης ποιότητας. Εάν αυτό είναι αδύνατο, πρέπει να προσπαθούν να διασφαλίσουν ότι ο κίνδυνος πληροφοριών προστίθεται στο μητρώο εταιρικών κινδύνων, το οποίο περιλαμβάνει μόνο επιχειρησιακούς, οικονομικούς κινδύνους καθώς και κινδύνους για την υγεία και την ασφάλεια.

2.7.6: Η επιρροή του ISO 27001 σε εταιρείες

Το πρότυπο ISO 27001 παρείχε και παρέχει καθοδήγηση σε ένα υγιές Σ.Δ.Α.Π. κατά την εποχή που η ασφάλεια πληροφοριών αποτελούσε και συνεχίζει να αποτελεί

ένα από τα προβλήματα της ανώτερης διοίκησης και το κόστος υλοποίησης της συμμόρφωσης στον Γ.Κ.Π.Δ. είναι σημαντικό.

Στην μελέτη «The Impact of ISO 27001 Certification on Firm Performance» των Carol Hsu, Tawei Wang και Ang Lu, διερευνήθηκε εάν η πιστοποίηση μπορεί να ωφελήσει τους οργανισμούς, σηματοδοτώντας τη στάση της διοίκησης απέναντι στη διαχείριση ασφάλειας. Ερευνήθηκε η εταιρική απόδοση μετά την πιστοποίηση ISO 27001 με δείγματα από τις Η.Π.Α. και άλλες επιλεγμένες ευρωπαϊκές χώρες. Δυστυχώς, δεν υπήρχαν πολλές έρευνες για την απόδοση των εταιρειών με πιστοποίηση ISO 27001 και έτσι η έρευνα βασίστηκε περισσότερο στο ISO 9001 που αποτελεί τον προκάτοχό του. Κατά τις έρευνες δεν βρέθηκαν στοιχεία που να αποδεικνύουν ότι η πιστοποίηση ISO 9001 απέφερε οφέλη στην πιστοποιημένη εταιρεία όσον αφορά την απόδοση των περιουσιακών στοιχείων και τις επιδόσεις του χρηματιστηρίου. Αυτό το αποτέλεσμα που αποδόθηκε στη φύση του ISO 9001 είναι ότι μια καλή διαχείριση της ασφάλειας πληροφοριών θα θεωρηθεί ως υποχρέωση, αντί ως ανταγωνιστικό πλεονέκτημα. Το κείμενο, μάλιστα, αναφέρει πως το ISO 27001 ίσως να προσφέρει οικονομικά οφέλη στις επιχειρήσεις έναντι του προκάτοχού του που δεν προσέφερε. Εν συνεχεία, αναφέρεται πως η φύση της πιστοποίησης ISO 27001 οδηγεί σε ασήμαντα ευρήματα καθώς το ISO 27001 είναι περισσότερο υποχρέωση αντί ανταγωνιστικό πλεονέκτημα, όπως και το ISO 9001. Βέβαια, πρέπει να ληφθεί υπόψιν πως το πεδίο εφαρμογής της πιστοποίησης προκαλούσε ανησυχία και ίσως αυτό επηρέασε αυτά τα αποτελέσματα, καθώς οι περισσότερες από τις εταιρείες του δείγματος είχαν μόνο μερική κάλυψη πιστοποίησης, αντί να το έχουν πιστοποιημένο σε οργανωτικό επίπεδο.

Τέλος, υπογραμμίζεται πως δεν υπήρχαν αρκετές εταιρείες που είχαν αναρτημένα τα στοιχεία απόδοσής τους αν και ήταν πιστοποιημένες με ISO 27001. Λοιπόν, αυτό το άρθρο θα μπορούσε να θεωρηθεί ως ένα σημείο εκκίνησης για την εξέταση των οικονομικών αποδόσεων που προκύπτουν από την πιστοποίηση ISO 27001.

2.7.7: Ο Γ.Κ.Π.Δ. σε μικρομεσαίες επιχειρήσεις μέσω σχεδίου προσαρμογής

Ο Γ.Κ.Π.Δ. είναι ένας κανονισμός της Ε.Ε. που επηρεάζει όλους τους οργανισμούς τόσο εντός της Ε.Ε. όσο και τους εκτός Ε.Ε., που θέλουν να συναλλάσσονται με αυτήν. Ο κανονισμός εισήγαγε αυστηρότερες απαιτήσεις για την επεξεργασία προσωπικών δεδομένων, τις οποίες ήταν δύσκολο πολλές μικρομεσαίες επιχειρήσεις να ακολουθήσουν χωρίς σημαντικές προσαρμογές.

Στο άρθρο «A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises» του Martin Brodin χρησιμοποιήθηκε η επιστήμη του σχεδιασμού για να αναπτύξει ένα πλαίσιο προσαρμογής των μικρομεσαίων επιχειρήσεων στην συμμόρφωση με τον Γ.Κ.Π.Δ.. Το πλαίσιο αξιολογήθηκε εμπειρικά σε τρεις διαφορετικούς τύπους οργανισμών. Αξιολογήθηκε θεωρητικά σε σχέση με την επιστημονική βιβλιογραφία, συμπεριλαμβανομένων των προσδιορισμένων επιπτώσεων του Γ.Κ.Π.Δ.. Τέλος, παρουσιάστηκε το πλαίσιο από την αρχική ανάλυση και σχεδιασμό έως την υλοποίηση και μελλοντική του μορφή, με συμβουλές για το πώς να επιτευχθεί η συμμόρφωση. Στο άρθρο επισημάνθηκαν, επίσης, μερικές από τις σημαντικότερες αλλαγές στον Γ.Κ.Π.Δ. σε σύγκριση με τον προκάτοχό του.

Η πρώτη εμπειρική περίπτωση έλαβε χώρα σε δημόσιο οργανισμό που είχε ως αποστολή την εξυπηρέτηση των πολιτών μιας μεγάλης σουηδικής πόλης και είχε νομική απαίτηση να διορίσει Υπεύθυνο Προστασίας Δεδομένων. Η δεύτερη περίπτωση

έλαβε χώρα σε μια ιδιωτική συμβουλευτική εταιρεία μεσαίου μεγέθους. Έγινε η ανάλυση για το πως λειτουργεί η επιχείρηση και στην συνέχεια της δόθηκε ένας τρόπος υλοποίησης που δημιουργήθηκε κατά τη φάση του σχεδιασμού, κυρίως μέσω της επικοινωνίας και της εκπαίδευσης. Στην τρίτη περίπτωση, ο οργανισμός ήταν μια εταιρεία προγραμματισμού εκδηλώσεων με 10–20 υπαλλήλους που επεξεργαζόταν πολλές προσωπικές πληροφορίες για τις εκδηλώσεις που αναλάμβανε και είχε αναθέσει σε εξωτερικούς συνεργάτες όλο το IT. Κατά τον σχεδιασμό εστίασαν στη δημιουργία νέων εγγράφων, αφού έλειπαν τα περισσότερα από τα απαραίτητα. Κατά τη διάρκεια της εφαρμογής, όλοι οι εργαζόμενοι έλαβαν εκπαίδευση για τον Γ.Κ.Π.Δ. ώστε να αποκτήσουν μια βασική κατανόηση του κανονισμού.

Στο έγγραφο αυτό παρουσιάστηκε ένα πλαίσιο συμμόρφωσης στον Γ.Κ.Π.Δ. για τις μικρομεσαίες επιχειρήσεις που θα μπορούσαν να χρησιμοποιήσουν στην εργασία τους. Το πλαίσιο αναπτύχθηκε χρησιμοποιώντας την επιστήμη του σχεδιασμού και τα αποτελέσματα συμμόρφωσης εξετάστηκαν και εγκρίθηκαν σε κάθε έναν από τους οργανισμούς, τόσο από ειδικούς όσο και από ανώτερα στελέχη. Τα αποτελέσματα υποδηλώνουν ότι το πλαίσιο μπορεί να βοηθήσει πολύ τις μικρομεσαίες επιχειρήσεις και να παρέχει μια ασφαλή και χαμηλού κόστους διαδικασία για τη συμμόρφωση με τον κανονισμό.

2.7.8: Συμμόρφωση των μικρομεσαίων επιχειρήσεων στον Γ.Κ.Π.Δ.

Η υποχρεωτική προσαρμογή των οργανισμών στον Γ.Κ.Π.Δ. συνεπάγεται ένα σύνολο νομικών, τεχνολογικών και λειτουργικών αλλαγών. Αποτελεί μια πρόκληση για όλους τους οργανισμούς και ειδικότερα για τις μικρομεσαίες επιχειρήσεις, που διαθέτουν λιγότερους ανθρώπινους και οικονομικούς πόρους για τη λήψη των απαραίτητων μέτρων ως προς τη συμμόρφωση με τη νομοθεσία.

Στο άρθρο «GDPR Compliance in SMEs: There is much to be done» των Maria da Conceição Freitas και Miguel Mira da Silva πραγματοποιείται έρευνα για να εξεταστεί αν προετοιμάστηκαν οι μικρομεσαίες επιχειρήσεις, πραγματοποιώντας συνεντεύξεις δια ζώσης με στελέχη από 10 μικρομεσαίες επιχειρήσεις. Ως συμπέρασμα αυτής της έρευνας ήταν ότι δεδομένης της έλλειψης επίγνωσης των υποχρεώσεων και των καθηκόντων τους σε σχέση με την Προστασία Δεδομένων Προσωπικού Χαρακτήρα, ήταν επείγον να καθοριστεί μια μεθοδολογία που θα μπορούσε να τις συμμορφώσει με τον Γ.Κ.Π.Δ..

Για να συλλεγούν πληροφορίες, που δεν είναι διαθέσιμες στην βιβλιογραφία αλλά ούτε μέσω από την διαδικασία της παρατήρησης, πραγματοποιήθηκαν συνεντεύξεις. Ο σχεδιασμός μιας συνέντευξης είναι πολύ σημαντικό κομμάτι για την απόκτηση της εμπιστοσύνης του ερωτώμενου. Επιλέχθηκαν ερωτήσεις που επέτρεπαν την αξιολόγηση των μικρομεσαίων επιχειρήσεων ως προς την συμμόρφωση και την εφαρμογή δραστηριοτήτων για την προσαρμογή στα πιο κρίσιμα ζητήματα του κανονισμού.

Τα αποτελέσματα από αυτή την έρευνα αξιολογήθηκαν με βάση την ανταγωνιστικότητα (ανθρώπινο δυναμικό και φυσικές υποδομές), καθώς και το βαθμό αποτελεσματικότητας στη στρατηγική τους, λαμβάνοντας υπόψη τα εκπαιδευτικά, επαγγελματικά, εταιρικά και παραγωγικά προφίλ. Η ανάλυση των αποτελεσμάτων οδήγησε σε μια σειρά από συμπεράσματα. Αυτά είναι τα ακόλουθα:

- Οι περισσότερες εταιρείες αγνοούσαν τις υποχρεώσεις τους σχετικά με πτυχές του εργατικού δικαίου, καθώς και τα καθήκοντά τους να εφαρμόζουν μηχανισμούς ασφαλείας στα προσωπικά δεδομένα που αποθηκεύουν και επεξεργάζονται.

- Όλες οι εταιρείες είχαν απαντήσει ότι αγνοούσαν τα δικαιώματα των υποκειμένων των δεδομένων, γι' αυτό και δεν είχαν εφαρμόσει διαδικασίες για τη διασφάλιση αυτών των δικαιωμάτων.
- Όλες οι εταιρείες είχαν απαντήσει ότι είχαν λιγότερους από 250 υπαλλήλους και ότι δεν είχαν διορίσει Υπεύθυνο Προστασίας Δεδομένων.
- Όλες οι εταιρείες που σύναπταν συμβάσεις με τρίτα μέλη δεν γνώριζαν την αναγκαιότητα της συμμόρφωσης των τρίτων μελών και εάν αυτές έπρεπε να συλλέγουν, να αποθηκεύουν, να έχουν πρόσβαση ή να επεξεργάζονται προσωπικά δεδομένα για την παροχή των υπηρεσιών τους.
- Καμία εταιρεία δεν μετέφερε δεδομένα σε χώρες εκτός Ε.Ε..

Ως συμπέρασμα, το άρθρο αναφέρει πως όλες οι επιχειρήσεις πρέπει να συμμορφώνονται στον κανονισμό, όχι μόνο για να αποφεύγουν τα βαριά πρόστιμα, αλλά και για να παρέχουν υπηρεσίες σε συμμορφούμενες εταιρείες. Έτσι, οι επιχειρήσεις θα μπορούν να εγγυηθούν τη βιωσιμότητά τους σε ένα όλο και πιο παγκοσμιοποιημένο κόσμο.

2.7.9: Η απόδοση των επιχειρήσεων με την χρήση του ISO 27001

Η ασφάλεια των πληροφοριακών συστημάτων είναι καθοριστικός παράγοντας για τις επιχειρήσεις, καθώς αυτή επηρεάζει την απόδοσή τους.

Το άρθρο «The Impact of ISO 27001 Certification on Firm Performance» των Carol Hsu, Tawei Wang και Ang Lu διερευνά εάν μια πιστοποίηση για το Σ.Δ.Α.Π. ωφελεί τις επιχειρήσεις που έχουν πιστοποιηθεί με το πρότυπο ISO 27001 προσφέροντάς τους ανταγωνιστικά πλεονεκτήματα. Σύμφωνα με το άρθρο αυτό για άλλα πρότυπα, όπως το ISO 9000, υπάρχουν πολλές έρευνες για την υιοθέτησή τους και τα αποτελέσματα που προσφέρουν. Κάτι τέτοιο όμως δεν ισχύει για το ISO 27001.

Επίσης υποστηρίζει ότι η φύση του πιστοποιητικού αυτού συνιστά κυρίως υποχρέωση της εταιρείας προς το κράτος. Για αυτόν τον λόγο η επιρροή που ασκεί στην επιχείρηση είναι μικρή και δεν εστιάζει στην απόκτηση ανταγωνιστικών πλεονεκτημάτων. Το πρόβλημα που αντιμετωπίστηκε σε αυτή την έρευνα ήταν ο μικρός αριθμός των διαθέσιμων πιστοποιημένων επιχειρήσεων που είχαν και τα οικονομικά τους στοιχεία αναρτημένα στο διαδίκτυο. Εκ των πραγμάτων, λοιπόν, αυτή ήταν περιορισμένη καθώς χωρίς ένα από τα δύο αυτά στοιχεία δεν μπορούσε να λάβει μέρος στην έρευνα. Επιπλέον, οι περισσότερες από αυτές είχαν υιοθετήσει μόνο την μερική κάλυψη πιστοποίησης αντί να έχουν πιστοποιηθεί σε οργανωτικό επίπεδο, γεγονός που ήταν ανησυχητικό και το καθιστούσε ως έναν ακόμα παράγοντα για την μη βελτίωση της απόδοσης της επιχείρησης.

Η ανωτέρω έρευνα αποτέλεσε ένα σημείο εκκίνησης για την εξέταση των οικονομικών αποδόσεων που μπορούν να προκύψουν από την πιστοποίηση ISO 27001.

2.8: Συμπεράσματα βιβλιογραφικής ανασκόπησης

Ανατρέχοντας στην σύγχρονη επιστημονική βιβλιογραφία για τον Γ.Κ.Π.Δ. και το πιστοποιητικό ISO 27001 αντιλαμβανόμαστε ότι υπάρχει ανάγκη για περαιτέρω ανάλυση και εμβάθυνση στο θέμα αυτό. Η σπουδαιότητα τους είναι αναμφισβήτητη, καθώς μιλάμε για το σημαντικότερο γεγονός στην ιστορία της προστασίας των προσωπικών δεδομένων, και ο υποχρεωτικός χαρακτήρας που τους έδωσε η Ε.Ε. μας οδηγεί στην ανάγκη εξαγωγής περισσότερων συμπερασμάτων.

Γνωρίζοντας τον υποχρεωτικό του χαρακτήρα θα πρέπει να εστιάσουμε στην θετική επιρροή που έχει σε μία εταιρεία και πως μπορεί να υλοποιηθεί με την βοήθεια του ISO 27001. Οι μεταρρυθμίσεις που απαιτούνται από μια εταιρεία για να εφαρμόσει

τον Γ.Κ.Π.Δ. διαφέρει από οργανισμό σε οργανισμό αλλά ο κορμός της υλοποίησης είναι ο ίδιος.

Όλα αυτά τα ζητήματα θα αναλυθούν στα κεφάλαια της παρούσας διπλωματικής εργασίας και στις επιμέρους ενότητες της. Πιο συγκεκριμένα θα ξεκινήσει η ανάλυση από την σημαντικότητα των προσωπικών δεδομένων και της ιδιωτικής ζωής, της ροής τους εντός των επιχειρήσεων και θα καταλήξει στην υλοποίηση του Γ.Κ.Π.Δ. με την βοήθεια του ISO 27001 και του ISO 27701.

3 ΟΙ 12 ΒΑΣΙΚΟΙ ΑΞΟΝΕΣ ΤΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ ISO/IEC 27001 ΚΑΙ ΤΡΟΠΟΙ ΥΛΟΠΟΙΗΣΗΣ ΤΟΥΣ

Το πρότυπο ISO/IEC 27001 δημοσιεύθηκε από τον Διεθνή Οργανισμό Τυποποίησης και τη Διεθνή Ηλεκτροτεχνική Επιτροπή. Οι οργανισμοί που πληρούν τις απαιτήσεις του προτύπου αυτού μπορούν να επιλέξουν να πιστοποιηθούν από διαπιστευμένο οργανισμό πιστοποίησης μετά την επιτυχή ολοκλήρωση ενός ελέγχου.

Οι περισσότεροι οργανισμοί διαθέτουν έναν αριθμό ελέγχων ασφάλειας πληροφοριών. Σημαντικό είναι να αναφερθεί πως χωρίς ένα Σ.Δ.Α.Π., οι έλεγχοι τείνουν να είναι ασύνδετοι μεταξύ τους, μη αποτελεσματικοί και μη επαναχρησιμοποιήσιμοι αφού έχουν εφαρμοστεί ως λύσεις σε συγκεκριμένες καταστάσεις και προβλήματα. Οι έλεγχοι ασφαλείας κατά τη λειτουργία τους συνήθως αφορούν συγκεκριμένες πτυχές της τεχνολογίας πληροφοριών ή της ασφάλειας δεδομένων, αφήνοντας τα περιουσιακά στοιχεία που δεν ανήκουν στην πληροφορική, μη προστατευμένα συνολικά σε υψηλό επίπεδο.

Το πρότυπο αυτό έχει ως βασικό στόχο την προστασία τριών πτυχών της πληροφορίας. Αυτές είναι οι ακόλουθες:

- Εμπιστευτικότητα: μόνο τα εξουσιοδοτημένα άτομα έχουν δικαίωμα πρόσβασης στις πληροφορίες.
- Ακεραιότητα: μόνο τα εξουσιοδοτημένα άτομα μπορούν να αλλάξουν τις πληροφορίες.
- Διαθεσιμότητα: οι πληροφορίες πρέπει να είναι προσβάσιμες σε εξουσιοδοτημένα άτομα όποτε χρειάζεται.

Σε αυτό το κεφάλαιο θα δούμε κάποιους από τους βασικούς άξονες της πιστοποίησης ISO 27001 καθώς και πως μπορεί να υλοποιηθεί εντός της επιχείρησης. Το πρότυπο μπορεί να αναλυθεί σε επιμέρους βασικούς ελέγχους πληροφοριών που στο πρότυπο αναφέρονται ως Παραρτήματα (Annex) :

- Πολιτικές ασφάλειας πληροφοριών (Annex A.5): Τα στοιχεία ελέγχου σε αυτό το παράρτημα περιγράφουν τον τρόπο χειρισμού των πολιτικών ασφάλειας πληροφοριών.
- Οργάνωση ασφάλειας πληροφοριών (Annex A.6): Οι έλεγχοι σε αυτό το παράρτημα παρέχουν το βασικό πλαίσιο για την εφαρμογή και λειτουργία της ασφάλειας πληροφοριών ορίζοντας την εσωτερική οργάνωση (π.χ. ρόλους, αρμοδιότητες κ.λπ.) αλλά και μέσω των οργανωτικών πτυχών της ασφάλειας πληροφοριών, όπως η διαχείριση έργων, η χρήση κινητών συσκευών και η τηλεργασία.
- Ασφάλεια ανθρώπινου δυναμικού (Annex A.7): Οι ελέγχου αυτού του παραρτήματος διασφαλίζουν ότι τα άτομα που βρίσκονται υπό τον έλεγχο του οργανισμού προσλαμβάνονται, εκπαιδεύονται και διοικούνται με ασφαλή τρόπο.
- Διαχείριση περιουσιακών στοιχείων (Annex A.8): Οι έλεγχοι αυτού του παραρτήματος διασφαλίζουν ότι τα στοιχεία ασφάλειας πληροφοριών (π.χ. πληροφορίες, συσκευές επεξεργασίας, συσκευές αποθήκευσης κ.λπ.) προσδιορίζονται, ότι έχουν καθοριστεί οι ευθύνες για την ασφάλειά τους και

πως οι άνθρωποι γνωρίζουν πώς να τα χειρίζονται σύμφωνα με προκαθορισμένη ταξινόμηση επίπεδα.

