ΠΑΝΕΠΙΣΤΗΜΙΟ
ΙΩΑΝΝΙΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΤΕΧΝΟΛΟΓΙΑ & ΝΟΜΟΛΟΓΙΑ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΝΑΛΛΑΓΩΝ ΜΕ ΓΝΩΜΟΝΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ-GDPR.

Ονοματεπώνυμο Σπουδαστή: Ζώτος Γρηγόριος

Επιβλέπων: Στύλιος Χρυσόστομος

Άρτα,2021

Technology & jurisprudence of electronic transactions based on the protection of personal data-GDPR.

Εγκρίθηκε από τριμελή εξεταστική επιτροπή

Τόπος, Ημερομηνία

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Επιβλέπων καθηγητής

   Όνομα Επίθετο,

2. Μέλος επιτροπής

   Όνομα Επίθετο,

3. Μέλος επιτροπής

   Όνομα Επίθετο,

Δήλωση μη λογοκλοπής

Δηλώνω υπεύθυνα και γνωρίζοντας τις κυρώσεις του Ν. 2121/1993 περί Πνευματικής Ιδιοκτησίας, ότι η παρούσα μεταπτυχιακή εργασία είναι εξ ολοκλήρου αποτέλεσμα δικής μου ερευνητικής εργασίας, δεν αποτελεί προϊόν αντιγραφής ούτε προέρχεται από ανάθεση σε τρίτους. Όλες οι πηγές που χρησιμοποιήθηκαν (κάθε είδους, μορφής και προέλευσης) για τη συγγραφή της περιλαμβάνονται στη βιβλιογραφία.

ΕΥΧΑΡΙΣΤΙΕΣ

Σε αυτό το σημείο , θα ήθελα να ευχαριστήσω ιδιαίτερα τον κ. Στύλιο, καθηγητή του τμήματος Πληροφορικής και Τηλεπικοινωνιών του Πανεπιστημίου Ιωαννίνων που εδρεύει στην Άρτα, για την απεριόριστη βοήθεια του και μέριμνα του για την αποπεράτωση της παρούσας εργασίας. Επίσης, να ευχαριστήσω τους γονείς μου που στάθηκαν συνοδοιπόροι σε όλη την πορεία μέχρι και πραγματοποίηση της εργασίας αυτής.

ΠΕΡΙΛΗΨΗ

Διαδίκτυο. Ένα πανίσχυρο εργαλείο στα χέρια μαθητή, φοιτητή, εργαζόμενου, επιχειρήσεων. Κάθε νόμισμα , όμως, έχει δύο όψεις. Πέραν τον απεριόριστων δυνατοτήτων που παρέχει, ελλοχεύει κινδύνους. Οι βασικότεροι φόβοι των χρηστών είναι η διέρευση προσωπικών τους δεδομένων και πώς αυτά μπορεί να επεξεργαστούν. Η παρούσα πτυχιακή , θα προσπαθήσει να αναφέρει τον τρόπο που κινήθηκε η Ευρωπαϊκή΄¨ένωση για την προστασία των πολιτών της , αναφέροντας τις διάφορες πτυχές του GDPR που εφαρμόστηκε το 2018.

Λέξεις-κλειδιά: GDPR, Διαδίκτυο, προσωπικά δεδομένα

ABSTRACT

Internet. A powerful tool in the hands of pupil, student, employee, business. Each coin, however, has two sides. In addition to the unlimited possibilities it provides, there are risks involved. The main fears of users are the management of their personal data and how it can be processed. This dissertation will try to report on how the European Union has moved to protect its citizens, citing the various aspects of the GDPR implemented in 2018.

Keywords: GDPR, Internet, personal data

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΔΙΑΓΡΑΜΜΑΤΩΝ/ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΕΙΣΑΓΩΓΗ

Ο 21ο αιώνας είναι ο αιώνας της τεχνολογικής ανάπτυξης και πληροφορίας. Οτιδήποτε χρειάζεται ο εκάστοτε , εύκολα μπορεί να εντοπιστεί. Δραστηριότητες της καθημερινότητάς αλλά και οικονομικές, πολιτικές, πολιτιστικές , ειδικά στα χρόνια της πανδημίας, πραγματοποιήθηκαν μέσω ένας πανίσχυρου εργαλείου, του Διαδικτύου. Ο εκάστοτε κατάλαβε τη δύναμη που έχει στα χέρια του αλλά και τις άπειρες πτυχές του. Παρόλα αυτά, ζώντας σε μια εποχή παγκοσμιοποίησης, ελλοχεύουν κίνδυνοι που ίσως τα προηγούμενα χρόνια να μην τους δόθηκαν ιδιαίτερη έμφαση. Οι κίνδυνοι αυτοί αφορούν κυρίως τα προσωπικά δεδομένα των χρηστών. Εκατομμύρια δεδομένα κινούνται ανά δευτερόλεπτο στο Διαδίκτυο, διερχόμενα από άπειρους υπολογιστές. Δεδομένα που είναι ιδιαίτερα σημαντικά για τον καθένα ένα χρήστη και που η διεύρυνση τους ή ακόμα και υποκλοπή τους μπορεί να οδηγήσουν σε καταστάσεις ιδιαίτερα δυσάρεστες. Για το λόγο αυτό, η Ευρωπαϊκή Ένωση, από σχετικά νωρίς , έθεσε κάποιες βάσεις και αρχές για την προστασία των δεδομένων αυτών. Η τελευταία προσπάθεια είναι ο γνωστός πια σε όλους GDPR, Γενικός Κανονισμός για τη Προστασία Δεδομένων. Για αυτόν τον κανονισμό θα γίνει αναφορά σε αυτή την εργασία, παρουσιάζοντας πτυχές του και εφαρμογές του.

1 Το Διαδίκτυο

Ο 21ος αιώνας χαρακτηρίζεται από πληθώρα πληροφοριών , εξελίξεων τεχνολογικών που ένα μεγάλο μέρος του είναι συνδεδεμένο με την έννοια του Διαδικτύου.

Το Διαδίκτυο ξεκίνησε ως μια ιδέα του Υπουργείο Άμυνας των Η.Π.Α τη δεκαετία του ’70. Στόχος του Υπουργείου ήταν να μπορούν δύο υπολογιστές να επικοινωνήσουν μεταξύ τους έτσι ώστε να διαμοιράζονται τα δεδομένα τους. Για την επίτευξη του σκοπού αυτού , συστήθηκε μια επιστημονική ομάδα η λεγόμενη ARPA, και το πρώτο δίκτυο που συστάθηκε είναι γνωστό ως και ARPANET (Advanced Research Projects Agency Network).

Βέβαια, η ιστορία δεν σταματάει εκεί. Λόγω έλλειψης επιστημονικού υπόβαθρου αλλά και τεχνολογικών υποδομών, αποφασίστηκε το εγχείρημα αυτό να δοθεί στα πανεπιστήμια έτσι ώστε να το εξελίξουν.

Έτσι, λοιπόν, το 1973 ξεκινά μια προσπάθεια των πανεπιστημίων να ξεπεράσουν τα προβλήματα διασυνδεσιμότητας μεταξύ διαφορετικών κόμβων που ανήκουν σε διαφορετικά δίκτυα. Η προσπάθεια αυτή είναι γνωστή ως και Intermetting Project (Πρόγραμμα Διαδικτύωσης). Από αυτή την προσπάθεια γεννιέται και το γνωστό , πια , πρωτόκολλο Internet Protocol ή αλλιώς IP , από το οποίο και απέκτησε το όνομα του το σημερινό Internet. Ταυτόχρονα, αναπτύσσεται και μια τεχνική για τον έλεγχο της μετάδοσης των δεδομένων από τον έναν υπολογιστή σε άλλον, γνωστό ως TCP.

Αυτή ήταν η αρχή του παντός. Τα πρωτόκολλά TCP και IP καθιερώνονται ως βασικά πρωτόκολλα και πια είναι στη διάθεση του Υπουργείου Άμυνας. Η υιοθέτηση τους και από το λειτουργικό σύστημα UNIX, συντελεί και αυτό από τη μεριά του, στην γρήγορη εξάπλωση της διασύνδεσης (διαδικτύωσης) των κόμβων. Εκατοντάδες πανεπιστήμια συμμετέχουν στη διασύνδεση αυτή και δεν αργεί η διασύνδεση αυτή ξεπερνά πια τα όρια της Αμερικής και όλο και περισσότερες χώρες συνδέονται. Η νέα πραγματικότητα διασυνδεσιμότητας έχει όνομα και αυτό είναι το NSFNET και λαμβάνει χώρα στο τέλος της δεκαετίας του 80. Το πλήθος των διασυνδεμένων κόμβων αυξάνεται με ραγδαίους ρυθμούς. Το ARPANET εγκαταλείπεται και το NSFNET μετονομάζεται σε INTERNET.

