ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

UNIVERSITY OF PIRAEUS

# ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ – ΕΦΑΡΜΟΓΗ ΚΑΙ ΣΥΝΕΠΕΙΕΣ

# GENERAL DATA PROTECTION REGULATION (GDPR) – APPLICATION AND CONSEQUENCES


**EXECUTIVE MBA**

ΒΑΛΑΒΑΝΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ ΜΙΧΑΗΛ ΣΦΑΚΙΑΝΑΚΗΣ

ΣΕΠΤΕΜΒΡΙΟΣ 2019

## Παράρτημα Β: Βεβαίωση Εκπόνησης Διπλωματικής Εργασίας

**ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ**

**ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΧΕΙΡΗΜΑΤΙΚΩΝ ΚΑΙ ΔΙΕΘΝΩΝ ΣΠΟΥΔΩΝ**

**ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ**

**ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ**

**ΣΤΗ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ ΓΙΑ ΣΤΕΛΕΧΗ**

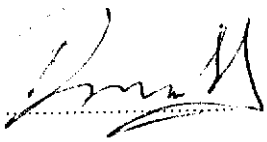
---

### 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 για Στελέχη : Ε-MBA» με τίτλο...ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ – ΕΦΑΡΜΟΓΗ ΚΑΙ ΣΥΝΕΠΕΙΕΣ….GENERAL DATA PROTECTION REGULATION (GDPR) – APPLICATION AND CONSEQUENCES.....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....ΒΑΛΑΒΑΝΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ…….....

Ημερομηνία.....27/09/2019.....

Περίληψη

Η οικονομική και κοινωνική ολοκλήρωση της Ευρωπαϊκής Ένωσης, οι ραγδαίες εξελίξεις της τεχνολογίας και η παγκοσμιοποίηση συντέλεσαν στο πέρασμα της ανθρωπότητας σε μία νέα εποχή, την εποχή της πληροφορίας. Στο πλαίσιο αυτό, άρχισε να αναπτύσσεται ο εύλογος προβληματισμός όσον αφορά στην προστασία των δεδομένων και της ιδιωτικότητας των πολιτών. Ως εκ τούτου, κρίνεται απαραίτητο να δημιουργηθούν ασφαλιστικές δικλίδες, οι οποίες να μπορούν να προστατεύουν επαρκώς τα θεμελιώδη δικαιώματα των ανθρώπων, ενώ δε θα δρουν περιοριστικά στην ανάπτυξη της αγοράς και της τεχνολογίας.

Στην Ευρωπαϊκή Ένωση, θεμελιώδης αρχή είναι η υποστήριξη των πολιτών και ιδιαίτερα εκείνων που δεν διαθέτουν τα μέσα για την προστασία των δικαιωμάτων τους. Αποτελεί εξίσου θεμελιώδες δικαίωμα, η προστασία δεδομένων των φυσικών προσώπων, έναντι της μη εγκεκριμένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Για τους λόγους αυτούς και στο πλαίσιο της ευρύτερης τεχνολογικής εξέλιξης που συντελείται, καθίσταται αναγκαία η αναθεώρηση του ευρωπαϊκού νομικού πλαισίου και η εφαρμογή ενός νέου ασφαλούς δικαίου για την προστασία των δεδομένων προσωπικού χαρακτήρα, προσαρμοσμένου στις απαιτήσεις της σύγχρονης εποχής.

Ο Γενικός Κανονισμός Προσωπικών Δεδομένων 2016/679 - General Data Protection Regulation, ο οποίος περιλαμβάνει πολλούς νεωτερισμούς και προσαρμόζει τους κανόνες προστασίας στα δεδομένα της ισχύουσας ψηφιακής πραγματικότητας, δημιουργήθηκε για την εξασφάλιση των προσωπικών δεδομένων των πολιτών της Ευρωπαϊκής Ένωσης. Η συμμόρφωση στο Γενικό Κανονισμό Προσωπικών Δεδομένων διασφαλίζει τα θεμελιώδη δικαιώματα των πολιτών, επηρεάζοντας εντέλει καθοριστικά την ποιότητα και το βάθος της δημοκρατίας.

Η εφαρμογή του Κανονισμού στην πράξη δείχνει κατά πόσον αντιμετωπίζεται το θέμα της παραβίασης των δεδομένων, πόσον ανταποκρίνεται στις ανησυχίες της κοινωνίας προς αυτό, καθώς και κατά πόσον μπορεί να είναι λειτουργικός ακόμα και εκτός των φυσικών ορίων της Ευρωπαϊκής Ένωσης.

## Συντομογραφίες - Ορισμοί

**Αρχή**: Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

**Δεδομένα**: Δεδομένα προσωπικού χαρακτήρα

**ΕΕ**: Ευρωπαϊκή Ένωση

**Υπεύθυνος επεξεργασίας**: Υπεύθυνος επεξεργασίας δεδομένων προσωπικού χαρακτήρα

**Εκτελών την επεξεργασία**: Εκτελών την επεξεργασία δεδομένων προσωπικού χαρακτήρα

**Ευαίσθητα δεδομένα**: Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα

**ΓΚΠΔ**: Γενικός Κανονισμός Προστασίας Δεδομένων

**Κανονισμός**: Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία δεδομένων αυτών

**Κράτος μέλος**: Κράτος μέλος της Ευρωπαϊκής Ένωσης

**Νόμος**: Νόμος 2472/1997

**Οδηγία**: Οδηγία 96/46/ΕΚ για την προστασία του ατόμου έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών

**Ομάδα Εργασίας**: Ομάδα προστασίας των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα του άρθρου 29 της Οδηγίας 96/46/ΕΚ

**Πρόστιμα υψηλού επιπέδου**: Το πρόστιμο 20.000.000 € ή το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, όποιο είναι μεγαλύτερο, του άρθρου 83 του Γενικού Κανονισμού για την Προστασία Δεδομένων (ΓΚΠΔ).

**Πρόστιμα χαμηλού επιπέδου**: Το πρόστιμο 10.000.000 € ή το 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, όποιο είναι μεγαλύτερο, του άρθρου 83.

**ΥΠΔ**: Υπεύθυνος προστασίας δεδομένων

# Πίνακας Περιεχομένων

# ΕΙΣΑΓΩΓΗ

Στη σύγχρονη πραγματικότητα, η ανθρωπότητα έχει αλλάξει τα δεδομένα και έχει περάσει σε μια διαφορετική εποχή, αυτή της πληροφορίας. Καθώς η τεχνολογία εξελίσσεται ραγδαία, η ανταγωνιστικότητα δημιουργεί όλο και μεγαλύτερη ανάγκη για χρήση ηλεκτρονικών επικοινωνιών σε όλες τις εκφάνσεις της καθημερινότητας, ιδίως στον χώρο εργασίας. Πρόκειται για μία νέα επανάσταση σε επιστημονικό και τεχνολογικό επίπεδο με δραματικές επιπτώσεις, που εκτείνονται σε κάθε τομέα της ανθρώπινης δραστηριότητας. Συνεπώς, η προστασία των προσωπικών δεδομένων των ατόμων αναδεικνύεται ως ένα ιδιαίτερα δυσχερές νομικό ζήτημα. Δύσκολα μπορεί κανείς να αμφισβητήσει το δικαίωμα του εργοδότη να ασκεί έλεγχο στον εργαζόμενο του, όσον αφορά στην απόδοσή του και τη συμπεριφορά του στον χώρο εργασίας. Από την άλλη πλευρά, ο σεβασμός της ιδιωτικότητας, της προσωπικότητας και της αξιοπρέπειας αποτελεί δικαίωμα κάθε ανθρώπου, την απεμπόληση του οποίου δε δικαιολογεί η επίκληση της αναγκαιότητας ελέγχου για εκπλήρωση των συμβατικών υποχρεώσεων. Ο σεβασμός και η προστασία της ιδιωτικής ζωής και της ελεύθερης ανάπτυξης της προσωπικότητας αποτελούν θεμελιώδη και πρωταρχική επιδίωξη κάθε δημοκρατικής κοινωνίας.

Η επανάσταση, που προαναφέρθηκε, βασίζεται στην ψηφιοποίηση της πληροφορίας. Κατά αυτόν τον τρόπο, επιτρέπεται η αποθήκευση μεγάλου όγκου πληροφοριών σε ηλεκτρονική μορφή, ο οποίος μέσω ειδικού λογισμικού μπορεί να μεταφέρεται από υπολογιστή σε υπολογιστή. Αυτός ο μεγάλος όγκος πληροφοριών αντιπροσωπεύει δεδομένα, τα οποία πολλές φορές αποτελούν προσωπικά δεδομένα που ανήκουν σε φυσικά πρόσωπα. Επιπλέον, η τεράστια πρόοδος στον τομέα της πληροφορικής, η ανάπτυξη νέων τεχνολογιών, οι νέες μορφές διαφήμισης, οι ηλεκτρονικές συναλλαγές και η ανάγκη της ηλεκτρονικής οργάνωσης του κράτους φέρουν ως αποτέλεσμα την αυξημένη ζήτηση των προσωπικών πληροφοριών από τον ιδιωτικό και δημόσιο τομέα. Επομένως, η ανεξέλεγκτη καταχώριση και επεξεργασία των προσωπικών δεδομένων σε ηλεκτρονικά και χειρόγραφα αρχεία υπηρεσιών, εταιρειών και οργανισμών μπορεί να προκαλέσει προβλήματα στην ιδιωτική ζωή των πολιτών. Οι κίνδυνοι αυτοί αυξάνονται με τις δυνατότητες ταχύτατης επεξεργασίας εκατομμυρίων δεδομένων, μέσω ηλεκτρονικού υπολογιστή και μεταφοράς πληροφοριών παγκοσμίως, μέσω του Διαδικτύου.

Ενώ παλαιότερα, η αποθήκευση και έρευνα μεγάλου όγκου δεδομένων θα απαιτούσε μεγάλους αποθηκευτικούς χώρους και επίπονη εργασία, πλέον έχει απλοποιηθεί και

γίνεται πολύ πιο άμεσα και με χαμηλότερο κόστος. Η συλλογή, συγκέντρωση και επεξεργασία δεδομένων προσωπικού χαρακτήρα αποτελεί έναν από τους μεγαλύτερους κινδύνους επέμβασης στην προσωπική και ιδιωτική ζωή του ατόμου. Κάθε δραστηριότητα του σύγχρονου ανθρώπου γίνεται καθημερινά αντικείμενο επεξεργασίας και ανάλυσης γεγονός που χρήζει αντιμετώπισης, νομικής κατοχύρωσης και προστασίας**.**

Η συγκέντρωση και επεξεργασία ηλεκτρονικών και μη δεδομένων αντιμετωπίστηκε από νωρίς και συνεχίζει να αντιμετωπίζεται ως ένας από τους μεγαλύτερους κινδύνους επέμβασης στην ιδιωτική ζωή**.** Η ισχύουσα νομοθεσία της Ευρωπαϊκής Ένωσης παρέχει προστασία στους πολίτες, αλλά με την πάροδο του χρόνου και την περαιτέρω ανάπτυξη της τεχνολογίας φαίνεται να χρειάζονται ειδικές διατάξεις, σύμφωνα με τις οποίες να εντοπίζεται με σαφήνεια σε ποια δεδομένα ποιος, πότε και με ποιο σκοπό έχει δικαίωμα πρόσβασης και επεξεργασίας. Στην Ευρώπη, γίνεται προσπάθεια εντοπισμού των προβλημάτων που απασχολούν την κοινωνία σήμερα, αλλά και αύριο, καθώς και τους νέους τομείς υπηρεσιών που είναι κρίσιμοι για την αγορά και τους πελάτες. Σε αυτό το πλαίσιο, η Ευρωπαϊκή Ένωση (ΕΕ) ενέκρινε το Γενικό Κανονισμό Προστασίας Δεδομένων (General Data Protection Regulation – GDPR), ο οποίος τέθηκε σε ισχύ στις 25 Μαρτίου 2018, με σκοπό την περαιτέρω εναρμόνιση των κανόνων για την προστασία των δεδομένων μεταξύ των κρατών μελών της και την αύξηση του επιπέδου προστασίας της ιδιωτικής ζωής για τους πολίτες.

Στην προσπάθεια του Ελληνικού κράτους για εξασφάλιση υψηλού βαθμού εμπιστευτικότητας των πολιτών στις νέες τεχνολογίες επικοινωνιών, είτε μέσω υπολογιστών είτε μέσω άλλων τηλεπικοινωνιακών μέσων, ιδρύθηκαν δύο αρχές προστασίας που σχετίζονται με τα προσωπικά δεδομένα, η Αρχή Προστασίας Προσωπικών Δεδομένων και η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών. Ο κίνδυνος που δημιουργείται από τη συλλογή και επεξεργασία των προσωπικών δεδομένων θεωρήθηκε πολύ σοβαρός, τόσο στην Ελλάδα όσο και διεθνώς, ώστε η προστασία των προσωπικών δεδομένων έχει πλέον ανυψωθεί σε συνταγματικά κατοχυρωμένο ατομικό δικαίωμα. Κατά συνέπεια, τα πρότυπα προστασίας δεδομένων γίνονται όλο και πιο αυστηρά, με αποτέλεσμα οι εταιρείες να αντιμετωπίζουν το πολύπλοκο καθήκον ελέγχου τήρησης της συμμόρφωσης σε διεθνές πλαίσιο.

Ο σκοπός της παρούσας εργασίας είναι να γίνει πλήρης και λεπτομερής αποτύπωση και καταγραφή της έννοιας των προσωπικών δεδομένων και του Κανονισμού που

εφαρμόστηκε για την προστασία αυτών, κάνοντας μια μικρή αναδρομή στην Ευρωπαϊκή πορεία προς το Γενικό Κανονισμό Προστασίας Δεδομένων - GDPR, καθώς και στην Ελληνική πραγματικότητα και νομοθεσία περί της προστασίας προσωπικών δεδομένων.

# ΚΕΦΑΛΑΙΟ 1: ΠΛΗΡΟΦΟΡΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

## 1.1 Η ΤΕΧΝΟΛΟΓΙΑ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Το Διαδίκτυο (Internet) έχει χαρακτηριστεί ως η σημαντικότερη συνεισφορά της Πληροφορικής στον 20ό αιώνα. Δημιουργήθηκε στις Ηνωμένες Πολιτείες με σκοπό την κάλυψη των αναγκών των ερευνητών της αμυντικής βιομηχανίας. Στη συνέχεια, με τη βοήθεια της αλληλεπίδρασης του Διαδικτύου με σχετικές τεχνολογίες, οι ηλεκτρονικοί υπολογιστές έγιναν χρήσιμοι για όλους, με την έννοια ότι δεν χρειάζονταν πλέον εξειδικευμένες γνώσεις πληροφορικής. Το Διαδίκτυο μετατράπηκε από ένα μέσο απεικόνισης κειμένου σε  ένα πλήρες σύστημα πολυμέσων.

Αποτελεί ένα δίκτυο που επιτρέπει την ανταλλαγή δεδομένων μεταξύ διασυνδεδεμένων υπολογιστών. Η τεχνολογία του είναι βασισμένη στη διασύνδεση επιμέρους δικτύων σε όλο τον κόσμο και σε πολυάριθμα πρωτόκολλα επικοινωνίας. Το φυσικό δίκτυο και τα πρωτόκολλα αποτελούν δύο από τα τρία στοιχεία της λειτουργίας του Διαδικτύου. Το τρίτο, είναι εκείνο που αφορά στην άμεση ανθρώπινη επέμβαση, μέσω των εργαλείων λογισμικού και των εφαρμογών δικτύου, με βασικό συστατικό τη δομή τους. Κάθε υπολογιστής που συνδέεται με ένα δίκτυο που το απαρτίζει, γίνεται και αυτός μέλος του. Στην πιο εξειδικευμένη μορφή του, με τον όρο Διαδίκτυο περιγράφεται το παγκόσμιο πλέγμα διασυνδεδεμένων υπολογιστών, το οποίο παρέχει στους χρήστες του υπηρεσίες και πληροφορίες. Η τεχνική και ο τρόπος της διασύνδεσης δικτύων μέσω μεταγωγής πακέτων και της στοίβας πρωτοκόλλων ονομάζεται Διαδικτύωση.

Σε συνδυασμό με την ολοένα αναπτυσσόμενη ψηφιακή τεχνολογία, έχει δημιουργηθεί μία τεράστια αγορά γνώσεων/πληροφοριών, στην οποία κάθε χρήστης έχει την δυνατότητα να μοιραστεί πληροφορίες με άλλους χρήστες γενόμενος, ακόμα και ο ίδιος δημιουργός και πάροχος των πληροφοριών αυτών. Ο όγκος των πληροφοριών στο Διαδίκτυο είναι μεγάλος, κατηγοριοποιώντας τις πληροφορίες σε ευκολότερα και δυσκολότερα προσβάσιμες από τον χρήστη. Ωστόσο, οι πληροφορίες που "ανεβαίνουν" στο Διαδίκτυο δεν ελέγχονται άμεσα από κάποιον ιεραρχικά ανώτερο χρήστη ή οργανισμό.