- Έλεγχος πρόσβασης (Annex A.9): Τα στοιχεία ελέγχου αυτού του παραρτήματος διασφαλίζουν ότι οι εργαζόμενοι μπορούν να έχουν πρόσβαση μόνο σε πληροφορίες που σχετίζονται με αυτούς ή που έχει δοθεί άδεια από τους ανωτέρους τους. Υπάρχει απαίτηση περιορισμού της πρόσβασης, διαχείρισης εξουσιοδοτημένων χρηστών, διαφύλαξης πληροφοριών με βάση την ευθύνη του χρήστη και αποτροπής μη εξουσιοδοτημένης πρόσβασης σε συστήματα και εφαρμογές.
- Κρυπτογραφία (Annex A.10): Στο παράρτημα αυτό υπάρχουν έλεγχοι που χρησιμοποιούνται για την διασφάλιση της κατάλληλης κρυπτογράφησης δεδομένων για την προστασία της εμπιστευτικότητας και της ακεραιότητας των δεδομένων. Δίνεται έμφαση στον τρόπο διαχείρισης των κλειδιών κρυπτογράφησης.
- Φυσική και περιβαλλοντική ασφάλεια (Annex A.11): Τα στοιχεία ελέγχου σε αυτό το παράρτημα αποτρέπουν τη μη εξουσιοδοτημένη πρόσβαση σε φυσικές περιοχές και προστατεύουν τον εξοπλισμό και τις εγκαταστάσεις από το να τεθούν σε κίνδυνο από ανθρώπινη ή φυσική παρέμβαση.
- Ασφάλεια λειτουργιών (Annex A.12): Τα στοιχεία ελέγχου αυτού του παραρτήματος διασφαλίζουν ότι τα συστήματα πληροφορικής, συμπεριλαμβανομένων των λειτουργικών συστημάτων και του λογισμικού, είναι ασφαλή και αποτρέπουν την απώλεια δεδομένων. Οι έλεγχοι χωρίζονται σε δύο ενότητες που περιγράφουν λεπτομερώς τη διαχείριση της ασφάλειας του δικτύου και την προστασία των πληροφοριών στις εγκαταστάσεις επεξεργασίας. Η πρώτη ομάδα ελέγχων ασχολείται με τη διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας αυτών των πληροφοριών, ενώ η δεύτερη ομάδα ελέγχων χειρίζεται τις πληροφορίες όταν μεταδίδονται από ένα μέρος σε άλλο είτε πρόκειται για τον οργανισμό είτε για τρίτο μέρος.
- Ασφάλεια επικοινωνιών (Annex A.13): Τα στοιχεία ελέγχου αυτής της ενότητας καλύπτουν τις απαιτήσεις ασφαλείας για εσωτερικά συστήματα και για υπηρεσίες σε δημόσια δίκτυα, διασφαλίζοντας την ασφάλεια των πληροφοριών του οργανισμού σε ολόκληρο τον κύκλο της ζωής τους.
- Απόκτηση, ανάπτυξη και συντήρηση συστήματος (Annex A.14): Οι έλεγχοι σε αυτήν την ενότητα διασφαλίζουν ότι η ασφάλεια των πληροφοριών λαμβάνεται υπόψη κατά την αγορά νέων πληροφοριακών συστημάτων ή την αναβάθμιση των υπαρχόντων.
- Σχέσεις με προμηθευτές (Annex A.15): Τα στοιχεία ελέγχου αυτής της ενότητας χωρίζονται σε δύο υποενότητες που περιγράφουν λεπτομερώς τις αλληλεπιδράσεις μεταξύ οργανισμών και τρίτων. Στην πρώτη εξετάζονται ποιες πληροφορίες περιουσιακών στοιχείων είναι διαθέσιμες σε τρίτους και ποιες πληροφορίες χρειάζονται ειδική προστασία. Στην δεύτερη χειρίζονται το επίπεδο υπηρεσιών και την ασφάλεια των πληροφοριών έτσι ώστε να είναι διαθέσιμες αρκετές πληροφορίες στους προμηθευτές προκειμένου να διατηρείται η παροχή υπηρεσιών σύμφωνα με τις συμφωνίες των προμηθευτών.
- Διαχείριση συμβάντων ασφάλειας πληροφοριών (Annex A.16): Οι έλεγχοι σε αυτήν την ενότητα παρέχουν ένα πλαίσιο για τη διασφάλιση της σωστής επικοινωνίας και χειρισμού περιστατικών και συμβάντων ασφάλειας, ώστε να μπορούν να επιλυθούν έγκαιρα. Καθορίζουν επίσης τον τρόπο διατήρησης των αποδεικτικών στοιχείων. Τέλος, μέσω των περιστατικών που επιλύνονται

πραγματοποιείται και η μελλοντική αποτροπή όμοιων περιστατικών μέσω της ανάλυσης των συμβάντων και δημιουργώντας νέες πολιτικές για την προστασία του οργανισμού.

- Πτυχές ασφάλειας πληροφοριών της διαχείρισης επιχειρησιακής συνέχειας (Annex A.17): Τα στοιχεία ελέγχου αυτής της ενότητας διασφαλίζουν τη συνέχεια της διαχείρισης της ασφάλειας πληροφοριών των επιχειρηματικών διαδικασιών σε περίπτωση διακοπής και τη διασφάλιση της συνεχούς παραγωγικότητας και τη διαθεσιμότητα των συστημάτων.
- Συμμόρφωση (Annex A.18): Οι έλεγχοι σε αυτήν την ενότητα παρέχουν ένα πλαίσιο για την αποτροπή νομικών, νομοθετικών, κανονιστικών και συμβατικών παραβιάσεων και ελέγχουν εάν η ασφάλεια των πληροφοριών εφαρμόζεται και είναι αποτελεσματική, σύμφωνα με τις καθορισμένες πολιτικές, διαδικασίες και απαιτήσεις του προτύπου ISO 27001.

Από τα Παραρτήματα του ISO/IEC 27001 που αναφέρθηκαν θα αναπτυχθούν τα πιο σημαντικά και αυτά που έχουν άμεση σχέση με το πρότυπο ISO/IEC 27701 που θα αναλυθεί στο κεφάλαιο 4. Σημαντικό είναι να αναφερθεί πως για την ανάλυση των Παραρτημάτων του ISO/IEC 27001 έχει χρησιμοποιηθεί ως αξιόπιστη πηγή πληροφόρησης το διαδικτυακό προφίλ της εταιρείας ISMS.online. Η εταιρεία αυτή, με έδρα το Sussex, ειδικεύεται στην προσφορά απλοποιημένων, ασφαλών και βιώσιμων λύσεων για τα cloud-based συστήματα διαχείρισης των εταιρειών. Κύριο μέλημά τους είναι η ασφάλεια των πληροφοριών, η ασφάλεια του απορρήτου (security) και η συμμόρφωση των συστημάτων στις επιθυμητές για την εταιρεία πιστοποιήσεις.

3.1: Πολιτικές ασφάλειας πληροφοριών

Συνήθως τα στελέχη των εταιρειών δεν γνωρίζουν πως η ασφάλεια πληροφοριών μπορεί να βοηθήσει τον οργανισμό τους. Ο σκοπός της πολιτικής ασφάλειας πληροφοριών είναι η ανώτατη διοίκηση να ορίζει τί ακριβώς θέλει να επιτευχθεί με την ασφάλεια πληροφοριών. Ακόμα, αποτελεί ένα έγγραφο που είναι εύκολα κατανοητό από τα στελέχη και με το οποίο θα μπορούν να ελέγχουν όλα όσα συμβαίνουν εντός των Σ.Δ.Α.Π., όπως τη διαχείριση ελέγχου πρόσβασης και τα αντίγραφα ασφαλείας.

Η πολιτική ασφάλειας πληροφοριών διαφέρει από οργανισμό σε οργανισμό. Δεν αποτελεί κάτι που είναι όμοιο αλλά κάτι που είναι πλήρως τροποποιημένο στις ανάγκες της εκάστοτε εταιρείας. Σε αυτήν πρέπει να αναφέρεται ο τρόπος με τον οποίο ορίζονται οι στόχοι, καθώς και πώς εγκρίνονται και πώς αναθεωρούνται.

Η φιλοσοφία του ISO 27001 βασίζεται πάνω στον κύκλο διαχείρισης διεργασιών P.D.C.A.. Συνοπτικά, το μοντέλο αυτό αποτελείται από 4 φάσεις:

- Κατά την πρώτη φάση, PLAN, γίνεται ο ορισμός στόχων της επιχείρησης.
- Κατά την δεύτερη φάση, DO, γίνεται ο ορισμός της μέτρησης, δηλαδή μέχρι ποιο σημείο θα έχουν επιτευχθεί οι στόχοι της.
- Κατά την τρίτη φάση, CHECK, γίνεται η πραγματική μέτρηση.
- Κατά την τέταρτη φάση, ACT, γίνεται η αξιολόγηση για το εάν επιτεύχθηκαν οι στόχοι ή όχι. Αν όχι, τότε πρέπει να δράσουν με διορθωτικές κινήσεις και να ξαναγυρίσουν στην πρώτη φάση του P.D.C.A..

Κατά τον ορισμό στόχων, σύμφωνα με το πρότυπο ISO 27001, πρέπει να τεθούν τουλάχιστον δύο διαφορετικά επίπεδα. Το ένα είναι οι στόχοι ολόκληρου του Σ.Δ.Α.Π., ενώ το δεύτερο είναι οι στόχοι για κάθε έλεγχο ασφαλείας. Σε κάποιες περιπτώσεις επιχειρήσεων, όπως των πολύ μεγάλων οργανισμών, κρίνεται αναγκαίο να τεθούν επιπλέον επίπεδα στόχων, όπως επίπεδα επιμέρους οργανικών μονάδων.

Άρα, κατά την συγγραφή της πολιτικής ασφαλείας πληροφοριών πρέπει να ορίζονται μετρήσιμοι στόχοι. Για να οριστούν αυτοί πρέπει να ακολουθείται το μοντέλο S.M.A.R.T.. Κατά το μοντέλο αυτό οι στόχοι είναι συγκεκριμένοι, μετρήσιμοι, επιτεύξιμοι, σχετικοί και βασισμένοι στον χρόνο (επίκαιροι).

Εικόνα 3.1.1: *Μοντέλο ορισμού στόχων S.M.A.R.T.*

Για να γίνει κατανοητό το μοντέλο S.M.A.R.T., θα αναφερθεί παρακάτω ένα παράδειγμα που δημοσιεύτηκε στο "ISO 27001 Guide.com" με τίτλο "Information Security Objectives in ISO 27001". Μια απαίτηση στρατηγικού επιπέδου μπορεί να είναι «να διασφαλίσει ότι τα συστήματα είναι διαθέσιμα ανά πάσα στιγμή σε όσους το απαιτούν και να ελαχιστοποιηθεί ο χρόνος αδράνειας». Αυτό προφανώς δεν είναι μετρήσιμο, αλλά καθορίζει τη στρατηγική κατεύθυνση για τον οργανισμό και υποδεικνύει ότι ο χρόνος διαθεσιμότητας είναι το κλειδί. Μπορεί να υποστηριχθεί από έναν στόχο τακτικού επιπέδου που δηλώνει πως «ο χρόνος λειτουργίας του συστήματος θα διατηρείται σε διαθεσιμότητα 95% κατά τη διάρκεια του έτους και τα συστήματα θα αποκαθίστανται πλήρως εντός 4 ωρών από την απώλεια". Η ποσοστιαία διαθεσιμότητα του συστήματος μέσα σε έναν χρόνο είναι ένα απτό και μετρήσιμο στοιχείο που υποστηρίζει την επίτευξη του στρατηγικού στόχου που προαναφέρθηκε.

Οι στόχοι ασφαλείας πληροφοριών στο ISO 27001 πρέπει να οδηγούνται από την κορυφή προς την βάση. Αυτό σημαίνει πως οι στρατηγικοί στόχοι υποστηρίζονται από πολλούς τακτικούς στόχους χαμηλού επιπέδου που μπορούν να μετρηθούν. Αυτό το βλέπουμε και στο παράδειγμα που αναφέρθηκε προηγουμένως, καθώς ο τακτικός έλεγχος που γίνεται είναι η ποσοστιαία διαθεσιμότητα ανά έτος. Τα αποτελέσματα πρέπει να είναι μετρήσιμα και να υποστηρίζουν τη συνεχή βελτίωση, ενώ οι στόχοι θα πρέπει να καθορίζουν τις περιόδους μέτρησης και να επανεξετάζουν τις μετρήσεις για την υποστήριξη των στόχων ελέγχου.

Συνοπτικά, για να συντάξει κανείς μια πολιτική ασφαλείας, σύμφωνα με το ISO 27001, δεν χρειάζεται να εστιάσει στο να αναθέσει πολλούς και αναλυτικούς στόχους και η πολιτική να βγει μεγάλη σε έκταση και δύσκολη στην κατανόηση. Ο στόχος της πολιτικής είναι να πραγματοποιηθεί η σύνδεση της ανώτατης διοίκησης και των δραστηριοτήτων της επιχείρησης σχετικά με την ασφάλεια πληροφοριών με γνώμονα την στρατηγική κατεύθυνση της εταιρείας. Σύμφωνα με τον Dejan Kosutic στο άρθρο "How to structure the documents for ISO 27001 Annex A controls", για να γράψει κανείς μια πολιτική ασφάλειας πληροφοριών πρέπει να ακολουθήσει τα εξείς βήματα:

1. Να ξεκινήσει γράφοντας για τομείς όπου μπορεί να κερδίσει γρήγορες νίκες. Αυτό σημαίνει να επιλέξει μια περιοχή όπου γνωρίζει ότι θα ολοκληρώσει στο έγγραφο γρήγορα καθώς έχει πολλές και επαρκείς γνώσεις στον τομέα αυτό.

2. Να συνεχίσει με τομείς όπου έχουν μεγαλύτερους κινδύνους. Με αυτόν τον τρόπο αρχίζει να επιλύει πρώτα τα μεγαλύτερα προβλήματα που μπορεί να μην ολοκληρωθούν τόσο γρήγορα. Αυτή η προσέγγιση είναι απαραίτητη εάν η αξιολόγηση κινδύνου έχει δείξει ότι υπάρχουν μερικά πολύ μεγάλα κενά που πρέπει να λυθούν καθώς επείγουν και αποτελούν σημείο μπλοκαρίσματος για τους υπόλοιπους τομείς.
3. Στην συνέχεια να ασχοληθεί με τομείς που είναι συμβατοί με άλλα έργα που εκτελούνται στην εταιρεία. Για παράδειγμα, η εταιρεία μπορεί να εφαρμόζει βοηθητικό λογισμικό γραφείου. Σε αυτή την περίπτωση χρειάζεται να συνταχθεί η διαδικασία διαχείρισης περιστατικών, καθώς αυτή θα ρυθμίσει τον τρόπο χρήσης αυτού του λογισμικού στο πλαίσιο του ISO 27001.
4. Τέλος θα ασχοληθεί με τα έγγραφα που καλύπτουν μεγαλύτερο αριθμό στοιχείων ελέγχου, όπως για παράδειγμα την Πολιτική Αποδεκτής Χρήσης. Με αυτόν τον τρόπο θα γνωρίζει ποια στοιχεία ελέγχου καλύπτονται από έγγραφα/πολιτικές και αυτά που δεν έχουν καλυφθεί μπορούν να περιγραφθούν σε ένα έγγραφο στο τέλος.

3.2: Οργάνωση ασφάλειας πληροφοριών

Αυτή η πτυχή της πιστοποίησης ISO 27001 αφορά την εσωτερική οργάνωση της επιχείρησης καθώς ορίζει οργανωτικά όπως τους ρόλους και τις αρμοδιότητες των ατόμων. Στόχος του είναι η δημιουργία ενός πλαισίου διαχείρισης για την έναρξη και τον έλεγχο της εφαρμογής και της λειτουργίας της ασφάλειας πληροφοριών εντός του οργανισμού.

3.2.1: Ρόλοι και Ευθύνες

Ο βασικός στόχος του είναι όλες οι ευθύνες για την ασφάλεια πληροφοριών να είναι καθορισμένες και κατανεμημένες. Έτσι, βασισμένος στην πολιτική ασφάλειας των πληροφοριών (Κεφάλαιο 3.1) κατανέμει τις αρμοδιότητες και ευθύνες εντός της επιχείρησης και προσδιορίζει τις ευθύνες για την προστασία των μεμονωμένων περιουσιακών στοιχείων του οργανισμού.

Πιο γενικά, μέσα στην οργάνωση ασφάλειας πληροφοριών γίνονται τα ακόλουθα:

- Καθορίζονται και ορίζονται τα περιουσιακά στοιχεία και οι διαδικασίες ασφάλειας πληροφοριών.
- Ανατίθεται στο άτομο που είναι υπεύθυνο για κάθε περιουσιακό στοιχείο ή διαδικασία ασφάλειας πληροφοριών η ευθύνη και η λεπτομερής περιγραφή της με πλήρη γραπτή τεκμηρίωση.
- Τα επίπεδα εξουσιοδότησης καθορίζονται και τεκμηριώνονται.
- Για να είναι σε θέση να εκπληρωθούν οι ευθύνες στον τομέα της ασφάλειας πληροφοριών, τα διορισμένα άτομα θα πρέπει να είναι ικανά και ενημερωμένα για τις τελευταίες εξελίξεις στον τομέα τους.
- Τέλος, ο συντονισμός και η εποπτεία των πτυχών ασφάλειας των πληροφοριών των σχέσεων με τους προμηθευτές θα πρέπει να προσδιορίζονται και να τεκμηριώνονται.

Συνήθως οι οργανισμοί αναθέτουν σε ένα πρόσωπο να αναλάβει την θέση διαχείρισης ασφάλειας πληροφοριών για να έχει όλη αυτή την ευθύνη, να εποπτεύει και να υποστηρίζει τον προσδιορισμό των ελέγχων. Βέβαια, παραμένει στα διευθυντικά στελέχη η ευθύνη παροχής πόρων και η εφαρμογή ελέγχων. Μια κοινή πρακτική είναι

να ορίζεται ένας ιδιοκτήτης για κάθε περιουσιακό στοιχείο, ο οποίος στη συνέχεια γίνεται υπεύθυνος για την καθημερινή προστασία του.

3.2.2: Διαχωρισμός καθηκόντων

Στην συνέχεια, αυτό το παράρτημα του ISO 27001 ασχολείται με τον διαχωρισμό καθηκόντων που έχει ως σκοπό να μειώσει τις ευκαιρίες για μη εξουσιοδοτημένη ή ακούσια τροποποίηση ή κατάχρηση των περιουσιακών στοιχείων του οργανισμού. Όταν ο διαχωρισμός των καθηκόντων σε μικρούς οργανισμούς θεωρείται δύσκολος, τότε εξετάζονται άλλοι έλεγχοι όπως η παρακολούθηση των δραστηριοτήτων που αποτυπώνονται ως μέρος της αξιολόγησης και της θεραπείας κινδύνου.

Ο διαχωρισμός καθηκόντων αναφέρεται σε πρακτικές όπου οι άδειες που απαιτούνται για την ολοκλήρωση μιας διαδικασίας κατανέμονται σε πολλούς χρήστες, έτσι ώστε κανένας να μην είναι σε θέση να εκτελέσει μία διεργασία από την αρχή μέχρι και το τέλος της μόνος του, αλλά ούτε να έχει την άδεια να την ελέγξει και να την εγκρίνει ο ίδιος.

Κάθε άτομο πρέπει να αξιοποιείται εκεί που έχει τις περισσότερες γνώσεις και δυνατότητες, καθώς ο καθένας έχει διαφορετικό φάσμα γνώσεων. Σκοπός είναι να μετριαστεί ο κίνδυνος απάτης, σπατάλης και λάθους καθώς κανένα άτομο δεν μπορεί να επιβλέπει περισσότερους από έναν τύπο λειτουργιών. Χωρίς αυτόν τον διαχωρισμό σε βασικές διαδικασίες, οι κίνδυνοι είναι πολύ λιγότερο διαχειρίσιμοι.

Ένα απλό παράδειγμα είναι πως σε μία εταιρεία δεν γίνεται ένα άτομο να έχει στα χέρια του όλη την γνώση για όλα τα συστήματα, τις πορείες εργασιών κ.τ.λ.. Αυτό γίνεται καθώς αν θελήσει να "σαμποτάρει" την εταιρεία που εργάζεται τώρα για οποιονδήποτε δόλιο λόγο, τότε θα είναι εύκολο για τον ίδιο να το κάνει χωρίς να τον αντιληφθεί και να τον σταματήσει κανείς πριν γίνει η ζημιά. Αυτό θα γίνει καθώς δεν θα τον ελέγχει κάποιος, μόνο ο ίδιος θα ελέγχει τον εαυτό του έχοντας όλη την δύναμη στα χέρια του.

Κάποιοι χρήσιμοι τρόποι διαχωρισμού καθηκόντων είναι:

- Διαδοχικός διαχωρισμός: όταν μια δραστηριότητα χωρίζεται σε βήματα που εκτελούνται από διαφορετικά άτομα. Ένα παράδειγμα αποτελεί η προσθήκη ενός νέου χαρακτηριστικού σε μία εφαρμογή που χρησιμοποιούν οι πελάτες της εταιρείας. Η ανώτερη ομάδα θα αναγνωρίσει την ανάγκη αυτή και θα δώσει την εντολή και τις οδηγίες υλοποίησης στο τμήμα πληροφορικής. Κάποια άτομα θα ολοκληρώσουν την υλοποίηση μέσω προγραμματισμού και όταν τελειώσουν, τότε θα δώσουν το νέο υλοποιημένο χαρακτηριστικό σε μία άλλη ομάδα που γνωρίζει τι έπρεπε να πραγματοποιηθεί και θα ελέγξει αν υλοποιήθηκε σωστά ή όχι. Κατά τον διαχωρισμό σε βήματα, λοιπόν, οι αρμοδιότητες, ευθύνες και έλεγχοι έχουν μοιραστεί σε διαφορετικά άτομα και ομάδες.
- Ατομικός χωρισμός: όταν τουλάχιστον δύο άτομα πρέπει να εγκρίνουν μια δραστηριότητα προτού πραγματοποιηθεί. Ένα παράδειγμα για αυτόν τον διαχωρισμό είναι κατά την επιλογή εξωτερικού συνεργάτη για την εταιρεία θα πρέπει να ελέγξουν τις προτάσεις, αλλά και την τελική επιλογή που θα πραγματοποιηθεί, τουλάχιστον δύο άτομα.
- Χωρικός διαχωρισμός: όταν εκτελούνται διαφορετικές δραστηριότητες σε διαφορετικές τοποθεσίες. Ένα τέτοιο παράδειγμα είναι όταν μια εταιρεία έχει πολλά υποκαταστήματα. Κάθε υποκατάστημα έχει έναν άνθρωπο που παίρνει αποφάσεις για το υποκατάστημα που εργάζεται αλλά λογοδοτεί

στον ανώτερο που βρίσκεται στα κεντρικά κτήρια της εταιρείας για τις αποφάσεις αυτές.

- Παραγοντικός διαχωρισμός: όταν αρκετοί παράγοντες συμβάλλουν στην ολοκλήρωση της δραστηριότητας. Για παράδειγμα, από την πανδημία που ξέσπασε οι περισσότερες εργασίες μεταφέρθηκαν είτε στο υβριδικό μοντέλο εργασίας, ποσοστιαία εργασία από κοντά και ποσοστιαία εργασία από το σπίτι, είτε με εξ ολοκλήρου εργασία από το σπίτι. Κατά την τηλεργασία, για λόγους ασφαλείας, οι εταιρείες πρόσθεσαν νέες δικλίδες ασφαλείας για τους υπαλλήλους της κατά την διαδικασία πρόσβασης σε εταιρικά στοιχεία. Ένα τέτοιο παράδειγμα είναι ο έλεγχος ταυτότητας πρόσβασης δύο παραγόντων που ζητάει από τον χρήστη τον κωδικό και το όνομα χρήστη αλλά και ένα ακόμα μοναδικό κλειδί που παράγεται εκείνη την στιγμή και αποστέλλεται, λόγου χάρη, με μήνυμα στο κινητό.

3.2.3: Επαφή με τις αρχές

Ο υπεύθυνος ασφαλείας πρέπει να διατηρεί επαφή με τις αρμόδιες αρχές. Κατά την εφαρμογή των ελέγχων πρέπει να έχει υπόψη του πάντα τις νομικές ευθύνες των αρμόδιων αρχών. Όταν προσαρμόζεται ο έλεγχος πρέπει να λαμβάνονται υπόψιν οι νομικές ευθύνες για την επικοινωνία με τις αρχές, όπως η Αστυνομία, το Γραφείο του Επιτρόπου Πληροφοριών και άλλους ρυθμιστικούς φορείς, γύρω από το Γ.Κ.Π.Δ.. Η επαφή, το ποιος θα έρθει σε επικοινωνία, ή κάτω από ποιες συνθήκες και η φύση των πληροφοριών που θα δοθούν είναι προκαθορισμένες από πριν.