Έκτοτε, το Internet αποτελεί μέρος της καθημερινότητας εκατομμυρίων χρηστών. Οι υπηρεσίες που προσφέρει απεριόριστες και οι δυνατότητες ακόμα περισσότερες. Και όπως

είναι λογικό, οι πτυχές που μπορεί να χρησιμοποιηθεί πια το Internet, δεν βρίσκεται πια στη σφαίρα φαντασίας , αλλά θα είναι πια μέρος της καθημερινότητας [1].

1.1 Υπηρεσίες του Διαδικτύου

Όπως προαναφέρθηκε , οι δυνατότητες που παρέχει το Διαδίκτυο πια είναι απεριόριστες. Στο παρόν κεφάλαιο, θα παρουσιαστούν οι πιο συχνές και ευρέως διαδεδομένες.

- Ηλεκτρονικό Ταχυδρομείο (e-mail): είναι από τις πρώτες υπηρεσίες του διαδικτύου. Πρόκειται για διασύνδεση υπολογιστών , που , όμως, η βασική τους επικοινωνία είναι μέσω γραπτών μηνυμάτων. Σήμερα, βέβαια, μαζί με το γραπτό μήνυμα, ο εκάστοτε χρήστης έχει τη δυνατότητα να αποστείλει και πολυμέσα όπως εικόνα, video κ.ο.κ.

Για την επικοινωνία των δύο κόμβων (χρηστών) απαιτείται να κατέχουν μια διεύθυνση email. Αυτή η διεύθυνση αποτελείται από ένα username συνοδευόμενο από το '@' και στη συνέχεια, το όνομα του παρόχου στον οποίο αποθηκεύονται τα e-mail. Αυτό είναι και ένα από τα πλεονεκτήματα του ηλεκτρονικού ταχυδρομείου. Ότι , δηλαδή, τα διάφορα ηλεκτρονικά μηνύματα e-mail , δεν διατηρούνται τοπικά στον εκάστοτε προσωπικό υπολογιστή, αλλά βρίσκονται στον server του διακομιστή. αυτό προσφέρει εύκολη πρόσβαση από οποιαδήποτε συσκευή και οποιοδήποτε σημείο καθώς και τη διαχείριση τους ανά πάσα στιγμή.

- Επικοινωνία μέσω Διαδικτύου ή αλλιώς VOIP: πρόκειται για την υπηρεσία που τάραξε τα νερά στον τρόπο επικοινωνίας. Ξεκίνησε παρέχοντας τη δυνατότητα επικοινωνίας , όχι μεταξύ τηλεφώνων, αλλά μεταξύ τηλεφώνου και ενός υπολογιστή. εκμεταλλευόμενη τη μεταφορά του ήχου στα χάλκινα καλώδια και στις προϋπάρχουσες τηλεφωνικές εγκαταστάσεις, η υπηρεσία αυτή, παρείχε χαμηλές χρεώσεις για αυτού του είδους επικοινωνία. Έγινε γρήγορα προτιμητέα ειδικά για επικοινωνίες μεταξύ χωρών.

Βέβαια, δεν σταμάτησε εκεί η συγκεκριμένη υπηρεσία. Με την αναβάθμιση των τηλεπικοινωνιακών υποδομών, έφτασε πια να μπορεί να παρέχει και βιντεοκλήση. Το διασημότερο πρόγραμμα, αντιπρόσωπος αυτής της υπηρεσίας , είναι το Skype αλλά , πια , και το ZOOM.

- Παγκόσμιος Ιστός: Είναι από τις πιο διάσημες υπηρεσίες του Διαδικτύου. Τόσο διαδεδομένη που αρκετές φορές συγχέονται οι δύο αυτοί όροι. Όμως, ο Παγκόσμιος Ιστός ή όπως είναι γνωστό WWW (World Wide Web), είναι μια υπηρεσία η οποί βασίζεται στη διαμοίραση υπερκειμένου (hypertext). Το υπερκείμενο είναι κείμενο το οποίο έχει τη δυνατότητα να μεταφέρει τον χρήστη σε περιεχόμενα που περιέχει ήχο, βίντεο κ.ο.κ. Είναι οργανωμένος σε ιστοσελίδες , που έχουν μοναδικό όνομα και ποικίλο περιεχόμενο. Βασικό του πρωτόκολλο είναι το HTTP (Hypertext Transfer Protocol), το οποίο επιτυγχάνει τη διαμοίραση του υπερκειμένου.
- Instant Messaging & Chat: Μια άλλη υπηρεσία είναι και η άμεση ανταλλαγή μηνυμάτων μεταξύ χρηστών. Η υπηρεσία αυτή επιτρέπει σε δύο - και όχι μόνο- χρήστες να επικοινωνήσουν ανεξαρτήτως απόστασης, κατάστασης και διαφορά ώρας. Το μόνο που χρειάζεται είναι , να υπάρχει το αντίστοιχο πρόγραμμα που υποστηρίζει τα άμεσα μηνύματα ή το chat, και να έχουν δημιουργήσει έναν λογαριασμό έτσι ώστε να μπορούν να εντοπίσουν ο ένας τον άλλον. Χαρακτηριστικοί αντιπρόσωποι αυτής της υπηρεσίας είναι το MSN της Microsoft,Mirc κ.ο.κ [2].

Εικόνα 1-1: Instant Messaging και άλλες υπηρεσίες Διαδικτύου

- Cloud Υπηρεσία ή Σύννεφο: Η υπηρεσία αυτή είναι γνωστή την τελευταία δεκαετία αλλά προϋπήρχε σε άλλες μορφές ίσως. Πρόκειται για μια υπηρεσία που προσφέρει στο χρήστη του, μεγάλο αποθηκευτικό χώρο για τα δεδομένα του και πρόσβαση από οπουδήποτε και αν είναι , αρκεί να έχει μια ηλεκτρονική συσκευή και πρόσβαση στο διαδίκτυο. Το βασικό πλεονέκτημα της είναι ό,τι τα δεδομένα δεν είναι αποθηκευμένα τοπικά σε κανέναν υπολογιστή του χρήστη αλλά είναι στον server της εκάστοτε εταιρείας. Τέτοιες υπηρεσίες προσφέρουν Google Drive, DropBox, OneDrive κ.ο.κ

Εικόνα 1-2: Cloud Υπηρεσία

Οι υπηρεσίες που προσφέρει το Διαδίκτυο είναι αναρίθμητες και δεν μπορούν να περιοριστούν σε ένα μόνο κεφάλαιο. Παρόλα αυτά, παρουσιάστηκαν οι βασικές υπηρεσίες για τις οποίες είναι εξοικειωμένος ο μεγαλύτερος αριθμός χρηστών του [3].

1.2 Πλεονεκτήματα του Διαδικτύου

Το Διαδίκτυο έφερε μια επανάσταση στο πώς αντιλαμβανόμαστε την πληροφορία, τους υπολογιστές και την τεχνολογία. Οι προαναφερόμενες υπηρεσίες ήταν απλά μια πτυχή του, που όμως κάνει εμφανές τη πληθώρα των τομέων που επηρεάζει θετικά. Παρακάτω, αναφέρονται κάποιοι από αυτούς και πώς επωφελούνται από τις υπηρεσίες του Διαδικτύου.

- Εκμηδένισε τις αποστάσεις: αυτό σημαίνει , ότι οι χρήστες έχουν τη δυνατότητα να συνομιλούν και να επικοινωνούν σε πραγματικό χρόνο με τους άλλους χρήστες χωρίς περιορισμό απόστασης.
- Εμπόριο & οικονομία: Εάν άλλο βασικό πλεονέκτημα, ειδικά για τους εργαζομένους, που απασχολούνται αρκετές ώρες και δεν έχουν την πολυτέλεια του χρόνου για τις αγορές τους, είναι και οι διαδικτυακές αγορές. Χιλιάδες ηλεκτρονικά καταστήματα με ή και χωρίς φυσική παρουσία, προσφέρον τα αγαθά και τις υπηρεσίες του με το πάτημα ενός κουμπιού.