Μέσω του διαδικτύου έγινε εφικτή η συγκέντρωση μεγάλου όγκου πληροφοριών και επηρεάστηκε σημαντικά τον τρόπο διάθεσής τους, παρ’ όλα αυτά δε συμβαίνει το ίδιο και στον τρόπο παραγωγής αυτών. Από την άλλη πλευρά, το Διαδίκτυο ασκεί μεγάλη επίδραση στην διαδικασία παραγωγής δημοσιογραφικών προϊόντων. Η δημιουργία της είδησης δεν αποτελεί πλέον μονοπώλιο λίγων, αφού ο κάθε χρήστης μπορεί εάν το επιθυμεί να δημιουργήσει πληροφορία ανά πάσα στιγμή. Επίσης, χάρη στη

μεγάλη συγκέντρωση γνώσης στο Διαδίκτυο, η έννοια της κοινωνικής ισότητας παίρνει και πάλι μεγάλη σημασία. Υπάρχει σαφώς χάσμα ανάμεσα σε πληροφοριακά πλούσιους και πληροφοριακά φτωχούς, το οποίο θα διευρύνεται όσο αυξάνεται η συγκέντρωση της γνώσης αυτής. Αυτό καθιστά έναν λόγο που κάνει πιο επιτακτική την ανάγκη για διερεύνηση του αρχικού ερωτήματος «ποιος θα ελέγξει τη γνώση αυτή».

Με σκοπό την διασαφήνιση του ορισμού του Διαδικτύου υπάρχουν τρία βασικά χαρακτηριστικά που το διέπουν. Το Διαδίκτυο αποτελεί:

- Δίκτυο υπολογιστών παγκόσμιας εμβέλειας
- Μέσο επικοινωνίας, το οποίο είναι ιδιαίτερα οικονομικό
- Μέσο άντλησης, πρόσβασης και εκμετάλλευσης πληροφοριών

**Worldwide Internet users**

| | 2005 | 2010 | 2017[a] |
|---|---|---|---|
| **World population**[6] | 6.5 billion | 6.9 billion | 7.4 billion |
| **Users worldwide** | 16% | 30% | 48% |
| **Users in the developing world** | 8% | 21% | 41.3% |
| **Users in the developed world** | 51% | 67% | 81% |

[a] Estimate.

Source: International Telecommunications Union.[7]

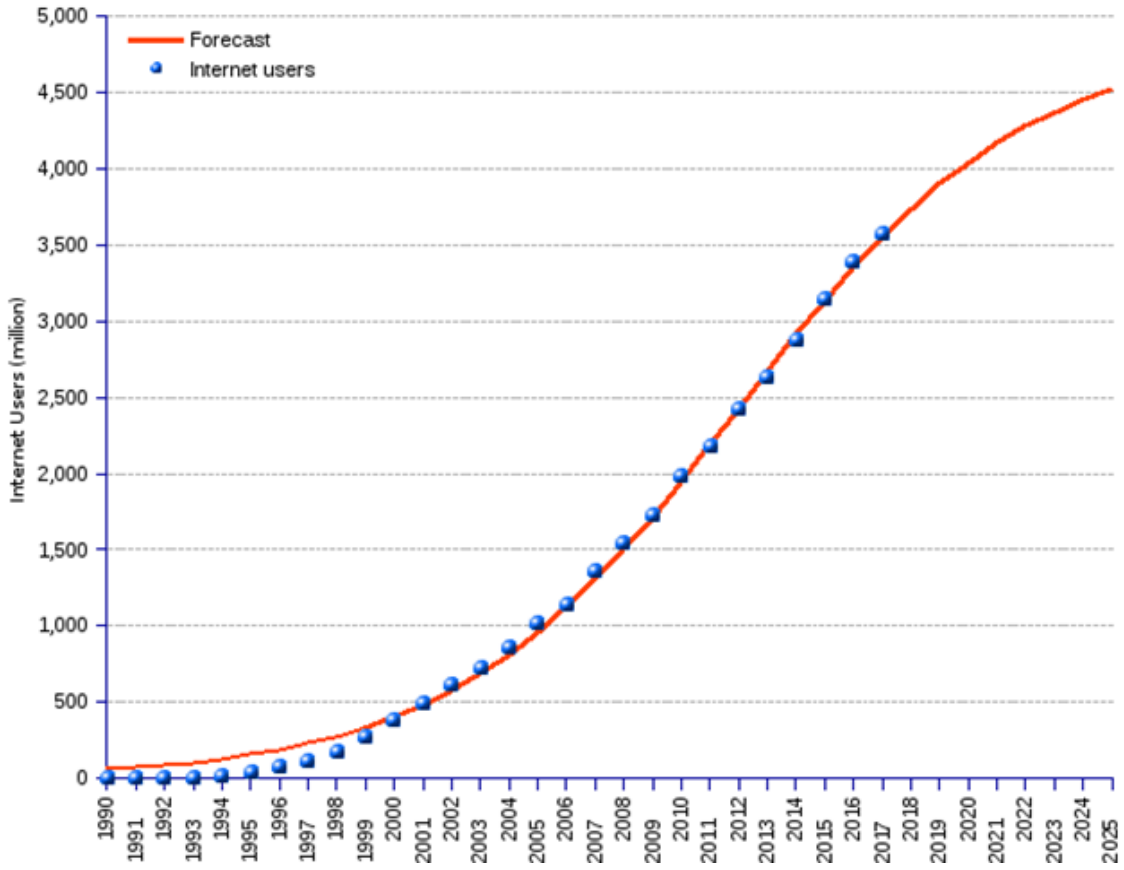
Επιπλέον, είναι σημαντικό ότι δεν υπάρχει ομάδα ανθρώπων που να ασκεί διοίκηση στο Διαδίκτυο. Είναι γνωστό ότι το Διαδίκτυο είναι μη ελεγχόμενο, με την έννοια ότι δεν υπάρχει κάποια ενιαία κυβερνητική ή άλλη αντίστοιχη αρχή, η οποία θα ελέγχει το περιεχόμενό του πριν αυτό δημοσιευθεί, καθώς αυτό θα αποτελούσε λογοκρισία. "Το Διαδίκτυο ελέγχεται από τους χρήστες του". Για το λόγο αυτό, τα ηλεκτρονικά εγκλήματα, η παραβίαση πνευματικών δικαιωμάτων, η ψευδοπροσωπία και η προσφορά παρανόμων προϊόντων είναι φαινόμενα υπαρκτά στο Ίντερνετ και ο περιορισμός τους είναι ιδιαίτερα δύσκολος. Βεβαίως, οι κρατικές υπηρεσίες, οι αστυνομικές αρχές σε κάθε χώρα, καθώς και οι αντίστοιχες νομοθετικές ρυθμίσεις, παρεμβαίνουν για την αναστολή των αξιόποινων και εγκληματικών πράξεων που διαπράττονται μέσω Διαδικτύου.

Όσον αφορά το Διαδίκτυο και Ευρωπαϊκή Ένωση, στο άρθρο 11 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης περί ελευθερίας της έκφρασης και της ενημέρωσης κατοχυρώνεται το δικαίωμα των Ευρωπαίων πολιτών για

ελεύθερη πρόσβαση στο Διαδίκτυο. Παράλληλα, έχει ψηφιστεί στο Ευρωπαϊκό Κοινοβούλιο τροπολογία σύμφωνα με την οποία «δεν μπορεί να επιβάλλεται περιορισμός επί των θεμελιωδών δικαιωμάτων και ελευθεριών των τελικών χρηστών, χωρίς να προηγηθεί δικαστική απόφαση, εκτός από περιπτώσεις όπου απειλείται η ασφάλεια των πολιτών και στις οποίες η απόφαση δύναται να είναι αντίστοιχη». Ωστόσο, η πρόσβαση στο Διαδίκτυο θα μπορεί να απαγορευτεί με σχετικές δικαστικές αποφάσεις που θα επιβάλλει η εκάστοτε εθνική νομοθεσία στο όνομα της απειλής της ασφάλειας.

Είναι πολύ σημαντικό να κατανοηθεί πως οι χρήστες του Διαδικτύου δεν είναι πελάτες αλλά πολίτες και ως τέτοιοι θα πρέπει να αντιμετωπίζονται σε θέματα που αφορούν αφενός την υποδομή του διαδικτύου και αφετέρου το δικαίωμα πρόσβασης σε αυτό. Σχετικά με την υποδομή οφείλει η εκάστοτε εθνική αρχή να μεριμνά για την επέκταση του δικτύου, ακόμη και στις περιοχές εκείνες που η ιδιωτική πρωτοβουλία αρνείται να προβεί στην απαιτούμενη επένδυση, διότι τη θεωρεί οικονομικά ασύμφορη. Με τον τρόπο αυτό θα διασφαλιστεί το δικαίωμα των πολιτών για ενημέρωση και ελευθερία έκφρασης. Συνεπώς, όσον αφορά την πρόσβαση πρέπει να κατοχυρώνεται το δικαίωμα των πολιτών για ελεύθερη και ισότιμη πρόσβαση.

Η Διεθνής Ένωση Τηλεπικοινωνιών - International Telecommunications Union (ITU) έδειξε ότι μέχρι το τέλος του 2017 ο αριθμός των παγκόσμιων χρηστών του Διαδικτύου ανήλθε στους 3,6 δισεκατομμύρια. Με άλλα λόγια, το 48% του παγκόσμιου πληθυσμού χρησιμοποιεί το Διαδίκτυο. Συνεπώς, υπάρχουν ακόμα 3,9 δισεκατομμύρια άνθρωποι που δεν είναι ακόμη συνδεδεμένοι στο Διαδίκτυο. Ο αριθμός των νοικοκυριών με πρόσβαση στο Διαδίκτυο αυξάνεται σε όλες τις περιφέρειες, αλλά εξακολουθούν να υπάρχουν μεγάλες διαφορές μεταξύ των ανεπτυγμένων και των αναπτυσσόμενων χωρών. Η χρήση του Ίντερνετ είναι πιθανό να συνεχίσει να αυξάνεται για μερικά ακόμα χρόνια, φθάνοντας το 90% της συνολικής δυνητικής αγοράς μόλις το 2023, για να ανέλθει στο εκτιμώμενο σημείο κορεσμού των 4.9 δισεκατομμυρίων χρηστών.




Πηγή: http://stats.areppim.com/

## 1.2 ΠΛΗΡΟΦΟΡΙΑ

Η πληροφορία είναι γεγονότα και απόψεις που προσφέρονται και λαμβάνονται από έμβια όντα, μέσα μαζικής επικοινωνίας, ηλεκτρονικούς υπολογιστές, μέσω διαδικτύου, και από πάσης φύσεως παρατηρήσιμα φαινόμενα στο ευρύτερο περιβάλλον. Η έννοια της πληροφορίας σχετίζεται με την έννοια των δεδομένων. Οι δύο έννοιες πολλές φορές συγχέονται γιατί αποκτώντας σημασία, τα δεδομένα μεταπίπτουν σε πληροφορία. Τα δεδομένα, μην έχοντας λάβει από τη νόηση συγκεκριμένη σημασία, δεν αποτελούν πληροφορία. Αντιθέτως, η πληροφορία είναι πάντα δεδομένα με σημασία, δεδομένα με «ουσιαστικό» περιεχόμενο.

Η πληροφορία είναι το αποτέλεσμα που προκύπτει από την κατάλληλη επεξεργασία δεδομένων, η οποία γίνεται με τη βοήθεια της σύγχρονης τεχνολογίας. Τα δεδομένα μετασχηματίζονται σε πληροφορίες μέσα από την διαδικασία της επεξεργασίας. Αυτή η διαδικασία γίνεται με σκοπό την επίλυση κάποιου συγκεκριμένου ζητήματος, την απάντηση κάποιου συγκεκριμένου ερωτήματος και γενικότερα παραπέμπει σε καινούριο στοιχείο γνώσης. Οι πληροφορίες που λαμβάνουμε από την επεξεργασία

δεδομένων μπορούν να χρησιμοποιηθούν ως νέα δεδομένα για περαιτέρω επεξεργασία και να δώσουν ως αποτέλεσμα νέες πληροφορίες.

Συγκεκριμένα σε ό,τι αφορά τη λειτουργία και τη βιωσιμότητα των επιχειρήσεων σήμερα, η ικανότητα επεξεργασίας και αξιοποίησης πληροφοριών αποτελεί καθοριστικό εργαλείο για την απόκτηση οικονομικής δύναμης όπως είναι το χρήμα, η γη, οι πρώτες ύλες και η τεχνολογία. Η ύπαρξη πληροφοριών είναι απαραίτητη σε όλους τους τομείς των επιχειρήσεων, κυρίως σε τμήματα που παίρνουν διοικητικές αποφάσεις και σε διοικητικά στελέχη που εκτελούν τις λειτουργίες σχεδιασμού (planning), της οργάνωσης (organizing), της στελέχωσης (staffing), της διεύθυνσης (directing) και του ελέγχου (controlling).


Πηγή: https://www.managementstudyhq.com/functions-of-management.html

Η πληροφορία είναι αγαθό που έχει οικονομική αξία, η οποία μπορεί να μετρηθεί και για να θεωρεί χρήσιμη θα πρέπει να χαρακτηρίζεται από:

- ακρίβεια, η οποία μπορεί να ορισθεί ως ο λόγος της σωστής πληροφορίας προς την παραγομένη μέσα σε μια χρονική περίοδο
- επικαιρότητα, χρειάζεται να αφορά άμεσα το παρόν και να μπορεί να χρησιμοποιηθεί έχοντας ακόμα αξία
- πληρότητα
- σχετικότητα

Ο Παγκόσμιος Ιστός άλλαξε ριζικά τον τρόπο που αναζητούμε και αποκτούμε πρόσβαση σε πληροφορίες. Η σύγχρονη τεχνολογία κατέστησε δυνατή την αύξηση συλλογής και άμεσης αποθήκευσης πληροφοριών, καθώς και τη μείωση του χρόνου πρόσβασης στα αρχεία. Μέσω του Διαδικτύου μπορούμε πολύ εύκολα και γρήγορα να βρούμε στοιχεία για ένα θέμα που μας ενδιαφέρει, να ενημερωθούμε για τις τρέχουσες εξελίξεις, να ψυχαγωγηθούμε, μέχρι και να δεχθούμε οδηγίες πλοήγησης για τις μετακινήσεις μας.

Παράλληλα, τα τελευταία χρόνια η συμμετοχή μας Διαδίκτυο γίνεται πιο ενεργητική, και ο χρήστης έχει ενεργό ρόλο στην παραγωγή και διακίνηση της διαδικτυακής πληροφορίας. Το γεγονός αυτό μετέβαλε τις συνήθειες των χρηστών του σε όλο τον κόσμο, οι οποίοι έσπευσαν να εκμεταλλευθούν τις νέες δυνατότητες που τους προσφέρονται, αναπτύσσοντας εργαλεία που σήμερα αποτελούν κομμάτι της καθημερινότητάς μας.

Από τις αρχές του 21$^{ου}$ αιώνα, λόγω της ραγδαίας εξέλιξης της τεχνολογίας και της διάδοσή της σε όλες τις εκφάνσεις της καθημερινής ζωής, παρατηρείται μια παγκόσμια κοινωνία της πληροφορίας. Η κοινωνία της πληροφορίας εφοδιάζει τον κόσμο με νέα δεδομένα και νέες ευκαιρίες για ανάπτυξη, απασχόληση, ευημερία και ποιότητα ζωής των πολίτων. Σήμερα, η κοινωνία της πληροφορίας τείνει να ταυτιστεί με το Διαδίκτυο , μέσω του οποίου οι άνθρωποι μπορούν να κάνουν συναλλαγές, να επικοινωνούν μεταξύ τους και να έχουν πρόσβαση σε ένα τεράστιο όγκο πληροφοριών. Ωστόσο, η ποιότητα των πληροφοριών που διατίθεται, χρήζει αξιολόγησης, ως προς την γνησιότητα και ακρίβεια των στοιχείων που εισάγονται. Μεταξύ των άλλων, και τα δεδομένα και οι πληροφορίες, που οι ίδιοι οι χρήστες παρέχουν, χρήζουν προστασίας.

## 1.3 ΔΙΑΔΙΚΤΥΑΚΟΙ ΚΙΝΔΥΝΟΙ

Το Διαδίκτυο αναμφισβήτητα αποτελεί ένα θαυμαστό εργαλείο της σύγχρονης εποχής. Ωστόσο η ραγδαία εξέλιξή του έχει προκαλέσει τη δημιουργία ποικίλων προβλημάτων καθώς και αρκετά εμπόδια στην επίλυση αυτών. Η πρόσβαση στο Διαδίκτυο σήμερα δεν είναι καθόλου ακίνδυνη, ανεξάρτητα από τον τρόπο χρήσης των υπηρεσιών του. Υπάρχουν πολλοί χρήστες που χαρακτηρίζονται κακόβουλοι, καθώς και αρκετές δυνατότητες πρόκλησης ζημιών, τόσο στο επίπεδο του χρησιμοποιούμενου λογισμικού και υλικού, όσο και σε προσωπικό επίπεδο.

**Μορφές διαδικτυακών κινδύνων αποτελούν οι εξής:**

- **Πρόκληση ζημιών στο υπολογιστικό σύστημα**

Ο κύριος κίνδυνος πρόκλησης ζημιών στο υπολογιστικό σύστημα ενός ανυποψίαστου χρήστη είναι η μόλυνση του συστήματος του υπολογιστή με κάποιον ιό. Η μόλυνση γίνεται όταν ο χρήστης λαμβάνει κάποιο φαινομενικά αθώο αρχείο, όπως ένα κείμενο ή μια φωτογραφία. Όταν δοκιμάσει να το χρησιμοποιήσει, ο ιός ενεργοποιείται, αναλαμβάνει δράση και επιμολύνει το σύστημα. Μπορεί να καταστρέψει από μερικά αρχεία μέχρι και ολόκληρο το σκληρό δίσκο του συστήματος. Επίσης, ο ιός μπορεί να αποσταλεί απευθείας από τον ιστότοπο που επισκέπτεται ο χρήστης, χωρίς να εμφανισθεί κάποια ένδειξη λήψης αρχείου. Στην περίπτωση αυτή, εκμεταλλεύεται τα κενά ασφαλείας στο λογισμικό του χρήστη. Παρόμοιας δράσης προγράμματα είναι τα αποκαλούμενα worms και οι δούρειοι ίπποι.