3.2.4: Επαφή με ομάδες ειδικών συμφερόντων

Η Ομάδα Ειδικού Ενδιαφέροντος είναι μια ομάδα ανθρώπων σε έναν οργανισμό που ως κοινό ενδιαφέρον έχουν μια συγκεκριμένη περιοχή γνώσης, μάθησης ή τεχνολογίας. Τα μέλη συνεργάζονται για να παράγουν λύσεις εντός του συγκεκριμένου τομέα και να τον βελτιώσουν. Αυτές οι ομάδες θα πρέπει να έχουν μόνο την κατάλληλη και απαραίτητη εξουσιοδότηση πρόσβασης στις πληροφορίες που χρειάζονται για να παράξουν το έργο που ανήκει στο φάσμα των γνώσεων της ομάδας.

Σε αυτό το στάδιο είναι σημαντικό να γίνει πλήρως αντιληπτό στις ομάδες ποιες συνεργάζονται και έχουν επαφές με ποιες. Μία ομάδα που εμπεριέχει προγραμματιστές, σε ορισμένες εταιρείες, πρέπει να έχει επαφές με την ομάδα ειδικού ενδιαφέροντος του εμπορικού τμήματος της εταιρείας. Αυτό γίνεται καθώς οι "εμπορικοί" θα πρέπει να έρθουν σε επαφή μαζί με τους "πληροφορικάριους" για να φτιάξουν νέα χαρακτηριστικά σε διάφορες πλατφόρμες που χρησιμοποιούν οι πελάτες της εταιρείας.

3.2.5:Ασφάλεια πληροφοριών στην διαχείριση έργων

Η ασφάλεια των πληροφοριών πρέπει να αποτελεί βασική προτεραιότητα του οργανισμό και η διαχείριση έργου να αποτελεί βασικό τομέα για αυτό. Πρέπει να υπάρχει η χρήση πλαισίων προτύπων για έργα που περιλαμβάνουν μια απλή επαναλαμβανόμενη λίστα ελέγχου για να δείξει ότι λαμβάνεται υπόψη η ασφάλεια των πληροφοριών.

Ο ελεγκτής, ο οποίος θα δώσει την έγκριση για την παροχή της πιστοποίησης ISO 27001, ελέγχει ότι όλα τα άτομα που εμπλέκονται σε έργα έχουν ως καθήκον να εξετάζουν την ασφάλεια των πληροφοριών σε όλα τα στάδια του κύκλου ζωής του έργου. Επομένως αυτό πρέπει να καλύπτεται στο μέρος της εκπαίδευσης και της ευαισθητοποίησης σύμφωνα με την Ασφάλεια Ανθρώπινου Δυναμικού.

Οι οργανισμοί συνδυάζουν την ασφάλεια πληροφοριών στην διαχείριση έργων με τις σχετικές υποχρεώσεις για προσωπικά δεδομένα και εξετάζουν την ασφάλεια βάσει σχεδιασμού μαζί με τις εκτιμήσεις επιπτώσεων προστασίας δεδομένων και παρόμοιες διαδικασίες για να αποδείξουν τη συμμόρφωση με τον Γ.Κ.Π.Δ..

3.3: Ασφάλεια ανθρώπινου δυναμικού

Αυτό το παράρτημα του ISO 27001 αναφέρεται στο ανθρώπινο δυναμικό πριν την πρόσληψή του. Πιο συγκεκριμένα, στόχος του είναι να διασφαλίσει ότι οι υποψήφιοι εργαζόμενοι κατανοούν τις ευθύνες τους και είναι κατάλληλοι για τους ρόλους για τους οποίους εξετάζονται. Επίσης ,καλύπτει τι συμβαίνει όταν αυτά τα άτομα φεύγουν από την εταιρεία ή αλλάζουν ρόλους εντός της επιχείρησης. Αυτό το κομμάτι αποτελεί πολύ σημαντικό μέρος του Σ.Δ.Α.Π. κατά την πιστοποίηση ISO 27001.

3.3.1: Διαλογή

Έπειτα από την συλλογή των βιογραφικών και πριν την πρόσληψη των υποψήφιων εργαζομένων, πάντα πρέπει να γίνεται επαλήθευση ιστορικού και έλεγχος ικανοτήτων σε όλους. Αυτά πρέπει να εκτελούνται σύμφωνα με τους σχετικούς νόμους, κανονισμούς και δεοντολογία και πρέπει να είναι ανάλογα με τις επιχειρηματικές απαιτήσεις, την ανάγκες για τον εκάστοτε ρόλο που πρέπει να καλυφθεί, τη διαβάθμιση των πληροφοριών στις οποίες θα προσπελαστούν και τους αντιληπτούς κινδύνους που συνδέονται.

Για παράδειγμα, το προσωπικό που έχει πρόσβαση σε περιουσιακά στοιχεία υψηλότερου επιπέδου, όπως οι λογιστές, ενέχουν μεγαλύτερο κίνδυνο και υπόκεινται σε πολύ πιο αυστηρούς ελέγχους από το προσωπικό που έχει πρόσβαση μόνο σε δημόσιες πληροφορίες ή χειρίζεται περιουσιακά στοιχεία με περιορισμένη απειλή, όπως το προσωπικό των τηλεφωνικών κέντρων.

Η εφαρμογή επαρκών και αναλογικών ελέγχων ανθρώπινου δυναμικού σε όλα τα στάδια της απασχόλησης συμβάλλει στη μείωση της πιθανότητας τυχαίων ή κακόβουλων απειλών. Πρέπει να υπάρχει μια διαδικασία ελέγχου με σαφείς διαδικασίες που εφαρμόζονται με συνέπεια κάθε φορά, ώστε να αποφευχθεί ακόμα και ο τυχόν κίνδυνος προτίμησης ατόμου με μη αντικειμενικό τρόπο ή να υπάρχει προκατάληψη προς τον υποψήφιο που θα οδηγήσει στην μη επιλογή του για την διαθέσιμη θέση εργασίας. Στην ιδανική περίπτωση, αυτό θα ευθυγραμμιστεί με τη συνολική διαδικασία πρόσληψης του οργανισμού.

Με λίγα λόγια, πρέπει να υπάρχουν σαφείς οδηγίες για τον τρόπο επιλογής του προσωπικού και με αντικειμενικά κριτήρια. Ακόμα, να ελέγχεται πως ο υποψήφιος για εργασία είναι όντως η σωστή επιλογή της επιχείρησης για την θέση αυτή μέσω της εξακρίβωσης και επαλήθευσης του βιογραφικού σημειώματος του.

3.3.2: Όροι και προϋποθέσεις απασχόλησης

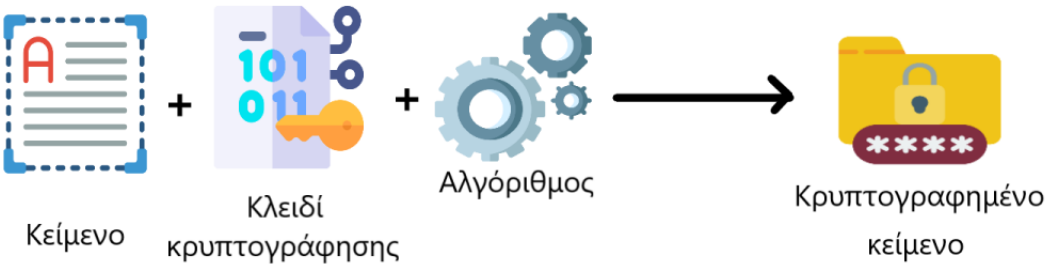
Η σύναψη συμφωνίας απασχόλησης πρέπει να αναφέρει τις ευθύνες των εργαζόμενων αλλά και του οργανισμού για την ασφάλεια των πληροφοριών. Αυτές οι συμφωνίες είναι ένα καλό σημείο για να τεθούν βασικές, γενικές και ατομικές ευθύνες για την ασφάλεια των πληροφοριών, καθώς έχουν νομική βαρύτητα.

Ο καλύτερος τρόπος για μια εταιρεία να είναι σίγουρη πως είναι πλήρως καλυμμένη νομικά έναντι των εργαζομένων της είναι να συνεργάζεται ή να έχει την δική της ομάδα δικηγόρων ανθρώπινου δυναμικού. Αυτή η πράξη είναι πολύ σημαντική, καθώς οι συνέπειες για λανθασμένες συμβάσεις εργασίας από την άποψη

της ασφάλειας πληροφοριών μπορεί να οδηγήσουν σε δαπανηρές και χρονοβόρες καταστάσεις.

3.4: Κρυπτογραφία

Η κρυπτογράφηση είναι μία διαδικασία που ανακατεύει τα δεδομένα που εισάγονται και δίνει ως αποτελέσματα ένα διαφορετικό σε σχέση με το αρχικό κείμενο. Για να προκύψει αυτό το διαφορετικό κείμενο χρησιμοποιείται κάποιο κλειδί κρυπτογράφησης και αποκρυπτογράφησης για να παραχθεί το κρυπτογραφημένο μη αναγνώσιμο κείμενο και το αρχικό αναγνώσιμο κείμενο αντίστοιχα.



Εικόνα 3.4.1: *Παράδειγμα κρυπτογράφησης*

Εικόνα 3.4.2: *Παράδειγμα αποκρυπτογράφησης*

Ο στόχος των κρυπτογραφικών ελέγχων είναι να εξασφαλιστεί η σωστή και αποτελεσματική χρήση της κρυπτογραφίας για την προστασία του απορρήτου, της γνησιότητας αλλά και της ακεραιότητας των πληροφοριών. Παραδείγματα χρήσης κρυπτογράφησης αποτελεί η προστασία πληροφοριών που εμπεριέχουν ευαίσθητες πληροφορίες, οι οποίες είτε αποθηκεύονται είτε μεταδίδονται, αλλά και η χρήση πιστοποιητικών ψηφιακής υπογραφής.

Το ISO 27001 δεν αναφέρει ρητά τη χρήση κρυπτογράφησης, ενώ το ISO 27002 την θεωρεί απαραίτητη. Αυτό γίνεται καθώς το ISO 27001 εστιάζει στην διαδικασία και όχι σε συγκεκριμένους ελέγχους και πολιτικές. Το ISO 27002 αναφέρει πως πρέπει να αναπτυχθεί ένα σύστημα κρυπτογράφησης, ενώ το ISO 27001 αναφέρει πως πρέπει να υπάρχει μια ομάδα ασφάλειας πληροφοριών. Ως αποτέλεσμα αυτών των δύο αρχών, οι περισσότερες ομάδες αναγνωρίζουν ως αδυναμία την μη ύπαρξη κρυπτογραφίας και υιοθετούν ένα σύστημα κρυπτογραφικών ελέγχων για να μετριάζουν τον συγκεκριμένο κίνδυνο. Για αυτό τον λόγο, συνήθως, τα δύο αυτά πρότυπα πάνε μαζί και για αυτό μιλάμε για απαραίτητη κρυπτογράφηση και στο ISO 27001.

3.4.1: Πολιτική σχετικά με τη χρήση κρυπτογραφικών στοιχείων ελέγχου

Η κρυπτογράφηση και οι κρυπτογραφικοί έλεγχοι θεωρούνται υψίστης σημασίας για την ασφάλεια. Αν και μπορεί να βοηθούν, η μη σωστή χρήση ή η λανθασμένη επιλογή τεχνολογιών και τεχνικών κρυπτογράφησης ή η κακή διαχείριση

κρυπτογραφικού υλικού, δηλαδή τα κλειδιά και πιστοποιητικά, μπορεί να δημιουργήσει ευπάθειες ασφαλείας.

Αν, για παράδειγμα, ένα τμήμα της επιχείρησης θέλει να μεταδώσει σε άλλο τμήμα της επιχείρησης μια ευαίσθητη πληροφορία, τότε θα πρέπει η πληροφορία αυτή να έχει κρυπτογραφηθεί. Έτσι είμαστε σίγουροι πως η πληροφορία δεν θα φτάσει στα χέρια ανθρώπων που δεν πρέπει. Είναι κατανοητό πως αυτό οδηγεί στην επιβράδυνση της διαδικασίας καθώς προστίθεται ο χρόνος κρυπτογράφησης και αποκρυπτογράφησης. Επομένως είναι σημαντικό να ληφθούν υπόψιν όλοι οι κίνδυνοι και να εξισορροπηθούν με τους ελέγχους σε ένα επαρκές επίπεδο, ενώ παράλληλα πληρούνται οι στόχοι απόδοσης.

Κατά την συγγραφή των κρυπτογραφικών ελέγχων πρέπει πάντα να λαμβάνονται υπόψιν οι νομικές απαιτήσεις σχετικά με την κρυπτογράφηση. Για παράδειγμα, το άρθρο 13 της απόφασης 165/2011 ορίζει την υποχρέωση της εταιρείας να χρησιμοποιεί κατάλληλους αλγορίθμους και συστήματα κρυπτογράφησης για να εξασφαλίζει την προστασία των δεδομένων επικοινωνίας ή άλλων στοιχείων που μπορεί να οδηγήσουν στην αποκάλυψη της ταυτότητας του χρήστη χωρίς την συγκατάθεσή του.

Μια πολιτική για τη χρήση κρυπτογράφησης μπορεί να είναι ένα καλό σημείο αναφοράς για τον προσδιορισμό των επιχειρηματικών απαιτήσεων, για το πότε πρέπει να χρησιμοποιείται κρυπτογράφηση και τα πρότυπα που πρόκειται να εφαρμοστούν στον οργανισμό.

3.4.2: Διαχείριση κλειδιών

Κατά τον έλεγχο κρυπτογραφίας πρέπει να αναφέρεται πώς αναπτύσσονται και εφαρμόζονται τα κατάλληλα κλειδιά καθ' όλη τη διάρκεια του κύκλου ζωής τους. Για τα κλειδιά θα πρέπει να αναφέρεται ο τρόπος δημιουργίας, η διανομή, οι αλλαγές, η δημιουργία αντιγράφων ασφαλείας και η αποθήκευση του κρυπτογραφικού κλειδιού μέχρι το τέλος της ζωής τους και τον τρόπο καταστροφής τους.

Η διαχείριση του υλικού πριν υποστεί κρυπτογράφηση είναι συχνά το πιο αδύναμο σημείο για την κρυπτογράφηση και οι εισβολείς μπορεί να επιδιώξουν να επιτεθούν σε αυτό και όχι στην ίδια την κρυπτογράφηση. Ως εκ τούτου, είναι σημαντικό να υπάρχουν ισχυρές και ασφαλείς διαδικασίες γύρω από αυτό. Η αντιμετώπιση παραβιασμένων κλειδιών είναι επίσης σημαντική και, όπου χρειάζεται, πρέπει να συνδέεται και με το παράρτημα της Διαχείρισης Συμβάντων Ασφαλείας.

3.4.3: Εφαρμογή κρυπτογράφησης

Η κρυπτογράφηση για κάθε επιχείρηση είναι μοναδική. Πρέπει να είναι κοντά στις ανάγκες της και να είναι τόσο αυστηρή όσο πιο ευαίσθητα είναι τα δεδομένα που διαχειρίζεται η επιχείρηση. Άρα, δεν υπάρχει κάποιος κοινός τρόπος υλοποίησης για όλους τους οργανισμούς.

3.4.3.1: Κανόνες κρυπτογράφησης

Έχοντας κατανοήσει το πότε χρειάζεται να εφαρμόζεται η κρυπτογράφηση, ήρθε η ώρα να δούμε τους βασικούς κανόνες κρυπτογράφησης. Όλοι όσοι συμμετέχουν στην ομάδα ασφάλειας πληροφοριών ή στην ανάπτυξη ασφαλούς λογισμικού πρέπει να γνωρίζουν τους κύριους κανόνες. Αυτοί είναι οι κάτωθι, σύμφωνα με τον Sieuwert van Otterloo στο άρθρο του με τίτλο "Information security – Cryptographic controls policy example":

1. Οι εμπιστευτικές και ευαίσθητες πληροφορίες που αποθηκεύονται σε αφαιρούμενα μέσα, όπως USB, πρέπει να προστατεύονται με κρυπτογράφηση.
2. Συσκευές όπως φορητοί υπολογιστές και κινητά τηλέφωνα πρέπει να προστατεύονται με κωδικό πρόσβασης και η κρυπτογράφηση δεδομένων πρέπει να είναι ενεργοποιημένη όπου είναι διαθέσιμη.
3. Πρέπει να χρησιμοποιούνται μόνο ισχυροί κρυπτογραφικοί αλγόριθμοι.
4. Πρέπει να χρησιμοποιούνται μόνο αλγόριθμοι που έχουν δημοσιευτεί και έχουν εξεταστεί από ερευνητές.
5. Πρέπει να χρησιμοποιούνται κλειδιά κρυπτογράφησης με μεγάλο μήκος. Όταν αυτό δεν γίνεται, τότε πρέπει να είναι γνωστοί οι κίνδυνοι των μικρού μήκους κλειδιών. Αν επιτρέπεται από τον αλγόριθμο κρυπτογράφησης να ορίσουμε το ελάχιστο μήκος κλειδιού, τότε μπορεί να επιλεχθεί το επιθυμητό μήκος του.
6. Τα κλειδιά πρέπει να δημιουργούνται με ασφάλεια, να αποθηκεύονται με ασφαλή τρόπο και να καταστρέφονται όταν δεν χρειάζονται πλέον.
7. Στα κλειδιά κρυπτογράφησης δεν πρέπει να έχουν πρόσβαση πολλά άτομα για να αποφευχθεί η γνωστοποίηση των κλειδιών σε τρίτους όταν οι άνθρωποι που γνωρίζουν τα κλειδιά εγκαταλείπουν τον οργανισμό.
8. Τα συμμετρικά κλειδιά αλγορίθμου και τα ιδιωτικά κλειδιά είναι σαν κωδικοί πρόσβασης και δεν πρέπει ποτέ να επαναχρησιμοποιούνται, ενώ πρέπει να αλλάζονται τουλάχιστον ετησίως.
9. Όλα τα κλειδιά πρέπει να δημιουργούνται τυχαία χρησιμοποιώντας μια ασφαλή γεννήτρια τυχαίων αριθμών και δεν πρέπει να αποθηκεύονται στον πηγαίο κώδικα.
10. Όταν προστίθεται ή αλλάζει κάποια λειτουργία που βασίζεται στην κρυπτογραφία στον πηγαίο κώδικα, τότε ένας δεύτερος προγραμματιστής πρέπει να ελέγχει τον πηγαίο κώδικα και να εξετάζει αν εφαρμόζονται οι κανόνες αυτής της πολιτικής.
11. Όταν χρησιμοποιούνται προϊόντα που εμπεριέχουν κρυπτογραφικό υλικό, πρέπει να ελέγχεται ότι το προϊόν αυτό χρησιμοποιεί ισχυρό κρυπτογραφικό αλγόριθμο και δεν έχει γνωστές αδυναμίες που κάποιος μπορεί να τις βρει εύκολα μέσω μιας αναζήτησης στο Google.
12. Η εξαγωγή κρυπτογράφησης σε ορισμένες χώρες είναι παράνομη, επειδή η τεχνολογία κρυπτογράφησης έχει ιστορικά ταξινομηθεί ως στρατιωτική τεχνολογία

3.4.3.2: Διαχείριση κλειδιών κρυπτογράφησης

Αφού αναφέρθηκαν οι βασικοί κανόνες κρυπτογράφησης, σειρά έχει να αναφερθούν οι τρόποι υλοποίησης της κρυπτογράφησης σε πιο τεχνικό επίπεδο. Οι λεπτομέρειες πρέπει να γίνονται κατανοητές από το προσωπικό πληροφορικής που ασχολείται με την εφαρμογή της κρυπτογραφίας. Ίσως το πιο σημαντικό κομμάτι της κρυπτογράφησης είναι η φύλαξη των κλειδιών. Για παράδειγμα, αν υπήρχε κάτι σημαντικό σε ένα δωμάτιο δεν θα φυλούσαμε το αντικείμενο αυτό αλλά ολόκληρο το δωμάτιο κλειδώνοντάς το και προστατεύοντας το κλειδί. Άρα, τα κλειδιά ασφαλείας είναι αυτά που θα πρέπει να φυλάσσονται. Από το στάδιο της δημιουργίας μέχρι το στάδιο της καταστροφής τους, δηλαδή σε όλο τον κύκλο της ζωής τους, θα πρέπει να είναι προστατευμένα.

Ως πρώτο στάδιο θεωρείται η δημιουργία των κλειδιών που συνήθως γίνεται μέσω κάποιου λογισμικού δημιουργίας κλειδιών ασφαλείας. Για παράδειγμα, η

γλώσσα προγραμματισμού JAVA έχει μια ισχυρή γεννήτρια τυχαίων αριθμών που μπορεί να χρησιμοποιηθεί για τη δημιουργία τους, αλλά επίσης έχει και μια πιο γρήγορη αλλά μη ασφαλή τυχαία λειτουργία που δεν προτείνεται να χρησιμοποιείται. Άλλο ένα παράδειγμα είναι η γλώσσα προγραμματισμού .NET που χρησιμοποιεί τον αλγόριθμο Aes για την δημιουργία ασύμμετρων κλειδιών ασφαλείας.

Ως δεύτερο στάδιο θεωρείται η αποθήκευση των κλειδιών. Όπως προείπαμε, η αποθήκευση των κλειδιών ασφαλείας δεν πρέπει να γίνεται στον πηγαίο κώδικα. Στον πηγαίο κώδικα πρέπει να καλούνται ως μεταβλητές και να χρησιμοποιούνται. Πρέπει να αποθηκεύονται με τέτοιο τρόπο ώστε η πρόσβαση να είναι περιορισμένη. Το Microsoft Technet προτείνει ειδικές συσκευές για ορισμένα κλειδιά υψηλής αξίας. Το Hashicorp Vault και το Barbican είναι μια λύση OSS για τη διαχείριση κλειδιών.

Τέλος, ακολουθεί το στάδιο της καταστροφής τους καθώς για λόγους ασφαλείας αυτά τα κλειδιά πρέπει να ανανεώνονται τακτικά. Αυτό σημαίνει πως καταστρέφονται και την θέση τους παίρνουν νέα κλειδιά που έχουν δημιουργηθεί από τον αλγόριθμο για τον ίδιο ακριβώς λόγο.

3.4.3.3: Επιλογή τύπου κρυπτογράφησης

Η επιλογή τρόπου κρυπτογράφησης θεωρείται σημαντική καθώς διαφέρει ανάλογα με τις ανάγκες της εταιρείας. Πριν την επιλογή του τρόπου κρυπτογράφησης πρέπει να έχει γίνει κατανοητό για ποιον λόγο χρησιμοποιείται ο κάθε τύπος κρυπτογράφησης.