Αυτή η δραστηριότητα έχει δύο όψεις. Αφενός, η διευκόλυνση των χρηστών αλλά και η προσφορά χιλιάδων προϊόντων σε ποικιλία ειδών και τιμών , αφετέρου τονώνει και την οικονομία των μεγάλων επιχειρήσεων αλλά και των μικρών – μικρομεσαίων. Και αυτό με τη σειρά του τονώνει την εγχώρια οικονομία του κάθε κράτους , αφού υπάρχει η δυνατότητα παραγγελίας και αποστολής προϊόντων και εκτός των συνόρων μιας χώρας.

- Τηλεϊατρική: ένας τομέας που τα τελευταία χρόνια γνωρίζει ανάπτυξη αλλά και αναγνώριση είναι η τηλεϊατρική. Σκοπός είναι όχι μόνο η παρακολούθηση των ασθενών εξ αποστάσεως , που αυτό από μόνο του είναι μεγάλο πλεονέκτημα γιατί έτσι οι ασθενείς δεν χρειάζονται να μετακινηθούν, αλλά έχει και σκοπό και τη θεραπεία. Δηλαδή, μέσω Διαδικτύου και ρομποτικών βραχιόνων , ο γιατρός είναι σε θέση να διεξάγει ακόμα και εγχείρηση και ο ίδιος να μην βρίσκεται στο ίδιο χώρο.
- Αναζήτηση & Εύρεση Πληροφοριών: με ένα κλικ και λίγη πληκτρολόγηση, γονέας, μαθητής φοιτητής ένας οποιοσδήποτε χρήστης μπορεί και έχει στη διάθεση του πληθώρα πληροφοριών για οποιοδήποτε θέμα τον ενδιαφέρει.

Τα πλεονεκτήματα δεν σταματούν στα προαναφερόμενα. Είναι πολλά και διάφορα ανάλογα και την πτυχή και την υπηρεσία ή τις υπηρεσίες που χρησιμοποιεί κάποιος. Ένα είναι το

σίγουρο , το Διαδίκτυο είναι κομμάτι της καθημερινότητας και σκοπεύει να εδραιωθεί ακόμα περισσότερο.

1.3 Κίνδυνοι του Διαδικτύου

Αν και υπάρχουν πολλά θετικά στη χρήση του Διαδικτύου , παρόλα αυτά ελλοχεύουν κάποιοι κίνδυνοι που έχουν διττό χαρακτήρα. Από τη μια οι κίνδυνοι που υπάρχουν και χρησιμοποιούν τους χρήστες για την απόκτηση των στοιχείων τους και από την άλλη που χρησιμοποιούν ευπάθειες στα λογισμικά των διαδικτυακών εφαρμογών.

Οι κίνδυνοι που ελλοχεύουν για τις διαδικτυακές εφαρμογές είναι οι εξής:

- Πλαστογράφηση: προσπάθεια του επιτιθέμενου να αποκτήσει πρόσβαση σε ένα σύστημα χρησιμοποιώντας ψεύτικη ταυτότητα
- Αλλοίωση: Μη εξουσιοδοτημένη τροποποίηση των δεδομένων
- Αποποίηση: Τρόπος με τον οποίο οι χρήστες απορρίπτουν μια διαδικτυακή ενέργεια, που όμως είναι ακόμα δύσκολα να αποδειχθεί.
- Δημοσιοποίηση δεδομένων: Ανεπιθύμητη διέρευση ευαίσθητων προσωπικών δεδομένων
- Άρνηση παροχής εξυπηρέτησης: ένα σύστημα ή εφαρμογή δεν είναι προσιτή στους εξουσιοδοτημένους χρήστες της
- Κλιμάκωση δικαιωμάτων: Χρήστης που χρησιμοποιεί τα δικαιώματα ενός άλλου χρήστη. [4]

Οι παραπάνω κίνδυνοι και απειλές , στοχεύουν σε ευαισθησίες των συστημάτων και εφαρμογών για την επίτευξη των σκοπών τους. Βέβαια, από τη μεριά των δημιουργών και των ιδιοκτητών των συστημάτων και των εφαρμογών έχουν προκύψει και κάποια αντίμετρα.

ΑΠΕΙΛΗ	ΑΝΤΙΜΕΤΡΟ
Πλαστογράφηση	Χρήση ισχυρών μηχανισμών ελέγχου ταυτότητας. Αποφυγή αποθήκευσης μυστικών (για παράδειγμα, διαπιστευτηρίων) μέσα σε απλό κείμενο. Αποφυγή μετάδοσης διαπιστευτηρίων σύνδεσης σε μορφή απλού κειμένου μέσω απροστάτευτης δικτυακής σύνδεσης.
Αλλοίωση	Αξιοποίηση μηχανισμών συναρτήσεων κατακερματισμού. Χρήση ψηφιακών υπογραφών. Χρήση ισχυρών μηχανισμών αυθεντικοποίησης. Χρήση πρωτοκόλλων που παρέχουν προστασία της ακεραιότητας του κάθε μεταδιδόμενου μηνύματος.
Αποποίηση	Τήρηση και προστασία αρχείων καταγραφής. Χρήση ψηφιακών υπογραφών.
Δημοσιοποίηση πληροφοριών	Χρήση ισχυρών μηχανισμών αυθεντικοποίησης. Χρήση ανθεκτικής κρυπτογράφησης. Χρήση πρωτοκόλλων που παρέχουν προστασία της εμπιστευτικότητας των μεταδιδόμενων μηνυμάτων. Αποφυγή αποθήκευσης μυστικών μέσα σε απλό κείμενο.
Άρνηση εξυπηρέτησης	Παρακολούθηση, διαχείριση και ρύθμιση της χρήσης των πόρων του υπολογιστικού συστήματος. Επικύρωση και φιλτράρισμα των δεδομένων εισόδου.
Κλιμάκωση προνομίων	Εφαρμογή της Αρχής του Ελάχιστου Προνομίου. Χρήση επαρκών λογαριασμών για την εκτέλεση των διεργασιών και την πρόσβαση στους πόρους.

Πίνακας 1-1: Απειλές συστημάτων και αντίμετρα [4]

Οι κίνδυνοι που ελλοχεύουν για τους χρήστες είναι οι εξής:

- Phishing ή Ψάρεμα: Πρόκειται για μια μέθοδο που ακολουθείται κυρίως για την υφαρπαγή δεδομένων που έχουν να κάνουμε με πιστωτικές κάρτες και τραπεζικούς λογαριασμούς αλλά και χρηματικών ποσών. Η μέθοδος που ακολουθείται είναι συνήθως η αποστολή ενός e-mail που αναπαριστά συνήθως μια τράπεζα. Στο e-mail αυτό ζητούνται αριθμοί καρτών, κωδικοί με την πρόφαση της κλοπής ή του κλειδώματος της κάρτας. Σε άλλες περιπτώσεις , το e-mail έχει απειλητικό χαρακτήρα, αναφέροντας την διαπόμπευση του χρήστη εκτός και αν καταθέσει ένα συγκεκριμένο ποσό σε λογαριασμό. Όποια και να είναι η μέθοδος, αρκετοί είναι οι χρήστες που πέφτουν θύματα.
- Spyware ή λογισμικό κατασκοπείας: είναι κομμάτι των κακόβουλών λογισμικών (malware) που όμως κρύβει τη μεγαλύτερή επικινδυνότητα. Το κακόβουλα λογισμικό εγκαθίσταται στους υπολογιστές των χρηστών , συνήθως , μετά από εγκατάσταση αμφιβόλου προελεύσεων προγράμματα αλλά ακόμα και από ένα κλικ σε κάποιο pop -up παράθυρο. Η κύρια διαφορά με τα άλλα κακόβουλα λογισμικά όπως virus, trojan horses κ.ο.κ, είναι ότι τα δεδομένα των χρηστών , πριν φτάσουν στον εκάστοτε server , κάνουν μια ‘στάση στον υπολογιστή του δημιουργού του spyware. Εκεί, ο δημιουργός είναι σε θέση να

αποθηκεύσει τα στοιχεία που τον ενδιαφέρουν και ανά πάσα στιγμή να τα χρησιμοποιήσει προς όφελος του, κυρίως χρηματικό.