- **Πρόκληση ζημιών σε προσωπικά δεδομένα**

Στην κατηγορία αυτή υπάγονται τόσο οι δούρειοι ίπποι, όσο και κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου. Με τον τρόπο αυτό, υπάρχει πιθανότητα υποκλοπής όχι μόνο προσωπικών δεδομένων κάποιου χρήστη, όπως ο αριθμός ταυτότητάς του ή το ΑΦΜ του, αλλά και αριθμοί πιστωτικών καρτών και λογαριασμών τραπέζης. Ανάλογα τεχνάσματα χρησιμοποιούνται και από ορισμένους ιστοτόπους, στους οποίους ο ανυποψίαστος χρήστης καταχωρεί παρόμοια στοιχεία παραγγέλλοντας ένα προϊόν, το οποίο όχι μόνο δεν υπάρχει και δε θα λάβει ποτέ, αλλά τα δεδομένα του μπορούν να χρησιμοποιηθούν από τους δημιουργούς του ιστοτόπου για να πραγματοποιήσουν οι ίδιοι αγορές που επιθυμούν, χρεώνοντας τον "πελάτη" τους. Η μέθοδος υφαρπαγής προσωπικών δεδομένων μέσω ηλεκτρονικού ταχυδρομείου αποκαλείται "Phishing". Οι χρήστες είναι καλό να γνωρίζουν ότι σε κανένα χρηματοπιστωτικό φορέα δεν επιτρέπεται να χρησιμοποιήσει το Διαδίκτυο για να ανανεώσει προσωπικές πληροφορίες και εκτός αυτού κάθε προστατευμένος ιστοτόπος αρχίζει πάντα με το πρόθεμα https (secure, ασφαλής).

- **Παραπλάνηση**

Πολλές φορές οι χρήστες του Διαδικτύου χρησιμοποιούν τις υπηρεσίες του για να βρουν κάποιες πληροφορίες που χρειάζονται. Μερικοί ιστότοποι, όμως, εμφανίζουν πληροφορίες, οι οποίες φαινομενικά είναι ακριβείς ή αναφέρουν απόλυτα αξιόπιστους δημιουργούς ή πηγές, αλλά στην πραγματικότητα δεν ισχύει. Ο σκοπός αυτών των πράξεων μπορεί να είναι είτε η αποκομιδή ιδίου οφέλους ή η χαρά της

παραπλάνησης των χρηστών. Ο όρος που περιγράφει αυτού του είδους την παραπλάνηση είναι "Hoax".

Οι πιο συνηθισμένες τακτικές εξαπάτησης των χρηστών είναι το Phishing και το Pharming:

- Phishing

Η μέθοδος “phishing” ορίζεται ως η αθέμιτη απόκτηση δεδομένων ή η διάπραξη απάτης στο διαδίκτυο. Η έκφραση “phishing” προέρχεται από την συνήθεια των hackers να χαρακτηρίζουν τους ηλεκτρονικούς τόπους στους οποίους έχουν πρόσβαση “phish”. Το phishing χαρακτηρίζεται η πράξη με την οποία κάποιος προσπαθεί να αποκτήσει πληροφορίες, όπως ονόματα χρηστών, κωδικούς πρόσβασης καθώς και στοιχεία πιστωτικών καρτών, καθώς και άμεσα ή έμμεσα χρήματα, έχοντας φαινομενικά την όψη μιας αξιόπιστης ηλεκτρονικής επικοινωνίας.

Ειδικότερα, ως “phishing” περιγράφεται η αποστολή ηλεκτρονικών μηνυμάτων (emails), αποσκοπώντας την κλοπή εμπιστευτικών στοιχείων που ανήκουν στον παραλήπτη του ηλεκτρονικού μηνύματος. Επίσης, με σκοπό να δελεάσουν το ανυποψίαστο κοινό και να αντιγράψουν πολλές φορές οικονομικά στοιχεία ή και κωδικούς πρόσβασης, χρησιμοποιούνται ανακοινώσεις που υποτίθεται ότι είναι από δημοφιλείς κοινωνικές ιστοσελίδες, ιστοσελίδες δημοπρασιών, τράπεζες ή γίνεται απευθείας σύνδεση των επεξεργαστών πληρωμής και στέλνουν phishing emails που περιέχουν συνδέσμους προς ιστοσελίδες που έχουν μολυνθεί με κακόβουλο λογισμικό.

Ως αποτέλεσμα επειδή η μέθοδος “phishing” βασίζεται στην πλάνη του θύματος με σκοπό την περιουσιακή του ζημία, οι κακόβουλοι χρήστες (phishers) καταφέρνουν μεταφέρουν στον εαυτό τους ή/και σε τρίτους παράνομο περιουσιακό όφελος. Η δε πράξη συνιστά απάτη και η παράνομη δραστηριότητα των κακόβουλων χρηστών διώκεται ποινικά. Συγκεκριμένα το “phishing”, κατά το άρθρο 386 του Ποινικού Κώδικα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών και αν η ζημία που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον δύο ετών.

- Pharming

Η τεχνική του “pharming” αποτελεί μέθοδο διαδικτυακής εξαπάτησης, η οποία λειτουργεί με παρόμοιο τρόπο όπως και το “phishing”. Πρόκειται για ένα ειδικό πρόγραμμα το οποίο εκμεταλλεύεται τα κενά ασφαλείας του συστήματος, διεισδύει στον υπολογιστή του θύματος και αλλάζει τις λειτουργίες κατά τέτοιο τρόπο, ώστε, ακόμη και αν ο χρήστης πληκτρολογεί τη σωστή διεύθυνση του διαδικτυακού τόπου

που θέλει να επισκεφτεί, ο συγκεκριμένος υπολογιστής τον “οδηγεί” μόνο σε πλαστές ιστοσελίδες. Ειδικά σε περιπτώσεις συναλλαγών μέσω on-line banking σε ιστοσελίδες τράπεζας, μπορεί τελικώς να καταλήγει να μεταφέρει τα χρήματά του στους δράστες (pharmers).

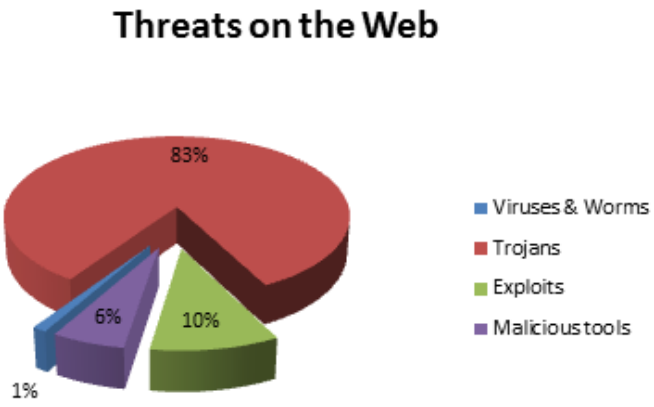
Γίνεται σαφές ότι η αύξηση των ωρών χρήσης του διαδικτύου βοηθάει και πολλαπλασιάζει τον κίνδυνο εγκατάστασης προγραμμάτων που καθιστούν δυνατό το “pharming”, το οποίο εξελίσσεται σε μία από τις πιο σοβαρές μορφές εγκληματικότητας στο διαδίκτυο.

Συμπερασματικά, οι ανωτέρω δύο τρόποι εξαπάτησης μπορούν να τιμωρηθούν, σύμφωνα με τις ισχύουσες διατάξεις του Ποινικού Κώδικα. Για την αντιμετώπιση τέτοιων φαινομένων είναι απαραίτητη η λήψη τεχνικών μέτρων ασφαλείας, καθώς και η ευαισθητοποίηση των χρηστών του Διαδικτύου, ώστε να μην γίνονται εύκολα θύματα.

Οι κυριότερες και πιο διαδεδομένες απειλές του Διαδικτύου είναι ακόλουθες:

- Κακόβουλες εισβολές σε δίκτυα (hacking, cracking)
- Ανεπιθύμητη αλληλογραφία (spamming)
- Ηλεκτρονικό «Ψάρεμα» (phising - pharming)
- Διασπορά κακόβουλου λογισμικού (ιοί- viruses, σκουλήκια- worms, δούρειοι ίπποι- trojan horses)
- Πειρατεία ονομάτων χώρου (domain names piracy)
- Επιθέσεις Άρνησης Εξυπηρέτησης (DoS, Denial of Service)

Για την αποφυγή των διαδικτυακών κινδύνων υπάρχουν ανάλογες μέθοδοι προστασίας. Οι πιο συνηθισμένες εξ αυτών είναι η χρήση τείχους προστασίας (firewall), η χρήση λογισμικού προστασίας ενάντια σε ιούς και προγράμματα κατασκοπείας (spyware) και η συνεχής ενημέρωση των χρηστών. Οι τρόποι αυτοί για να έχουν καλύτερο και πιο σίγουρο αποτέλεσμα, θα πρέπει να χρησιμοποιούνται σε συνδυασμό.




Πηγή: https://eugene.kaspersky.com/2012/05/25/the-dangers-of-exploits-and-zero-days-and-their-prevention/

## 1.4 ΔΙΑΔΙΚΤΥΑΚΕΣ ΑΠΕΙΛΕΣ ΚΑΙ ΠΡΟΓΡΑΜΜΑΤΑ

Η ύπαρξη του Διαδικτύου συνέβαλε στη διευκόλυνση της σύγχρονης ζωής, καθώς και την ανάπτυξη των ηλεκτρονικών μέσων μεταφοράς δεδομένων. Εντούτοις, δημιουργήθηκαν οι προϋποθέσεις για την τέλεια υποκλοπή των δεδομένων αυτών. Μέσω της υπάρχουσας τεχνολογίας, είναι δυνατή όχι μόνο η παρακολούθηση όλων των δεδομένων που διακινούνται στον πλανήτη, αλλά και ο αυτόματος διαχωρισμός των άχρηστων και περιττών πληροφοριών, η αποθήκευση των χρήσιμων και η διαχείριση των αποτελεσμάτων. Παρόλα αυτά, η υποκλοπή των πληροφοριών και δεδομένων φυσικών προσώπων αποτελεί την ενδεχόμενη συνέπεια της χρήσης του Διαδικτύου. Η υποκλοπή δεν είναι δυνατόν να γίνει άμεσα αντιληπτή από το στόχο.

Υποκλοπές δεδομένων καθώς και ζημίες στο λογισμικό σύστημα ηλεκτρονικών υπολογιστών παρατηρείται ότι μπορούν να προκληθούν από τρία είδη απειλών του Διαδικτύου. Οι απειλές αυτές είναι προγράμματα γνωστά και ως Ιοί, Σκουλήκια, Δούρειοι Ίπποι. Τα προγράμματα αυτά έχουν την ικανότητα να κρύβονται μέσα σε εικόνες ή κείμενα, παραπλανώντας το χρήστη ή κάνοντας δύσκολο τον εντοπισμό τους από αυτόν.

**Ιοί - Viruses**

Ο πρώτος ιός εμφανίστηκε το 1982 και ήταν το πρόγραμμα Elk Cloner. Σχεδιάστηκε από τον Rich Skrenta και διαδόθηκε μέσω δισκετών. Εκείνη την εποχή οι περισσότεροι ιοί μεταδίδονταν μέσω δισκετών, συνεχίζοντας με τον ίδιο τρόπο και τα επόμενα χρόνια και μετά την έλευση των προσωπικών υπολογιστών (personal computers) όπου η ανταλλαγή πληροφοριών και προγραμμάτων πραγματοποιούταν μέσω δισκετών. Στα μέσα του 1970, ο εν λόγω όρος χρησιμοποιούταν σε

λογοτεχνικά βιβλία επιστημονικής φαντασίας και σε κινηματογραφικές ταινίες. Ωστόσο, στον ακαδημαϊκό χώρο, ο όρος «ιός» (virus) χρησιμοποιήθηκε για πρώτη φορά από τον Fred Cohen το 1984.

Ως ιός ορίζεται το πρόγραμμα που αναπαράγει τον εαυτό του, χωρίς την έγκριση του χρήστη, μολύνοντας αρχεία που βρίσκονται σε δισκέτες και σκληρούς δίσκους. Ο ιός προσπαθεί να αναπαραχθεί και να εξαπλωθεί, μολύνοντας όσο το δυνατόν περισσότερα αρχεία ή άλλους υπολογιστές σε τοπικό επίπεδο ή στο Διαδίκτυο. Ανάλογα με το είδος του ιού, οι συνέπειες από τη μόλυνση μπορεί να είναι από μηδαμινές έως καταστροφικές.

Οι ιοί κατηγοριοποιούνται με δύο διαφορετικούς τρόπους. Συγκεκριμένα, οι ιοί διαχωρίζονται με βάση το αντικείμενο που προσβάλλουν και ανάλογα με τον τρόπο δράσης τους.

Αντικείμενο προσβολής ιών:

- Τομέα εκκίνησης (boot sector): Ο ιός φορτώνεται πριν το λειτουργικό σύστημα και προσβάλλει τον τομέα εκκίνησης ενός αποθηκευτικού χώρου, όπως ενός σκληρού δίσκου, επηρεάζοντας τον τρόπο εκκίνησης του υπολογιστή. Η κατηγορία αυτή ιών αν και ήταν η πρώτη που εμφανίστηκε, στη σημερινή εποχή δε συναντάται συχνά.
- Μακροεντολών (macro): Η κατηγορία αυτή προσβάλλει το Microsoft Word, Microsoft Excel ή άλλες παρεμφερείς εφαρμογές και προκαλεί αυτόματα την εκτέλεση μιας αλληλουχίας ενεργειών.
- Προγραμμάτων ή αρχείων (program or file): Ο ιός προσβάλλει ένα εκτελέσιμο αρχείο (π.χ. .exe, .dll, .com, .bat), αλλάζοντας τμήμα του κώδικα του αρχείου χωρίς να μεταβάλλει το μέγεθος του, ή προσκολλάται σε αυτό.
- Υβριδικοί (hybrid) ή Πολυμερής (Multi-part or Multiprtite): Είναι αρκετά επικίνδυνοι ιοί, καθώς συνδυάζουν χαρακτηριστικά διαφόρων τύπων, μολύνοντας τόσο αρχεία προγραμμάτων όσο και τομείς του συστήματος.

Τρόπος δράσης ιών:

- Πολυμορφικοί (polymorphic): Ο τύπος αυτός κρυπτογραφεί συνεχώς τον κώδικά του, διαφοροποιώντας τον κάθε φορά που προσβάλλει ένα αρχείο, με αποτέλεσμα να δυσχεραίνεται η αντιμετώπισή του.
- Resident: Ο ιός σε πρώτη φάση ελέγχει την εκπλήρωση συγκεκριμένων προϋποθέσεων προτού προσβάλλει τον υπολογιστή. Αν οι συνθήκες δεν

επαρκούν παραμένει στη μνήμη, αναμένοντας τα κατάλληλα προγράμματα να εκκινήσουν ώστε να δράσει.

- Overwrite: Η κατηγορία αυτή αχρηστεύει τα δεδομένα των αρχείων που προσβάλλουν μετά την μόλυνση, διαγράφοντας τα πολλαπλές φορές ώστε να μην μπορούν να ανακτηθούν.
- Αόρατοι (Stealth): Οι ιοί αυτοί αποκρύπτουν τις τροποποιήσεις, τις οποίες προκαλούν στον υπολογιστή, καταλαμβάνοντας τις λειτουργίες του συστήματος που διαβάζουν αρχεία ή τομείς συστήματος. Με τη συγκεκριμένη μέθοδο όταν άλλα προγράμματα αναζητούν πληροφορίες από τμήματα του δίσκου, ο ιός αναφέρει τη σωστή πληροφορία, χωρίς τις τροποποιήσεις, αντί για την πραγματική κατάσταση.
- Γρήγοροι και Αργοί (Fast and slow): Προσβάλλουν οποιοδήποτε προσβάσιμο αρχείο κι όχι μόνο αυτό που μπορεί να εκτελεστεί. Οι όροι «γρήγορος» και «αργός» δηλώνει τη συχνότητα και τις συνθήκες κάτω από τις οποίες πραγματοποιείται η μόλυνση. Συνήθως, ο ιός φορτώνεται στη μνήμη και περιμένει να εκτελεστεί ένα πρόγραμμα με σκοπό να το μολύνει. Ένας γρήγορος εισβολέας μολύνει προγράμματα, τα οποία είναι προσβάσιμα, χωρίς να χρειάζεται να εκτελεστούν. Αντιθέτως, ο αργός εισβολέας ενεργεί προσβάλλοντας αρχεία κατά την κατασκευή ή μορφοποίησή τους.
- Sparse: Ο ιός αυτός χρησιμοποιεί μια πληθώρα από τεχνικές προκειμένου να καλύψει την ύπαρξη του, με σκοπό να μολύνει ανενόχλητος τα αρχεία.
- Θωρακισμένοι (Armored): Ο τύπος αυτός υπερκαλύπτει τους άλλους ιούς και με τη χρήση διαφόρων τεχνασμάτων ξεγελάει τα αντιβιοτικά προγράμματα (antivirus programs).
- Κούφιοι (Cavity or spacefiller): Ο ιός εγκαθίσταται αρχικά σε ένα αρχείο και στη συνέχεια το προσβάλλει. Οι περισσότεροι ιοί συνήθως εγκαθίστανται στο τέλος του αρχείου και μετά αλλάζουν την αρχή του, ώστε πρώτα να παρατηρείται ο ιός και μετά το πρόγραμμα. Χρησιμοποιούν τεχνικές ώστε να γίνονται αόρατοι και έτσι ο χρήστης να μη βλέπει την αλλαγή του μήκους του προγράμματος, οπότε και να μην καταλαβαίνει ότι έχει προσβληθεί από ιό. Εντούτοις, η κατηγορία των κούφιων ιών δρα πιο έξυπνα. Συγκεκριμένα, ορισμένα προγράμματα έχουν κάποιο άδειο χώρο στο εσωτερικό τους. Στο χώρο αυτό ο ιός δρα χωρίς να καταστρέφει το πρόγραμμα και χωρίς να τροποποιεί το μέγεθος του, οπότε δεν χρειάζεται να χρησιμοποιήσει τεχνικές για να μη φαίνεται.