Η συμμετρική και ασύμμετρη κρυπτογράφηση βοηθά στην εμπιστευτικότητα. Ένας συμμετρικός αλγόριθμος κρυπτογράφησης χρησιμοποιεί ένα κλειδί για να μετατρέψει ένα απλό κείμενο σε ένα κρυπτογραφημένο. Το κρυπτογραφημένο κείμενο δεν είναι αναγνώσιμο από κάποιον που δεν έχει πρόσβαση στο κλειδί. Ένας αλγόριθμος ασύμμετρης κρυπτογράφησης χρησιμοποιεί ένα ζεύγος κλειδιών που αποτελείται από ένα τμήμα δημόσιου κλειδιού και ένα τμήμα ιδιωτικού κλειδιού. Ο αλγόριθμος παίρνει το μέρος του δημόσιου κλειδιού και ένα απλό κείμενο για να δημιουργήσει ένα κρυπτογραφημένο κείμενο. Το κρυπτογραφημένο κείμενο είναι κατανοητό μόνο από αυτούς που έχουν το τμήμα του ιδιωτικού κλειδιού.

Οι λειτουργίες κατακερματισμού και οι ψηφιακές υπογραφές βοηθούν στην ακεραιότητα. Μια συνάρτηση κατακερματισμού παίρνει ένα μεγάλο απλό κείμενο και υπολογίζει ένα μικρό κατακερματισμό ή δακτυλικό αποτύπωμα. Οποιοσδήποτε έχει το απλό κείμενο μπορεί να υπολογίσει το ίδιο δακτυλικό αποτύπωμα. Εάν δεν έχει το απλό κείμενο, δεν είναι δυνατό να ανακαλύψει τίποτα για το απλό κείμενο μόνο μέσω του δακτυλικού αποτυπώματος. Οι αλγόριθμοι ψηφιακής υπογραφής χρησιμοποιούν ένα ζεύγος κλειδιών που αποτελείται από ένα τμήμα δημόσιου κλειδιού και ένα τμήμα ιδιωτικού κλειδιού. Ο αλγόριθμος παίρνει το μέρος του ιδιωτικού κλειδιού και ένα απλό κείμενο για να δημιουργήσει ένα αρχείο ψηφιακής υπογραφής. Οποιοσδήποτε έχει το δημόσιο κλειδί και το απλό κείμενο μπορεί να ελέγξει την εγκυρότητα της υπογραφής. Δεν είναι δυνατή η δημιουργία έγκυρης υπογραφής χωρίς το τμήμα του ιδιωτικού κλειδιού.

Όταν και οι δύο ιδιότητες είναι σημαντικές, συχνά απαιτείται συνδυασμός αυτών των τύπων κρυπτογράφησης.

3.4.3.4: Επιλογή αλγορίθμου

Είναι πολύ σημαντικό να διαλέγεται ένας επιστημονικά αποδεδειγμένος αλγόριθμος. Όσο πιο γνωστός, τόσο πιο αξιόπιστος. Ισχυροί αλγόριθμοι έχουν δοκιμαστεί από εμπειρογνώμονες κρυπτογράφησης και είναι δύσκολο να παραβιαστούν ακόμη και από αποφασισμένους εισβολείς. Πριν την επιλογή του αλγορίθμου, καλό θα ήταν να γίνει κάποια αναζήτηση στο Google και να βρεθούν, αν

υπάρχουν, οι αδυναμίες του. Μόνο όταν γνωρίζει κανείς τα τρωτά του σημεία μπορεί να αποφασίσει αν ταιριάζει στις ανάγκες του.

Η επιλογή αλγορίθμου γίνεται με βάση ποιόν τύπο κρυπτογράφησης θέλει η εκάστοτε εταιρεία να κάνει, με βάση τις ανάγκες της. Στον παρακάτω πίνακα θα δούμε τους πιο γνωστούς αλγορίθμους ανά τύπο κρυπτογράφησης.

Τύπος κρυπτογράφησης	**Προτεινόμενοι Αλγόριθμοι**
Ασύμμετρος	AES, RC6, Serpent, Twofish
Συμμετρικός	RSA, Elliptic Curve
Συνάρτηση κατακερματισμού	SHA2
Ψηφιακές υπογραφές	RSA, DSA, ECDSA

Πίνακας 3.4.3.4.1: *Αλγόριθμοι κρυπτογράφησης ανά τύπο κρυπτογράφησης*

Οι συστάσεις που γίνονται βασίζονται στο ερευνητικό άρθρο της ENISA.

3.5: Ασφάλεια επικοινωνιών

Η ασφάλεια επικοινωνιών αφορά τη διαχείριση της ασφάλειας δικτύου και στόχος της είναι να διασφαλίζει την προστασία των πληροφοριών εντός όλων των συστημάτων που χρησιμοποιούνται από την επιχείρηση.

3.5.1: Ασφάλεια δικτύου

Στα δίκτυα που εντός τους γίνονται οι μεταφορές και επεξεργασίες πληροφοριών, πρέπει να ελέγχονται για να διασφαλίζεται η σωστή και συνεχής προστασία τους. Στους ελέγχους δικτύου πρέπει να εξετάζονται προσεκτικά όλες οι λειτουργίες της επιχείρησης. Αυτό συμβαίνει γιατί σύμφωνα με τις λειτουργίες της επιχείρησης μπορεί κανείς να αναγνωρίσει πότε και πού χρειάζεται να εφαρμόζονται οι έλεγχοι. Μέσω των λειτουργιών της επιχείρησης φαίνονται αναλυτικά οι επικοινωνίες των συστημάτων και κατ' επέκτασιν τα σημεία που πραγματοποιείται η επεξεργασία, αποθήκευση και μεταφορά των πληροφοριών.

Το πιο γνωστό μοντέλο ασφάλειας δικτύου που χρησιμοποιείται από όλες σχεδόν τις επιχειρήσεις είναι το "Firewall". Με τον όρο αυτό εννοούμε πως υπάρχει μια προστασία στα δίκτυα της επιχείρησης μέσω ενός τείχους, όπως το λέει και το όνομα της λέξης. Ο «τεχνητός τείχος» αυτός ελέγχει την εισερχόμενη και εξερχόμενη κίνηση στα δίκτυα με βάση προκαθορισμένους κανόνες ασφαλείας. Κατά αυτό τον τρόπο επιτρέπει να περάσουν τα τείχη του μόνο όσα ακολουθούν τους κανόνες ασφαλείας και εμποδίζει την είσοδο σε μη φιλικές κινήσεις

Άλλη μια, πλέον, ευρέως γνωστή ασφάλεια δικτύου είναι το VPN. Είναι ένα εικονικό ιδιωτικό δίκτυο απομακρυσμένης πρόσβασης που επιτρέπει στους χρήστες που εργάζονται εξ αποστάσεως να έχουν πρόσβαση και να χρησιμοποιούν με ασφάλεια εφαρμογές και δεδομένα που βρίσκονται στο εταιρικό κέντρο δεδομένων και στα κεντρικά γραφεία, κρυπτογραφώντας όλη την κίνηση που στέλνουν και λαμβάνουν οι χρήστες.

Γενικότερα, η ασφάλεια δικτύου βασίζεται στα τείχη προστασίας και πιο συγκεκριμένα στα τείχη προστασίας επόμενης γενιάς. Αυτά τα τείχη είναι μια πιο εξελιγμένη μορφή των κλασσικών τειχών ασφαλείας, τα οποία επικεντρώνονται στον αποκλεισμό επιθέσεων κακόβουλου λογισμικού.

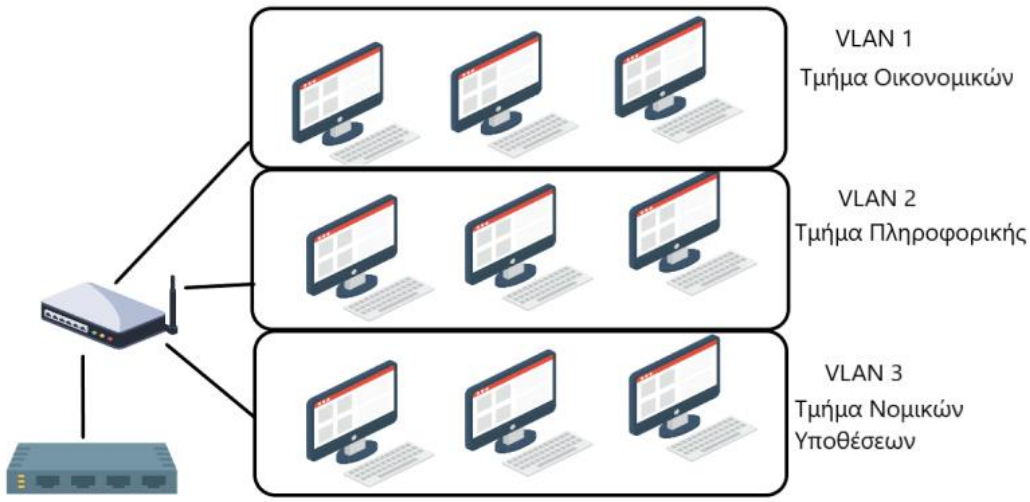
3.5.2: Ασφάλεια υπηρεσιών δικτύου - Διαχωρισμός σε δίκτυα

Ο έλεγχος αυτός αναπτύχθηκε από το ISO 27001 για την ασφάλεια των υπηρεσιών δικτύου. Όταν λέμε δίκτυα υπηρεσιών εννοούμε τη διεύθυνση IP, το DNS, την υπηρεσία email, την πρόσβαση στο διαδίκτυο, το φιλτράρισμα περιεχομένου ιστού,

τα προϊόντα ασφαλείας (π.χ. τείχη προστασίας), τα συστήματα τερματισμού VPN, τα συστήματα αποτροπής εισβολής (IPS) και τα απαραίτητα εργαλεία και προσωπικό για την υποστήριξη αυτών. Ο σκοπός του ελέγχου αυτού είναι ο εντοπισμός μηχανισμών ασφάλειας, επιπέδων υπηρεσίας και απαιτήσεις διαχείρισης που σχετίζονται με όλα τα δίκτυα υπηρεσιών.

Το ISO ορίζει κάποια χαρακτηριστικά ασφαλείας υπηρεσιών δικτύου, τα οποία είναι:

- Τεχνολογία ασφάλειας δικτύου: μπορεί να εφαρμοστεί μέσω του διαχωρισμού των δικτύων. Για παράδειγμα, η διαμόρφωση VLAN μπορεί να γίνει με δρομολογητές/διακόπτες (switch).



Εικόνα 3.5.2.1: *Ρούτερ με VLAN switch.*

Ένα ενσύρματο δίκτυο LAN συνδέει πολλούς υπολογιστές μεταξύ τους. Όπως φαίνεται στην εικόνα 3.5.2.1, το LAN μπορεί να χωριστεί μέσω του VLAN σε διαφορετικά μικρότερα δίκτυα (βλέπε VLAN1, VLAN2, VLAN3). Στα δίκτυα VLAN η μεταφορά δεδομένων πραγματοποιείται μέσω του μεταγωγέα ή αλλιώς switch/switcher και η έξοδος τον δεδομένων γίνεται με την χρήση του router/δρομολογητή. Ο διαχωρισμός σε μικρότερα δίκτυα γίνεται για να ευθυγραμμίζονται και να υποστηρίζουν τις πολιτικές ταξινόμησης πληροφοριών και να καλύπτονται οι απαιτήσεις διαχωρισμού.

- Διαμόρφωση τεχνικών παραμέτρων: μπορεί να υλοποιηθεί μέσω εικονικών ιδιωτικών δικτύων VPN που χρησιμοποιούν ισχυρούς αλγόριθμους κρυπτογράφησης. Έτσι καθιερώνεται μια ασφαλής διαδικασία για τον έλεγχο ταυτότητας όπως, για παράδειγμα, γίνεται με τα ηλεκτρονικά πιστοποιητικά.
- Μηχανισμοί περιορισμού της πρόσβασης IDS και IPS: μπορεί να εφαρμοστεί με τείχη προστασίας, όπως είδαμε και προηγουμένως, που χρησιμοποιούν συστήματα ανίχνευσης εισβολής. Από τα πιο γνωστά συστήματα ανίχνευσης εισβολής είναι το “SolarWinds Security Event Manager” που παρακολουθεί συνεχώς τις συνδέσεις για να ανιχνεύει πιθανές εισβολές στο δίκτυο του οργανισμού. Κάποια συστήματα ανίχνευσης εισβολής ανιχνεύουν μόνο τις εισβολές ενώ άλλα προσπαθούν και να τις αποτρέψουν. Σημαντικό είναι να σημειωθεί πως αυτά τα συστήματα δεν καθορίζονται από το πρότυπο ούτε αποτελούν αποτρεπτικό παράγοντα πιστοποίησης αν δεν υπάρχουν, αλλά είναι πολύ χρήσιμα και μπορούν επίσης να βοηθήσουν τα τείχη προστασίας.

3.5.3: Συνοπτική αναφορά υλοποίησης

Συμπερασματικά, αν επιθυμούμε να χτιστεί η υπηρεσία δικτύου της επιχείρησης με ασφάλεια, τότε θα πρέπει να χρησιμοποιηθούν τα παρακάτω:

- Δρομολογητές/διακόπτες,
- Τείχη προστασίας ή παρόμοιες συσκευές περιμετρικής ασφάλειας και
- IDS/IPS .

Αφού έχουν εντοπιστεί οι υπηρεσίες δικτύου και θέλουμε να πιστοποιηθεί ο οργανισμός με το ISO 27001, τότε πρέπει αυτές τις υπηρεσίες δικτύου να τις συμπεριλάβουμε στις συμφωνίες υπηρεσιών δικτύου, ή όπως είναι ευρέως γνωστές στις SLA. Οι SLA ισχύουν και για εσωτερικές υπηρεσίες που παρέχονται από το δυναμικό της επιχείρησης αλλά και από τους εξωτερικούς συνεργάτες. Το SLA είναι μια συμφωνία μεταξύ ενός παρόχου υπηρεσιών πληροφορικής και ενός πελάτη.

Για την ανάπτυξη μιας συμφωνίας παροχής υπηρεσιών δικτύου πρέπει να εξεταστούν και να καταγραφούν ποιες υπηρεσίες δικτύου δημιουργούνται, πώς προσφέρονται, τα επίπεδα υπηρεσιών και άλλα βασικά στοιχεία είτε αυτά γίνονται εντός του οργανισμού είτε από εξωτερικούς συνεργάτες. Ένα παράδειγμα τους είναι το ακόλουθο αποτυπωμένο σε εικόνα SLA από την Sophia Vergara στο άρθρο “The Ultimate Guide to Service Level Agreements (SLAs)”.

ΠΕΡΙΕΧΟΜΕΝΑ

1 ΕΙΣΑΓΩΓΗ 5
1.1 Ο σκοπός του Service Level Agreement 5
1.2 Σκοπός 5
1.3 Ιστορικό 5
1.4 Εμπλεκόμενες ομάδες 5
1.5 Παραδοχές 5
1.6 Ρόλοι και ευθύνες 5
1.7 Επικοινωνία 5
2 ΛΕΠΤΟΜΕΡΕΙΕΣ ΥΠΗΡΕΣΙΩΝ 5
2.1 Απαιτήσεις 5
2.2 Service Level Expectations 5
2.3 Ενέργειες κλιμάκωσης/προβλήματος 6
2.4 Service πάροχος / Service αποδέκτης 6
2.5 Απόδοση 6
2.6 Συμφωνηθέντα αλλαγή διενεργειών 6
3 ΣΥΜΦΩΝΗΘΕΝΤΑ 7

Εικόνα 3.5.3: *Παράδειγμα απαιτήσεων για την δημιουργία ενός SLA*

Από την εικόνα 3.5.3 καταλαβαίνουμε ότι το SLA είναι κάποιο είδος εγγράφου που σε αυτό γίνονται οι συμφωνίες μεταξύ 2 ή περισσοτέρων ομάδων. Καθώς οι ανάγκες της κάθε ομάδας αλλά και οι υποχρεώσεις τους μπορεί να αλλάξουν, στην πρώτη του σελίδα αναγράφονται οι προηγούμενες εκδόσεις αλλά και η πιο πρόσφατη. Έτσι, σαν επόμενο βήμα πρέπει να μετατραπεί αυτός ο πίνακας σε έγγραφο της μορφής του SLA που θα αναγράφονται σε αυτό τα συμφωνημένα μεταξύ των δύο ομάδων για τους τομείς που φαίνονται στην εικόνα 3.5.3. Οι μηχανισμοί ασφάλειας, τα επίπεδα υπηρεσιών και οι απαιτήσεις διαχείρισης όλων των υπηρεσιών δικτύου πρέπει να προσδιορίζονται και να περιλαμβάνονται στο SLA.

Για τους μηχανισμούς ασφαλείας που περιλαμβάνονται στο SLA, η επιλογή θα μπορούσε να βασίζεται στα αποτελέσματα της αξιολόγησης κινδύνου χρησιμοποιώντας τους ελέγχους ασφαλείας των παραρτημάτων του ISO 27001, ή ακόμα και χρήση των επαφών του οργανισμού με ομάδες ειδικών συμφερόντων για

συγκεκριμένα περιβάλλοντα, όπου θα μπορούσε να χρειαστεί η εφαρμογή συγκεκριμένων κανονισμών.

Με απλά λόγια, ο οργανισμός θα πρέπει να περιλαμβάνει στο SLA όλα τα μέτρα ασφαλείας που λαμβάνει προκειμένου να διασφαλίσει τις υπηρεσίες δικτύου του. Για την απόκτηση της πιστοποίησης ISO, ο αρμόδιος ελεγκτής θέλει να δει ότι ο σχεδιασμός και η υλοποίηση των δικτύων λαμβάνει υπόψιν τόσο τις επιχειρηματικές απαιτήσεις όσο και τις απαιτήσεις ασφάλειας, επιτυγχάνοντας μια ισορροπία που είναι επαρκής. Ακόμα ζητάει, αποδεικτικά στοιχεία όλων όσων προειπώθηκαν αλλά και αποδείξεις αξιολόγησης κινδύνου.

3.6: Διαχείριση συμβάντων ασφάλειας πληροφοριών

Σε αυτό το παράρτημα του ISO 27001 αναγράφεται αναλυτικά ο τρόπος διαχείρισης συμβάντων και αδυναμιών ασφάλειας πληροφοριών. Ο σκοπός του είναι να διασφαλίσει μια αποτελεσματική προσέγγιση στον κύκλο ζωής συμβάντων σε περίπτωση εμφάνισης μη προσδοκώμενου συμβάντος.

Η εκάστοτε εταιρεία πρέπει να είναι προετοιμασμένη για τέτοιες περιπτώσεις και όχι να βρεθεί απροετοίμαστη αντιμέτωπη με μία τέτοια κατάσταση, που θα πρέπει να την λύσει εκείνη την στιγμή χωρίς κάποια εγγεγραμμένη διαδικασία. Όταν αναφερόμαστε σε μη προσδοκώμενα συμβάντα εννοούμε τα συμβάντα, διαδικασίες και ενέργειες που μπορεί να δει η επιχείρηση και τα οποία δεν είναι τα αποδεκτά. Ένα παράδειγμα μπορεί να αποτελέσει η προσπάθεια εισβολής κάποιου στο “Firewall” με μη αποδεκτή μορφή, σύμφωνα με τους κανόνες της επιχείρησης. Φυσικά το “Firewall” θα τον εμποδίσει να εισβάλει, αλλά η εταιρεία θα πρέπει στην συνέχεια να κάνει κάποιες επιπλέον διερευνητικές ενέργειες για να δει από που προέρχεται αυτό και πως μπορεί να αποκλείσει στο μέλλον άλλη πιο εξελιγμένη προσπάθειά του.

Η διαχείριση συμβάντων ασφαλείας είναι πολύ σημαντική για την πιστοποίηση ISO 27001 καθώς δείχνει πως η επιχείρηση είναι έτοιμη να λύσει οποιοδήποτε πρόβλημα στα Σ.Δ.Α.Π. που μπορούν να εμφανιστούν.

Μέσα σε αυτή την ενότητα πρέπει να περιγράφεται με απλά λόγια η διαδικασία αντιμετώπισης όταν έχει συμβεί κάποια μορφή απώλειας σχετικά με την εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα. Οι διαδικασίες για τον σχεδιασμό αντιμετώπισης περιστατικών, συμβάντων και αδυναμιών πρέπει να έχουν καθοριστεί σαφώς πριν συμβεί ένα περιστατικό και να έχουν εγκριθεί από την ηγεσία της επιχείρησης.

3.6.1: Υπεύθυνος διαχείρισης συμβάντων

Ένα άτομο θα πρέπει να είναι υπεύθυνο για την αντιμετώπιση του συμβάντος ασφαλείας ή αδυναμίας και την αποκατάσταση ενός κανονικού επιπέδου ασφάλειας. Αυτό το άτομο θα πρέπει να συλλέγει αποδεικτικά στοιχεία το συντομότερο δυνατόν μετά την αναφορά του περιστατικού και να διεξάγει έρευνα ανάλυσης ασφάλειας. Αυτή η διαδικασία έχει μεγάλη διάρκεια αλλά από εκεί λύνονται όλες οι απορίες σχετικά με το ποια ήταν η βασική αιτία για το τί συνέβη, το ποιος εμπλέκεται καθώς και άλλες σημαντικές πληροφορίες που θα βοηθήσουν στην αναγνώριση του περιστατικού, στην απονομή ευθυνών και στην μελλοντική αποτροπή όμοιων συμβάντων. Ακόμα, αν το πρόβλημα είναι πολύ μεγάλο, τότε αυτός θα πρέπει να επικοινωνήσει με τις αρμόδιες αρχές και να αναφέρει το συμβάν.

Μόλις επιλυθεί ένα περιστατικό, θα πρέπει να τεθεί σε κατάσταση αναθεώρησης και εκμάθησης. Σε αυτή την φάση ο υπεύθυνος θα συζητήσει τυχόν αλλαγές που απαιτούνται στο Σ.Δ.Α.Π. για να αποτρέψει παρόμοια περιστατικά στο

μέλλον. Το αρμόδιο προσωπικό πρέπει να ενημερωθεί και να επανεκπαιδευτεί, εάν αυτό απαιτείται.

Η διαδικασία αυτή αποτελεί έναν αέναο κύκλο. Με κάθε λήξη ενός περιστατικού, τότε ξεκινάει η έρευνα ενός νέου, με πρώτο στάδιο του να είναι η έρευνα, μετά η επίλυση και ανάλυσή του και τέλος η αποτροπή όμοιου περιστατικού στο μέλλον. Γενικά, ο υπεύθυνος διαχείρισης συμβάντων προσπαθεί αρχικά να αντιμετωπίσει αποτελεσματικά το συμβάν και στην συνέχεια να διασφαλίσει ότι όλες οι εμπλεκόμενες δραστηριότητες απόκρισης έχουν καταγραφεί κατάλληλα για μεταγενέστερη ανάλυση.