- Διεύρεση ευαίσθητων δεδομένων: ενώ ο κάθε χρήστης μπορεί να προστατεύσει το ‘σερφάρισμα’ του εγκαθιστώντας κατάλληλες εφαρμογές και προγράμματα στον υπολογιστή του, αυτό που ,όμως, δεν μπορεί να ελέγχει και να προστατεύσει είναι την αρπαγή των δεδομένων του κατά τη διάρκεια της αποστολής τους στο φυσικό μέσο. Ο κίνδυνος είναι , ότι έτσι όπως είναι δομημένο το Διαδίκτυο, τα πακέτα πληροφοριών που εξέρχονται από τον εκάστοτε υπολογιστή, μέχρι να φτάσουν στον τελικό προορισμό, κάνουν ‘στάση’ στους ενδιάμεσους κόμβους/υπολογιστές. Κάποιοι από αυτούς μπορεί να αντιγράψουν τα δεδομένα των πακέτων για την μελλοντική εκμετάλλευση τους. ένας τρόπος προστασίας είναι η λεγόμενη κρυπτογράφηση, με διασημότερο πρωτόκολλο ασφαλείας για τις διαδικτυακές συναλλαγές το SSL που συναντάται και σε URL , το HTTPS.

Στην διερευση ευαίσθητων δεδομένων, μπορούν να συμμετέχουν και τα λεγόμενα cookies. Πρόκειται για κωδικοποιημένα αρχεία που αφήνουν πίσω τους οι ιστοσελίδες για την ευκολότερη πλοήγηση και περιήγηση του χρήστη στα περιεχόμενα τους. Τα cookies ,μεταξύ άλλων , αποθηκεύουν κωδικούς (passwords), προτιμήσεις χρηστών κ.ο.κ. Για τα δεδομένα που περιέχουν αρκετές φορές γίνονται στόχοι κακόβουλων ενεργειών για την αντιγραφή τους και την χρησιμοποίηση τους [5].

Αν και υπάρχουν και άλλοι κίνδυνοι, παρόλα αυτά, οι προαναφερόμενοι είναι αυτοί που ‘απειλούν’ τα ευαίσθητα προσωπικά δεδομένα των χρηστών. Στην παρούσα πτυχιακή, θα γίνει αναφορά στον τρόπο που θεσμοθετήθηκε για την προστασία των ευαίσθητων προσωπικών δεδομένων και πώς αυτός εφαρμόζεται πια.

2.Προστασία Δεδομένων

Τα τελευταία χρόνια τα δεδομένα έχουν γίνει πολύτιμο περιουσιακό στοιχείο. Και η κατοχή τους αποτελεί το άγγιγμα του Μίδα. Ειδικά, τα τελευταία χρόνια που η τεχνολογία έχει εξελιχθεί κυρίως μέσω του Διαδικτύου, δίνεται η δυνατότητα πρόσβασης σε προσωπικά δεδομένα εκατομμυρίων χρηστών ανά τον κόσμο. Διευθύνσεις, ,τηλέφωνα, κωδικοί , αριθμοί ταυτότητας είναι κάποια από τα παραδείγματα προσωπικών δεδομένων που γίνονται στόχος υποκλοπής.

Για αυτό και από το Μάιο του 2018, η Ε.Ε ενέκρινε έναν κανονισμό για την γενική προστασία των δεδομένων μεταξύ των κρατών μελών της. Όμως, πριν γίνει αναφορά σε αυτόν τον κανονισμό και την εφαρμογή του στο τομέα της πληροφορικής, θα γίνει μια μικρή ιστορική αναδρομή , στα καίρια σημεία που οδήγησαν στην απόφαση αυτή.

2.1 Ευρώπη και προστασία δεδομένων

Η επικινδυνότητα διέρευσης και υποκλοπής δεδομένων τόσο των χρηστών όσο και των κυβερνήσεων , είναι και ήταν πάντα ένα καίριο ζήτημα για την Ευρωπαϊκή ένωση. Το ζήτημα της προστασίας των δεδομένων ξεκίνησε το 1968 με τη Σύσταση 509 για τα Ανθρώπινα Δικαιώματα και τις Σύγχρονές και Επιστημονικές Τεχνολογικές Εξελίξεις. Βασιζόμενη η Ευρωπαϊκή Ένωση σε αυτή την σύσταση, προχώρησε το 1973-74 στα Ψηφίσματα 73/22 και 74/29. Τα Ψηφίσματα αυτά έθεσαν τις βάσεις και τις αρχές για τη προστασία των προσωπικών δεδομένων που βρίσκονται αποθηκευμένα σε βάσεις δεδομένων όχι όμως μόνο για το δημόσιο τομέα αλλά και στον ιδιωτικό τομέα.

Επόμενος σταθμός ορόσημο είναι η 28 Ιανουαρίου 1981 κατά την οποία το Συμβούλιο της Ευρώπης υπερψήφισε τη συνθήκη του 1973-74 και την επικύρωσαν και τα 47 μέλη της. Προϋπόθεση είναι να εφαρμοστεί και σε εθνικό επίπεδο για να υπάρξει μια συντονισμένη προσπάθεια στην προστασία των δεδομένων αυτών. Η συνθήκη που υπεγράφη είναι γνωστή ως Συνθήκη 108.

Παρόλες τις προσπάθειες της Ευρωπαϊκής Ένωσης, επειδή οι προαναφερόμενες συνθήκες είχαν ελλείψεις στο καθορισμό αυτών των στόχων, τα πρότυπα ασφαλείας δεν εφαρμόστηκαν με πλήρη επιτυχία. Για διόρθωση αυτών των κακών κειμένων και

παραλείψεων, εκδίδει την Οδηγία Προστασίας Δεδομένων ή αλλιώς Data Protection Directive.

Έκτοτε, έχουν γίνει πολλά βήματα για την περαιτέρω προστασία των δεδομένων, αφού και η τεχνολογία με τη σειρά της έκανε πολλά βήματα προόδου βαδίζοντας στα χνάρια της παγκοσμιοποίησης. Στο πνεύμα αυτό, διεξάχθηκε η υπογραφή του Χάρτη Θεμελιωδών Δικαιωμάτων το Δεκέμβριο του 2000 στη Νίκαια καθώς και στις 4 Νοεμβρίου 2010 ,αποφασίζεται μια κοινή στρατηγική προστασίας των δεομένων περιορίζοντας τη γραφειοκρατία για τις επιχειρήσεις.

Τελευταία ημερομηνία πριν την καταλυτική για τον κανονισμό GDPR ο οποίο θα αναλυθεί σε επόμενο κεφάλαιο, είναι η 25 Δεκεμβρίου 2010 που εκδίδεται μια γενική οδηγία λεγόμενη General Data Protection Regulation η οποία , πέραν το ότι περιλαμβάνει τις προ υπάρχουσες οδηγίες, συστήνει και τρόπους για την επεξεργασία των δεδομένων για την επιβολή του νόμου.

Σκοπός των προαναφερόμενων οδηγιών και κανονισμών ήταν να καθοριστούν τρόποι προστασίας των ευαίσθητων προσωπικών δεδομένων και δεδομένων εθνικών σε ευρωπαϊκό επίπεδο, από την στιγμή που σε εθνικό επίπεδο χωρών δεν είχε γίνει αξιοσημείωτη προσπάθεια. Ελάχιστες χώρες ήταν αυτές που έθεσαν και ενσωμάτωσαν την προστασία των δεδομένων στο Σύνταγμα τους όπως η Ισπανία , Πορτογαλία και Αυστρία [10], [11]

2.2 Ελλάδα και προστασία δεδομένων

Ως μέλος της Ευρωπαϊκής Ένωσης , οι προαναφερόμενε οδηγίες και κανονισμοί αναφέρονται και συστήνονται να εφαρμοστούν καις την Ελλάδα.

Έτσι , λοιπόν, το 1985 γίνεται μια προσπάθεια για τη προστασία των προσωπικών δεδομένων από την επιτροπή Χαλαζωνίτη. Από εκεί και για τα επόμενα χρόνια , μέχρι και το 1992, παρότι υπήρχαν αρκετές προτάσεις, παρόλα αυτά καμία δεν προτάθηκε και δεν υιοθετήθηκε. Καμία ιδιαίτερη νύξη δεν έγινε ακόμα και μετά την έκδοση της σύμβασης 108 από την Ευρωπαϊκή Ένωση.

Η πρώτη προσπάθεια ,και κατά ανάγκη για την προσαρμογή στην αντίστοιχη οδηγία της Ευρωπαϊκής ένωσης , είναι ο Νόμος 2472/97 κατά τον οποίο τίθενται αρχές και προβλέψεις για τα προσωπικά δεδομένα. Το μειονέκτημα του συγκεκριμένου νόμου, είναι ότι έθεσε

πολύ αυστηρούς τρόπους επεξεργασίας των δεδομένων που οδηγούσε σε δυσχέρεια τόσο των δημόσιων οργανισμών αλλά και των ιδιωτικών.