- Υπόγειες γαλαρίες (Tunnelling): Το είδος αυτό προσπαθεί να ανοίξει μια «σήραγγα» στα ελεγκτικά προγράμματα των αντιβιοτικών, ώστε να μη γίνει αντιληπτό από αυτά.
- NTFS ADS: Το σύστημα αυτό αλλάζει τη ροή των δεδομένων στο αρχείο, επιτρέποντας την προσθήκη δεδομένων στο αρχείο αυτό.
- Virus Droppers: Αφορά ένα πρόγραμμα το οποίο όταν εκτελεστεί ένας ιός εγκαθίσταται στο σκληρό δίσκο.

Αξίζει να επισημανθεί ότι πολλές φορές η πλειονότητα των χρηστών χρησιμοποιεί τον όρο «ιό» για να περιγράψει όλα τα κακόβουλα προγράμματα στο σύνολό τους, τα οποία προκαλούν αρνητικά αποτελέσματα στην λειτουργία του υπολογιστή. Η άποψη αυτή είναι λανθασμένη, καθώς στις περισσότερες περιπτώσεις η δυσλειτουργία του υπολογιστή οφείλεται δύο διαφορετικές μορφές κακόβουλων προγραμμάτων, τα σκουλήκια (worms) και τους δούρειους ίππους (trojan horses).

Στον παρακάτω πίνακα εμφανίζονται οι ιοί-σκουλήκια με την μεγαλύτερη απήχηση στα τέλη του 2004. Παρατηρείται ότι το μεγαλύτερο πρόβλημα στην σημερινή κοινωνία της πληροφορίας δεν προκαλείται από τους ιούς, αλλά από τα σκουλήκια. Συμπερασματικά, λανθασμένα η πλειονότητα των χρηστών τα συγχέει με τους ιούς.

| Ονομασία Ιού | Ποσοστό |
|---|---|
| Worm/Netsky.P | 22,6% |
| Worm/Zafi.B | 18,8% |
| Worm/Sasser | 14,2% |
| Worm/Netsky.B | 7,4% |
| Worm/Netsky.D | 6,1% |
| Worm/Netsky.Z | 3,7% |
| Worm/MyDoom.A | 2,4% |
| Worm/Sober.I | 1,9% |
| Worm/Netsky.C | 1,8% |
| Worm/Bagle.AA | 1,6% |
| Άλλοι | 19,5% |
| Πηγή: Sophos Plc. | |

**Σκουλήκια - Worms**

Ένα σκουλήκι υπολογιστή (computer worm) είναι ένα κακόβουλο πρόγραμμα υπολογιστή, το οποίο αυτό-αναπαράγεται. Χρησιμοποιεί δίκτυο υπολογιστών για να στείλει αντίγραφα του εαυτού του σε άλλους κόμβους (υπολογιστές του δικτύου) και μπορεί να το πράξει χωρίς την παρέμβαση του χρήστη. Το γεγονός αυτό οφείλεται σε κενά ασφαλείας που προκύπτουν στον υπολογιστή προορισμού.

Τα σκουλήκια (worms) κάνουν χρήση των υπηρεσιών του δικτύου, με ιδιαίτερη προτίμηση στο ηλεκτρονικό ταχυδρομείο, αλλά και σε εφαρμογές οι οποίες συμβάλλουν στον άμεσο πολλαπλασιασμό και στην εξάπλωσή τους και με μεγάλη ταχύτητα λόγω εύκολης επικοινωνίας των χρηστών. Συνήθως, δε μολύνουν τα αρχεία από τον υπολογιστή που περνούν.

Πολύ γνωστές περιπτώσεις καθιστούν οι επονομαζόμενες ως Melissa και Love Letter. Τα σκουλήκια αυτά εξαπλώθηκαν στο δίκτυο με αστραπιαίο ρυθμό. Η μέθοδος επίθεσης είναι εξαιρετικά ύπουλη, καθώς από τη στιγμή που καταφέρουν να διεισδύσουν σε έναν υπολογιστή, στέλνουν μολυσμένα και καμουφλαρισμένα μηνύματα ηλεκτρονικού ταχυδρομείου (e-mail), σε όλη τη λίστα επαφών του. Έτσι, ο ανυποψίαστος χρήστης λαμβάνει ένα e-mail από κάποιον γνωστό του, δείχνοντας εμπιστοσύνη, ανοίγει το επισυναπτόμενο αρχείο και μαζί το επικίνδυνο πρόγραμμα. Η μαζική αποστολή e-mail, επιβαρύνει δραματικά τους κεντρικούς διακομιστές αλληλογραφίας του Internet, έχοντας ως αποτέλεσμα την κατηγοριοποίηση των μηνυμάτων του θύματος - χρήστη ως spam ή ακόμα και το μπλοκάρισμα του λογαριασμού του ηλεκτρονικού ταχυδρομείου του.

Πολλές φορές συγχέεται το σκουλήκι υπολογιστή (worm) με τον ιό υπολογιστή (virus), διότι παρουσιάζουν πολλές ομοιότητες στη λειτουργία τους. Παρόλα αυτά υπάρχουν κάποιες σημαντικές διαφορές ως προς τον τρόπο μετάδοσης τους και ως προς την περιοχή του συστήματος που θα προσβάλουν, που τους κάνει να ξεχωρίζουν.

Οι διαφορές σκουληκιών με ιούς:

- Το σκουλήκι δημιουργεί κλώνους του εαυτού του στο δίκτυο χωρίς τη χρησιμοποίηση ενός οικείου αρχείου με αποτέλεσμα την συμφόρηση του δικτύου.
- Μολονότι τα σκουλήκια γενικά βρίσκονται μέσα σε αρχεία (π.χ. MS Word ή MS Excel), όπως και οι ιοί, ο τρόπος που χρησιμοποιούν τα σκουλήκια τον ξενιστή είναι διαφορετικός από τον τρόπο που τον χρησιμοποιούν οι ιοί.

Συνήθως ένα σκουλήκι θα απελευθερώσει ένα αρχείο το οποίο έχει ήδη προσβληθεί από κάποιο σκουλήκι.

- Ένα σκουλήκι μπορεί να τρέξει μόνο του, ενώ ένας ιός χρειάζεται ένα πρόγραμμα-ξενιστή (host program).
- Ολόκληρο το αρχείο θα ταξιδέψει από υπολογιστή σε υπολογιστή, οπότε ολόκληρο το αρχείο θα περιέχει το σκουλήκι.
- Τα σκουλήκια βρίσκονται εκεί που υπάρχει δίκτυο.

**Χρονική Εξέλιξη των σκουληκιών από το 1988-2004:**

- **1998:** Το σκουλήκι Morris προσβάλλει μηχανήματα που συνδέονται στο Internet και είναι το πρώτο σκουλήκι που επεκτάθηκε ευρέως σε όλο τον κόσμο.
- **1999:** Το σκουλήκι Melissa απελευθερώνεται και στοχεύει στο MS Word και το MS Outlook, δημιουργώντας μεγάλη συμφόρηση στα δίκτυα.
- **2000:** Το σκουλήκι VBS/Love Letter εμφανίζεται και μέχρι το 2004 ήταν το πιο πολυέξοδο σκουλήκι για τις επιχειρήσεις, αφού οι ζημιές που προκάλεσε κόστισαν υπέρογκα ποσά σε επιχειρήσεις και νοικοκυριά.
- **2001:** Το σκουλήκι Code Red επιτίθεται στον διακομιστή της Microsoft παραλύοντας το σύστημα. Το θέμα πήρε μεγάλη δημοσιότητα, γιατί είχε σκοπό να προσβάλλει την ιστοσελίδα του Λευκού Οίκου. Το σκουλήκι Sircam απελευθερώνεται και διαδίδεται με e-mails.
- **2003:** Δύο πολύ σημαντικά σκουλήκια, ο Sobig και ο Blaster ξεκίνησαν να προσβάλλουν χιλιάδες υπολογιστές που είχαν Microsoft Windows, αυτό δημιούργησε μεγάλα οικονομικά και πολιτικά προβλήματα. Πιο συγκεκριμένα, ο Blaster ήταν προγραμματισμένος να επιτεθεί στο δικτυακό τόπο της Microsoft. Οι τεχνικοί της εταιρείας όμως πρόλαβαν και άλλαξαν τις διευθύνσεις των διακομιστών (server) της εταιρείας και η επίθεση απέτυχε. Ο Sobig μεταδιδόταν μέσω ηλεκτρονικού ταχυδρομείου (e-mail) και επιβάρυνε τα συστήματα ηλεκτρονικής αλληλογραφίας, στέλνοντας μολυσμένα μηνύματα.
- **2004:** Το σκουλήκι Sasser δημιουργεί προβλήματα στα δίκτυα, σε μερικές περιπτώσεις διακόπτει και τις εργασίες. Το Mydoom σκουλήκι είναι ένα από τα πιο επικίνδυνα και πιο γρήγορα μεταδιδόμενα σκουλήκια, σχεδιασμένο να επιτίθεται στα δίκτυα της Microsoft.

Πηγή: Βιβλίο Μιχαήλ Σφακιανάκης, «Εισαγωγή στην Πληροφορική Σκέψη»

**Δούρειοι Ίπποι (Trojan Horses):**

Ένας από τους μεγαλύτερους κινδύνους, τους οποίους διατρέχει ένας χρήστης είναι αυτός του Δούρειου Ίππου (Trojan Horse). Πρόκειται για προγράμματα που αποτελούνται από δύο μέρη, τον πελάτη και το διακομιστή. Ο διακομιστής κρύβεται με ύπουλο τρόπο στον υπολογιστή του θύματος και ο πελάτης εκτελείται στο μηχάνημα του θύτη. Από τη στιγμή που ο χρήστης του υπό επίθεση υπολογιστή συνδεθεί με το Διαδίκτυο, ο διακομιστής του Δούρειου Ίππου, που εκτελείται σιωπηρά στο παρασκήνιο (background), στέλνει ένα σήμα το οποίο λαμβάνει ο πελάτης (στο μηχάνημα του θύτη). Στη συνέχεια εγκαθιδρύεται μεταξύ τους μια συνεδρία και ο κακός χρήστης (cracker) αποκτά πρόσβαση στον υπολογιστή-στόχο.

Ο χρόνος που διαρκεί αυτός ο έλεγχος του επιτιθέμενου στο άλλο μηχάνημα και τι καταστροφές μπορεί να προκαλέσει είναι άγνωστος και εξαρτάται από το είδος του δούρειου ίππου και το λόγο για τον οποίο κατασκευάστηκε. Ο διακομιστής του δούρειου ίππου παρακολουθεί συνεχώς τις κινήσεις του χρήστη. Τοιουτοτρόπως, όταν εκείνος πληκτρολογεί κωδικούς πρόσβασης ή αριθμούς πιστωτικών καρτών, το πρόγραμμα τα καταγράφει με σκοπό να τα στείλει αργότερα στο θύτη.

Ως Δούρειος Ίππος ορίζεται το κακόβουλο πρόγραμμα που ξεγελάει τον χρήστη και τον κάνει να πιστεύει ότι εκτελεί κάποια χρήσιμη λειτουργία στον υπολογιστή του, ενώ στα κρυφά εγκαθιστά άλλα κακόβουλα προγράμματα. Το όνομά του προκύπτει από την Αινειάδα του Βιργίλιου. Αναγράφεται ότι ο Οδυσσέας εμπνεύστηκε την κατασκευή ενός ξύλινου αλόγου, στην κοιλιά του οποίου κρύβονταν Αχαιοί πολεμιστές, και ξεγελώντας τους κάτοικους της Τροίας, εισήγαγε τον στρατό των Αχαιών μέσα στην πόλη και την κυρίευσε.

Εξωτερικά εμφανίζονται ως κανονικά προγράμματα τα οποία εκτελούν χρήσιμες λειτουργίες, είναι ενδιαφέροντα και δίνουν την εντύπωση στον χρήστη ότι είναι ακίνδυνα. Όταν όμως ο χρήστης εκτελέσει αυτό το πρόγραμμα, τότε ενεργοποιείται ο κακόβουλος κώδικας με αποτέλεσμα ο υπολογιστής να μολυνθεί. Ως αποτέλεσμα της μόλυνσης από δούρειο ίππο εγκαθίσταται κάποιο πρόγραμμα που επιτρέπει σε μη εξουσιοδοτημένους χρήστες να έχουν πρόσβαση στον μολυσμένο υπολογιστή και να τον χρησιμοποιούν για να ξεκινήσουν άλλες επιθέσεις προς άλλους υπολογιστές του διαδικτύου. Σε αντίθεση με τους ιούς, οι δούρειοι ίπποι δε μεταδίδονται μολύνοντας αρχεία.

Ένα αρχείο χαρακτηρίζεται ως δούρειος ίππος στις ακόλουθες περιπτώσεις:

- Ένα μη εξουσιοδοτημένο πρόγραμμα περιέχεται στο εσωτερικό ενός άλλου νόμιμου προγράμματος. Το μη εξουσιοδοτημένο πρόγραμμα περιέχει άγνωστες και ανεπιθύμητες λειτουργίες.
- Ένα νόμιμο πρόγραμμα το οποίο έχει τροποποιηθεί από την τοποθέτηση μη εξουσιοδοτημένου κώδικα, ο οποίος εμπεριέχει άγνωστες και ανεπιθύμητες λειτουργίες.
- Κάθε πρόγραμμα το οποίο φαίνεται να εκτελεί τις επιθυμητές ενέργειες αλλά (λόγω μη εξουσιοδοτημένου κώδικα στο εσωτερικό του εν αγνοία του χρήστη) εκτελεί λειτουργίες άγνωστες και προφανώς ανεπιθύμητες από τον χρήστη.

Η σημαντικότερη διαφορά των δούρειων ίππων με τους ιούς είναι ότι οι ιοί αντιγράφουν τον εαυτό τους, ενώ οι δούρειοι ίπποι όχι. Οι δούρειοι ίπποι περιλαμβάνουν έναν κακόβουλο κώδικα, ο οποίος αποσκοπεί στο να χάνει ή ακόμα και να κλέβει δεδομένα του χρήστη. Παράδειγμα δούρειου ίππου αποτελεί ο PWSteal.

Οι περισσότεροι δούρειοι ίπποι χρησιμοποιούν μεθόδους αυτόματης εκκίνησης (auto-starting), οπότε ακόμη και σε περίπτωση που σβήσει ο υπολογιστής που έχουν προσβάλλει, η λειτουργία τους να μπορεί να ξαναρχίζει, συνεχίζοντας την επίθεση όταν τεθεί σε λειτουργία ξανά ο υπολογιστής.

**Κατηγορίες Δούρειων Ίππων:**

- Απομακρυσμένης πρόσβασης (remote access): Καθιστά το πιο γνωστό είδος δούρειων ίππων καθώς επιτρέπει στον εισβολέα να κάνει περισσότερα στον υπολογιστή του θύματος από ό,τι το θύμα μόνο του όταν βρίσκεται μπροστά από τον υπολογιστή.
- Αποστολής κωδικών (password sending): Στοχεύει στο να υποκλέπτει όλους τους κωδικούς που πληκτρολογεί ο χρήστης, να τους αποθηκεύει και να τους αποστέλλει σε μια συγκεκριμένη διεύθυνση, χωρίς την επίγνωση του χρήστη.
- Keyloggers: Η κατηγορία αυτή δρα σπάζοντας αρχικά το κλειδί του θύματος-χρήστη και έπειτα αναζητά κωδικούς και άλλα προσωπικά δεδομένα.
- Καταστρεπτικοί (Destructive): Η λειτουργία τους είναι άκρως κακόβουλη και καταστρεπτική, διαλύοντας τα αρχεία τα οποία προσβάλλει.

- Άρνησης Υπηρεσίας (Denial of service): Αποτελεί την πιο διαδεδομένη κατηγορία δούρειων ίππων τα τελευταία χρόνια. Ο ίππος προσβάλλει πολλούς χρήστες και επιτίθεται προκαλώντας συμφόρηση μην επιτρέποντας την πρόσβαση στο Διαδίκτυο (Internet).
- Proxy/wingate: Μετατρέπει τον υπολογιστή του θύματος προσβάσιμο σε όλο τον κόσμο ή μόνο στον θύτη. Με τον τρόπο αυτό ο θύτης μπορεί να δρα παράνομα από τον υπολογιστή του θύματος διατηρώντας την ανωνυμία του.
- File Transfer Protocol - FTP: Η κατηγορία αυτή λειτουργεί ανοίγοντας ορισμένες θύρες επικοινωνίας του υπολογιστή συνδέοντας τον υπολογιστή του θύματος με αυτόν του θύτη.
- Φάρσες (Hoaxes): Πρόκειται για μηνύματα ηλεκτρονικού ταχυδρομείου που προτρέπουν το χρήστη να τα ανοίξει και να τα προωθήσει σε τρίτους ή να εκτελέσει μόνος του βλαβερές ενέργειες για τον υπολογιστή του, χωρίς αυτός να το γνωρίζει.