3.6.2: Αποδεικτικά στοιχεία

Όταν στον υπεύθυνο έχει γίνει αναφορά για περιστατικό ασφάλειας ή ο ίδιος υποπτεύεται ότι έχει πραγματοποιηθεί κάποιο, τότε θα πρέπει να ξεκινήσει προσεκτικά τη συλλογή αποδεικτικών στοιχείων και να διασφαλίσει μια καλή αλυσίδα φύλαξης του συστήματος και των αποδεικτικών, αποφεύγοντας οποιαδήποτε απειλή από κακή διαχείριση.

Τα αποδεικτικά στοιχεία αποτελούν πολύ σημαντικό σύμμαχο της επιχείρησης καθώς είναι εκείνα που θα αποδείξουν στις νομικές και πειθαρχικές αρχές πως δεν υπήρχε τέτοιο συμβάν ή ότι αν υπήρχε αντιμετωπίστηκε καταλλήλως και πως είναι έτοιμοι για τις πειθαρχικές και νομικές επιπτώσεις.

3.6.3: Εργαζόμενοι

Όλοι οι εργαζόμενοι και οι εξωτερικοί συνεργάτες πρέπει να αναφέρουν τα περιστατικά ασφάλειας στον υπεύθυνο. Είναι κάτι που θα μπορούσε να ενταχθεί και στην εκπαίδευση των εργαζομένων. Έτσι, αν έχει συμβεί ή ο εργαζόμενος πιστεύει ότι έχει συμβεί παραβίαση ασφάλειας πληροφοριών, τότε πρέπει να το αναφέρει στον διορισμένο διαχειριστή ασφάλειας πληροφοριών και στην συνέχεια να διερευνηθεί.

Τα συμβάντα ασφάλειας πληροφοριών πρέπει να αξιολογούνται και στη συνέχεια να ταξινομούνται ως συμβάντα ασφάλειας πληροφοριών και συμβάντα αδυναμιών. Αν κάποιος υπάλληλος έχει αναφέρει ένα πιθανό συμβάν, θα πρέπει να αξιολογηθεί προκειμένου να καθοριστεί η καλύτερη πορεία δράσης. Αυτή η ενέργεια πρέπει να αποσκοπεί στην ελαχιστοποίηση οποιουδήποτε συμβιβασμού σχετικά με τη διαθεσιμότητα, την ακεραιότητα ή το απόρρητο των πληροφοριών και την πρόληψη περαιτέρω περιστατικών. Στην ιδανική περίπτωση, θα έχει το ελάχιστο δυνατόν αντίκτυπο στους υπόλοιπους χρήστες των υπηρεσιών.

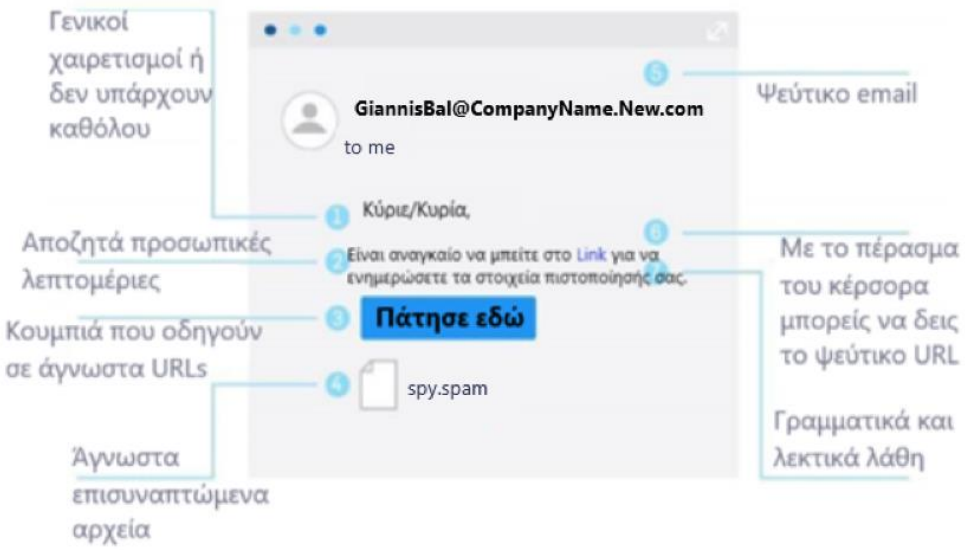
Είναι σημαντικό για τους εργαζόμενους να γνωρίζουν ότι όταν ανακαλύπτουν μια αδυναμία ασφάλειας στο εταιρικό σύστημα, δεν πρέπει να προσπαθούν να αποδείξουν αυτήν την αδυναμία. Αν προσπαθήσουν να την αποδείξουν, τότε η δοκιμή μπορεί να ερμηνευθεί ως κακή χρήση του συστήματος και παράλληλα βάζει σε κίνδυνο το σύστημα και τις αποθηκευμένες πληροφορίες του, προκαλώντας περιστατικά παραβίασης ασφαλείας.

3.6.4: Παράδειγμα

Το πιο γνωστό σε όλους παράδειγμα είναι το “Phishing attack”. Αν π.χ. σε έναν υπάλληλο έχει έρθει ένα email τέτοιου τύπου, αν είναι εκπαιδευμένος και μπορεί να αναγνωρίσει ότι δεν είναι αληθινό, τότε θα το αναφέρει στο υπεύθυνο διαχείρισης συμβάντων και αυτός θα το ερευνήσει.

Είναι σαφές πως η εκπαίδευση του προσωπικού είναι σημαντική και μπορεί να οδηγήσει στην αποτροπή του περιστατικού, εφόσον ο υπάλληλος γνωρίζει πως τα "Phishing emails" :

- Έχουν μια μορφή που υποδεικνύουν πως κάτι επείγει να γίνει.
- Συνήθως έχουν γραμματικά λάθη.
- Το email του αποστολέα προσπαθεί να φανεί επαγγελματικό αλλά με πολύ μικρά λάθη. Για παράδειγμα αν θέλει να δείξει πως είναι από κάποια τράπεζα θα έχει το όνομα της τράπεζας μέσα στο όνομα αλλά μαζί με κάτι ακόμα, π.χ. αντί για Lastname.name@alphabank.com θα γράφει Lastname.name@alphabank23.com.
- Εμπεριέχει μέσα κάποιο link που μέσα σε αυτό θα ζητάει να βάλει ο υπάλληλος κάποιο όνομα χρήστη και κωδικό για να εισέλθει σε εταιρικά στοιχεία.
- Θα ζητάνε από τον παραλήπτη του email να κατεβάσει κάποιο αρχείο μέσω του link, έτσι ώστε να εγκαταστήσει ιό ή κατασκοπικό υλικό στον υπολογιστή.



Εικόνα 3.6.4: *Γενικά χαρακτηριστικά Phishing Attack*

Στην εικόνα 3.6.4 παρουσιάζεται ένα email που αποτελεί "Phishing attack" και εμπεριέχει αυτά που προειπώθηκαν. Το απεικονιζόμενο email αποτελεί παράδειγμα τέτοιου συμβάντος που έχει δημοσιευτεί στο "Security Metrics" στο άρθρο με τίτλο " 7 Ways to Recognize a Phishing Email: Email Phishing Examples".

Αποστολέας	GiannisBal@CompanyName.New.com
Παραλήπτης	Μαζική αποστολή σε emails
Θέμα	Επείγουσα ανάγκη ανανέωσης στοιχείων
Κείμενο	Καλησπέρα σας, Παρατηρήσαμε πως έχετε να σνδεθείτε στον λογαριασμό σας εδώ και 12 μήνες. Πρέπει να μπείτε το **<u>παρακάτω link</u>** για να ανανεώσετε τα στοιχεία πιστοποίησής σας εντώς 24 ωρών αλλιώς θα διαγραφτεί ο λογαριασμός σας.
Link	CompanyName/spam.fake.com

Πίνακας 3.6.5: *Παράδειγμα Phishing email*

Αν ο υπάλληλος δεν καταλάβει πως πρόκειται για τέτοια επίθεση τότε κάποιος που δεν επιτρέπεται θα αποκτήσει πρόσβαση στα αρχεία της επιχείρησης. Με αυτό τον

τρόπο, καταλαβαίνουμε πως η εκπαίδευση του προσωπικού είναι σημαντική και για την αποτροπή συμβάντων αλλά και για την αναγνώριση και αναφορά τους.

4 ΠΙΣΤΟΠΟΙΗΣΗ ISO/IEC 27701

Το ISO/IEC 27701 επεκτείνει την έννοια της ασφάλειας πληροφοριών που περιγράφεται στην οικογένεια πιστοποιήσεων ISO/IEC 27000 και πιο συγκεκριμένα στο ISO 27001 καθώς αποτελεί μια πιστοποίηση επέκτασης απορρήτου δεδομένων. Απευθύνεται σε εταιρείες που επιθυμούν να δημιουργήσουν συστήματα για την υποστήριξη της συμμόρφωσης με τον Γ.Κ.Π.Δ. και τις απαιτήσεις απορρήτου δεδομένων. Αποτελεί έναν τρόπο απόδειξης προς τους πελάτες και εξωτερικούς συνεργάτες ότι υπάρχουν αποτελεσματικά συστήματα για την υποστήριξη της συμμόρφωσης με τον κανονισμό και τις άλλες σχετικές νομοθεσίες περί απορρήτου. Σε αυτό το σημείο θα ήταν καλό να αναφέρουμε πως ο Γ.Κ.Π.Δ. εστιάζει στην προστασία δεδομένων ενώ το ISO 27701 εστιάζει στην ιδιωτικότητα.

Για να λάβει κάποιος οργανισμός την πιστοποίηση ISO/IEC 27701 πρέπει είτε να διαθέτει ήδη την πιστοποίηση ISO 27001 είτε να εφαρμόσει το ISO 27001 και ISO 27701 μαζί ως ενιαίο έλεγχο εφαρμογής. Αυτό γίνεται καθώς το ISO 27701 είναι μια φυσική επέκταση των απαιτήσεων και των οδηγιών που ορίζονται στο ISO 27001. Ένα παράδειγμα των προαναφερθέντων είναι το δημοσιευμένο άρθρο από τον οργανισμό NQA με τίτλο “ISO/IEC 27701 IMPLEMENTATION GUIDE” που παρέχει τις ακόλουθες πληροφορίες οι οποίες δηλώνουν σε ποιους άξονες του ISO 27001 μπορεί να παράσχει επέκταση απορρήτου η χρήση του ISO 27701. Στην πρώτη στήλη του πίνακα βλέπουμε κάποιους άξονες του ISO 27001 που έχουν προαναφερθεί στο κεφάλαιο 3 και στην δεύτερη στήλη αναγράφεται πως το ISO 27701 μπορεί να προσφέρει επιπλέον ασφάλεια σε κάθε έναν από αυτούς.

Άξονες του ISO 27001	**ISO 27701 επέκταση**
Πολιτικές ασφάλειας πληροφοριών **Ασφάλεια ανθρωπίνου δυναμικού**	Ενσωμάτωση του Σ.Δ.Π.Α. στο Σ.Δ.Α.Π., συμπεριλαμβανομένων: 1. Εξοπλισμός πόρων/καθιέρωση ρόλων 2. Επικοινωνία (Εσωτερική /Εξωτερική) 3. Αναμενόμενο αποτέλεσμα 4. Έλεγχος και Καθοδήγηση 5. Συνεχής Βελτίωση του Σ.Δ.Π.Α.
Οργάνωση ασφάλειας πληροφοριών	Εφαρμογή Σ.Δ.Π.Α. και στόχοι απορρήτου
Ασφάλεια ανθρωπίνου δυναμικού	Ικανά προφίλ ατόμων που έχουν ανατεθεί σε ρόλους προστασίας της ιδιωτικής ζωής.
Ασφάλεια ανθρωπίνου δυναμικού	Επίγνωση της πολιτικής Σ.Δ.Π.Α. και του τρόπου με τον οποίο το προσωπικό συμβάλλει στη δημιουργία και τη βελτίωση του συστήματος.
Ασφάλεια ανθρωπίνου δυναμικού	Γνώση της πολιτικής του Σ.Δ.Π.Α. και προσωπική συμβολή για την χρήση και την βελτίωση του συστήματος αυτού.
Διαχείριση περιουσιακών στοιχείων	Ενεργοποίηση θεραπείας κινδύνου για το Σ.Δ.Π.Α..

Διαχείριση περιουσιακών στοιχείων	Διαδικασία αξιολόγησης κινδύνου Σ.Δ.Π.Α..
Διαχείριση περιουσιακών στοιχείων	Σχέδιο αντιμετώπισης κινδύνων Σ.Δ.Π.Α., συμπεριλαμβανομένων τροποποιήσεων σε υπάρχοντα μητρώα κινδύνου
Διαχείριση ελέγχου	Σ.Δ.Π.Α. απόδοση και ανάλυση της αποτελεσματικότητας, συμπεριλαμβανομένων: 1. Εσωτερικός Έλεγχος 2. Επιθεώρηση Διοίκησης
Κρυπτογραφία	Θέματα συνεχούς βελτίωσης Σ.Δ.Π.Α..

Πίνακας 4.1: *Επέκταση απορρήτου με την συμβολή του ISO 27701*

4.1: Τομείς υλοποίησης ISO 27701

Στο άρθρο της Svetlana A. Grishaeva με τίτλο "Development and Implementation of Privacy Information Management for Compliance with International Standard ISO 27701:2019" έχει πραγματοποιηθεί μια εκτενής έρευνα για το πως μπορεί να πραγματοποιηθεί η υλοποίηση του προτύπου αυτού.

Η εκάστοτε εταιρεία διαχειρίζεται πολλές διαδικασίες εντός του Σ.Δ.Α.Π. της σύμφωνα με τον κύκλο "Plan, Do, Check, Act" και με βάση την προσέγγιση διαχείρισης κινδύνου, όπως έχουμε δει και αναφέρει στο κεφάλαιο 3. Για την διαχείριση των ιδιωτικών πληροφοριών έχουν περιγραφεί 5 διαδικασίες.

4.1.1: Προστασία και διατήρηση πληροφορίων απορρήτου

Η προστασία και διατήρηση των πληροφοριών απορρήτου πρέπει να γίνεται από τις εταιρείες αλλά και από τους εξωτερικούς συνεργάτες τους. Στόχος είναι η προστασία των προσωπικών πληροφοριών απορρήτου από μη εξουσιοδοτημένη πρόσβαση, χρήση και επεξεργασία.

Ένα απλό παράδειγμα εξωτερικού συνεργάτη είναι τα τηλεφωνικά κέντρα. Η εταιρεία τους αποστέλλουν ένα αρχείο Excel που μέσα εμπεριέχονται τα στοιχεία των πελατών που πρέπει να επικοινωνήσουν μαζί τους. Το ερώτημα που τίθεται σε αυτό το σημείο είναι πώς θα προστατευτούν αυτά τα αρχεία. Τα αρχεία αυτά θα προστατευτούν με κάποιο είδος κρυπτογράφησης. Πριν σταλεί το αρχείο στο τηλεφωνικό κέντρο, το αρχείο αυτό μπορεί να κλειδωθεί με κάποιον γνωστό μόνο στον αποστολέα και παραλήπτη κωδικό ή να κρυπτογραφηθούν τα ευαίσθητα στοιχεία πριν σταλούν. Έτσι, όταν θα προσπαθήσει κάποιος μη εξουσιοδοτημένος να πάρει πρόσβαση στο αρχείο αυτό δεν θα μπορέσει.

Είναι σημαντικό να αναφέρουμε πως δεν είναι ασφαλές να στέλνεται ο κωδικός ξεκλειδώματος του αρχείου ή ο κωδικός αποκρυπτογράφησης σε ξεχωριστό Email από αυτό της αποστολής του Excel αρχείου προς το τηλεφωνικό κέντρο. Φυσικά, ούτε να στέλνεται στο ίδιο email. Πρέπει να αποστέλλονται με διαφορετικό τρόπο επικοινωνίας για να αποφεύγεται η πιθανότητα του να φτάσει το αρχείο σε λάθος χέρια. Μια καλή πρακτική θα ήταν να σταλεί το αρχείο Excel μέσω Email και να χρειάζεται κωδικό για να ανοιχθεί, ενώ ο κωδικός να σταλεί στον αρμόδιο/παραλήπτη, δηλαδή τον υπεύθυνο του τηλεφωνικού κέντρου, σε μήνυμα στο εταιρικό του κινητό τηλέφωνο.

4.1.2: Κοινή χρήση πληροφοριών απορρήτου

Πρέπει να εφαρμόζονται πολιτικές και διαδικασίες για την προστασία των προσωπικών δεδομένων, οι οποίες μπορούν να μεταφερθούν ως ανάγκη γνώσης. Όταν λέμε ανάγκη γνώσης εννοούμε ότι αυτές οι πληροφορίες πρέπει να δοθούν, αλλιώς δεν

θα μπορέσει να ολοκληρωθεί κάποια διαδικασία. Ένα παράδειγμα είναι η παροχή των προσωπικών στοιχείων, όπως διεύθυνση και κινητό τηλέφωνο, ενός πελάτη προς την εταιρεία ταχυμεταφορών που θα παραδώσει το δέμα στον πελάτη.

Η εταιρεία θα πρέπει να λαμβάνει υπόψη τις διαδικασίες διαχείρισης δεδομένων προμηθευτών και συνεργατών ως κριτήριο επιλογής συνεργατών. Δεν αρκεί όμως μόνο αυτό. Η εταιρεία πρέπει να παραμένει ενήμερη για το πως επεξεργάζονται από τους συνεργάτες της αυτά τα δεδομένα.

4.1.3: Διεθνείς μεταφορές προσωπικών πληροφοριών

Πλέον υπάρχει ένας πολύ σημαντικός αριθμός εταιρειών που πραγματοποιούν διαβιβάσεις προσωπικών πληροφοριών με διάφορες διεθνείς εταιρείες. Ένα παράδειγμα αυτής της λειτουργίας είναι παγκόσμιες συμβουλευτικές εταιρείες όπως η Deloitte και η Accenture που έρχονται σε επαφή αλλά και επεξεργάζονται προσωπικά δεδομένα από άλλες εταιρείες που τους έχουν δοθεί. Δεν είναι αναγκαίο η Deloitte Ελλάδος να ασχολείται με υποθέσεις που αφορούν μόνο την Ελλάδα. Οι περισσότερες διεθνές εταιρείες έχουν συνεργάτες από όλη την Ε.Ε..

Έτσι, για να ανταποκρίνονται οι εταιρείες στις απαιτήσεις απορρήτου, πρέπει να εφαρμόζουν εγκεκριμένες διαδικασίες και σχετικούς ελέγχους. Ένα παράδειγμα θα μπορούσε να αποτελεί η χρήση του VPN από τους εξωτερικούς συνεργάτες κατά την επεξεργασία των προσωπικών πληροφοριών. Κατά αυτό τον τρόπο η εταιρεία πάροχος θα κρατάει εντός της επιχείρησής της τα αρχεία αυτά και θα ελέγχει την χρήση τους ενώ ο εξωτερικός συνεργάτης παρέχει τις υπηρεσίες του.

4.1.4: Διαδικασία αλλαγής και διαγραφής πληροφοριών απορρήτου

Ο κάτοχος προσωπικών πληροφοριών έχει την δυνατότητα να αιτηθεί αλλαγή ή ακόμα και διαγραφή των δεδομένων που υπάρχουν στον οργανισμό. Η εταιρεία από την πλευρά της πρέπει να έχει προκαθορισμένες διαδικασίες για τον τρόπο διαγραφή ή επεξεργασίας των δεδομένων αυτών.

4.1.5: Διατήρηση προσωπικών δεδομένων

Η περίοδος αποθήκευσης των προσωπικών δεδομένων πρέπει να καθορίζεται ανάλογα με τις επιχειρηματικές εργασίες και να μην ξεπερνάει αυτή που έχει προκαθοριστεί από την εκάστοτε εταιρεία σύμφωνα με τον Γ.Κ.Π.Δ.. Όταν λήξει αυτή η περίοδος, η εταιρεία πρέπει να διαγράψει αυτά τα δεδομένα.

4.2: Υλοποίηση ISO 27701

Η δημιουργία αποτελεσματικής και πλήρως τεκμηριωμένης πρακτικής για την προστασία δεδομένων είναι μια από τις μεγάλες προκλήσεις για τον οργανισμό. Στο έγγραφο «Δήλωση απορρήτου» πρέπει να αναλυθούν οι πρακτικές απορρήτου που εφαρμόζονται από την εταιρεία ως προς τα δεδομένα απορρήτου. Στην «Δήλωση απορρήτου» θα πρέπει να αναγράφονται τα ακόλουθα:

- Ποιες προσωπικές πληροφορίες συλλέγονται, αποθηκεύονται ή χρησιμοποιούνται,
- Σε ποιους μπορούν να κοινοποιηθούν οι πληροφορίες (σε πελάτες, εξωτερικούς συνεργάτες και άλλους οργανισμούς) και
- Πως ο κάτοχος προσωπικών δεδομένων μπορεί να διορθώσει ή να αιτηθεί διαγραφή των προσωπικών του δεδομένων.

Η «Δήλωση απορρήτου» είναι ένα χρήσιμο έγγραφο καθώς είναι αυτό που θα δοθεί στους υποψήφιους εξωτερικούς συνεργάτες αλλά και στα άτομα που εργάζονται στην εταιρεία. Είναι ένα έγγραφο που αποτυπώνει την στάση της εταιρείας προς τα ευαίσθητα προσωπικά δεδομένα και θέτει τις κατευθυντήριες οδηγίες για όλους τους εργαζομένους αλλά και τους συνεργάτες της.

Οι επιχειρήσεις αναπτύσσονται καθημερινά. Ένα πρότυπο όπως το ISO 27701 μπορεί να δημιουργήσει την ευκαιρία για μια συνεπή προσέγγιση στην ανάπτυξη της ψηφιακής οικονομίας και ταυτόχρονα είναι αρκετά ευέλικτο ώστε να βοηθά στην προσαρμογή της επιχείρησης στις αλλαγές που πραγματοποιούνται στο εξωτερικό περιβάλλον της.

4.3: Παράδειγμα «Δήλωσης απορρήτου»

Ως παράδειγμα θα δούμε την «Δήλωση απορρήτου» της εταιρείας Euromat που είναι δημοσιευμένη στο διαδίκτυο. Αρχικά γίνεται αναφορά στον οργανισμό και στο γεγονός πως προσπαθεί πάντα να διατηρεί τα δεδομένα προστατευμένα, όπως βλέπουμε στην εικόνα 4.3.1.

Δήλωση περί Απορρήτου και Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Η Epsilon (E) Euromat Ελλάς Α.Ε., εφεξής «Euromat» είναι αφοσιωμένη στην προστασία της εμπιστευτικότητας και της ιδιωτικότητας των πληροφοριών που της παρέχονται και συμμορφώνεται με την ισχύουσα νομοθεσία για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα. Παρακαλούμε να μελετήσετε την παρούσα Δήλωση περί Απορρήτου και Προστασίας Προσωπικών Δεδομένων (εφεξής «η Δήλωση») προκειμένου να μάθετε περισσότερα σχετικά με τον τύπο των πληροφοριών που συλλέγουμε για εσάς για την εκτέλεση της μεταξύ μας σύμβασης και πώς χρησιμοποιούμε αυτές τις πληροφορίες.