Το επόμενο, ώριμο βήμα, έγινε το 2011 και με την επικύρωση του νόμου 3917/2011. Σύμφωνα με το νόμο αυτό, καθορίζονται τρεις βασικές δικλείδες ασφαλείας , που αφορούν και το δημόσιο και τον ιδιωτικό τομέα. Οι δικλείδες αυτές είναι οι εξής:

1) Καθορισμός νόμιμων τρόπων επεξεργασίας των δεδομένων
2) Παροχή δικαιώματος σε άτομα και τα δεδομένα τους
3) Οργάνωση και έλεγχος της προστασίας των δεδομένων

Παράλληλα με αυτές, καθορίζεται η υποχρέωση τηλεπικοινωνιακών φορέων για παροχή πληροφοριών σε ιδιαίτερα νομικά ζητήματα αλλά και τους τρόπους με τους οποίους επιτρέπεται να επεξεργάζονται τα δεδομένα αυτά οι φορείς. Ορίζονται εποπτικές αρχές όπως η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα που δίνει την σκυτάλη στην Αρχή Διασφάλισης Απορρήτου Επικοινωνιών.

Με λίγα λόγια, με την τελευταία αναθεώρηση νόμου, ορίζονται όπως πρέπει , με τις πλήρεις υποχρεώσεις και δικαιώματα αλλά και συγκεκριμένες περιπτώσεις επεξεργασία των προσωπικών δεδομένων,

Χαρακτηριστικό είναι και το απόσπασμα που υπάρχει πια στο Σύνταγμα της Ελλάδος: «Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα , των προσωπικών δεδομένων , όπως ο νόμος ορίζει» [10]

3.Γενικός Κανονισμός Προστασίας Δεδομένων - GDPR

Οι προσπάθειες της Ευρωπαϊκής Ένωσης για την προστασία των δεδομένων ξεκίνησε από σχετικά νωρίς, όπως αναφέρθηκε και σε προηγούμενες παραγράφους. Όμως, λόγω της τεράστιας εξέλιξης του Διαδικτύου και των δυνατοτήτων που παρέχει, υπήρξε η ανάγκη να καθοριστούν κάποιοι κανόνες για τα νέα αυτά δεδομένα. Αυτοί οι κανόνες ενσωματώνονται στον GDPR ή αλλιώς στον Γενικό Κανονισμός Προστασίας Δεδομένων

3.1 GDPR

Ο Γενικός Κανονισμός Προστασίας δεδομένων είναι ένα σύνολο από κανόνες για το απόρρητο των δεδομένων. Ο κανονισμός αυτός αφορά όλους τους τομείς , δημοσίου και ιδιωτικού χαρακτήρα , και θέτει όρους και περιορισμούς για την επεξεργασία, αποθήκευση δεδομένων και απορρήτου.

Στον κανονισμό αυτό , επίσης , γίνεται σαφής ο όρος των προσωπικών δεδομένων για τα οποία αναφέρεται και η προστασία. Συγκεκριμένα, το άρθρο 4 του GDPR αναφέρει ότι προσωπικό δεδομένο είναι οτιδήποτε μπορεί να χρησιμοποιηθεί για να τακτοποιηθεί ένα άτομο. Παραδείγματος χάριν, αριθμοί ταυτότητας, ΑΦΜ, ΑΜΚΑ, στην περίπτωση της Ελλάδας, θεωρούνται προσωπικά δεδομένα , γιατί καθένα από αυτά ανήκουν σε ένα και μοναδικό πολίτη και η κατοχή τους οδηγεί στην αποκάλυψη της ταυτότητας του. Βέβαια, προσωπικά δεδομένα είναι και ότι σχετίζεται με ηλεκτρονικά και online μέσα όπως email, IP διευθύνσεις, κωδικοί τραπεζών κ.ο.κ. Εξαιρέσεις είναι σε περιπτώσεις θανάτου του ατόμου αλλά δεν αποτελούν εξαίρεση οι απόγονοι και οι συγγενείς του αποθανόντος.

Πέραν, βέβαια, της σαφής καταγραφής των περιπτώσεων που πρέπει να προστατεύονται τα προσωπικά δεδομένα, ο κανονισμός αυτός έχει θέσει και περιπτώσεις κατά τις οποίες επιτρέπεται η επεξεργασία των προσωπικών δεδομένων. Συγκεκριμένα, έχει θέσει τέσσερις διαφορετικές περιπτώσεις. Οι περιπτώσεις αυτές ήταν αναγκαστικές να διατυπωθούν αφού μιλάμε για μια κοινωνία ανθρώπων στην οποία συμπεριλαμβάνεται βία και διαφθορά από τη μια πλευρά του νομίσματος. Από την άλλη, από την στιγμή που το Διαδίκτυο έχει κατακτήσει διάφορους τομείς και οι περισσότερες δραστηριότητες των πολιτών γίνονται

μέσω αυτού, θεώρησαν οι νομοθέτες ότι έπρεπε να προστατεύουν και οι εν λόγω επιχειρήσεις. Οι περιπτώσεις αυτές είναι οι εξής:

- Σε περίπτωση πολιτικής ασφάλειας: σε περιπτώσεις που κινδυνεύει η σωματική ακεραιότητα πολιτών, τότε , τα προσωπικά δεδομένα δεν έχουν προστασία λόγω της μεγαλύτερης εικόνας προστασίας ζωής πολιτών.
- Σε περίπτωση ποινικής δίωξης.
- Σε περίπτωση οικονομικής δραστηριότητας με επιχείρηση όπως online booking, online διασκέδαση κ.ο.κ
- Σε περίπτωση προσωπικής ή οικιακής δραστηριότητας. Σε αυτήν την περίπτωση συγκαταλέγονται και τα κοινωνικά δίκτυα, τα οποία ναι μεν δεν αλληλοεπιδρούν με τους χρήστες βασιζόμενες σε οικονομικές δραστηριότητες, αλλά απαιτούνται κάποια δεδομένα για την σύνδεση τους σε αυτά.

Εν κατακλείδι, ο GDPR θέτει τα όρια και τις βάσεις κατά τις οποίες τα προσωπικά δεδομένα υφίστανται επεξεργασία. Σε οποιαδήποτε περίπτωση – πέραν των εξαιρέσεων-, ο πολίτης θα πρέπει να είναι ενήμερος για το ποια δεδομένα του αποθηκεύονται και μπορεί να επεξεργαστούν, από ποιους θα τεθούν σε επεξεργασία και εάν βέβαια είναι σύμφωνος με την αποθήκευση των δεδομένων του και τυχόν μελλοντική του επεξεργασία.

3.1.1 Άρθρα του GDPR

Ο Γενικός κανονισμός για τη προστασία των δεδομένων είναι χωρισμένος σε άρθρα. Το κάθε ένα από αυτά έχει συγκεκριμένο θέμα και ορίζει τους στόχους , όρους , προϋποθέσεις και υποχρεώσεις όσων συμμετέχουν στην επεξεργασία των δεδομένων αυτών. Στις παρακάτω παραγράφους θα παρουσιαστούν τα άρθρα αυτά παρουσιάζοντας και κάποιες σημαντικές διατυπώσεις τους.

Άρθρο 1: Στο συγκεκριμένο άρθρο ορίζονται τα αντικείμενα και οι στόχοι του κανονισμού. Χαρακτηριστικές είναι οι παράγραφοι 2) και 3).

«2. Ο παρών κανονισμός προστατεύει θεμελιώδη δικαιώματα και ελευθερίες των φυσικών προσώπων και ειδικότερα το δικαίωμά τους στην προστασία των δεδομένων προσωπικού χαρακτήρα.» *«*

«3. Η ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα εντός της Ένωσης δεν περιορίζεται ούτε απαγορεύεται για λόγους που σχετίζονται με την προστασία των φυσικών

προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.»

Άρθρο 2: Ουσιαστικό πεδίο εφαρμογής.

Στο συγκεκριμένο άρθρο ξεχωρίζει η παράγραφος 1) καθώς και η 2) η οποία τονίζει σε ποιες περιπτώσεις δεν εμπίπτει ο κανονισμός για τα προσωπικά δεδομένα. Οι παράγραφοι παρατίθενται παρακάτω.