**Τρόποι μολύνσεως υπολογιστή:**

- Προγράμματος ICQ
- Συνημμένα (attachments)
- Φυσικής πρόσβασης (physical access)
- Φυλλομετρητή (browser) και e-mail
- Netbios

Μία ενδιαφέρουσα επισήμανση του Norton Antivirus, το οποίο αποτελεί ένα από τα πιο διάσημα προγράμματα εντοπισμού και καταστροφής ιών και άλλων παρόμοιων προγραμμάτων είναι ότι πρέπει να ακολουθούνται κάποιοι βασικοί κανόνες ώστε να αποφευχθούν οι υποκλοπές και καταστροφές δεδομένων των ηλεκτρονικών υπολογιστών. Ακολουθούν οι εξής κανόνες:

- Αναβάθμιση των προγραμμάτων που χρησιμοποιούνται στον υπολογιστή με νεότερες εκδόσεις.
- Χρήση αντιβιοτικών (antivirus) προγραμμάτων τα οποία να αναβαθμίζονται και αυτά συχνά.
- Έλεγχος των μηνυμάτων ηλεκτρονικού ταχυδρομείου και η αποφυγή μηνυμάτων και συνημμένων αρχείων αγνώστου προέλευσης.
- Αποφυγή αρχείων μορφής Word ή Excel αγνώστου προέλευσης διότι μπορεί να κρύβουν ιούς μακροεντολών.

**Τρόποι πρόληψης από ιούς:**

- Ρύθμιση των επιλογών του ηλεκτρονικού υπολογιστή ώστε να εμφανίζει το πλήρες όνομα των αρχείων.
- Ρύθμιση των επιλογών ασφάλειας των μακροεντολών ώστε να μην εκτελούνται αυτόματα (Υψηλό ή Μεσαίο επίπεδο ασφάλειας).
- Να μην ανοίγονται συνημμένα αρχεία τα οποία ο χρήστης δε γνωρίζει τον αποστολέα.

**Τρόποι προστασίας από δούρειους ίππους**

- Χρήση αντιβιοτικών Δούρειων Ίππων (anti-trojan software) και προγράμματα αντιβιοτικά (antivirus): Υπάρχουν ειδικά προγράμματα που προστατεύουν τον υπολογιστή από τους δούρειους ίππους, όπως: TDS-3, TFAK5, Trojan remover, Pest patrol, Anti-Trojan, Tauscan, The cleaner, PC Door Guard, Trojan Hunter, Anti-Keylogger, Log Monitor, Prc View.
- Χρήση προσωπικής αντιπυρικής ζώνης (firewall): Ένα σύνολο προγραμμάτων που προστατεύουν τους πόρους ενός ιδιωτικού δικτύου από τους χρήστες άλλων δικτύων. Κάθε φορά που ένας διακομιστής δούρειου ίππου προσπαθεί να βγει στο Διαδίκτυο, η αντιπυρική ζώνη προειδοποιεί το χρήστη.
- Εγκατάσταση προγραμμάτων στον υπολογιστή αποκλειστικά από γνωστές και επίσημες τοποθεσίες (sites).

# ΚΕΦΑΛΑΙΟ 2: ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ

## 2.1 ΈΝΝΟΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Είναι γνωστό ότι η πρόσβαση στην πληροφορία σήμερα έχει ασύλληπτες διαστάσεις. Η τεχνολογική εξέλιξη της πληροφορίας είναι τόσο γρήγορη που δημιουργούνται συνεχώς αυξημένες απαιτήσεις από κάθε χρήστη. Τόσο για τα φυσικά πρόσωπα όσο και για τις επιχειρήσεις και τις δημόσιες αρχές ενέχουν κίνδυνοι που αφορούν την πρόσβαση και παραβίαση των δεδομένων προσωπικού χαρακτήρα.

Η απώλεια ψηφιακών δεδομένων αποτελεί μία από τις μεγαλύτερες απειλές και απρόβλεπτες ζημιές που είναι πιθανό να προκληθούν κατά τη χρήση του Διαδικτύου και γενικότερα των ηλεκτρονικών υπολογιστών. Η προστασία των δεδομένων από ποικίλους διαδικτυακούς κινδύνους και η διασφάλιση της ομαλής λειτουργίας των υπολογιστικών συστημάτων αποτελεί πρωταρχικό μέλημα για διεθνείς οργανισμούς και κράτη. Η νομοθεσία καλείται να ανταποκριθεί άμεσα στις σύγχρονες εξελίξεις και αλλαγές και ταυτόχρονα να διαχειριστεί την αύξηση της πολυπλοκότητας όσον αφορά την παρακολούθηση των δεδομένων. Γίνεται σαφές ότι είναι απαραίτητη η λήψη κατάλληλων μέτρων για να προστατευτούν οι πολίτες από τους κίνδυνους που εισάγει η τεχνολογία της πληροφορίας.

Σύμφωνα με το Νόμο 2472/1997 και την Οδηγία 95/46/ΕΚ, προσωπικό δεδομένο συνιστά κάθε πληροφορία που αφορά ταυτοποιήσιμο φυσικό πρόσωπο, το οποίο ονομάζεται «υποκείμενο των δεδομένων». Το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, κυρίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όνομα, αριθμό ταυτότητας, δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσδιορίζουν τη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.

Η ανάπτυξη των νέων τεχνολογιών και οι νέες μορφές διαφήμισης και ηλεκτρονικών συναλλαγών οδήγησαν στην ολοένα και υψηλότερη ζήτηση προσωπικών πληροφοριών από τον ιδιωτικό και δημόσιο τομέα. Οι προσωπικές πληροφορίες, οι οποίες αναφέρονται σε κάθε είδους προσωπική είτε επαγγελματική δραστηριότητα του ατόμου, ονομάζονται προσωπικά δεδομένα. Δεν απαιτείται οι πληροφορίες να είναι αληθείς και εξακριβωμένες.

Ειδικότερα, ως δεδομένα προσωπικού χαρακτήρα χαρακτηρίζεται κάθε πληροφορία που αναφέρεται σε ένα άτομο και μπορεί να το περιγράψει, όπως είναι στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή

κατάσταση), φυσικά χαρακτηριστικά, εκπαίδευση, εργασία (προϋπηρεσία, εργασιακή συμπεριφορά), οικονομική κατάσταση (μισθός, έσοδα, έξοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά), ενδιαφέροντα, δραστηριότητες, συνήθειες, δημοσιεύσεις σε ιστοτόπους κοινωνικής δικτύωσης, IP διεύθυνση , δεδομένα θέσης, όνομα χρήστη (username), κωδικό (password), ιστορικό περιήγησης. Το φυσικό πρόσωπο, κάθε ηλικίας, φύλου, φυλής ή προέλευσης, που ζει σε κάποιο κράτος μέλος της Ε.Ε., στο οποίο ανήκουν και αναφέρονται τα δεδομένα, ονομάζεται υποκείμενο των δεδομένων. Όσον αφορά τα κοινά δεδομένα, ο νόμος καταρχήν προβλέπει ότι αρκεί η απλή συγκατάθεση του ενδιαφερόμενου για τη νομιμότητα της επεξεργασίας.

Τα δεδομένα αφορούν φυσικά πρόσωπα. Εξ ορισμού δε νοούνται προσωπικά δεδομένα για νομικά πρόσωπα όπως εταιρείες, σωματεία ή δημόσιες αρχές. Για να αφορά ένα φυσικό πρόσωπο, το δεδομένο πρέπει να σχετίζεται άμεσα με εκείνο. Επιπλέον, ένα πρόσωπο μπορεί να ταυτοποιηθεί όταν ξεχωρίζει από κάποιο άλλο πρόσωπο. Η ταυτοποίηση επιτυγχάνεται μέσω ειδικών χαρακτηριστικών γνωρισμάτων, τα οποία είναι συνδεδεμένα με ένα συγκεκριμένο άτομο, όπως στοιχεία εμφάνισης ή μη εμφανή αλλά σαφή χαρακτηριστικά.

Η ταυτοποίηση μπορεί να γίνεται είτε άμεσα είτε έμμεσα. Είναι αρκετά εύκολο να ταυτοποιηθεί κανείς άμεσα μέσω του ονόματός του. Ένα φυσικό πρόσωπο μπορεί να ταυτοποιηθεί από τον τηλεφωνικό του αριθμό, τον ΑΦΜ του, τον αριθμό της αστυνομικής του ταυτότητας ή έναν συνδυασμό που ξεχωρίζει το άτομο από την ομάδα. Σε κάθε περίπτωση, η χρήση του ονόματος, μαζί με κάποια χαρακτηριστικά που οδηγούν σε ένα μόνο πρόσωπο, είναι ο βασικός παράγοντας στην άμεση ταυτοποίηση ενός προσώπου.

Χρήζει ιδιαίτερης προσοχής το γεγονός ότι οι πληροφορίες που μπορούν να συλλεγούν σε σύνολο και να οδηγήσουν στην ταυτοποίηση ενός προσώπου, αποτελούν και αυτές προσωπικά δεδομένα. Προσωπικά δεδομένα που, μετά από επεξεργασία, έχουν καταστεί ανώνυμα ή έχουν κρυπτογραφηθεί ή ψευδωνυμοποιηθεί, αλλά ταυτοχρόνως μπορούν να χρησιμοποιηθούν για να ταυτοποιήσουν ένα πρόσωπο, εξακολουθούν να θεωρούνται προσωπικά δεδομένα και εμπίπτουν στο πεδίο εφαρμογής της προστασίας προσωπικών δεδομένων.

Από τα παραπάνω προκύπτει ότι:

- Τα προσωπικά δεδομένα είναι οι απλές, βασικές πληροφορίες όπως είναι το ονοματεπώνυμο, αλλά και πιο ιδιαίτερες, όπως τα πολιτικά φρονήματα τα οποία από την ώρα που συνδέονται με ένα πρόσωπο μπορούν να το ταυτοποήσουν.
- Όταν οι πληροφορίες χάνουν τη σύνδεση και δεν ταιριάζουν με ένα άτομο, δεν υφίστανται ως προσωπικά δεδομένα.
- Προσωπικό μπορεί να είναι κάθε δεδομένο που χαρακτηρίζει ένα φυσικό πρόσωπο, είτε αφορά κάτι αντικειμενικό, όπως το ύψος, το βάρος ή το χρώμα των ματιών, είτε κάτι υποκειμενικό, όπως προσωπικές πεποιθήσεις, απόψεις και δηλώσεις.
- Τα προσωπικά δεδομένα αφορούν πρόσωπα που είτε έχουν ταυτοποιηθεί είτε μπορούν να ταυτοποιηθούν και είναι εν ζωή.
- Ο ορισμός των δεδομένων προσωπικού χαρακτήρα δεν περιλαμβάνει και νομικά πρόσωπά, όπως είναι εταιρείες, σωματεία και σύλλογοι.
- Οι αξιολογικές κρίσεις ή οι επιστημονικές αξιολογήσεις δε θεωρούνται προσωπικά δεδομένα, καθώς δεν έχουν "επίσημο" χαρακτήρα.


Πηγή: https://amagno.co.uk/gdpr-legal-issues-protection-of-personal-data/22099/

Στοχεύοντας στο να γίνει η ιστορική αναδρομή των γεγονότων που συντέλεσαν στη δημιουργία νόμων και κανόνων προστασίας των δεδομένων, παραθέτεται η πορεία της καταπάτησης των προσωπικών δεδομένων στα προηγούμενα χρόνια. Η αρχή έγινε το 1947, όταν η Μεγάλη Βρετανία και οι Ηνωμένες Πολιτείες Αμερικής υπέγραψαν ένα μυστικό σύμφωνο με την ονομασία UKUSA (U.K. και U.S.A.). Με το σύμφωνο οι δύο χώρες ανέλαβαν την ευθύνη της από κοινού παρακολούθησης διαφόρων πληροφοριών σε επιλεγμένες περιοχές του πλανήτη. Στα τέλη της δεκαετίας του 1960, δημιουργήθηκε το Echelon, ένα δίκτυο από δορυφόρους που παρείχε τη δυνατότητα διηπειρωτικών τηλεπικοινωνιών.

Τα κράτη – μέλη της UKUSA, μέσω των μυστικών υπηρεσιών τους, δημιουργήσαν τις δικές τους μυστικές επίγειες βάσεις, σε άριστα επιλεγμένο σημείο από επιστημονική άποψη, έτσι ώστε να υποκλέπτουν συνομιλίες και τηλεματικές επικοινωνίες (telex) μέσω των δορυφόρων Intelsat και Inmarsat. Επιπρόσθετα, το δίκτυο Echelon συμπεριλαμβάνει υποδομή, κατασκευαστικούς δορυφόρους και εξοπλισμό για την υποκλοπή ραδιοσημάτων των επίγειων τηλεπικοινωνιακών δικτύων, μέσω του μυστικού δικτύου από ραντάρ που είναι εγκατεστημένο στις διάφορες βάσεις ανά τον κόσμο.

Το Echelon φτιάχτηκε με σκοπό τη σύνδεση υπολογιστών που προϋπάρχουν και σαρώνουν κείμενα για λέξεις - κλειδιά, έτσι ώστε να επικοινωνούν και να λειτουργούν σαν ένα ολοκληρωμένο σύνολο. Μέχρι τότε, οι πληροφορίες ανταλλάσσονταν μεταξύ των μυστικών υπηρεσιών αποσπασματικά. Με το Echelon η κάθε μυστική υπηρεσία είχε πλέον πρόσβαση στο σύνολο των λέξεων - κλειδιών κάθε υπολογιστή που την αφορούσε.

Τα μέσα για τη μαζική παρακολούθηση είναι διαθέσιμα και βρίσκονται καθημερινά σε λειτουργία. Αυτή η μαζική και συνεχής υποκλοπή πραγματοποιείται από:

- Τις μυστικές υπηρεσίες που μπορούν να κατασκοπεύσουν κάθε πληροφορία που διακινείται στον πλανήτη.
- Την αστυνομία που μπορεί να κατασκοπεύσει κάθε πληροφορία που διακινείται γενικώς και άπτεται των «ενδιαφερόντων» της.
- Παρόχους Υπηρεσιών Διαδικτύου (Internet Service Provider, ISP) που μπορούν να κατασκοπεύσουν κάθε πληροφορία που διακινείται μέσω Διαδικτύου.
- Εργοδότες οι οποίοι έχουν τη δυνατότητα να κατασκοπεύουν κάθε πληροφορία που διακινείται στην εταιρεία.

Συγκεκριμένα, στο FBI χρησιμοποιείται το διάσημο πρόγραμμα “Carnivore” και διάφορα παρόμοια προγράμματα με τη χρήση του Internet, αποτελώντας κίνδυνο για την προστασία των δεδομένων των φυσικών προσώπων. Δεδομένου ότι το πρόγραμμα αυτό χρησιμοποιείται και από την ελληνική αστυνομία, δημιουργούνται ανησυχίες για την προστασία των δεδομένων και στην Ελλάδα. Επιπλέον, αποτελεί άμεσο προβληματισμό και η παρακολούθηση των δεδομένων των υπαλλήλων από

τους εργοδότες, καθώς η τεχνολογία επιτρέπει την πλήρη υποκλοπή όλων των δεδομένων που διακινούνται από τον υπολογιστή μας.

Συν τοις άλλοις, ο κλάδος στον οποίο ο προσωπικός χώρος του πολίτη καταργείται σε πολύ μεγάλο βαθμό είναι ο τόπος εργασίας. Η παρακολούθηση των δεδομένων από τον εργοδότη ή και από τον συνάδελφο αφορά τον καθένα, καθώς καθίσταται σαφές ότι κάθε υπάλληλος αποτελεί στόχο. Συγχρόνως η τεχνολογία επιτρέπει την πλήρη υποκλοπή όλων των δεδομένων που διακινούνται από τον υπολογιστή του χώρου εργασίας. Επιπλέον, η συχνότερη δικαιολογία των εταιρειών σχετίζεται με τον έλεγχο των υπαλλήλων ως προς την κακόπιστη χρήση των υπολογιστών και του δικτύου τους, στοχεύοντας στη διαφύλαξη της φήμης και των επιχειρηματικών τους μυστικών και δραστηριοτήτων. Στην πραγματικότητα, όμως, γίνεται χρήση ενός σύγχρονου μέσου για να ελέγχουν την παραγωγικότητα, την προσωπικότητα, την αποτελεσματικότητα και την επιχειρηματική πίστη τους.

Τέλος, πολλοί χρήστες θεωρούν ότι τα δεδομένα τους είναι πιο ασφαλή στο χώρο του σπιτιού τους, έχοντας ιδιωτική πρόσβαση υπηρεσιών Διαδικτύου. Ωστόσο, οι εταιρείες πάροχοι υπηρεσιών Διαδικτύου (Internet Service Provider, ISP) προειδοποιούν τους πελάτες τους σχετικά με το απαραβίαστο των μηνυμάτων τους. Οι περισσότερες εταιρείες είναι προγραμματισμένες να αποθηκεύουν όλα τα μηνύματα και δεδομένα που διακινούν. Ως εκ τούτου, η διαδικασία ελέγχου και ανάγνωσης μηνυμάτων είναι πολύ απλή και εφικτή για οποιοδήποτε λόγο κρίνει κάθε εταιρεία.

## 2.2 ΑΠΛΑ ΚΑΙ ΕΥΑΙΣΘΗΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ

Τα προσωπικά δεδομένα, γνωστά ως προσωπικές πληροφορίες, προσωπικές πληροφορίες ταυτοποίησης (Personally Identifying Information, PII) ή ευαίσθητα προσωπικά δεδομένα (Sensitive Personal Information, SPI), είναι οποιαδήποτε πληροφορία σχετικά με ένα πρόσωπο με δυνατότητα αναγνώρισης. Η συντομογραφία PII είναι ευρέως αποδεκτή στις Ηνωμένες Πολιτείες. Σύμφωνα με τα ευρωπαϊκά και άλλα καθεστώτα προστασίας δεδομένων, τα οποία επικεντρώνονται κυρίως στον Κανονισμό Γενικής Προστασίας Δεδομένων (GDPR), ο όρος "προσωπικά δεδομένα" είναι ευρύτερος και καθορίζει το πεδίο εφαρμογής του ρυθμιστικού καθεστώτος.