Ως μέρος αυτής της θεμελιώδους υποχρέωσης, η Euromat έχει δεσμευτεί να προστατεύει και να χρησιμοποιεί κατά τον αρμόζοντα τρόπο τις προσωπικές πληροφορίες/δεδομένα που έχουν συλλεγεί μέσω των υπηρεσιών που σας παρέχει. Γενικά, ο σκοπός μας είναι να συλλέγουμε μόνο τα προσωπικά δεδομένα που παρέχονται οικειοθελώς από τους αντισυμβαλλόμενους έτσι ώστε να μπορούμε να παρέχουμε σ' αυτούς τις υπηρεσίες για τις οποίες συμβλήθηκαν.

Παρακαλούμε να μελετήσετε την παρούσα Δήλωση προκειμένου να μάθετε περισσότερα σχετικά με τον τρόπο που συλλέγουμε, αποθηκεύουμε, χρησιμοποιούμε, διαβιβάζουμε και προστατεύουμε τις πληροφορίες/προσωπικά δεδομένα που λαμβάνουμε.

Εικόνα 4.3.1: *Εισαγωγή «Δήλωσης απορρήτου»*

Στην συνέχεια αναφέρει τον τρόπο συλλογής και χρήσης των προσωπικών δεδομένων. Ο τρόπος συλλογής τους μπορεί να γίνεται είτε από την συγκατάθεση του χρήστη μέσω της εγγραφής του, για παράδειγμα κατά την παραγγελία, αλλά και από την χρήση βοηθητικών προς την εταιρεία εργαλείων για την κατανόηση της πελατειακής συμπεριφοράς του χρήστη. Αυτό το σημείο είναι που θα αναφερθεί ότι ο χρήστης «παρακολουθείται» για να του παρασχεθεί στο μέλλον η καλύτερη πελατειακή εμπειρία αλλά και για να του προταθούν προϊόντα με βάση αυτά που έχει δει ήδη, δηλαδή προϊόντα πιο κοντά στις προτιμήσεις του.

1. **Συλλογή και χρήση των Προσωπικών Δεδομένων**

1.1 Ποια δεδομένα συλλέγουμε

Λαμβάνουμε τα προσωπικά δεδομένα σας εφόσον εσείς επιλέξετε να τα παρέχετε — για παράδειγμα, εάν επικοινωνήσετε μέσω ηλεκτρονικού ταχυδρομείου ή αν επιλέξετε την τηλεφωνική επικοινωνία για την εξυπηρέτησή σας στις συμβεβλημένες υπηρεσίες. Επιπλέον και μόνο αν εσείς το επιθυμείτε θα λάβουμε από εσάς τα στοιχεία των οδηγών (ονοματεπώνυμο, περιοχή που κινούνται τα οχήματα και τηλέφωνο) με σκοπό την εισαγωγή τους στο reporting που εσείς έχετε επιλέξει και μόνο για δική σας χρήση.

Με την υπογραφή της μεταξύ μας σύμβασης και την υποβολή των προσωπικών δεδομένων σας στην Euromat, συναινείτε επίσης στη χρήση αυτών των δεδομένων σύμφωνα με την παρούσα Δήλωση. Τα προσωπικά σας δεδομένα δεν χρησιμοποιούνται για άλλους σκοπούς, εκτός αν λάβουμε την άδειά σας, ή εκτός αν κάτι τέτοιο απαιτείται ή επιτρέπεται από το νόμο ή από τις επαγγελματικές προδιαγραφές.

1.2 Η νομιμοποιητική βάση για τη χρήση των προσωπικών σας δεδομένων.

Η Euromat γενικά συλλέγει μόνον προσωπικά δεδομένα που είναι απαραίτητα προκειμένου να ικανοποιηθούν τα αιτήματά σας. Όπου αναζητούνται πρόσθετες, προαιρετικές πληροφορίες, θα ενημερωθείτε σχετικά κατά τη στιγμή της συλλογής των δεδομένων.

Η Ελληνική και κοινοτική νομοθεσία μας επιτρέπει να επεξεργαζόμαστε προσωπικά δεδομένα, εφόσον έχουμε την νόμιμη βάση να προβούμε σε αυτή την πράξη. Επίσης απαιτείται να σας γνωστοποιήσουμε τους λόγους αυτούς επεξεργασίας. Ως αποτέλεσμα, όταν επεξεργαζόμαστε τα προσωπικά σας δεδομένα, στηριζόμαστε σε μία από τις ακόλουθες περιπτώσεις επεξεργασίας:

- Εκτέλεση συμβάσεως: αυτό συμβαίνει όταν η επεξεργασία των προσωπικών σας δεδομένων είναι απαραίτητη για την εκπλήρωση των υποχρεώσεών μας που προκύπτουν από τη σύμβαση.
- Νομική υποχρέωση: αυτό συμβαίνει όταν υποχρεούμαστε να επεξεργαζόμαστε τα προσωπικά σας δεδομένα ώστε να συμμορφωθούμε με μία νομική υποχρέωση, όπως να τηρούμε αρχεία για φορολογικούς σκοπούς είτε να παρέχουμε πληροφορίες σε ένα δημόσιο φορέα ή αρχή επιβολής του νόμου.
- Έννομο συμφέρον: ενδέχεται να επεξεργαστούμε δεδομένα σχετικά με εσάς όταν έχουμε έννομο συμφέρον κατά την εκτέλεση μίας σύννομης δραστηριότητας έτσι ώστε να διασφαλίσουμε την συνέχεια της δραστηριότητας αυτής, αρκεί αυτή να μην υπερβαίνει τα συμφέροντα σας, είτε
- Η συναίνεση σας: ενδέχεται περιστασιακά να σας ζητήσουμε ειδική άδεια να επεξεργαστούμε κάποια προσωπικά σας δεδομένα, και η επεξεργασία των προσωπικών σας δεδομένων θα γίνει μόνο με αυτόν τον τρόπο, εάν συμφωνήσετε προς αυτό. Μπορείτε να αποσύρετε την συναίνεση σας οποτεδήποτε, επικοινωνώντας με την Euromat στο cs@euromat.gr

Η Euromat δεν συλλέγει «ευαίσθητα» προσωπικά δεδομένα. Παρακαλούμε να μην παρέχετε σε καμία περίπτωση ευαίσθητα δεδομένα στην Euromat, εκτός αν δια της παρούσας συναινείτε στη χρήση από την Euromat αυτών των δεδομένων για τους νόμιμους επιχειρηματικούς σκοπούς της Euromat.

1.3 Αυτόματη συλλογή Προσωπικών Δεδομένων

Η Euromat συλλέγει αυτόματα προσωπικά δεδομένα.

1.3.1 Διευθύνσεις IP

Η διεύθυνση IP είναι ένας αριθμός που αποδίδεται στον ηλεκτρονικό σας υπολογιστή κάθε φορά που αποκτάτε πρόσβαση στο διαδίκτυο. Επιτρέπει στους ηλεκτρονικούς υπολογιστές και στους υπολογιστές εξυπηρέτησης δικτύου (servers) να αναγνωρίζονται και να επικοινωνούν μεταξύ τους. Οι διευθύνσεις IP από τις οποίες φαίνεται ότι προέρχονται οι επισκέπτες μπορεί να καταγράφονται για λόγους ασφάλειας της τεχνολογίας της πληροφορίας και διάγνωσης των συστημάτων. Αυτά τα δεδομένα μπορεί επίσης να χρησιμοποιούνται σε συγκεντρωτική μορφή προκειμένου να πραγματοποιηθεί ανάλυση των τάσεων και της απόδοσης του ιστότοπου.

1.3.2 Cookies

Ενδέχεται να τοποθετούνται cookies στον υπολογιστή σας ή στην συσκευή σας με δυνατότητα σύνδεσης στο διαδίκτυο, κάθε φορά που μας επισκέπτεστε στο διαδίκτυο. Αυτό επιτρέπει στην ιστοσελίδα να θυμάται τον υπολογιστή ή τη συσκευή σας και να εξυπηρετεί περισσότερους σκοπούς.

Ένα δευτερεύον είδος cookies, τα οποία αναφέρονται ως «user-input» cookies, ενδέχεται να απαιτούνται προκειμένου να διασφαλιστεί η απαραίτητη λειτουργικότητα.

Αν και τα περισσότερα προγράμματα περιήγησης δέχονται αυτόματα τα cookies, μπορείτε να επιλέξετε να αποδεχθείτε ή όχι τα cookies μέσω των ρυθμίσεων του προγράμματος περιήγησής σας (επιλογή που βρίσκεται συχνά στο μενού Εργαλείων ή Προτιμήσεων του προγράμματος περιήγησής σας). Μπορείτε επίσης να διαγράψετε τα cookies από τη συσκευή σας οποτεδήποτε. Ωστόσο, πρέπει να γνωρίζετε ότι αν δεν αποδεχθείτε τα cookies, ενδέχεται να μην είστε σε θέση να γνωρίσετε πλήρως κάποια από τα χαρακτηριστικά του ιστότοπου μας.

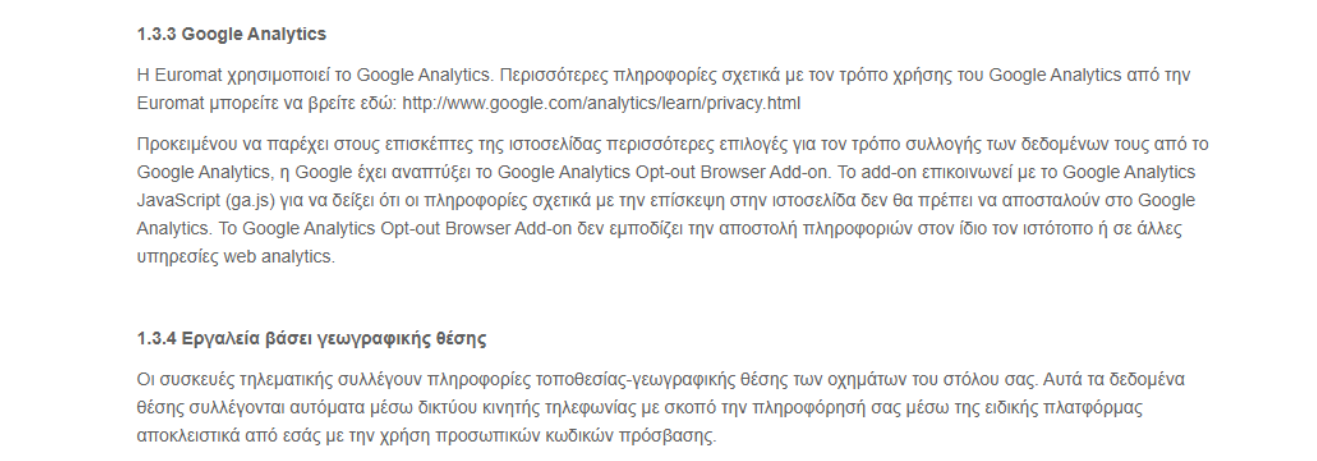
Επιπρόσθετες πληροφορίες αναφορικά με τη διαχείριση των cookies μπορείτε να βρείτε στο φάκελο «Βοήθεια» του προγράμματος περιήγησής σας ή μέσω ιστοσελίδων όπως η ιστοσελίδα www.allaboutcookies.org.

Ακολουθεί λίστα με τα είδη cookies που χρησιμοποιούμε στις ιστοσελίδες μας.

Ενδέχεται να χρησιμοποιούνται άλλα εργαλεία τρίτων και widgets στις επί μέρους ιστοσελίδες μας προκειμένου να παρέχουν πρόσθετη λειτουργικότητα. Η χρήση αυτών των εργαλείων ή των widgets ενδέχεται να εγκαταστήσει ένα cookie στη συσκευή σας για να κάνει την υπηρεσία τους πιο εύκολη στη χρήση, και να εξασφαλίσει ότι η δραστηριότητά σας εμφανίζεται σωστά στις ιστοσελίδες μας.

Τα cookies από μόνα τους δεν μας γνωστοποιούν τη διεύθυνση ηλεκτρονικού ταχυδρομείου σας ή σας ταυτοποιούν προσωπικά καθ' οιονδήποτε άλλο τρόπο. Στις αναλυτικές αναφορές μας, ενδέχεται να λαμβάνουμε πληροφορίες ταυτοποίησης συμπεριλαμβανομένων διευθύνσεων IP, αλλά μόνο για τον προσδιορισμό του αριθμού των μοναδικών επισκεπτών σε ιστοσελίδες μας και τη γεωγραφική προέλευση των επισκεπτών, και όχι για την ταυτοποίηση μεμονωμένων επισκεπτών.

Με την περιήγηση στις ιστοσελίδες μας και με την εισαγωγή των στοιχείων για την σύνδεση σας (login) ώστε να έχετε πρόσβαση σε περιοχές μόνο για εγγεγραμμένους χρήστες, συμφωνείτε ότι έχουμε τη δυνατότητα να τοποθετούμε cookies στον ηλεκτρονικό σας υπολογιστή είτε στη συσκευή σας με δυνατότητα σύνδεσης στο διαδίκτυο.



1.3.3 Google Analytics

Η Euromat χρησιμοποιεί το Google Analytics. Περισσότερες πληροφορίες σχετικά με τον τρόπο χρήσης του Google Analytics από την Euromat μπορείτε να βρείτε εδώ: http://www.google.com/analytics/learn/privacy.html

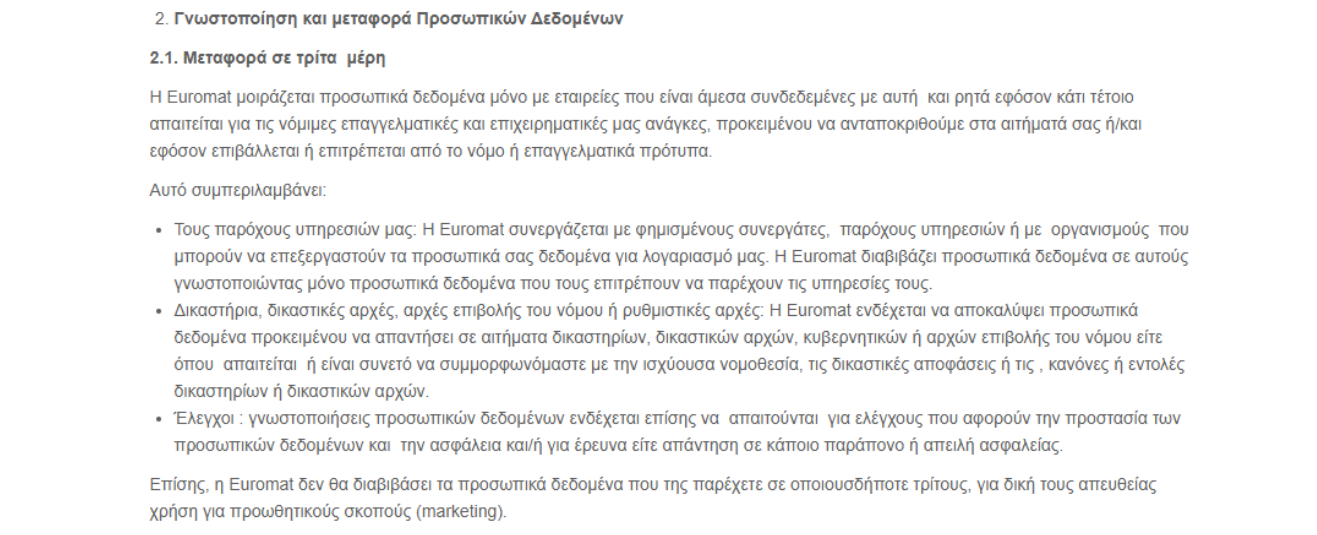
Προκειμένου να παρέχει στους επισκέπτες της ιστοσελίδας περισσότερες επιλογές για τον τρόπο συλλογής των δεδομένων τους από το Google Analytics, η Google έχει αναπτύξει το Google Analytics Opt-out Browser Add-on. Το add-on επικοινωνεί με το Google Analytics JavaScript (ga.js) για να δείξει ότι οι πληροφορίες σχετικά με την επίσκεψη στην ιστοσελίδα δεν θα πρέπει να αποσταλούν στο Google Analytics. Το Google Analytics Opt-out Browser Add-on δεν εμποδίζει την αποστολή πληροφοριών στον ίδιο τον ιστότοπο ή σε άλλες υπηρεσίες web analytics.

1.3.4 Εργαλεία βάσει γεωγραφικής θέσης

Οι συσκευές τηλεματικής συλλέγουν πληροφορίες τοποθεσίας-γεωγραφικής θέσης των οχημάτων του στόλου σας. Αυτά τα δεδομένα θέσης συλλέγονται αυτόματα μέσω δικτύου κινητής τηλεφωνίας με σκοπό την πληροφόρησή σας μέσω της ειδικής πλατφόρμας αποκλειστικά από εσάς με την χρήση προσωπικών κωδικών πρόσβασης.

Εικόνα 4.3.2: *Τρόπος συλλογής δεδομένων*

Η εταιρεία αναφέρει για ποιόν λόγο και πότε μοιράζεται τα προσωπικά δεδομένα των πελατών με τρίτες εταιρείες.



2. **Γνωστοποίηση και μεταφορά Προσωπικών Δεδομένων**

2.1. Μεταφορά σε τρίτα μέρη

Η Euromat μοιράζεται προσωπικά δεδομένα μόνο με εταιρείες που είναι άμεσα συνδεδεμένες με αυτή και ρητά εφόσον κάτι τέτοιο απαιτείται για τις νόμιμες επαγγελματικές και επιχειρηματικές μας ανάγκες, προκειμένου να ανταποκριθούμε στα αιτήματά σας ή/και εφόσον επιβάλλεται ή επιτρέπεται από το νόμο ή επαγγελματικά πρότυπα.

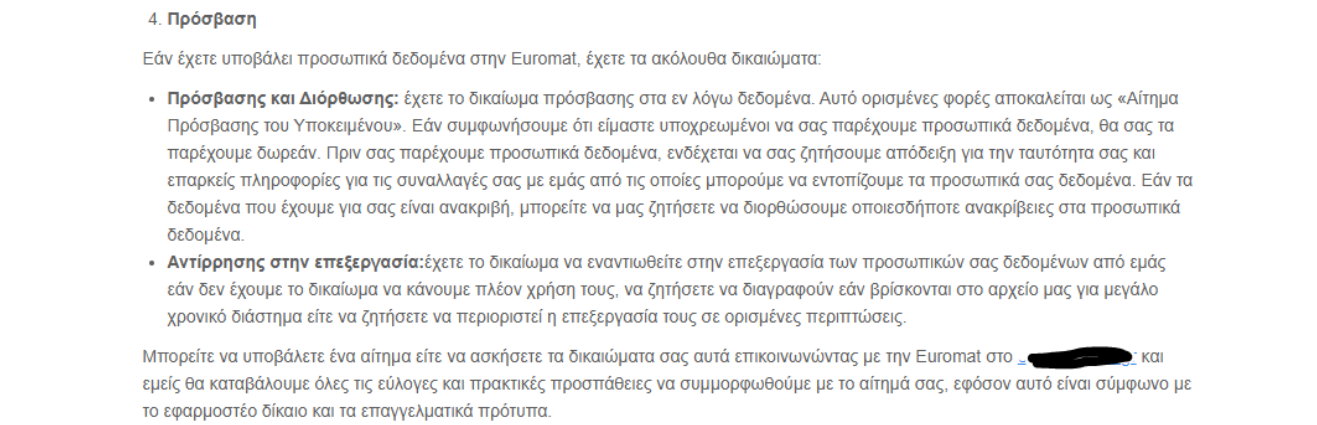
Αυτό συμπεριλαμβάνει:

- Τους παρόχους υπηρεσιών μας: Η Euromat συνεργάζεται με φημισμένους συνεργάτες, παρόχους υπηρεσιών ή με οργανισμούς που μπορούν να επεξεργαστούν τα προσωπικά σας δεδομένα για λογαριασμό μας. Η Euromat διαβιβάζει προσωπικά δεδομένα σε αυτούς γνωστοποιώντας μόνο προσωπικά δεδομένα που τους επιτρέπουν να παρέχουν τις υπηρεσίες τους.
- Δικαστήρια, δικαστικές αρχές, αρχές επιβολής του νόμου ή ρυθμιστικές αρχές: Η Euromat ενδέχεται να αποκαλύψει προσωπικά δεδομένα προκειμένου να απαντήσει σε αιτήματα δικαστηρίων, δικαστικών αρχών, κυβερνητικών ή αρχών επιβολής του νόμου είτε όπου απαιτείται ή είναι συνετό να συμμορφωνόμαστε με την ισχύουσα νομοθεσία, τις δικαστικές αποφάσεις ή τις , κανόνες ή εντολές δικαστηρίων ή δικαστικών αρχών.
- Έλεγχοι : γνωστοποιήσεις προσωπικών δεδομένων ενδέχεται επίσης να απαιτούνται για ελέγχους που αφορούν την προστασία των προσωπικών δεδομένων και την ασφάλεια και/ή για έρευνα είτε απάντηση σε κάποιο παράπονο ή απειλή ασφαλείας.

Επίσης, η Euromat δεν θα διαβιβάσει τα προσωπικά δεδομένα που της παρέχετε σε οποιουσδήποτε τρίτους, για δική τους απευθείας χρήση για προωθητικούς σκοπούς (marketing).

Εικόνα 4.3.3: *Μεταφορά δεδομένων σε τρίτες εταιρείες*

Το επόμενο θέμα που πρέπει να καλύψει είναι πως ο κάτοχος των δεδομένων απορρήτου μπορεί να αιτηθεί διόρθωση ή διαγραφή των προσωπικών στοιχείων του.