«1. Ο παρών κανονισμός εφαρμόζεται στην, εν όλω ή εν μέρει, αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης.
2. Ο παρών κανονισμός δεν εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα:
α) στο πλαίσιο δραστηριότητας η οποία δεν εμπίπτει στο πεδίο εφαρμογής του δικαίου της Ένωσης,
β) από τα κράτη μέλη κατά την άσκηση δραστηριοτήτων που εμπίπτουν στο πεδίο εφαρμογής του κεφαλαίου 2 του τίτλου V της ΣΕΕ,
γ) από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας,
δ) από αρμόδιες αρχές για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, συμπεριλαμβανομένης της προστασίας και πρόληψης έναντι κινδύνων που απειλούν τη δημόσια ασφάλεια.»

Άρθρο 3: Εδαφικό πεδίο εφαρμογής

Το συγκεκριμένο άρθρο ορίζει πότε και υπό ποιες συνθήκες γίνεται λόγος για επεξεργασία προσωπικών δεδομένων και στη συνέχεια για τη προστασία τους. Χαρακτηριστική είναι η παράγραφος 2:

«2. Ο παρών κανονισμός εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα υποκειμένων των δεδομένων που βρίσκονται στην Ένωση από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία μη εγκατεστημένο στην Ένωση, εάν οι δραστηριότητες επεξεργασίας σχετίζονται με:

α) την προσφορά αγαθών ή υπηρεσιών στα εν λόγω υποκείμενα των δεδομένων στην Ένωση, ανεξαρτήτως εάν απαιτείται πληρωμή από τα υποκείμενα των δεδομένων, ή
β) την παρακολούθηση της συμπεριφοράς τους, στον βαθμό που η συμπεριφορά αυτή λαμβάνει χώρα εντός της Ένωσης»

Άρθρο 3: Ορισμοί

Στο συγκεκριμένο άρθρο διατυπώνονται με σαφήνεια ορισμοί , ιδιαίτερα σημαντικοί τόσο για τον κανονισμό όσο και τις εθνικές διατάξεις του εκάστοτε κράτους-μέλους. Παρακάτω, αναφέρονται κάποιοι από αυτούς:

«1) «δεδομένα προσωπικού χαρακτήρα»: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου,
2) «επεξεργασία»: κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή,
3) «περιορισμός της επεξεργασίας»: η επισήμανση αποθηκευμένων δεδομένων προσωπικού χαρακτήρα με στόχο τον περιορισμό της επεξεργασίας τους στο μέλλον»

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

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

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

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

14) «βιομετρικά δεδομένα»: δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλο σκοπικά δεδομένα,
15) «δεδομένα που αφορούν την υγεία»: δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, περιλαμβανομένης της παροχής υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του»

«23) «διασυνοριακή επεξεργασία»:

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

επεξεργασία στην Ένωση αλλά που επηρεάζει ή ενδέχεται να επηρεάσει ουσιωδώς υποκείμενα των δεδομένων σε περισσότερα του ενός κράτη μέλη»

Άρθρο 5: Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα

Εδώ διακρίνονται οι παράγραφοι 1 β) και 1 ε), όπως:

«β) συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς· η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1 («περιορισμός του σκοπού»)

ε) διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα· τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον τα δεδομένα προσωπικού χαρακτήρα θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, σύμφωνα με το άρθρο 89 παράγραφος 1 και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο παρών κανονισμός για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων («περιορισμός της περιόδου αποθήκευσης»)»

Άρθρο 6: Νομιμότητα της επεξεργασίας

Πολύ σημαντικό άρθρο το οποίο με τις παραγράφους ορίζει τις συνθήκες που η επεξεργασία των δεδομένων είναι νόμιμα, όπως:

«α) το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς,
β) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης,
γ) η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας,

δ) η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,
ε) η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας,
στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί»

Άρθρο 10: Επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα.

Άρθρο 11: Επεξεργασία η οποία δεν απαιτεί την εξακρίβωση ταυτότητας.

Πέραν των προϋποθέσεων της επεξεργασίας των δεδομένων, στο Κεφάλαιο ΙΙΙ του Γενικού Κανονισμού ορίζονται και τα δικαιώματα των χρηστών των οποίων τα δεδομένα υφίστανται επεξεργασία.

Συγκεκριμένα , στο Άρθρο 15 του αντίστοιχου κεφαλαίου , ορίζονται τα δικαιώματα πρόσβασης του υποκειμένου των δεδομένων. Δηλαδή, το δικαίωμα του χρήστη να γνωρίζει πότε, από ποιον και αν υφίστανται επεξεργασία τα δεδομένα του.

«1 Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει από τον υπεύθυνο επεξεργασίας επιβεβαίωση για το κατά πόσον ή όχι τα δεδομένα προσωπικού χαρακτήρα που το αφορούν υφίστανται επεξεργασία και, εάν συμβαίνει τούτο, το δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα και στις ακόλουθες πληροφορίες:

α) τους σκοπούς της επεξεργασίας,
β) τις σχετικές κατηγορίες δεδομένων προσωπικού χαρακτήρα,
γ) τους αποδέκτες ή τις κατηγορίες αποδεκτών στους οποίους κοινολογήθηκαν ή πρόκειται να κοινολογηθούν τα δεδομένα προσωπικού χαρακτήρα, ιδίως τους αποδέκτες σε τρίτες χώρες ή διεθνείς οργανισμούς,

δ) εάν είναι δυνατόν, το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω διάστημα,
ε) την ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που αφορά το υποκείμενο των δεδομένων ή δικαιώματος αντίταξης στην εν λόγω επεξεργασία,
στ) το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή,
ζ) όταν τα δεδομένα προσωπικού χαρακτήρα δεν συλλέγονται από το υποκείμενο των δεδομένων, κάθε διαθέσιμη πληροφορία σχετικά με την προέλευσή τους,
η) την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων»

Άρθρο 16 & 17: Δικαίωμα διόρθωσης και διαγραφής από το υποκείμενο των δεδομένων.

Άρθρο 21:Δικαίωμα εναντίωσης. Χαρακτηριστικές είναι οι πρώτες δύο παράγραφοί του συγκεκριμένου άρθρου , το οποίο δίνει το δικαίωμα στο υποκείμενο να εναντιωθεί σε επεξεργασία των δεδομένων του.

«1. Το υποκείμενο των δεδομένων δικαιούται να αντιτάσσεται, ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν, η οποία βασίζεται στο άρθρο 6 παράγραφος 1 στοιχείο ε) ή στ), περιλαμβανομένης της κατάρτισης προφίλ βάσει των εν λόγω διατάξεων. Ο υπεύθυνος επεξεργασίας δεν υποβάλλει πλέον τα δεδομένα προσωπικού χαρακτήρα σε επεξεργασία, εκτός εάν ο υπεύθυνος επεξεργασίας καταδείξει επιτακτικούς και νόμιμους λόγους για την επεξεργασία οι οποίοι υπερισχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του υποκειμένου των δεδομένων ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

2. Εάν δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης, το υποκείμενο των δεδομένων δικαιούται να αντιταχθεί ανά πάσα στιγμή στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν για την εν λόγω εμπορική προώθηση, περιλαμβανομένης της κατάρτισης προφίλ, εάν σχετίζεται με αυτήν την απευθείας εμπορική προώθηση.

Στο Κεφάλαιο IV, του προαναφερόμενο κανονισμού , αναφέρονται και οι υποχρεώσεις των υπευθύνων επεξεργασίας των δεδομένων.

Στο παρόν κεφάλαιο, στα άρθρα 32,33,34 αναφέρεται και η ασφάλεια επεξεργασίας των δεδομένων . [6]

Τα άρθρα δεν τελειώνουν , βέβαια , σε αυτούς τους αριθμούς. Έγινε μια αναφορά των πιο σημαντικών για να γίνει κατανοητός ο στόχος και ο τρόπος που τέθηκαν οι όροι για την επεξεργασία των δεδομένων.

Τα άρθρα καταμετρώνται μέχρι το 98 και το καθένα από αυτά προβλέπει ενδελεχώς οποιασδήποτε πτυχές της τυχόν επεξεργασίας των δεδομένων και από τη μεριά του χρήστη αλλά και των επιχειρήσεων/οργανισμών.

Αυτό που πρέπει να γίνει κατανοητό με τα παραπάνω, όπως ορίστηκε και από τον ίδιο κανονισμό, τα παραπάνω άρθρα δεν είναι έχουν στόχο των περιορισμό της ελεύθερης διακίνησης των δεδομένων εντός της ευρωπαϊκής Ένωσης. Αντιθέτως, βάζοντας τις κατάλληλες προϋποθέσεις , οι χρήστες νιώθουν πιο ασφαλείς στις συναλλαγές τους και στην καθημερινή τους δραστηριότητα στο Διαδίκτυο.