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας, ορίζει τις πληροφορίες ταυτοποίησης ως "οποιαδήποτε πληροφορία για ένα άτομο που διατηρείται από μια υπηρεσία, συμπεριλαμβανομένων και οποιωνδήποτε πληροφοριών που μπορούν να χρησιμοποιηθούν για τη διάκριση ή τον εντοπισμό της ταυτότητας ενός ατόμου, το όνομα, τον αριθμό κοινωνικής ασφάλισης, την ημερομηνία και τον τόπο γέννησης, το πατρικό όνομα της μητέρας ή τα βιομετρικά αρχεία και οποιεσδήποτε άλλες πληροφορίες που συνδέονται ή συνδέονται με ένα άτομο, όπως ιατρικές,

εκπαιδευτικές, οικονομικές πληροφορίες και πληροφορίες για την απασχόληση. Η διεύθυνση IP ενός χρήστη δεν ταξινομείται ως πληροφορία ταυτοποίησης - PII από μόνη της. Ωστόσο, στην Ευρωπαϊκή Ένωση, η διεύθυνση IP ενός συνδρομητή Διαδικτύου μπορεί να χαρακτηριστεί ως προσωπικό δεδομένο.

Η έννοια της πληροφορία ταυτοποίησης - PII έχει γίνει διαδεδομένη καθώς η τεχνολογία της πληροφορίας και το Διαδίκτυο έχουν διευκολύνει τη συλλογή δεδομένων και πληροφοριών ταυτοποίησης που οδηγεί σε μια κερδοφόρα αγορά συλλογής και μεταπώλησης της πληροφορία ταυτοποίησης. Η πληροφορία ταυτοποίησης μπορεί επίσης να αξιοποιηθεί από τους εγκληματίες για να καταδιώξουν ή να κλέψουν την ταυτότητα ενός προσώπου ή να βοηθήσουν στο σχεδιασμό εγκληματικών πράξεων. Ως αντίδραση σε αυτές τις απειλές, πολλές πολιτικές απορρήτου ιστοσελίδων ασχολούνται ειδικά με τη συγκέντρωση του προσωπικών δεδομένων και νομοθέτες όπως το Ευρωπαϊκό Κοινοβούλιο έχουν θεσπίσει μια σειρά νομοθετικών ρυθμίσεων όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) για τον περιορισμό της διανομής και της προσβασιμότητας των προσωπικών δεδομένων.

Η προσωπική ταυτοποίηση των πληροφοριών είναι μια νομική έννοια, όχι μια τεχνική έννοια, και δεν χρησιμοποιείται σε όλες τις δικαιοδοσίες. Λόγω της ευελιξίας και της δύναμης των σύγχρονων αλγορίθμων επαναπροσδιορισμού, η έλλειψη δεδομένων πληροφορίας ταυτοποίησης δε σημαίνει ότι τα υπόλοιπα δεδομένα δεν εντοπίζουν τα άτομα. Ενώ ορισμένα χαρακτηριστικά μπορεί να μην αναγνωρίζονται μεμονωμένα από μόνα τους, κάθε χαρακτηριστικό μπορεί δυνητικά να εντοπίζεται σε συνδυασμό με άλλο. Αυτά τα χαρακτηριστικά έχουν αναφερθεί ως αναγνωριστικά ή ψευδο-αναγνωριστικά. Παρόλο που τα δεδομένα αυτά ενδέχεται να μην αποτελούν πληροφορίες ταυτοποίησης στις Ηνωμένες Πολιτείες, είναι πολύ πιθανό να καθιστούν δεδομένα προσωπικού χαρακτήρα σύμφωνα με το Ευρωπαϊκό Δίκαιο προστασίας δεδομένων.

Τα προσωπικά δεδομένα διακρίνονται σε απλά και σε ευαίσθητα, όσον αφορά την πληροφοριακή βαρύτητά τους σε σχέση με την ιδιωτικότητα. Ο νόμος χρησιμοποιεί μόνο τον όρο ευαίσθητα προσωπικά δεδομένα, ως ειδική κατηγορία της ευρύτερης έννοιας των δεδομένων προσωπικού χαρακτήρα. Παρ’ όλα αυτά, η νομοτεχνική αυτή επιλογή πρέπει να συνεκτιμάται κατά την ερμηνεία του νόμου, έτσι ώστε οι ρυθμίσεις για τα ευαίσθητα δεδομένα να μπορούν να λειτουργούν προσθετικά με τις ισχύοντες ρυθμίσεις για τα απλά δεδομένα.

Είναι αλήθεια ότι για την επεξεργασία των απλών προσωπικών δεδομένων αρκεί η προφορική συγκατάθεση του υποκειμένου, ενώ για την επεξεργασία των ευαίσθητων

προσωπικών δεδομένων απαιτείται η γραπτή συγκατάθεση του. Άρα, σκοπός της διάκρισης των προσωπικών δεδομένων, σε απλά και σε ευαίσθητα, είναι η ύπαρξη μιας ενισχυμένης νομικής προστασίας.

Στην κατηγορία των **απλών προσωπικών δεδομένων** ανήκουν τα δεδομένα που δεν είναι δυνατό να απαριθμηθούν στον κατάλογο του νόμου, στον οποίο αναφέρονται τα ευαίσθητα προσωπικά δεδομένα. Παραδείγματα απλών προσωπικών δεδομένων συνιστούν το όνομα, το επώνυμο, η κατοικία, το επάγγελμα, το μορφωτικό επίπεδο, οι καταναλωτικές συνήθειες, η ταξιδιωτική δραστηριότητα, η οικογενειακή και περιουσιακή κατάσταση, ο μισθός, οι τραπεζικοί λογαριασμοί, η IP διεύθυνση.

Από την άλλη πλευρά, ως **ευαίσθητα προσωπικά δεδομένα** ορίζονται οι πληροφορίες οι οποίες ταιριάζουν και είναι εφικτή η άμεση σύνδεσή τους με την πλέον ιδιωτική ζωή του ατόμου. Είναι εκείνα που συνδέονται εκ της φύσεώς τους με θεμελιώδη δικαιώματα και ελευθερίες και χρήζουν ειδικής και αυξημένης προστασίας.

Ευαίσθητα δεδομένα προσωπικού χαρακτήρα είναι οι πληροφορίες που αναφέρονται στο παρελθόν, το παρόν και το μέλλον και αφορούν:

- φυλετική ή εθνική προέλευση (υπηκοότητα ή ιθαγένεια δεν αποτελεί ευαίσθητο προσωπικό δεδομένο)
- πολιτικά φρονήματα
- θρησκευτικές ή φιλοσοφικές πεποιθήσεις
- συμμετοχή σε συνδικαλιστικές οργανώσεις, όπως μέλος σε σωματείο εργαζομένων
- ιατρικά δεδομένα, υγεία και πληροφορίες για τη φυσική, ψυχική ή πνευματική κατάσταση, για χρήση ναρκωτικών ή κατάχρηση οινοπνεύματος, για αναπηρίες ή για λήψη φαρμάκων
- κοινωνική πρόνοια
- σεξουαλικό προσανατολισμό
- ποινικές διώξεις ή καταδίκες (ποινικό μητρώο)
- συμμετοχή σε ενώσεις προσώπων και σε ευαίσθητες κοινωνικές ομάδες
- γενετικά δεδομένα, κληρονομικά χαρακτηριστικά ή πρότυπα κληρονομικότητας

Κατά συνέπεια, η πρόσβαση σε αυτές πληροφορίες, αλλά και η χρήση των προσωπικών δεδομένων αυτού του τύπου, ενέχει σοβαρότατους κινδύνους για τους πολίτες, καθώς είναι πιθανό να οδηγήσουν σε κατηγοριοποίηση των ανθρώπων και τελικώς στον στιγματισμό και τον κοινωνικό αποκλεισμό τους.

## 2.3 ΕΠΕΞΕΡΓΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Σύμφωνα με το Νόμο 2472/1997, Άρθρο 2, επεξεργασία προσωπικών δεδομένων αποτελεί κάθε εργασία ή σειρά εργασιών που πραγματοποιείται, από το Δημόσιο ή από νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων.

Η επεξεργασία δεδομένων είναι η συλλογή και ο χειρισμός δεδομένων με στόχο την εξαγωγή χρήσιμων πληροφοριών. Η διαδικασία της επεξεργασίας έχει διάφορα στάδια όπως είναι η επαλήθευση, τακτοποίηση με κάποια σειρά, κατηγοριοποίηση, περίληψη, αναφορά, ανάλυση και ερμηνεία των δεδομένων.

Στις εργασίες της επεξεργασίας που εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, περιλαμβάνονται επίσης:

- η συλλογή (αναζήτηση, εύρεση και συγκέντρωση των δεδομένων)
- η καταχώρηση (τοποθέτηση σε βάση δεδομένων)
- η οργάνωση (κατηγοριοποίηση δεδομένων με βάση συγκεκριμένα κριτήρια)
- η διατήρηση ή αποθήκευση σε οποιοδήποτε μέσο
- η τροποποίηση (κρυπτογράφηση, ανωνυμοποίηση, ψευδωνυμοποίηση)
- η εξαγωγή (ανάκτηση πληροφοριών από μη δομημένα ή ημιδομημένα δεδομένα)
- η χρήση των πληροφοριών
- η διαβίβαση (μετάδοση των πληροφοριών προς τρίτα πρόσωπα)
- η διάδοση ή κάθε άλλης μορφής διάθεση (μετάδοση προς μεγαλύτερο αριθμό αποδεκτών)
- η συσχέτιση ή συνδυασμός
- η διασύνδεση (σύνδεση των δεδομένων ενός αρχείου με δεδομένα άλλου ή άλλων αρχείων, τα οποία τηρούνται από διαφορετικό υπεύθυνο επεξεργασίας ή από τον ίδιο, αλλά για άλλου είδους σκοπό)
- η δέσμευση (κλείδωμα και αποκλεισμός περαιτέρω επεξεργασίας)
- η διαγραφή – καταστροφή

Να σημειωθεί ότι η επεξεργασία μπορεί να γίνεται με τον παραδοσιακό τρόπο και με φυσικά μέσα, όπως είναι οι καρτέλες και τα έγγραφα, αλλά ακόμη και ψηφιακά. Οι τεχνολογικές εξελίξεις στον χώρο της πληροφορικής έχουν επιτρέψει την ταυτόχρονη συλλογή, αξιολόγηση και ταξινόμηση μεγάλου όγκου δεδομένων, των οποίων η επεξεργασία γίνεται σε τεράστια έκταση και ανάλυση με ελάχιστο κόστος. Με τη χρήση υπολογιστικών συστημάτων, τα κράτη και οι μεγάλες ή μικρές επιχειρήσεις έχουν τη δυνατότητα να δημιουργήσουν τράπεζες δεδομένων, καθώς και να

βελτιώσουν τη συλλογή και ανταλλαγή προσωπικών δεδομένων. Έτσι επιτεύχθηκε η αποτελεσματικότερη και αποδοτικότερη επεξεργασία.

Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα είναι η βάση για τις κρίσιμες διεργασίες έρευνας και λειτουργίας των επιχειρήσεων και των φορέων προς όφελος του κοινωνικού συνόλου. Παρά την επιφύλαξη ως προς την επεξεργασία των δεδομένων, αποτελεί μία εργασία που χωρίς αυτήν δε θα ήταν δυνατή η λειτουργία οργανωμένων δομών, όπως του κράτους και των επιχειρήσεων. Σήμερα, η συλλογή δεδομένων γίνεται μέσω ηλεκτρονικών υπολογιστών και κινητών τηλεφώνων, κάθε μήνυμα αποθηκεύεται, ακόμα και οι οικονομικές συναλλαγές των φυσικών προσώπων γίνονται ηλεκτρονικά. Εντούτοις, κρίνεται αναγκαίος ο έλεγχος της επεξεργασίας των προσωπικών δεδομένων, καθώς θα πρέπει να οριοθετείται και να επιτρέπεται μόνο όταν είναι δίκαιη και νόμιμη.

## 2.4 ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΩΣ ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Οι πολίτες των κρατών ανέκαθεν αναζητούσαν τη σωστή ισορροπία μεταξύ της ασφάλειάς τους και του σεβασμού των θεμελιωδών δικαιωμάτων των ατόμων, συμπεριλαμβανομένου του δικαιώματος στην ιδιωτικότητα, του δικαιώματος στην προστασία των ευαίσθητων προσωπικών δεδομένων και του δικαιώματος στην ελευθερία της έκφρασης. Παρατηρείται ότι η ανάγκη για προστασία των προσωπικών δεδομένων συγχέεται με την έννοια της ανάγκης της προστασίας της ιδιωτικότητας. Η ελεύθερη κυκλοφορία δεδομένων προσωπικού χαρακτήρα εντός της εσωτερικής αγοράς είναι μεν χρήσιμη και σημαντική για την πλήρη λειτουργία της, αποτελεί όμως απειλή για την ιδιωτικότητα των δεδομένων.

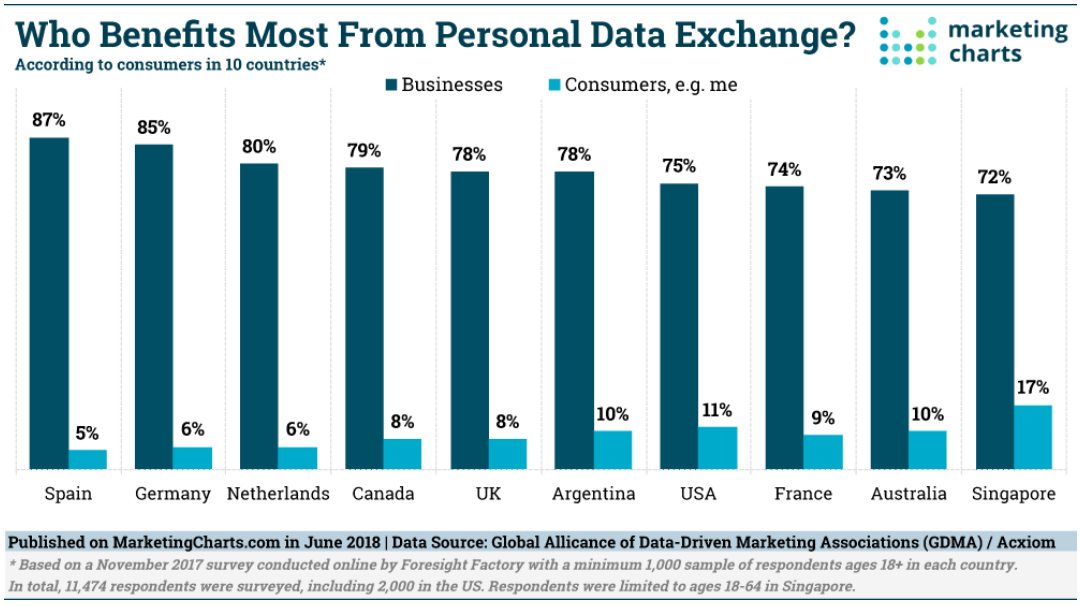
Για να καθοριστεί με καλύτερο τρόπο ο λόγος της σπουδαιότητας της προστασίας των προσωπικών δεδομένων, χρειάζεται να διασαφηνιστεί η σχέση των προσωπικών δεδομένων με την ιδιωτικότητα. Έχοντας αναλύσει το ζήτημα των προσωπικών δεδομένων διευκολύνεται ο λόγος της προστασίας αυτών από την αθέμιτη επεξεργασία.

Η ιδιωτικότητα αποτελεί μία ιδιαίτερα αφηρημένη έννοια, η οποία περιλαμβάνει μια πληθώρα από δικαιώματα και υποχρεώσεις. Πρόκειται για τη βάση της απαγόρευσης της κρατικής παρέμβασης, ως προς την ιδιωτική και οικογενειακή ζωή των ανθρώπων. Παράλληλα, παρουσιάζεται σαν το θεμέλιο για την ελευθερία της σκέψης και τις προσωπικές επιλογές του ατόμου. Υπάρχει άμεση σύνδεση της ιδιωτικότητας με τον περιορισμό της χρήσης των δεδομένων προσωπικού χαρακτήρα. Η

ιδιωτικότητα εκτείνεται και εφαρμόζεται σε πολυποίκιλα ζητήματα και εκφράζει μία ιδέα προσωπικού χώρου, στον οποίο κάθε άτομο μπορεί να συμπεριφερθεί και να κινηθεί ελεύθερα και αυτόνομα σύμφωνα με τις επιλογές του.

Γεγονός αποτελεί ότι οι αρχικοί προβληματισμοί, όσον αφορά την επεξεργασία προσωπικών δεδομένων και την ιδιωτικότητα, ξεκίνησαν από τον δημόσιο τομέα. Η χρήση των στοιχείων των πολιτών από την κρατική εξουσία αποτελούσε σοβαρό κίνδυνο για αυτούς. Τα αρχεία που κατείχαν και η επεξεργασία των δεδομένων ήταν το ίδιο εκτεταμένη με την παραβίαση της ιδιωτικής ζωής των ανθρώπων. Η παρακολούθηση που γινόταν σε αρχεία, όπως ληξιαρχικά στοιχεία, περιουσιακά στοιχεία, παραβατική συμπεριφορά, πολιτικές πεποιθήσεις, ακόμα και τηλεφωνικές επικοινωνίες, προβλημάτισαν και δίχασαν την τότε κοινή γνώμη. Συνεπώς, προκλήθηκαν πολλές αντιδράσεις ως προς την αιτία και τον σκοπό που το κράτος επεξεργαζόταν αυτά τα δεδομένα προσωπικού χαρακτήρα, καταλήγοντας στην σταδιακή αλλαγή της ισχύουσας κατάστασης.