4. **Πρόσβαση**

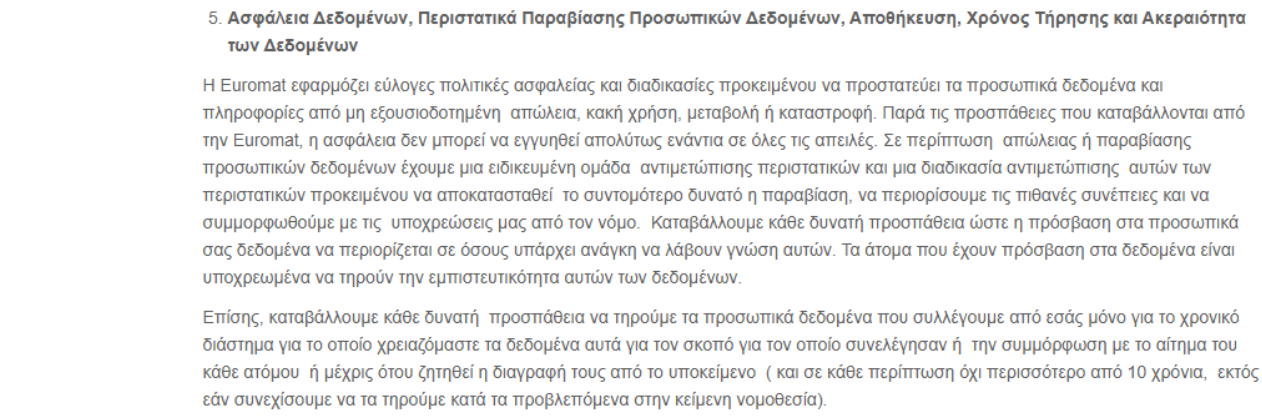
Εάν έχετε υποβάλει προσωπικά δεδομένα στην Euromat, έχετε τα ακόλουθα δικαιώματα:

- **Πρόσβασης και Διόρθωσης:** έχετε το δικαίωμα πρόσβασης στα εν λόγω δεδομένα. Αυτό ορισμένες φορές αποκαλείται ως «Αίτημα Πρόσβασης του Υποκειμένου». Εάν συμφωνήσουμε ότι είμαστε υποχρεωμένοι να σας παρέχουμε προσωπικά δεδομένα, θα σας τα παρέχουμε δωρεάν. Πριν σας παρέχουμε προσωπικά δεδομένα, ενδέχεται να σας ζητήσουμε απόδειξη για την ταυτότητα σας και επαρκείς πληροφορίες για τις συναλλαγές σας με εμάς από τις οποίες μπορούμε να εντοπίζουμε τα προσωπικά σας δεδομένα. Εάν τα δεδομένα που έχουμε για σας είναι ανακριβή, μπορείτε να μας ζητήσετε να διορθώσουμε οποιεσδήποτε ανακρίβειες στα προσωπικά δεδομένα.
- **Αντίρρησης στην επεξεργασία:**έχετε το δικαίωμα να εναντιωθείτε στην επεξεργασία των προσωπικών σας δεδομένων από εμάς εάν δεν έχουμε το δικαίωμα να κάνουμε πλέον χρήση τους, να ζητήσετε να διαγραφούν εάν βρίσκονται στο αρχείο μας για μεγάλο χρονικό διάστημα είτε να ζητήσετε να περιοριστεί η επεξεργασία τους σε ορισμένες περιπτώσεις.

Μπορείτε να υποβάλετε ένα αίτημα είτε να ασκήσετε τα δικαιώματα σας αυτά επικοινωνώντας με την Euromat στο [redacted] και εμείς θα καταβάλουμε όλες τις εύλογες και πρακτικές προσπάθειες να συμμορφωθούμε με το αίτημά σας, εφόσον αυτό είναι σύμφωνο με το εφαρμοστέο δίκαιο και τα επαγγελματικά πρότυπα.

Εικόνα 4.3.4: *Αίτηση διόρθωσης ή διαγραφής δεδομένων προσωπικού χαρακτήρα*

Το επόμενο σημαντικό σημείο είναι αυτό που αναγράφει για πόσο καιρό μπορεί να έχει η εταιρεία τα προσωπικά δεδομένα του πελάτη μετά την συναίνεσή του. Αυτό σημαίνει πως μετά το πέρας αυτού του χρονικού διαστήματος, η εταιρεία είναι υποχρεωμένη να τα διαγράψει αλλιώς θα βρεθεί αντιμέτωπη με νομικές επιπτώσεις.



5. **Ασφάλεια Δεδομένων, Περιστατικά Παραβίασης Προσωπικών Δεδομένων, Αποθήκευση, Χρόνος Τήρησης και Ακεραιότητα των Δεδομένων**

Η Euromat εφαρμόζει εύλογες πολιτικές ασφαλείας και διαδικασίες προκειμένου να προστατεύει τα προσωπικά δεδομένα και πληροφορίες από μη εξουσιοδοτημένη απώλεια, κακή χρήση, μεταβολή ή καταστροφή. Παρά τις προσπάθειες που καταβάλλονται από την Euromat, η ασφάλεια δεν μπορεί να εγγυηθεί απολύτως ενάντια σε όλες τις απειλές. Σε περίπτωση απώλειας ή παραβίασης προσωπικών δεδομένων έχουμε μια ειδικευμένη ομάδα αντιμετώπισης περιστατικών και μια διαδικασία αντιμετώπισης αυτών των περιστατικών προκειμένου να αποκατασταθεί το συντομότερο δυνατό η παραβίαση, να περιορίσουμε τις πιθανές συνέπειες και να συμμορφωθούμε με τις υποχρεώσεις μας από τον νόμο. Καταβάλλουμε κάθε δυνατή προσπάθεια ώστε η πρόσβαση στα προσωπικά σας δεδομένα να περιορίζεται σε όσους υπάρχει ανάγκη να λάβουν γνώση αυτών. Τα άτομα που έχουν πρόσβαση στα δεδομένα είναι υποχρεωμένα να τηρούν την εμπιστευτικότητα αυτών των δεδομένων.

Επίσης, καταβάλλουμε κάθε δυνατή προσπάθεια να τηρούμε τα προσωπικά δεδομένα που συλλέγουμε από εσάς μόνο για το χρονικό διάστημα για το οποίο χρειαζόμαστε τα δεδομένα αυτά για τον σκοπό για τον οποίο συνελέγησαν ή την συμμόρφωση με το αίτημα του κάθε ατόμου ή μέχρις ότου ζητηθεί η διαγραφή τους από το υποκείμενο (και σε κάθε περίπτωση όχι περισσότερο από 10 χρόνια, εκτός εάν συνεχίσουμε να τα τηρούμε κατά τα προβλεπόμενα στην κείμενη νομοθεσία).

Εικόνα 4.3.5: *Χρόνος διατήρησης δεδομένων*

Στη συγκεκριμένη «Δήλωση απορρήτου» βλέπουμε και κάποιες επιπλέον υποενότητες που θεώρησε η επιχείρηση πως ήταν σημαντικές. Κάποιες από αυτές είναι οι «Συνδέσεις με άλλους χρήστες» και «Παροχή επαγγελματικών υπηρεσιών». Τα πιο σημαντικά κομμάτια που αναφέρονται πάντα σε μία «Δήλωση απορρήτου» είναι αυτά που προαναφέραμε και στην συνέχεια προσθέτει η εκάστοτε εταιρεία ό,τι άλλο θεωρεί σημαντικό η ίδια.

4.4: Συμπεράσματα

Η πιστοποίηση ISO 27701 αποτελεί μια πιστοποίηση επέκτασης απορρήτου της ISO 27001. Ενώ η πιστοποίηση ISO 27001 εστιάζει στην προστασία των πληροφοριών, η ISO 27701 εστιάζει στην προστασία των προσωπικών δεδομένων.

Η πιστοποίηση αυτή προσφέρει επιπλέον προστασία στα ευαίσθητα δεδομένα που διαχειρίζεται η επιχείρηση και ως τρόπος υλοποίησης για μια μικρομεσαία επιχείρηση είναι η χρήση του εγγράφου «Δήλωση απορρήτου». Έτσι δηλώνει η επιχείρηση προς τους πελάτες της αλλά και υπάρχοντες και υποψήφιους συνεργάτες της το πως επεξεργάζεται αυτές τις ευαίσθητες πληροφορίες.

5 Γ.Κ.Π.Δ., ISO 27001 ΚΑΙ ISO 27701: ΣΥΣΧΕΤΙΣΗ

Όπως έχει αναφερθεί και στα προηγούμενα κεφάλαια, οι πιστοποιήσεις ISO έχουν δημιουργηθεί για να αποδεικνύουν πως μία επιχείρηση έχει συμμορφωθεί πλήρως στον Γ.Κ.Π.Δ.. Η απόδειξη ότι η επιχείρηση συμμορφώνεται στον Γ.Κ.Π.Δ. αποτελεί τον βασικό άξονα ομοιότητα ανάμεσα στον Γ.Κ.Π.Δ. και τις πιστοποιήσεις της οικογένειας ISO/IEC 27000.

Ολοένα και περισσότερες εταιρείες προσπαθούν να αυξήσουν την ασφάλεια τους για να κερδίσουν την εμπιστοσύνη των πελατών αλλά και των συνεργατών τους. Επίσης, κάθε εταιρεία θέλει να διασφαλίσει το γεγονός πως δεν θα έρθει αντιμέτωπη με κάποιο υπέρογκο ποσό προστίμου σε περίπτωση μη συμμόρφωσης με τον Γ.Κ.Π.Δ.. Έτσι, οι περισσότερες εταιρείες έχουν ξεκινήσει εδώ και κάποια χρόνια και στρέφονται προς τις πιστοποιήσεις ISO/IEC της οικογένειας 27000.

5.1: Διαφορά και ομοιότητα ISO 27001 με Γ.Κ.Π.Δ.

Το ISO 27001 είναι μια πιστοποίηση που απαιτεί από τους οργανισμούς να υιοθετήσουν μια προσέγγιση για τον τρόπο διαχείρισης ευαίσθητων δεδομένων με βάση τον κίνδυνο απώλειάς τους. Αντίθετα, ο Γ.Κ.Π.Δ. στοχεύει στην προστασία των προσωπικών δεδομένων των πολιτών της Ε.Ε. και η συμμόρφωση με αυτόν είναι υποχρεωτική για τους περισσότερους οργανισμούς που εδρεύουν στην Ε.Ε. ή που συνεργάζονται με πολίτες της Ε.Ε..

Εκεί που διαφέρουν είναι στις απαιτήσεις τους. Ο Γ.Κ.Π.Δ. περιλαμβάνει το δικαίωμα ενός καταναλωτή να αφαιρέσει τα δεδομένα του, καθώς και το δικαίωμα ελέγχου του τρόπου με τον οποίο κοινοποιούνται τα δεδομένα σε τρίτους, γνωστό και ως φορητότητα δεδομένων. Το ISO 27001 δεν περιλαμβάνει άμεσα τέτοιες διατάξεις.

Τόσο το ISO 27001 όσο και ο Γ.Κ.Π.Δ. περιστρέφονται γύρω από τον κίνδυνο και κατευθύνουν τους οργανισμούς στον εντοπισμό ορισμένων κινδύνων και ελέγχων που μπορούν να φέρουν αυτούς τους κινδύνους σε αποδεκτό επίπεδο.

Σε ό,τι αφορά τα προσωπικά δεδομένα, το ISO 27001 ενσωματώνει την κρυπτογράφηση ως μέρος της διαχείρισης της συνέχειας της επιχείρησης. Ο Γ.Κ.Π.Δ. θεωρεί τα προσωπικά δεδομένα ως κάτι που όλοι οι οργανισμοί πρέπει να προσπαθήσουν να προστατεύσουν.

5.2: ISO 27001 και ISO 27701

Οι δύο πιστοποιήσεις αυτές είναι συμπληρωματικές όπως έχει αναφερθεί και εξηγηθεί στο κεφάλαιο 4. Η ISO 27701 δεν μπορεί να υπάρξει χωρίς την εφαρμογή της ISO 27001.

5.3: Εταιρείες που ωφελούνται από τις πιστοποιήσεις ISO 27001 & 27701

Οποιαδήποτε εταιρεία έρχεται σε επαφή με ευαίσθητα δεδομένα μπορεί να πιστοποιηθεί με ISO 27001. Ένα παράδειγμα εταιρείας που έχει και τις 2 πιστοποιήσεις

είναι η "dacadoo". Η "dacadoo" είναι μια ελβετική Insurtech και Healthtech εταιρεία που πιστοποιήθηκε και με τα δύο ISO τον Μάιο του 2021.

Γενικότερα, οι εταιρείες πληροφορικής, οι εταιρείες τηλεπικοινωνιών και οι χρηματοοικονομικές εταιρείες είναι αυτές που θα επωφεληθούν περισσότερο από την χρήση ISO 27001 και 27701. Αυτό συμβαίνει επειδή πρέπει να αποδείξουν στους πελάτες τους ότι μπορούν να προστατεύσουν κάθε ευαίσθητη πληροφορία.

Σε αυτό το σημείο θα ήταν σημαντικό να αναφέρουμε πως οι δύο μεγαλύτεροι όμιλοι τηλεπικοινωνιών που εδρεύουν στην Ελλάδα, η "Cosmote" και η "Vodafone", έχουν και τις δύο πιστοποιήσεις της οικογένειας ISO 27000 που αναφέρονται σε αυτή την διπλωματική εργασία. Άλλη μια εταιρεία που έχει και τις δύο πιστοποιήσεις είναι η "Groupama Ασφαλιστική" και δραστηριοποιείται στον χώρο της παροχής ασφαλιστικών προγραμμάτων.

5.4: Συμπερασματική συσχέτιση του Γ.Κ.Π.Δ. με τις πιστοποιήσεις ISO/IEC 27001 και 27701

Τα συμπεράσματα της συσχέτισης του Γ.Κ.Π.Δ. με το ISO 27001 θα αναφερθούν στον πίνακα 5.4.1. Πιο συγκεκριμένα, θα δούμε πως τα άρθρα του Γ.Κ.Π.Δ. συνδέονται με τα Παραρτήματα του ISO/IEC 27001. Βασική πηγή για αυτή την συσχέτιση αποτελεί το άρθρο «GDPR V ISO 27001 Mapping Table» τους Chris Smith, διακεκριμένος στο επάγγελμά του ως αξιολογητής ασφάλειας πληροφοριών. Ακόμα, χρησιμοποιήθηκε ως πηγή η έρευνα του Kabir Barday και J. Trevor Hughes με τίτλο «IAPP-OneTrust Research: Bridging ISO 27001 to GDPR», με τον J. Trevor Hughes να αποτελεί έναν από τους ευρέως γνωστό ως κορυφαίος ειδικός σε θέματα απορρήτου έχοντας συνεισφέρει στην New York Times και στην Ομοσπονδιακή Επιτροπή Εμπορίου των Η.Π.Α..

Γ.Κ.Π.Δ.		**ISO 27001**	
Άρθρο	Περιεχόμενο	**Παράρτημα**	Περιεχόμενο
5	Τα προσωπικά δεδομένα πρέπει να είναι ακριβή, να διατηρούνται ενημερωμένα και να επεξεργάζονται με τέτοιο τρόπο έτσι ώστε να προστατεύεται η εμπιστευτικότητα και η ακεραιότητά τους.	1. Πολιτικές Ασφάλειας Πληροφοριών 2. Οργάνωση Ασφάλειας Πληροφοριών 3. Έλεγχος πρόσβασης 4. Φυσική & Περιβαλλοντική Ασφάλεια 5. Ασφάλεια Λειτουργίας 6. Σχέσεις με προμηθευτές 7. Διαχείριση συμβάντων ασφάλειας πληροφοριών 8. Συμμόρφωση	Η πλειοψηφία των ελέγχων που καλύπτονται από την πιστοποίηση ISO/IEC 27001 εξυπηρετούν το περιεχόμενο του άρθρου 5 του Γ.Κ.Π.Δ.. Τα Παραρτήματα αυτά του ISO/IEC 27001 έχουν ως σκοπό να καλύπτουν πολλούς από τους ισχύοντες κανόνες και κανονισμούς του Γ.Κ.Π.Δ..
	Τα άτομα έχουν δικαίωμα	1. Οργάνωση Ασφάλειας	Σε αυτά τα Παραρτήματα του ISO/IEC 27001

15	πρόσβασης στα δεδομένα τους. Μπορούν να ζητήσουν πληροφορίες για το ποιος έχει πρόσβαση στις δεδομένα που αντιστοιχούν σε αυτούς και πως θα τις χρησιμοποιήσουν.	2. Έλεγχος πρόσβασης 3. Ασφάλεια Λειτουργίας	καλύπτεται από την εταιρεία το που και πως χρησιμοποιούνται τα δεδομένα των ατόμων.
24	Ο υπεύθυνος για τον έλεγχο της επεξεργασίας προσωπικών δεδομένων, πρέπει να διασφαλίζει και να παρέχει αποδεικτικά στοιχεία για την ασφάλεια των δεδομένων σύμφωνα με τις σύγχρονες πολιτικές.	1. Πολιτικές Ασφάλειας Πληροφοριών 2. Οργάνωση Ασφάλειας Πληροφοριών 3. Έλεγχος πρόσβασης 4. Ασφάλεια Λειτουργίας 5. Σχέσεις με προμηθευτές	Η πιστοποίηση καλύπτει σε μεγάλο βαθμό το άρθρο 24 του Γ.Κ.Π.Δ, καθώς εξασφαλίζει τις Πολιτικές Ασφάλειας και οι ρόλοι των ατόμων είναι ορισμένοι με αποτέλεσμα να ενισχύει τους ελέγχους πρόσβασης.
25	Για να διασφαλιστεί ένα βέλτιστο επίπεδο προστασίας δεδομένων “by default” και “by design”, ο Γ.Κ.Π.Δ. απαιτεί την κατάλληλη λήψη τεχνικών και οργανωτικών μέτρων.	1. Πολιτικές Ασφάλειας Πληροφοριών 2. Οργάνωση Ασφάλειας Πληροφοριών 3. Έλεγχος πρόσβασης 4. Ασφάλεια Λειτουργίας 5. Σχέσεις με προμηθευτές	Η πιστοποίηση προσδιορίζει αρκετούς ελέγχους που υπάρχουν στο άρθρο 25 του Γ.Κ.Π.Δ.. Ορισμένοι από αυτούς τους ελέγχους ασχολούνται με τον έλεγχο πρόσβασης και δραστηριότητας του εταιρικού προσωπικού και των εξωτερικών συνεργατών.
28	Όταν τα δεδομένα επεξεργάζονται από εξωτερικούς συνεργάτες, τότε η εταιρεία που	1. Ασφάλεια επικοινωνιών 2. Σχέσεις με προμηθευτές	Αυτά τα παραρτήματα της πιστοποίησης αναφέρονται στον έλεγχο των σχέσεων με τους προμηθευτές για την διασφάλιση της ασφάλειας των πληροφοριών και για την επιβεβαίωση ότι οι εταιρείες συμμορφώνονται με τις εσωτερικές απαιτήσεις. Το

	συνεργάζεται με αυτούς είναι υπεύθυνη για το εάν τηρούν τους κανονισμούς του Γ.Κ.Π.Δ..	3. Συμμόρφωση	παράρτημα «Ασφάλεια επικοινωνιών» προσδιορίζει συγκεκριμένα μέτρα ασφάλειας για να επιτύχει τον σκοπό αυτό.
29	Ο Γ.Κ.Π.Δ. απαιτεί από αυτούς που επεξεργάζονται τα δεδομένα να έχουν πρόσβαση και να τα επεξεργάζονται μόνο όταν αυτό κρίνεται αναγκαίο και πάντα σύμφωνα με τις οδηγίες του υπεύθυνου επεξεργασίας.	1. Πολιτικές Ασφάλειας Πληροφοριών 2. Έλεγχος πρόσβασης 3. Συμμόρφωση	Η «Πολική Ασφάλειας Πληροφοριών» και η «Συμμόρφωση» προσφέρουν τις κατάλληλες γνώσεις στο άτομο που θέλει να επεξεργαστεί τα δεδομένα. Ο «Έλεγχος Πρόσβασης» βοηθάει στην πιστοποίηση ότι το συγκεκριμένο άτομα έχει την άδεια να επεξεργαστεί τα δεδομένα αυτά.
30	Οι υπεύθυνοι πρέπει να κρατάνε λεπτομερή αναφορά παρακολούθησης όλων των δεδομένων που υπόκεινται σε μεταποιητικές δραστηριότητες κάτω από την δική τους ευθύνη.	1. Οργάνωση Ασφάλειας Πληροφοριών 2. Έλεγχος πρόσβασης 3. Σχέσεις με προμηθευτές	Η «Οργάνωση Ασφάλειας Πληροφοριών» βοηθάει στον καθορισμό του πλήθους των πολιτικών ασφαλείας που τίθενται σε εφαρμογή, δίνοντας στους αρμόδιους την δυνατότητα να ελέγχουν τους χρήστες. Τα άλλα 2 παραρτήματα δίνουν έναν εφαρμόσιμο τρόπο στους εξωτερικούς συνεργάτες για να συμμορφώνονται με τις πολιτικές ασφαλείας.
32	Ο Γ.Κ.Π.Δ απαιτεί αξιολόγηση κινδύνου ασφάλειας και εφαρμογή αυστηρών πολιτικών για την εξασφάλιση της διαθεσιμότητας των δεδομένων, διατηρώντας παράλληλα την ακεραιότητα και την εμπιστευτικότητα ώστε να μην επηρεαστεί σε περίπτωση συμβάντος	1. Πολιτικές Ασφάλειας Πληροφοριών 2. Οργάνωση Ασφάλειας Πληροφοριών 3. Έλεγχος πρόσβασης 4. Διαχείριση συμβάντων ασφάλειας πληροφοριών 5. Συμμόρφωση	Αρκετοί έλεγχοι του ISO/IEC 27001 εξυπηρετούν αυτό το άρθρο του Γ.Κ.Π.Δ.. Ενεργοποιούν τους οργανισμούς ώστε να υιοθετούν και διατηρούν ένα ολιστικό κύκλο ασφάλειας, από τον ορισμό των πολικών (π.χ. Πολιτική ασφαλείας) μέχρι την υλοποίησή και αξιολόγησή τους.