Εικόνα 3-1: GDPR

3.2 Επεξεργασία δεδομένων με την συγκατάθεση του πολίτη/χρήστη

Το νόημα του προαναφερόμενου κανονισμού είναι, ουσιαστικά, να αναδείξει τη σημαντικότητα των πληροφορικών, ειδικά που διακινούνται μεσώ Διαδικτύου ,καθώς και τη σημαντικότητα της προστασίας τους. Δεν έχει σκοπό να σταματήσει ή να ανακόψει οποιαδήποτε δραστηριότητα τόσο στο χώρο της ΕΕ όσο και στο Διαδίκτυο.

Για αυτό και ο ίδιος ο πολίτης θα πρέπει να ενημερώνεται για το τρόπο που τα προσωπικά δεδομένα του αποθηκεύονται, επεξεργάζονται και από ποιους γίνεται αυτό. Και σε επόμενο βήμα, να είναι ο ίδιος που θα επιλέξει εάν επιθυμεί να προχωρήσει η διαδικασία ή να την διακόψει.

Στο πνεύμα αυτό, ο Κανονισμός αναφέρει ξεκάθαρα ότι οποιαδήποτε επεξεργασία επι των δεδομένων του χρήστη θα πρέπει να γίνεται με τη συγκατάθεση του. Με τον όρο συγκατάθεση, ο κανονισμός ορίζει ότι ο χρήστης με ξεκάθαρη, ελεύθερη βούληση , ενημερωμένη ενέργεια παραχωρεί το δικαίωμα της επεξεργασίας των δεδομένων του. Βέβαια, προηγουμένως, θα πρέπει να έχει γίνει ανάδειξη των σκοπών και των τρόπων που θα γίνει η επεξεργασία εκ μέρους του υπεύθυνου διαχείρισης.

Ειδικά, στο Διαδίκτυο, που η πλειοψηφία των πληροφοριών απαιτούν και κάποιο προσωπικό δεδομένων των χρήστη, για την εξασφάλιση της νομιμότητας, τα προαναφερόμενα θα πρέπει να εφαρμόζονται. Με κάποιον τρόπο, θα πρέπει, λοιπόν, ο χρήστης να δίνει το ‘’οκ’’ στην επεξεργασία των δεδομένων του.

Ένας τρόπος , λοιπόν, είναι να υπάρχει ένα ειδικό μέρος στην εκάστοτε ιστοσελίδα για την συγκατάθεση ή όχι του χρήστη, απλά κλικάρωντας το.

Ένας άλλος τρόπος, που πια συναντάται σε όλες τις ιστοσελίδες που εναρμονίζονται με τον παραπάνω κανονισμό, είναι η συγκατάθεση ή όχι των cookies. Όπως προαναφέρθηκε σε προηγούμενο εδάφιο, τα cookies πέραν κάποιων επιλογών του χρήστη που αποθηκεύουν και έχουν σκοπό την εύκολη περιήγηση του σε μια ιστοσελίδα, μπορεί να αποτελέσει και κακόβουλο μέσο για την υποκλοπή των δεδομένων του. Για αυτό και μετέπειτα από την εφαρμογή του κανονισμού, εμφανίζονται πια οι λόγοι και οι τρόποι που γίνεται η επεξεργασία των cookies και δίνεται το δικαίωμα του χρήστη στην επιλογή ή όχι της αποθήκευσης τους.

Η συγκατάθεση του χρήστη είναι σημαντική ενέργεια γιατί ο κανονισμός δεν έχει σκοπό την αποκοπή των χρηστών από τη διαδικτυακή του δραστηριότητα και τον περιορισμό της επιχειρηματικής δραστηριότητας ενός οργανισμού, αλλά σκοπό έχει και την έγκυρη και έγκαιρη ενημέρωση του χρήστη για τα δεδομένα του και πως αυτά επεξεργάζονται.

Εδώ, βέβαια, εύλογα τίθεται το εξής ερώτημα «Σε περίπτωση που ο χρήστης είναι ανήλικος, ποιες είναι οι διαδικασίες που πρέπει να ακολουθούνται;». Ο κανονισμός σε αυτή την περίπτωση ορίζει ότι οποιαδήποτε επεξεργασία για άτομα κάτω των 16 γίνεται μόνο με την συγκατάθεση κηδεμόνα. Αν και η τακτική αυτή και ο τρόπος που εφαρμόζεται δημιουργεί ασάφειες στην εφαρμογή του και κενά.

3.3 Επεξεργασία Ιδιαίτερων Προσωπικών Δεδομένων

Πέραν των προσωπικών δεδομένων που ορίστηκαν στον κανονισμό όπως πχ αριθμό ταυτότητας, Username και κωδικοί τραπεζών κ.ο.κ, υπάρχουν και δεδομένα που αποτελούν ιδιαίτερα ευαίσθητα για τα άτομα. Σύμφωνα με το Άρθρο 9 Παράγραφος 1 του Κανονισμού, πληροφορίες που αφορούν τέτοια ιδιαίτερα ευαίσθητα δεδομένα γενικά απαγορεύεται να τίθενται σε οποιαδήποτε επεξεργασία. Τα ιδιαίτερα ευαίσθητα δεδομένα αυτά είναι τα εξής:

- Πληροφορίες για τη φυλετική ή την εθνική καταγωγή ενός ατόμου. Τόπος γέννησής, μητρική του γλώσσα κ.ο.κ επειδή εύκολα μπορούν να στοχοποιήσουν το εκάστοτε άτομο βρίσκονται σε αυτήν την κατηγορία δεδομένων
- Πληροφορίες για την πολιτική άποψη και γενικά πολιτικές δράσεις του ατόμου όπως π.χ. εάν είναι μέλος συνδικαλισμού ή μετέχει σε ένα κόμμα.
- Πληροφορίες για τις θρησκευτικές ή φιλοσοφικές του απόψεις και κατευθύνσεις. Ο τρόπος που επιλέγει κάποιος να ζει και να ακολουθεί κάποιες αρχές είναι καθαρά προσωπικός και δεν μπορεί να τίθεται σε κριτική ή και σε χειρότερες πρακτικές.
- Πληροφορίες για την υγεία και το υγειονομικό παρελθόν του ατόμου. Παρότι υπάρχει ενημέρωση παρόλα αυτά υπάρχουν κάποιες ασθένειες που ακόμα και σήμερα αποτελούν ταμπού για κάποιους πολίτες πχ AIDS κ.ο.κ
- Πληροφορίες για τη σεξουαλική ζωή και σεξουαλικές προτιμήσεις του ατόμου.
- Πληροφορίες για τα γενετικά και βιομετρικά δεδομένα όπως είναι τα δαχτυλικά αποτυπώματα, κληρονομικότητα του ατόμου κ.ο.κ

Όπως εύκολα μπορεί να συμπεράνει κάποιος, ο λόγος που αυτά τα δεδομένα θεωρούνται ιδιαίτερα προσωπικά είναι γιατί η τυχόν διέυρευση τους και ίσως δημοσιοποίησης τους θα θέσει σε κίνδυνο την ασφάλεια του ατόμου αυτού. Ήταν επιτακτική ανάγκη της Ευρωπαϊκής Ένωση, με την διαπολιτισμικότητα που διακρίνει τα κράτη – μέλη μεταξύ τους, να οχυρώσει την προστασία των πολιτών/χρηστών.

Υπάρχουν , βέβαια, και περιπτώσεις που αίρονται οι κανόνες προστασίας τους , όχι όμως για την δημοσίευση τους αλλά για καίριους και σημαντικούς λόγους όπως είναι : υγειονομική περίθαλψη, κοινωνική ασφάλιση, ερευνητικοί σκοποί κ.ο.κ. Σε αυτές τις περιπτώσεις οι κοινοποίηση των δεομένων γίνεται μόνο στα πλαίσια του σκοπού και απαγορεύεται να δημοσιευτούν εκτός αυτών των πλαισίων [7], [10].

4. Μέτρα προστασίας των δεδομένων από επιχειρήσεις και οργανισμούς

Σύμφωνα με όλα όσα αναφέρθηκαν στις παραπάνω σελίδες ο Γενικός Κανονισμός ορίζει τους πότε , πώς και υπό ποιες προϋποθέσεις τα δεδομένων των πολιτών/χρηστών της Ευρωπαϊκής Ένωσης μπορούν τα τεθούν υπό επεξεργασία. Στο παρόν κεφάλαιο, θα γίνει αναφορά στο πώς οι επιχειρήσεις και οι οργανισμοί συμπεριέλαβαν και εφάρμοσαν τον κανονισμό αυτό για τους χρήστες τους.