Σε έρευνα ζητήθηκε από περισσότερους από 11.000 ανθρώπους σε 10 παγκόσμιες αγορές, να δώσουν την άποψή τους για το ποιοι πιστεύουν ότι σήμερα επωφελούνται περισσότερο από την ανταλλαγή προσωπικών δεδομένων – μεταξύ επιχειρήσεων και καταναλωτών. Το παρακάτω διάγραμμα δείχνει ότι κατά μέσο όρο, το 78% των ερωτηθέντων θεωρεί ότι οι επιχειρήσεις επωφελούνται περισσότερο από την ανταλλαγή προσωπικών δεδομένων, σε σύγκριση με μόλις 9%, οι οποίοι πιστεύουν ότι οι καταναλωτές επωφελούνται περισσότερο.




Πηγή: http://trends.e-strategyblog.com/2018/09/11/who-benefits-personal-data/29866

Η προστασία δεδομένων προσωπικού χαρακτήρα εισήχθη στα προηγμένα τεχνολογικά κράτη κατά τα τέλη της δεκαετίας του ’60, με πρωταρχικό στόχο την προστασία των πολιτών από την αυτοματοποιημένη επεξεργασία των δεδομένων τους. Την εποχή εκείνη ο δημόσιος τομέας μόλις είχε ξεκινήσει τη διεργασία των προσωπικών δεδομένων των πολιτών. Παράλληλα, οι υπολογιστές ήταν πολύ ακριβοί και πολύ ογκώδεις τότε για να χρησιμοποιούνται από τον ιδιωτικό τομέα, ο οποίος δεν είχε όφελος από την επεξεργασία προσωπικών στοιχείων.

Η κατάσταση σήμερα είναι εντελώς διαφορετική, γνωρίζοντας ότι η τεχνολογική ισχύς έχει αλλάξει ριζικά και έχει γίνει προσιτή στον καθένα. Επιπλέον, η ανάδυση παγκόσμιων χρηματοπιστωτικών αγορών και η ανάγκη για αύξηση των πωλήσεων, καθιέρωσαν νέες υπηρεσίες, όπως το στρατηγικό marketing ή τη μεταπωλητική υποστήριξη. Με βασικό σκοπό την επίτευξη κέρδους, η κατάσταση αυτή συντέλεσε στη μαζική πλέον συλλογή και επεξεργασία προσωπικών δεδομένων από τον ιδιωτικό τομέα. Ωστόσο, η νομοθεσία περί προστασίας δεδομένων κλήθηκε να αντιμετωπίσει μια ποσοτική και ποιοτική ανατροπή των στόχων της. Η νομοθεσία επιχείρησε να θέσει περιορισμούς κυρίως στο ηλεκτρονικό εμπόριο, στο στρατηγικό marketing, στη γενετική έρευνα και στις τηλεπικοινωνίες. Οι περισσότεροι εξ αυτών δεν έγιναν άμεσα αποδεκτοί, καθώς εξυπηρετούσαν επικερδείς δραστηριότητες σε πολλούς κλάδους της αγοράς. Συνεπώς, ενώ η αγορά συνεργάστηκε με τη νομική επιστήμη σε τομείς δικαίου όπου ο κεντρικός έλεγχος ήταν ευπρόσδεκτος, στον τομέα της προστασίας προσωπικών δεδομένων αναπτύχθηκε μία σχετική αντιπαλότητα.

Ο χρηματοπιστωτικός τομέας, το ηλεκτρονικό εμπόριο, οι τεχνικές marketing και η βιοτεχνολογία αποτελούν τομείς της αγοράς, επεξεργασία των οποίων δημιουργεί τις σημαντικότερες δυσχέρειες για τη νομοθεσία της προστασίας δεδομένων προσωπικού χαρακτήρα. Ο τομέας της χρηματικής πίστης συνιστά πηγή πολλών ζητημάτων σχετικά με την προστασία προσωπικών δεδομένων, καθώς υπάρχουν εταιρείες οι οποίες παρέχουν πληροφορίες οικονομικής συμπεριφοράς για επιχειρήσεις και ιδιώτες. Φυσικά γίνεται διαχωρισμός των δεδομένων των οποίων η επεξεργασία είναι νόμιμη. Στη συνέχεια, η επεξεργασία δεδομένων προσωπικού χαρακτήρα για την άμεση προώθηση πωλήσεων παρουσιάζει εξίσου μεγάλο ενδιαφέρον. Οι επιχειρήσεις έχοντας ως κυρίαρχο στόχο την αύξηση των πωλήσεων και μείωση του κόστους, έκαναν επιθετική χρήση της τεχνολογίας για τους σκοπούς του marketing. Με το μικρότερο δυνατό κόστος, οι επιχειρήσεις θέλουν να προσεγγίσουν όσους περισσοτέρους αποδέκτες. Για το λόγο αυτό ότι επεκτείνεται ολοένα και περισσότερο η κυκλοφορία καταλόγων με στοιχεία καταναλωτών, τα

οποία αφορούν δεδομένα προσωπικού χαρακτήρα και η χρήση των οποίων και η μετάδοσή τους αξιολογείται ως νόμιμη μόνο στην περίπτωση της συναίνεσης από τον καταναλωτή.

Το ηλεκτρονικό εμπόριο (e-commerce) αποτελεί έναν ιδιαίτερα σημαντικό κλάδο της σύγχρονης ζωής και τεχνολογικής εξέλιξης ο οποίος χρήζει προστασίας. Περιλαμβάνει όλα τα ηλεκτρονικά μέσα με τα οποία μπορεί να είναι εφικτή και να πραγματοποιηθεί μια αγοροπωλησία μέσω Διαδικτύου. Με τη συμβολή της ραγδαίας ανάπτυξης των δικτύων επικοινωνίας και ειδικότερα του Διαδικτύου, αναπτύχθηκε το ηλεκτρονικό εμπόριο και γενικότερα ο τρόπος με τον οποίο πραγματοποιούνται πλέον οι συναλλαγές.

Η ανάπτυξη του Διαδικτύου, το ηλεκτρονικό εμπόριο και οι συναλλαγές μέσω δικτύων αυξάνουν την ανάγκη ασφάλειας στις ηλεκτρονικές συναλλαγές. Ο χρήστης που συναλλάσσεται ηλεκτρονικά αποζητά να μην μπορούν να αποκαλυφθούν τα δεδομένα του ή να διατεθούν σε μη εξουσιοδοτημένα άτομα και να υπάρχει να αίσθηση εμπιστευτικότητας. Τα προσωπικά δεδομένα δε θα πρέπει να αλλοιώνονται κατά την μετάδοσή τους και ο παραλήπτης θα πρέπει να τα λάβει όπως ακριβώς και στη μορφή που τα έστειλε ο αποστολέας. Ο παραλήπτης οφείλει να είναι σίγουρος ότι τα δεδομένα που λαμβάνει είναι εκείνα που ο αποστολέας έχει στείλει, δηλαδή να υπάρχει ακεραιότητα. Συν τοις άλλοις, σε μία τέτοια συναλλαγή, είναι απαραίτητο ο παραλήπτης να είναι σίγουρος για την ταυτότητα του αποστολέα. Επομένως, κρίνεται απαραίτητη η αυθεντικότητα των δεδομένων. Τέλος, συμμετέχοντας σε μία ηλεκτρονική συναλλαγή θα πρέπει να μην είναι δυνατόν τα εμπλεκόμενα μέρη να αρνηθούν εκ των υστέρων την συμμετοχή τους στη συναλλαγή αυτή, δηλαδή τη μη αποποίηση ευθύνης.

Σήμερα η άνθιση του ηλεκτρονικού εμπορίου είναι σε πλήρη λειτουργία το οποίο σημαίνει ότι η ανάγκη για μυστικότητα και ασφάλεια είναι απαραίτητη. Η εμπιστευτικότητα, η ακεραιότητα, η αυθεντικότητα, η μη αποποίηση ευθύνης στον ηλεκτρονικό κόσμο, αποτελούν αντικείμενο της επιστήμης που ασχολείται με την ασφάλεια των πληροφοριών και προσωπικών δεδομένων. Ως αποτέλεσμα, έχουν δημιουργηθεί πολλοί μηχανισμοί, τεχνικές και τεχνολογίες, αποσκοπώντας να διασφαλίσουν τις ιδιότητες αυτές σε μία ηλεκτρονική συναλλαγή.

# ΚΕΦΑΛΑΙΟ 3: ΝΟΜΟΘΕΤΙΚΗ ΑΝΑΔΡΟΜΗ ΚΑΤΟΧΥΡΩΣΗΣ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

## 3.1 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Η προστασία των προσωπικών δεδομένων θα ήταν πολύ δύσκολη αν δεν υπήρχαν κοινά σημεία στο θεσμικό πλαίσιο μεταξύ των κρατών. Η βασική αιτία αποδίδεται στην ανταγωνιστικότητα που μπορεί να προκληθεί μεταξύ των κρατών. Για το λόγο αυτό, από τα μέσα του 20ού αιώνα, η Ευρωπαϊκή Ένωση είχε αναγνωρίσει την προστασία των προσωπικών δεδομένων ως ένα από σημαντικότερα θεμελιώδη δικαιώματα των ανθρώπων. Αξίζει να επισημανθεί ότι οι πρώτες προσπάθειες προστασίας των δεδομένων προσωπικού χαρακτήρα έγιναν σε διεθνές επίπεδο και όχι σε επίπεδο κράτους.

Σημείο αφετηρίας στα νομοθετήματα προστασίας δεδομένων αποτέλεσε η Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου. Το κείμενο δεν είχε δεσμευτική ισχύ και δεν επέτρεπε στους πολίτες να διεκδικήσουν τα δικαιώματα που αναφέρονται σε αυτό. Εντούτοις, ήταν το πρώτο βήμα και έμπνευση για τους εθνικούς νομοθέτες. Το 1950, το Συμβούλιο της Ευρώπης υπέγραψε την Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου, το οποίο αποτέλεσε μια διεθνή συμφωνία και τέθηκε επισήμως σε εφαρμογή το 1953. Από τότε μέχρι σήμερα, η τεχνολογία έχει κάνει τεράστια άλματα προόδου και οι νόμοι της Ευρωπαϊκής Ένωσης, όσον αφορά την προστασία των δεδομένων, έχουν προσαρμοστεί με τέτοιο τρόπο ώστε να θεωρούνται ως πρότυπο για την παγκόσμια κοινότητα.

Από τα τέλη της δεκαετίας του '60 έως τη δεκαετία του 1980, πολλές χώρες στην Ευρώπη, πήραν το πρωτοβουλία θέσπισης νομοθεσίας με στόχο τον έλεγχο της χρήσης των προσωπικών δεδομένων από κυβερνητικούς οργανισμούς και εταιρείες. Σε αυτές εντάσσονται η Αυστρία, η Δανία, η Γαλλία, η Ομοσπονδιακή Δημοκρατία της Γερμανίας, το Λουξεμβούργο, η Νορβηγία και η Σουηδία. Ακόμη και στην Ισπανία, την Πορτογαλία και την Αυστρία, η προστασία των δεδομένων είχε ενσωματωθεί στο σύνταγμά τους ως θεμελιώδες δικαίωμα.

Επιπλέον, υπήρξε η δικαιολογημένη ανησυχία ότι στο πλαίσιο της ανάπτυξης της τεχνολογίας, οι εθνικές νομοθεσίες δεν προστάτευαν επαρκώς το δικαίωμα στην ιδιωτικότητα. Ως αποτέλεσμα, το Συμβούλιο της Ευρώπης αποφάσισε να θεσπίσει ένα ειδικό πλαίσιο αρχών και προτύπων για την πρόληψη της αθέμιτης συλλογής και επεξεργασίας προσωπικών δεδομένων.

Στη συνέχεια, το 1968 έγινε δημοσίευση της Σύστασης 509 για τα Ανθρώπινα Δικαιώματα και τις Σύγχρονες και Επιστημονικές Τεχνολογικές Εξελίξεις

(Recommendation 509 on Human Rights and Modern and Scientific Technological Developments) και το 1974 το Συμβούλιο της Ευρώπης βασίστηκε σε αυτή τη Σύσταση για να καταλήξει στα Ψηφίσματα 73/22 και 74/29, τα οποία θέσπισαν αρχές για την προστασία των προσωπικών δεδομένων σε αυτοματοποιημένες βάσεις δεδομένων τόσο στον ιδιωτικό όσο και στον δημόσιο τομέα, στοχεύοντας την ανάπτυξη εθνικών νομοθεσιών.

Στις 28η Ιανουαρίου 1981, η συνθήκη για την προστασία των ατόμων όσον αφορά την αυτοματοποιημένη επεξεργασία των προσωπικών τους δεδομένων υπογράφηκε ως Σύμβαση 108 του Συμβουλίου της Ευρώπης και τέθηκε σε ισχύ από την 1η Οκτωβρίου 1985. Εξαιρουμένης της Τουρκίας, τα 47 μέλη του Συμβουλίου της Ευρώπης επικύρωσαν τη συνθήκη. Παρ' όλα αυτά, αναπτύχθηκε ένα διαφορετικό σύνολο καθεστώτων προστασίας των δεδομένων μεταξύ του μικρού αριθμού χωρών που υιοθέτησαν εθνικούς νόμους με βάση αυτήν. Αυτό συνέβη εξαιτίας του ότι δεν είχαν οριστεί αυστηρά τα πρότυπα ασφαλείας, κάνοντας αντιληπτό ότι η υιοθέτηση αυτών των αρχών θα μπορούσε να έχει σοβαρές επιπτώσεις για τα θεμελιώδη δικαιώματα των ατόμων.

Στην προσπάθεια να διορθώσει τα κακώς κείμενα της Σύμβασης 108, δημιουργήθηκε η Οδηγία 95/46/ΕΚ, σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας προσωπικών δεδομένων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Ο στόχος της Οδηγίας ήταν να εξασφαλιστεί η προστασία των θεμελιωδών δικαιωμάτων των ατόμων με την ελεύθερη ροή δεδομένων μεταξύ των κρατών μελών.

Στις 7 Δεκεμβρίου 2000, στη Νίκαια της Γαλλίας, ανακηρύχθηκε και υπογράφτηκε επίσημα ο Χάρτης Θεμελιωδών Δικαιωμάτων, από το Ευρωπαϊκού Κοινοβουλίου, το Συμβουλίου και την Επιτροπής για λογαριασμό των θεσμικών οργάνων τους. Αρκετά σημαντικό αποτελεί το γεγονός ότι στις 4 Νοεμβρίου 2010, η Ευρωπαϊκή Επιτροπή αναπτύσσει και καθορίζει νέα στρατηγική για τον τρόπο προστασίας των προσωπικών δεδομένων, μειώνοντας παράλληλα την γραφειοκρατία για τις επιχειρήσεις και διασφαλίζοντας την ελεύθερη κυκλοφορία δεδομένων εντός της Ευρωπαϊκής Ένωσης.

Τέλος, στις 25 Ιανουαρίου 2012, η Ευρωπαϊκή Επιτροπή πρότεινε μια συνολική μεταρρύθμιση των κανόνων που θεσπίστηκαν το 1995 για την προστασία των δεδομένων, με σκοπό την ενίσχυση της διαδικτυακής ανωνυμίας και την ενίσχυση της ψηφιακής οικονομίας της Ευρώπης. Η Επιτροπή αναγνώρισε ότι η τεχνολογική πρόοδος και η παγκοσμιοποίηση έχουν αλλάξει ουσιαστικά τον τρόπο συλλογής,

πρόσβασης και χρήσης των δεδομένων. Παράλληλα με την πρόταση για τον Κανονισμό 5853/12, η Επιτροπή εισήγαγε ειδική οδηγία σχετικά με την επεξεργασία δεδομένων για σκοπούς επιβολής του νόμου.

Στην Ελλάδα, η πρώτη προσπάθεια για την προστασία των προσωπικών δεδομένων έγινε με την επιτροπή Χαλαζωνίτη το 1985, στην οποία έγινε αναφορά στα υπερευαίσθητα δεδομένα. Στην συνέχεια, από το 1989 έως το 1992, το Υπουργείο Δικαιοσύνης πρότεινε σχέδια νόμου για τέσσερις συνεχόμενες χρονιές, όμως κανένα δεν συζητήθηκε. Σημαντικό γεγονός αποτέλεσε το 1992, όπου και πραγματοποιήθηκε Κύρωση της Ευρωπαϊκής Σύμβασης 108 του Συμβουλίου της Ευρώπης, χωρίς ωστόσο να θεσπιστούν νομοθετικά μέτρα αντίστοιχης διάταξης στο ελληνικό δίκαιο. Η Ελλάδα επικύρωσε τη Σύμβαση 108 με την ψήφιση του Νόμου 2068/1992. Το 1997, με το Νόμο 2472/1997 ξεκίνησε η διαδικασία προσαρμογής της Κοινοτικής Οδηγίας 95/46/ΕΚ της Ευρωπαϊκής Ένωσης στα ελληνικά δεδομένα. Μάλιστα, έγινε σοβαρή προσπάθεια για να υιοθετηθούν οι αρχές και οι προβλέψεις της Οδηγίας με αρκετά αυστηρό τρόπο, επιδιώκοντας όσο το δυνατόν υψηλότερο επίπεδο προστασίας. Ωστόσο, οι αποκλίσεις του Νόμου από την αντίστοιχη Κοινοτική Οδηγία ήταν προφανείς και ουσιώδεις.