	ασφάλειας πληροφοριών.		
33	Η παραβίαση προσωπικών δεδομένων πρέπει να γνωστοποιηθεί στις εποπτικές αρχές εντός 72 ωρών.	1. Διαχείριση συμβάντων ασφάλειας πληροφοριών	Το παράρτημα αυτό του ISO/IEC 27001 δίνει τις κατευθυντήριες γραμμές για την διαχείριση περιστατικών παραβίασης προσωπικών δεδομένων.
35	Πριν περάσει στο στάδιο επεξεργασίας δεδομένων, ο υπεύθυνος θα πρέπει να αξιολογήσει την πιθανότητα κινδύνου και τις επιπτώσεις από την επεξεργασία δεδομένων σε πληροφορίες που εμπεριέχουν τα χαρακτηριστικά της εμπιστευτικότητας και ακεραιότητας.	1. Οργάνωση Ασφάλειας Πληροφοριών	Οι έλεγχοι αυτού του παραρτήματος βοηθάνε στο να παρασχεθεί στον υπεύθυνο η ολοκληρωμένη ορατότητα των χρηστών. Έτσι, έχοντας την πλήρη ορατότητα γύρω από την χρήση των δεδομένων από αυτούς που έχουν την άδεια να τα επεξεργαστούν, παρέχεται μια σημαντική πληροφορία στον υπεύθυνο για την εφαρμογή νέων μελλοντικών πολιτικών για την καλύτερη προστασία των δεδομένων.
40	Οι εποπτικές αρχές αναμένεται να εφαρμόζουν βέλτιστες πρακτικές ασφάλειας κα να θεσπίζουν κώδικες συμπεριφοράς για να διασφαλίζουν την ορθή εφαρμογή του Γ.Κ.Π.Δ..	1. Πολιτικές Ασφάλειας Πληροφοριών 2. Οργάνωση Ασφάλειας Πληροφοριών 3. Συμμόρφωση	Το παράρτημα «Πολιτικές Ασφάλειας» και «Οργάνωση Ασφάλειας» βοηθάνε να καθοριστούν σε όλο τον οργανισμό οι πολιτικές για την ασφάλεια των πληροφοριών. Για να γίνει αυτό, οι κώδικες συμπεριφοράς που καθορίζονται από τις εποπτικές αρχές μπορούν και πρέπει να καθορίζονται από τις απαιτήσεις εσωτερικής ασφάλειας και τους ισχύοντες κανονισμούς.
	Ανεξάρτητες δημόσιες αρχές που τους έχει ανατεθεί η		Ενώ η ανεξάρτητη δημόσια αρχή έχει το

58	παρακολούθηση της συμμόρφωσης των εταιρειών με τον Γ.Κ.Π.Δ. για να προστατεύουν τα ευρωπαϊκά προσωπικά δεδομένα, έχουν δικαίωμα πρόσβασης και επεξεργασίας οποιασδήποτε πληροφορίας είναι απαραίτητη για να επιτελέσουν το έργο τους.	1. Οργάνωση Ασφάλειας Πληροφοριών 2. Έλεγχος πρόσβασης	δικαίωμα πρόσβασης και επεξεργασίας δεδομένων, οι υπεύθυνοι επεξεργασίας πρέπει να ξέρουν πότε και σε ποια δεδομένα έχουν πρόσβαση και επεξεργάζονται. Έτσι είναι σύμφωνοι με τις βέλτιστες πρακτικές ασφάλειας στον κυβερνοχώρο (cyber security).
59	Οι υπεύθυνοι ασφάλειας πληροφοριών της εκάστοτε εταιρείας πρέπει να συντάσσουν ετήσια έκθεση για όλες τις δραστηριότητές τους (π.χ. μέτρα ασφάλειας που λαμβάνονται για την ενίσχυση της προστασίας δεδομένων).	7. Διαχείριση συμβάντων ασφάλειας πληροφοριών	Η συμμόρφωση με αυτό το άρθρο του Γ.Κ.Π.Δ. απαιτεί την διασφάλιση της διαχείρισης περιστατικών ασφάλειας πληροφοριών. Απαντώντας στους στόχους των ελέγχων, η εταιρεία θα βοηθηθεί στο να συντάξει την αναφορά δραστηριοτήτων της.

Πίνακας 5.4.1: *Συσχέτιση Γ.Κ.Π.Δ. με ISO 27001*

Στην συνέχεια, θα δούμε τον πίνακα από το κεφάλαιο 4 που αναφέρει την συσχέτιση των δύο πιστοποιήσεων ISO.

Άξονες του ISO 27001	**ISO 27701 επέκταση**
Πολιτικές ασφάλειας πληροφοριών **Ασφάλεια ανθρωπίνου δυναμικού**	Ενσωμάτωση του Σ.Δ.Π.Α. στο Σ.Δ.Α.Π., συμπεριλαμβανομένων: 1. Εξοπλισμός πόρων/καθιέρωση ρόλων 2. Επικοινωνία (Εσωτερική/ Εξωτερική) 3. Αναμενόμενο αποτέλεσμα 4. Έλεγχος και Καθοδήγηση 5. Συνεχής Βελτίωση του Σ.Δ.Π.Α.
Οργάνωση ασφάλειας πληροφοριών	Εφαρμογή Σ.Δ.Π.Α. και στόχοι απορρήτου
Ασφάλεια ανθρωπίνου δυναμικού	Ικανά προφίλ ατόμων που έχουν ανατεθεί σε ρόλους προστασίας της ιδιωτικής ζωής.
Ασφάλεια ανθρωπίνου δυναμικού	Επίγνωση της πολιτικής Σ.Δ.Π.Α. και του τρόπου με τον οποίο το προσωπικό συμβάλλει στη δημιουργία και τη βελτίωση του συστήματος.

Ασφάλεια ανθρωπίνου δυναμικού	Γνώση της πολιτικής του Σ.Δ.Π.Α. και προσωπική συμβολή για την χρήση και την βελτίωση του συστήματος αυτού.
Διαχείριση περιουσιακών στοιχείων	Ενεργοποίηση θεραπείας κινδύνου για το Σ.Δ.Π.Α..
Διαχείριση περιουσιακών στοιχείων	Διαδικασία αξιολόγησης κινδύνου Σ.Δ.Π.Α..
Διαχείριση περιουσιακών στοιχείων	Σχέδιο αντιμετώπισης κινδύνων Σ.Δ.Π.Α., συμπεριλαμβανομένων τροποποιήσεων σε υπάρχοντα μητρώα κινδύνου
Διαχείριση ελέγχου	Σ.Δ.Π.Α. απόδοση και ανάλυση της αποτελεσματικότητας, συμπεριλαμβανομένων: 1. Εσωτερικός Έλεγχος 2. Επιθεώρηση Διοίκησης
Κρυπτογραφία	Θέματα συνεχούς βελτίωσης Σ.Δ.Π.Α..

Πίνακας 5.4.2: *Συσχέτιση ISO 27001 με ISO 27701*

Κατά αυτόν τον τρόπο ολοκληρώθηκε η σύντομη ανακεφαλαίωση στην συσχέτιση του Γ.Κ.Π.Δ. με τα δύο πρότυπα της οικογένειας ISO/IEC 27000, που αναλύθηκαν εκτενώς σε αυτή την διπλωματική εργασία.

6 ΣΥΜΠΕΡΑΣΜΑΤΑ

Καθώς στην Ε.Ε. εισήγαγαν νέο νόμο που αντικαθιστούσε παλαιότερες οδηγίες συμμόρφωσης για την προστασία του απορρήτου των χρηστών, αυτή η διπλωματική εργασία προσπάθησε να καλύψει το πώς θα μπορούσε μια επιχείρηση να διασφαλίσει την ασφάλεια δεδομένων εντός της επιχείρησης αλλά και γενικότερα την ασφάλεια των χρηστών της.

Η διπλωματική αυτή επικεντρώθηκε σε έναν από τους πρώτους και πιο περιεκτικούς νόμους περί απορρήτου, τον Γ.Κ.Π.Δ., του οποίου το πεδίο εφαρμογής εκτείνεται σε κάθε εταιρεία που εδρεύει στην Ε.Ε. ή εξυπηρετεί πολίτες της Ε.Ε. ή τρίτων χωρών. Πιο συγκεκριμένα εστίασε στην χρήση δύο πιστοποιήσεων, ISO/IEC 27001 και ISO/IEC 27701, που μπορούν να βοηθήσουν μια εταιρεία να αποδείξει ότι συμμορφώνεται με τον κανονισμό.

Μερικά από τα συμπεράσματα είναι τα ακόλουθα:

- Όλες οι επιχειρήσεις πρέπει να συμμορφώνονται με τον Γ.Κ.Π.Δ.. Η συνεχής εξέλιξη της τεχνολογίας μπορεί να οδηγήσει σε ξεπερασμένη συμμόρφωση στον κανονισμό και στην συνέχεια σε έκθεση κινδύνων ασφάλειας δεδομένων. Οι επιχειρήσεις πρέπει να μεριμνούν πάντα για την ασφάλεια των δεδομένων και να ελέγχουν τακτικά την συμμόρφωσή τους με τον κανονισμό.
- Τα κενά ασφαλείας μπορούν να οδηγήσουν σε ισχυρότερα προστατευμένα δεδομένα. Οι περιπτώσεις κενών ασφαλείας μπορούν να οδηγήσουν μια εταιρεία στο να χτίσει πιο ισχυρά φυλασσόμενα δεδομένα και να προστατευτεί από μελλοντικές κακόβουλες επιθέσεις. Για αυτόν τον λόγο πρέπει οι εργαζόμενοι των εταιρειών να είναι καλά εκπαιδευμένοι στην αναγνώριση κακόβουλων ενεργειών και να τα αναφέρουν αμέσως στην αρμόδια ομάδα διασφάλισης ασφάλειας δεδομένων.
- Η μη συμμόρφωση με τον Γ.Κ.Π.Δ. ή η ξεπερασμένη συμμόρφωση με αυτόν ή η ύπαρξη κενών ασφαλείας δεδομένων μπορεί να οδηγήσει σε υπέρογκα ποσά προστίμων.
- Η συμμόρφωση με το απόρρητο είναι πιθανό να γίνει η ειδοποιός διαφορά της επιχείρησης, όσον αφορά την απόκτηση περισσότερων πελατών. Η πιστοποίηση ISO/IEC 27001, αλλά και όλες οι πιστοποιήσεις της οικογένειας ISO/IEC 27000, δημιουργήθηκαν για να βοηθήσουν τους οργανισμούς στο να αποδείξουν στους πελάτες και συνεργάτες τους ότι συμμορφώνονται με τον κανονισμό. Μία τέτοια πιστοποίηση, όπως γίνεται αντιληπτό, είναι αναγκαία για να κερδίσει την εμπιστοσύνη των πελατών και συνεργατών της.
- Οι σωστά ορισμένοι στόχοι της επιχείρησης που είναι γνωστοί σε όλους τους εργαζόμενους οδηγεί στην ευκολότερη επεξεργασία των δεδομένων. Η επεξεργασία προσωπικών δεδομένων γίνεται ευκολότερη εάν οι υπεύθυνοι επεξεργασίας αυτών και αυτοί που επεξεργάζονται τα δεδομένα χρησιμοποιούν μια «κοινή γλώσσα» για να καθορίσουν τους σκοπούς για τους οποίους ζητούν άδεια για την επεξεργασία προσωπικών δεδομένων, καθώς και τυποποιημένες διαδικασίες για τη μεταφορά πληροφοριών. Το μοντέλο S.M.A.R.T. βοηθάει σε

αυτή την διαδικασία καθώς μέσω αυτού θα έχουν οριστεί ήδη οι στόχοι της επιχείρησης με τέτοιο τρόπο ώστε η κατανόηση των αναγκών στην επεξεργασία των δεδομένων να είναι ξεκάθαρη.

- Οι εταιρείες πρέπει να διαλέγουν εξωτερικούς συνεργάτες που συμμορφώνονται με τον Γ.Κ.Π.Δ.. Για αυτό τον λόγο είναι σημαντικό και οι εξωτερικοί συνεργάτες να πιστοποιούνται με τα ISO/IEC της οικογένειας 27000. Αν κατά την συνεργασία της εταιρείας με έναν εξωτερικό συνεργάτη εμφανιστεί κάποιο κενό ασφαλείας δεδομένων, τότε η εταιρεία θα φέρει ευθύνη και όχι ο εξωτερικός συνεργάτης.
- Ο Γ.Κ.Π.Δ. έχει υποχρεωτικό χαρακτήρα για τους οργανισμούς της Ε.Ε., ενώ το ISO 27001 αποτελεί μια πιστοποίηση που εμπεριέχει οδηγίες για τον τρόπο διαχείρισης των ευαίσθητων δεδομένων με βάση τον κίνδυνο απώλειάς τους.
- Τόσο το ISO 27001 όσο και ο Γ.Κ.Π.Δ. περιστρέφονται γύρω από τον κίνδυνο ασφάλειας δεδομένων/απορρήτου και κατευθύνουν τους οργανισμούς στον εντοπισμό ορισμένων από αυτούς και διεξάγουν ελέγχων που μπορούν να φέρουν αυτούς τους ανωτέρω σε αποδεκτό επίπεδο.
- Για την καλύτερη ασφάλεια των δεδομένων οι επιχειρήσεις πρέπει να έχουν συμμορφωθεί και στις 2 πιστοποιήσεις ISO/IEC 27001 και ISO/IEC 27701. Αν και η ISO/IEC 27001 είναι μια πιστοποίηση που θα μπορούσε να «σταθεί» μόνη της, έχει κάποια σημαντικά κενά ασφαλείας δεδομένων που καλύπτονται από την πιστοποίηση ISO/IEC 27701.

7

7: ΒΙΒΛΙΟΓΡΑΦΙΑ

- Neil Hodge, «30 Biggest GDPR Fines So Far (2020, 2021, 2022)», TESSIAN, Compliance Week , 05 Μαΐου 2022
- «GDPR fines by industry: Telecoms far outpace Big Tech»,
- Michal S Gal & Oshrit Aviv, «The competitive effects of the GDPR», Journal of Competition Law & Economics, Τόμος 16, Έκδοση 3, Σελίδες 349–391, Σεπτέμβριος 2020
- Razieh Nokhbeh Zaeem & K. Suzanne Barber, «The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise», ACM Transactions on Management Information Systems, Τόμος 12, έκδοση 1, Μάρτιος 2021
- Isabel Maria Lopes & Teresa Guarda & Pedro Oliveira, « How ISO 27001 Can Help Achieve GDPR Compliance», Institute of Electrical and Electronics Engineers, 2019
- Colin Tankard, «What the GDPR means for businesses», Network Security, Τόμος 2016, Έκδοση 6, Σελίδες 5-8, Ιούνιος 2016
- Daniel Bastos & Fabio Giubilo & Mark Shackleton & Fabi El-Mousa, «GDPR Privacy Implications for the Internet of Things», 4th Annual IoT Security Foundation Conference, Λονδίνο, Δεκέμβριος 2018
- Carol Hsu & Tawei Wang & Ang Lu, « The Impact of ISO 27001 Certification on Firm Performance», Annual Hawaii International Conference on System Sciences (HICSS), Έκδοση 49, 2016
- Jan Philipp Albrecht, «How the GDPR will change the world», European Data Protection Law Review (EDPL), Τόμος 2, έκδοση 3, σελίδες 287-289, 2016
- Lawrence Ryz & Laure Grest, «A new era in data protection», Computer Fraud & Security, Τόμος 2016, Έκδοση 3, σελίδες 18-20, Μάρτιος 2016
- Claire Laybats & John Davies, «GDPR: Implementing the regulations», Sage Journals, 3 Ιουνίου 2018
- Jan Philip Albrecht, «How the GDPR will change the world», European Data Protection Law Review (EDPL) 2 Eur. Data Prot., Έκδοση 3, Σελίδες 287-289, 2016
- Samuel Greengard, «Weighing the impact of GDPR», Communications of the ACM, Τόμος 61, Έκδοση 11 , Σελίδες 16-18, 2018
- Ibrahim Al-Mayahi, Sa'ad P. Mansoor, « ISO 27001 Gap Analysis - Case Study», School of Computer Science, Bangor University, Bangor, Gwynedd, UK, 2012
- Tal Z. Zarsky, «Incompatible: The GDPR in the Age of Big Data», Seton Hall Law Review 47 Seton Hall L. Rev., Σελίδες 995-1020, 2016-2017
- Xuehui Hu & Nishanth Sastry, «Characterising Third Party Cookie Usage in the EU after GDPR», WebSci '19: Proceedings of the 10th ACM Conference on Web Science, Σελίδες 137–141, Ιούνιος 2019
- Pietro Ferrara & Fausto Spoto, «Static Analysis for GDPR Compliance», Conference Paper, Ιανουάριος 2018

- Marc Cornock, «General Data Protection Regulation (GDPR) and implications for research», Editorial | Τόμος 111, PA1-A2, Φεβρουάριος 2018
- Phil Beckett, «GDPR compliance: your tech department's next big opportunity», Computer Fraud & Security, Τόμος 2017, Έκδοση 5, Σελίδες 9-13, Μάιος 2017
- Sabina-Daniela Axinte & Gabriel Petrică & Ioan Bacivarov, « GDPR Impact on Company Management and Processed Data», Τόμος 19, Έκδοση 165, Σελίδες 150-153, Αύγουστος 2018
- Cath Everett, «Is ISO 27001 worth it?», Computer Fraud & Security, Τόμος 2011, Έκδοση 1, Σελίδες 5-7, Ιανουάριος 2011
- Colin Tankard, «What the GDPR means for businesses», Network Security, Τόμος 2016, Έκδοση 6, Σελίδες 5-8, Ιούνιος 2016
- Paul Breitbarth, «The impact of GDPR one year on», Network Security, Τόμος 2019, Έκδοση 7, Σελίδες 11-13, Ιούλιος 2019
- Martin Brodin, «A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises», European Journal for Security Research, Τόμος 4, Σελίδες 243–264, Ιούνιος 2019
- Tzanko Tzolov, «One Model For Implementation GDPR Based On ISO Standards», 2018 International Conference on Information Technologies (InfoTech), Σεπτέμβριος 2018
- Cesare Bartolini & Gabriela Gheorghe & Andra Giurgiu & Mehrdad Sabetzadeh & Nicolas Sannier, « Assessing IT Security Standards Against the Upcoming GDPR for Cloud Systems», Μάρτιος 2015
- Maria da Conceição Freitas & Miguel Mira da Silva, « GDPR Compliance in SMEs: There is much to be done», Journal of Information Systems Engineering & Management, Τόμος 3, Έκδοση 4, Άρθρο νούμερο 30, Νοέμβριος 2018
- Alit Yuniargan Eskaluspita, «ISO 27001:2013 for Laboratory Management Information System at School of Applied Science Telkom University», IOP Conference Series: Materials Science and Engineering, Τόμος 879, Ιούνιος 2020
- Graham Greenleaf, «'European' Data Privacy Standards Implemented in Laws Outside Europe», (2017) 149 Privacy Laws & Business International Report 21-23 ,UNSW Law Research Paper No. 18-2, Ιούλιος 2018
- Awanthika Senarath & Nalin Asanka Gamagedara Arachchilage, «Understanding Software Developers' Approach towards Implementing Data Minimization», USENIX Symposium on Usable Privacy and Security (SOUPS), Baltimore USA, Αύγουστος 2018
- Yod-Samuel Martín & Antonio Kung, «Methods and Tools for GDPR Compliance through Privacy and Data Protection Engineering», IEEE European Symposium on Security and Privacy Workshops, 2018
- Timothy Libert & Lucas Graves & Rasmus Kleis Nielsen, «Changes in Third-Party Content on European News Websites after GDPR», Published by the Reuters Institute for the Study of Journalism with the support of the Google News Initiative, 2018
- Vasiliki Diamantopoulou & Aggeliki Tsohou & Maria Karyda, «From ISO/IEC27001:2013 and ISO/IEC27002:2013 to GDPR compliance controls», Journals: Information and Computer Security, Τόμος 28, Έκδοση 4, Ιούνιος 2020
- Abdulrahman Alhazmi & Nalin Asanka Gamagedara Arachchilage, «I'm all ears! Listening to software developers on putting GDPR principles into software

development practice», Personal and Ubiquitous Computing, 25:879–892, Μάιος 2021
- Abdulrahman Alhazmi & Nalin Asanka Gamagedara Arachchilage, «Why are Developers Struggling to Put GDPR into Practice when Developing Privacy-Preserving Software Systems?», La Trobe University, 2020
- Abdulrahman Alhazmi & Nalin A G Arachchilage, «A Serious Game Design Framework for Software Developers to Put GDPR into Practice», ARES 2021: The 16th International Conference on Availability, Reliability and Security, Νούμερο άρθρου 64, Σελίδες 1–6, Αύγουστος 2021
- Michal S Gal & Oshrit Aviv, «The Competitive Effects of the GDPR», Journal of Competition Law & Economics, Τόμος 16, Έκδοση 3, Σελίδες 349–391, Σεπτέμβριος 2020
- Dara Hallinan, «Broad consent under the GDPR: an optimistic perspective on a bright future», Life Sciences, Society and Policy, Τόμος 16, Νούμερο άρθρου 1, Ιανουάριος 2020
- W. Gregory Voss, «One Year and Loads of Data Later, Where are We? An Update on the Proposed European Union General Data Protection Regulation», Journal of Internet Law -- Aspen Publishers Inc.-- Wolters Kluwer Law & Business, Τόμος 16, Έκδοση 10, Απρίλιος 2013
- «What Are the Different Types of Phishing?», TREND MICRO
- Ellie Mirman, «The Ultimate Guide to Service Level Agreements (SLAs)», HubSpot, Ιανουάριος 2019
- «ISO 27001 – Annex A.5: Information Security Policies», isms.online
- «ISO 27001 – Annex A.6: Organisation of Information Security», isms.online
- «ISO 27001 – Annex A.7: Human Resource Security», isms.online
- «ISO 27001 – Annex A.8: Asset Management», isms.online
- «ISO 27001 – Annex A.9: Access Control», isms.online
- «ISO 27001 – Annex A.10: Cryptography», isms.online
- «ISO 27001 – Annex A.11: Physical & Environmental Security», isms.online
- «ISO 27001 Annex A.12.1», isms.online
- «ISO 27001 – Annex A.13: Communications Security», isms.online
- «ISO 27001 – Annex A.14: System Acquisition, Development & Maintenance», isms.online
- «ISO 27001 – Annex A.15: Supplier Relationships», isms.online
- «ISO 27001 – Annex A.16: Information Security Incident Management», isms.online
- «ISO 27001 – Annex A.17: Information Security Aspects of Business Continuity Management», isms.online
- «ISO 27001 – Annex A.18: Compliance», isms.online
- Sieuwert van Otterloo, «Information security – Cryptographic controls policy example», ICT Institute, 4 Ιανουαρίου 2017
- Emil R Kaburuan & Asl Lindawati, «Implementation of security system on humanitarian organization: case study of dompet dhuafa foundation», Νοέμβριος 2019
- Dejan Kosutic, «What is the ISO 27001 Information Security Policy, and how can you write it yourself?», 27001 Academy, 30 Μαΐου 2016
- «SMART Goals», toolshero, 9 Ιουλίου 2018
- Julian Russell, «ISO 27001:2013 INFORMATION SECURITY IMPLEMENTATION GUIDE», nqa, 2019
- Julian Russell, « ISO/IEC 27701 IMPLEMENTATION GUIDE», nqa, 2019

- Svetlana A. Grishaeva, «Development and Implementation of Privacy Information Management for Compliance with International Standard ISO 27701:2019», IEEE Xplore, Δεκέμβριος 2021
- «Δήλωση απορρήτου», EUROMAT
- Roman Kozlov, «How to segment a network using VLAN», ipsystem, 16 Οκτωβρίου 2020
- «Information Security Objectives in ISO 27001», ISO 27001 GUIDE.COM, 23 Ιανουαρίου 2021
- «What is Encryption and how does it work?», Middlebury, 17 Μαΐου 2019
- Chris Smith, « GDPR V ISO 27001 Mapping Table», Νοέμβριος 2018
- Kabir Barday & J. Trevor Hughes, «IAPP-OneTrust Research: Bridging ISO 27001 to GDPR», iapp OneTrust Privacy Management Software, Μάρτιος 2018
- Tristan Caulfield & Ingolf Becker , «"It may be a pain in the backside but..." Insights into the impact of GDPR on business after three years», Gerard Buckley, arxiv.org, Οκτώβριος 2021

Για την δημιουργία των εικόνων χρησιμοποιήθηκε ο ιστότοπος **"www.flaticon.com"** για την εύρεση έγχρωμων και ασπρόμαυρων εικονιδίων, που υπάρχουν εντός των εικόνων, και το πρόγραμμα **"3D Paint"** για την προσθήκη κειμένων και την τελική μορφοποίηση των εικόνων που υπάρχουν μέσα στην διπλωματική εργασία.