4.1 Απαιτήσεις ασφάλειας για την προστασία των δεδομένων

Για να είναι σε θέση μια επιχείρηση ή οργανισμός να ανταπεξέλθει στις απαιτήσεις ασφαλείας που καθορίζει ο γενικός κανονισμός , υπάρχουν κάποιες άτυπες ενέργειες τις οποίες μπορεί να ακολουθήσει. Όπως:

- Προστασία από μη εξουσιοδοτημένη πρόσβαση
- Απαραίτητη η κωδικοποίηση για τη μεταφορά των δεδομένων μεταξύ server
- Πρόσβαση μόνο με τη ταυτοποίηση του χρήστη όπως με χρήση username και password.
- Συνεχής ενημέρωση και αναβάθμιση των λογισμικών και του τείχους προστασίας τους
- Συνεχής ενημέρωση και εκπαίδευση των εργαζομένων για την ασφάλεια των δεδομένων και τους νέους κινδύνους που προκύπτουν ανά καιρούς κ.ο.κ

Στις παρακάτω γραμμές αναφέρονται κάποιες από τις ενέργειες σε επίπεδο συστημάτων για την εκάστοτε επιχείρηση [4], [10].

4.2 Ασφάλεια στους πόρους συστήματος (asset management)

Ο όρος «πόρος συστήματος» αναφέρεται σε όλη την υποδομή την τεχνολογική συμπεριλαμβανομένου ηλεκτρικές συσκευές όπως server, υπολογιστές κ.ο.κ αλλά και στα δίκτυα τα οποία διαθέτει μια επιχείρηση ή οργανισμός. Για να είναι σε θέση, λοιπόν, να παρέχει τη μέγιστη δυνατή ασφάλεια σε αυτό το επίπεδο, συστήνονται κάποιες μέθοδοι και ενέργειες όπως:

- Πλήρη καταγραφή όλων των πόρων και των εργαζομένων που έχουν πρόσβαση σε αυτά
- Πλήρης οργάνωση των δεδομένων και την σημαντικότητα τους έτσι ώστε να τεθεί και το αντίστοιχο επίπεδο πρόσβασης στους χρήστες
- Συνεχής αναβάθμιση και ενημέρωση των πόρων [10]

4.3 Ασφάλεια σε αλλαγές συστημάτων (change management)

Τα δεδομένα των συστημάτων των οργανισμών μπορούν να αντιστοιχηθούν με τους έμβιους οργανισμούς. Όπως οποιαδήποτε αλλαγή στη φυσιολογική λειτουργία τους την αντιλαμβάνονται ως ενδεχόμενο κίνδυνο, έτσι και οποιαδήποτε αλλαγή των συστημάτων μπορεί να αποτελεί κίνδυνο όχι μόνο για τα δεδομένα αλλά και για καταστροφή τους.

Για την οποιαδήποτε αλλαγή και για την αναγνώριση της μη εξουσιοδοτημένης αλλαγής των δεδομένων των πόρων αναλαμβάνει ο υπεύθυνος ασφαλείας συστημάτων. Αυτός καθορίζει τα επίπεδα της ασφαλείας, αυτός θα πρέπει να ορίζει , γνωστοποιεί και πραγματοποιεί αλλαγές στα συστήματα. Θα πρέπει να ορίζει μεταξύ άλλων ένα προστατευόμενο περιβάλλον για την ανάπτυξη νέων συστημάτων.

Όπως διαφαίνεται και με τα παραπάνω, η ασφάλεια των δεδομένων για τις επιχειρήσεις ξεπερνάει το απλό κλικ του χρήστη αλλά περιλαμβάνει ένα σύνολο λειτουργειών, και ειδικοτήτων για να ανταπεξέλθουν στις απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων. [10]

Συμπεράσματα

Το Διαδίκτυο αποτελεί πια ένα εργαλείο στα χέρια του εκάστοτε. Καθημερινές δραστηριότητες διευκολύνονται μέσω αυτού. Οικονομικές δραστηριότητες πια για αρκετές επιχειρήσεις και οργανισμούς γίνονται εξ ολοκλήρου μέσω του Διαδικτύου. Ο φόβος όμως παραμένει για όλους τους χρήστες. Κατά πόσο τα δεδομένα τους, κάποια από αυτά, ιδιαιτέρως ευαίσθητα και προσωπικά, είναι ασφαλή και μπορούν να διατηρήσουν την ανωνυμία που προσφέρει το Διαδίκτυο.

Η Ευρωπαϊκή Ένωση επιθυμώντας την προστασία των δεδομένων που διακινούνται στο χώρο της και αφορούν και δημόσιο και ιδιωτικό τομέα αποφάσισε να πάρει δραστικά μέτρα. Αν και η προσπάθεια τους, ξεκίνησε , πριν ακόμα την εμφάνιση του Διαδικτύου, παρόλα αυτά κορυφώθηκε τον Γενικό Κανονισμό Προστασίας Δεδομένων ή όπως αλλιώς είναι πια γνωστός GDPR.

Στα εδάφια της εργασίας αυτής, καταγράφηκαν και αναφέρθηκαν σημαντικά άρθρα και παράγραφοι αυτού του κανονισμού καθώς επίσης και τους τρόπους που ένας οργανισμός έχει τη δυνατότητα να ενημερώνει τον χρήστη για τα δεδομένα του αλλά και το δικαίωμα του χρήστη να εναντιώνεται στην επεξεργασία τους.

Αυτό , βέβαια, απαιτεί συμμόρφωση των οργανισμών και από την άλλη ενημέρωση των δικαιωμάτων τους εκ μέρους των χρηστών. Όπως και να έχει, ο GDPR αποτελεί μια ολοκληρωμένη προσπάθεια για τη προστασία των δεδομένων.

Το μόνο, όμως, που είναι σίγουρο , είναι ότι ο κανονισμός αυτός θα χρειαστεί μια αναβάθμιση , ίσως σε λίγα χρόνια ή ίσως σε δεκαετία, διότι το Διαδίκτυο συνεχώς αναπτύσσεται, εξελίσσεται και μαζί του και οι υπηρεσίες που αυτό προσφέρει στους χρήστες του.

ΠΑΡΑΡΤΗΜΑ

Γενικός Κανονισμός Προστασίας Δεδομένων:

2 https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EL

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] «Ιστορία του Διαδικτύου», 2012. Διαθέσιμο στον ιστότοπο: https://www.retrocomputers.gr/2012-04-19-12-21-04/history-of-internet/content/history-of-the-internet

[2]Πανσελήνας Γ et al. , "Εφαρμογές Πληροφορικής Α΄Λυκείου», 2013, Εκδόσεις Διόφαντος, Αθήνα

[3]Παρασκευάς Μ., «΄Κοινωνίας της Πληροφορίας», 2015, Εκδόσεις Καλλίπος, Αθήνα

[4]Μαυρίδης Ι., «Ασφάλεια πληροφοριών στο Διαδίκτυο», 2015, Εκδόσεις Καλλίπος, Αθήνα

[5]Συρμακέσης Σ., «Το περιεχόμενο , η ασφάλεια και η εμπιστοσύνη στο διαδίκτυο», 2015, Εκδόσεις Καλλίπος, Αθήνα

[6] «Γενικός Κανονισμός για την Προστασία Δεδομένων στην Ευρωπαϊκή Ένωση». Διαθέσιμο στον ιστότοπο: https://www.franklintempletonglobal.com/content-common/miscellaneous/educational-materials/en_GB/local-GB/privacy/gdpr-sychnes-erotiseis.pdf

[7] «Γενικοί Κανονισμό», Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. Διαθέσιμο στον ιστότοπο:

https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EL

[8] Αυγουστιανάκης Μ, «Προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων», 2001

[9] Βασιλειάδου Χ., Διπλωματική Εργασία, «Ευρωπαϊκός Γενικός Κανονισμός Προστασίας Δεδομένων , κίνδυνοι κυβερνοχώρου και ο ρόλος της ασφάλισης έναντι των διαδικτυακών κινδύνων»,2019, Πανεπιστήμιο Μακεδονίας

[10]Κουλάκος Ηλίας, Διπλωματική εργασία, «Το νέο θεσμικό πλαίσιο προστασίας προσωπικών δεδομένων».

[11] «Προστασία Δεδομένων στην ΕΕ». Διαθέσιμο στον ιστότοπο: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_el