**Οι βασικοί άξονες του Νόμου είναι τρεις και αφορούν τα εξής:**

- την ύπαρξη συστήματος προϋποθέσεων νομιμότητας της επεξεργασίας
- την παροχή δικαιωμάτων στα άτομα
- την οργάνωση ελέγχου προστασίας των δεδομένων

Το επόμενο βήμα πραγματοποιήθηκε το 2011, με το Νόμο 3917/2011, στον οποίο αναφέρθηκε για πρώτη φορά η υποχρέωση των τηλεπικοινωνιακών παρόχων να προσφέρουν τις απαραίτητες πληροφορίες για την εξακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Περιλάμβανε, επίσης, διατάξεις για την εδραίωση την προστασίας των ηλεκτρονικών επικοινωνιών του ελληνικού πληθυσμού, αλλά ακόμα και τρόπους με τους οποίους πρέπει να επεξεργάζονται τα δεδομένα οι πάροχοι, ορίζοντας ταυτόχρονα τις υποχρεώσεις τους και τις ποινές στην περίπτωση μη συμμόρφωσης. Επιπλέον, έγινε αναφορά στις εποπτικές αρχές, οι οποίες ήταν υπεύθυνες για την τήρηση των κανονισμών. Εκείνη την εποχή υπεύθυνη για την τήρηση του Νόμου 2472/1997 ήταν η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

## 3.2 ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Η νομοθετική κατοχύρωση της προστασίας προσωπικών δεδομένων και η εξασφάλιση της νόμιμης επεξεργασίας από το κράτος και τις επιχειρήσεις πραγματοποιήθηκε ως λογικό επακόλουθο της εξέλιξης της βιομηχανικής κοινωνίας σε κοινωνία της πληροφορίας και ψηφιακής πραγματικότητας. Για αρκετά χρόνια, η Σύμβαση 108 αποτελούσε το βασικό νομοθετικό κείμενο για την προστασία των δεδομένων που εφαρμοζόταν σε όλα τα έθνη. Με τη Συνθήκη του Μάαστριχτ καθώς και τη δημιουργία της Ευρωπαϊκής Ένωσης, η σύνδεση των κρατών μελών επεκτάθηκε τόσο σε πολιτικά όσο και κοινωνικά ζητήματα. Ωστόσο, υπήρχε η ανάγκη για ισχυρή σύγκλιση των εθνικών νομοθεσιών, κυρίως για τα κράτη μέλη της Ευρωπαϊκής Ένωσης, ώστε να αντιμετωπιστούν οι διαφορές που εμφάνιζαν και να υπάρξει ουσιαστική ρύθμιση στη διασυνοριακή μεταφορά προσωπικών δεδομένων.

Η Οδηγία 95/46/ΕΚ συνέβαλε καθοριστικά στην προστασία των πολιτών έναντι της επεξεργασίας των προσωπικών δεδομένων και στην ισορροπία της σχέσης της προστασίας των δεδομένων με την απαραίτητη διασυνοριακή ροή πληροφοριών μεταξύ των κρατών μελών. Θέτοντας, για πρώτη φορά, τις βασικές αρχές που πρέπει να διέπουν την επεξεργασία των δεδομένων, η Οδηγία αποτυπώνει τα δικαιώματα των υποκειμένων σε σχέση με την επεξεργασία που υφίστανται τα δεδομένα τους. Εντός των άλλων, η Οδηγία επισήμανε τη σημαντικότητα της ίδρυσης ανεξάρτητων εποπτικών αρχών, με σκοπό την προάσπιση των δικαιωμάτων των πολιτών.

Στην Ελλάδα, ο πρώτος ελληνικός νόμος, ο οποίος εναρμόνισε το ελληνικό δίκαιο με την Οδηγία, ήταν ο Νόμος 2472/1997. Στο Σύνταγμα της χώρας η προστασία των προσωπικών δεδομένων αποτελούσε πλέον πρωταρχικό μέλημα της ελληνικής νομοθεσίας. Σύμφωνα με το άρθρο 9Α του Συντάγματος, “καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει”.

Στο Νόμο ορίζεται και η ίδρυση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) ως αρμόδιας ανεξάρτητης εποπτικής αρχής, η οποία είναι συνταγματικά κατοχυρωμένη ανεξάρτητη διοικητική Αρχή. Η λειτουργία της Αρχής ξεκίνησε στις 10 Νοεμβρίου 1997. Σκοπός της Αρχής είναι ο σεβασμός και η προστασία της αξιοπρέπειας, της ιδιωτικής ζωής και της ελεύθερης ανάπτυξης της προσωπικότητας. Άλλες αρχές που εποπτεύουν την επεξεργασία προσωπικών

δεδομένων είναι στην Ελλάδα η Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών και στην Ευρώπη ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων.

Φτάνοντας στο πρόσφατο παρελθόν, στις 12 Μαρτίου 2014 το Ευρωπαϊκό Κοινοβούλιο υπερψήφισε για την ανάγκη δημιουργίας νέου σχεδίου Κανονισμού σχετικά με την προστασία των δεδομένων. Την επόμενη χρονιά, στις 6 Μαΐου 2015, σηματοδοτήθηκε ένα σημείο καμπής για την ευρωπαϊκή νομοθεσία. Ο πρόεδρος της Ευρωπαϊκής Επιτροπής, με δήλωσή του, σήμανε την έναρξη της λειτουργίας ενός νέο κανονισμού, που θέτει καινούργια θεμέλια για το ψηφιακό μέλλον της Ευρώπης. Στα μέσα του Ιουνίου της ίδιας χρονιάς, το Συμβούλιο καταλήγει σε μια γενική προσέγγιση επί της διαμόρφωσης του νέου σχεδίου Κανονισμού. Στην προσπάθεια ύπαρξης μιας πλήρως ψηφιακής ενιαίας αγοράς, επινοήθηκαν 16 βήματα στρατηγικής για την ένταξη στη νέα ψηφιακή εποχή.

**Οι 16 δράσεις αυτές που προήγαγε η Επιτροπή βασίζονται σε τρεις πυλώνες:**

- στην καλύτερη πρόσβαση των καταναλωτών και των επιχειρήσεων σε ψηφιακά αγαθά και υπηρεσίες σε όλη την Ευρώπη
- στη δημιουργία των συνθηκών και των κανόνων που θα συμβάλουν στην εξέλιξη των ψηφιακών δικτύων και επιχειρήσεων.
- στη ενίσχυση της δυναμικής ανάπτυξης για την ψηφιακή οικονομία.

Η τελική συμφωνία μεταξύ του Κοινοβουλίου, της Επιτροπής και του Συμβουλίου επήλθε το Δεκέμβριο του 2015. Ο Κανονισμός ψηφίστηκε εντέλει, το Μάιο του 2016 και δόθηκε διετής περίοδος προσαρμογής στα κράτη μέλη της Ευρωπαϊκής Ένωσης έως το Μάιο του 2018.

**Σημαντικές ημερομηνίες έως την έναρξη εφαρμογής του Κανονισμού:**

- **24/10/1995:** Θεσπίζεται η Οδηγία 95/46/ΕΚ.
- **10/11/1997:** Νόμος 2472/1997 για την προστασία του ατόμου από την επεξεργασία των δεδομένων προσωπικού χαρακτήρα
- **2006:** Νόμος 3471/2006 για την προστασία δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Νόμου 2472/1997
- **22/06/2011:** Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων δημοσιεύει γνώμη σχετικά με την ανακοίνωση της Ευρωπαϊκής Επιτροπής για την προστασία των προσωπικών δεδομένων στην ΕΕ.
- **25/01/2012:** Η Ευρωπαϊκή Επιτροπή επισημαίνει την ανάγκη τροποποίησης της Οδηγίας.

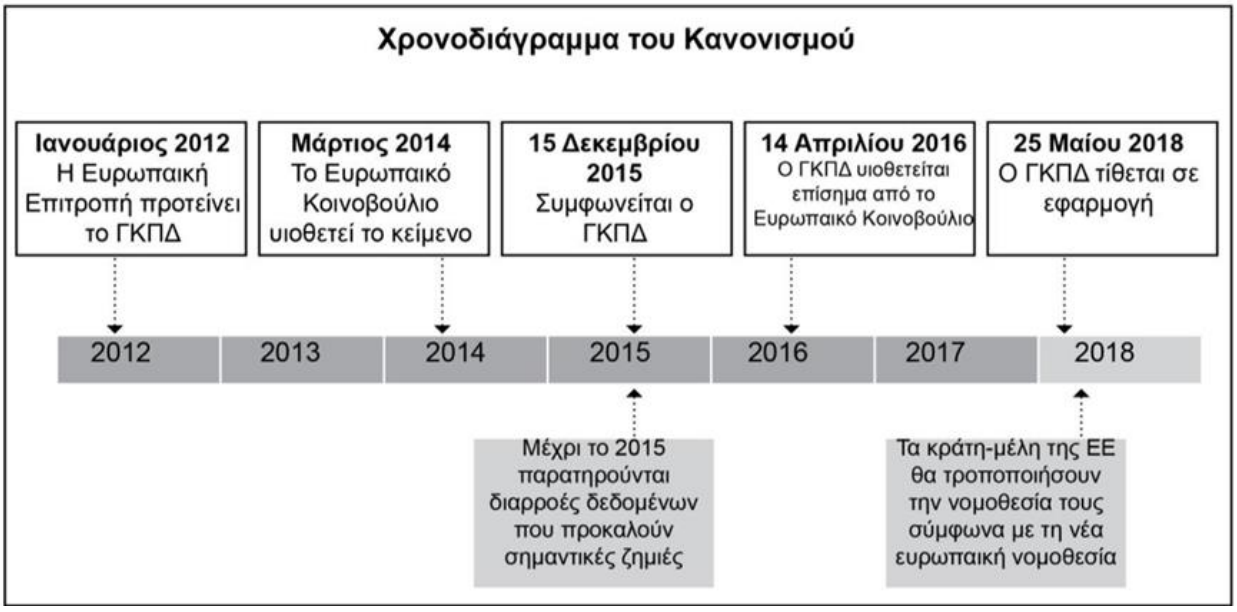
- **07/03/2012:** Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων δημοσιεύει γνώμη επί της προτεινόμενης (από την Επιτροπή) τροποποίησης της Οδηγίας.
- **23/03/2012:** Το “Article 29 Working Party” δημοσιεύει γνώμη επί της προτεινόμενης (από την Επιτροπή) τροποποίησης της Οδηγίας.
- **05/10/2012:** Το “Article 29 Working Party” δημοσιεύει περαιτέρω σχόλια επί της προτεινόμενης (από την Επιτροπή) τροποποίησης της Οδηγίας.
- **12/03/2014:** Το Ευρωπαϊκό Κοινοβούλιο υπερψηφίζει το σχέδιο Κανονισμού.
- **15/06/2015:** Το Συμβούλιο καταλήγει σε μια γενική προσέγγιση επί του σχεδίου Κανονισμού.
- **27/07/2015:** Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων δημοσιεύει συστάσεις προς την Επιτροπή σύνταξης του τελικού κειμένου του Κανονισμού.
- **15/12/2015:** Επέρχεται τελική συμφωνία μεταξύ του Κοινοβουλίου, της Επιτροπής και του Συμβουλίου.
- **02/02/2016:** Το “Article 29 Working Party” δημοσιεύει το χρονοδιάγραμμα υλοποίησης του Κανονισμού.
- **27/04/2016:** Κανονισμός (ΕΕ) αριθμός 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και για την κατάργηση της οδηγίας 95/46 / ΕΚ (Κανονισμός Γενικής Προστασίας Δεδομένων)
- **24/05/2016:** Δημοσιεύεται ο Κανονισμός.
- **10/01/2017:** Η Ευρωπαϊκή Επιτροπή προτείνει δύο νέους Κανονισμούς σχετικά με την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες (ePrivacy) και επιπλέον τους κανόνες προστασίας δεδομένων που ισχύουν για τα θεσμικά όργανα της ΕΕ (επί του παρόντος Κανονισμός 45/2001) που ευθυγραμμίζουν τους ισχύοντες κανόνες με το Γενικό Κανονισμό.
- **06/05/2018:** Έναρξη εφαρμογής της Οδηγίας ΕΕ/2016/680 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.
- **22/05/2018:** Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα της Ένωσης
- **25/05/2018**: Έναρξη εφαρμογής του Κανονισμού 2016/679.

Πηγή: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

## 3.3 ΣΧΕΤΙΚΑ ΜΕ ΤΟΝ ΓΕΝΙΚΟ ΚΑΝΟΝΙΣΜΟ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (ΕΕ) 2016/679

Ο Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων από την επεξεργασία των προσωπικών τους δεδομένων και την ελεύθερη κυκλοφορία των δεδομένων αυτών, συνιστά το θεσμικό εργαλείο που ρυθμίζει την προστασία των δεδομένων. Ο Κανονισμός καλύπτει κάθε πιθανή επεξεργασία δεδομένων, αυτοματοποιημένης ή μη, αφορά εξίσου την επεξεργασία στον ιδιωτικό, αλλά και στον δημόσιο τομέα, σύμφωνα με τις προκλήσεις της παγκόσμιας οικονομίας, τις αναδυόμενες τεχνολογίες και τα νέα επιχειρηματικά μοντέλα. Στόχος του παραμένει η θέσπιση ενός υψηλού επιπέδου προστασίας δεδομένων χωρίς να περιορίζεται η ελεύθερη κυκλοφορία δεδομένων στην Ευρωπαϊκή Ένωση. Ο Κανονισμός έχει άμεση εφαρμογή από την ημέρα κατά την οποία τέθηκε σε ισχύ και εφαρμόζεται με τον ίδιο τρόπο καθολικά και πιστά σε όλη την Ευρώπη.

Τον Ιανουάριο του 2012, η Ευρωπαϊκή Επιτροπή κατέθεσε την πρότασή της για μια ριζική αναθεώρηση και αλλαγή της Οδηγίας που ίσχυε, προκειμένου να ενισχυθούν αποτελεσματικά η προστασία των δεδομένων και οι ηλεκτρονικές συναλλαγές στο διαδίκτυο. Στις 12 Μαρτίου 2014, το Ευρωπαϊκό Κοινοβούλιο υιοθέτησε κατά πλειοψηφία την πρόταση για τον νέο σχέδιο Κανονισμού. Και έπειτα από ενάμιση χρόνο διαβουλεύσεων και συστάσεων από όλες τις αρμόδιες αρχές, το Ευρωπαϊκό Κοινοβούλιο, η Επιτροπή και το Συμβούλιο της Ευρωπαϊκής Ένωσης κατέληξαν και συμφωνήσαν στο τελικό κείμενο του Κανονισμού. Ο Κανονισμός (ΕΕ) 2016/679, η ημέρα της θέσης σε ισχύ του οποίου ήταν στις 24 Μαΐου 2015, όρισε ότι η υποχρέωση συμμόρφωσης με τις διατάξεις του θα ξεκινούσαν δύο χρόνια αργότερα, στις 25 Μαΐου 2018, δίνοντας έτσι ένα χρονικό περιθώριο δύο ετών ώστε οι οργανισμοί να μπορέσουν να προσαρμοστούν στη νέα πραγματικότητα.




Πηγή: Βιβλίο Ειρηνικός Πλατής. «Προσωπικά Δεδομένα - Προστασία GDPR»

Βασικά χαρακτηριστικά του Κανονισμού είναι:

- Η γενική εφαρμογή σε όλες τις επιχειρήσεις, ανεξαρτήτως μεγέθους και κλάδου δραστηριοποίησης, αλλά και στους φορείς δημοσίου
- Οι έντονες και πολυετείς διαπραγματεύσεις για το τελικό κείμενο
- Η αμετάκλητη ημερομηνία έναρξης εφαρμογής του, στις 25 Μαΐου 2018
- Η ύπαρξη πολλών διατάξεων στη διακριτική ευχέρεια των κρατών-μελών για περαιτέρω εξειδίκευση
- Τα υψηλά διοικητικά πρόστιμα

Τα κράτη μέλη οφείλουν να λάβουν τα κατάλληλα νομοθετικά μέτρα για την υιοθέτηση του Κανονισμού. Στις απαραίτητες δράσεις περιλαμβάνονται η σύσταση εποπτικής αρχής και η ενεργοποίηση του μηχανισμού συνεκτικότητας. Επίσης, τα κράτη μέλη είναι υποχρεωμένα να λάβουν ειδικά μέτρα για τον προσδιορισμό και την εξειδίκευση της εφαρμογής των διατάξεων. Να επισημανθεί ότι τα κράτη μέλη πρέπει να θεσπίσουν δικές τους εθνικές διατάξεις, όσον αφορά στην επεξεργασία δεδομένων που γίνεται προς συμμόρφωση με νομική υποχρέωση και για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που ανατίθεται στον υπεύθυνο επεξεργασίας. Επιπροσθέτως ο Κανονισμός παρέχει περιθώρια χειρισμού στα κράτη μέλη ώστε να μπορούν να εξειδικεύσουν τους κανόνες του, συμπεριλαμβανομένων αυτών που αφορούν την επεξεργασία των ευαίσθητων προσωπικών δεδομένων.

Ο Κανονισμός επιφέρει σημαντικές αλλαγές στο ρυθμιστικό περιβάλλον για τους «Υπεύθυνους Επεξεργασίας» και «Εκτελούντες την Επεξεργασία». Δηλαδή επηρεάζει τη λειτουργία των επιχειρήσεων και των δημόσιων φορέων, κυρίως σε τρία επίπεδα:

έχει ως κεντρική λογική την ελαχιστοποίηση της συλλογής, διατήρησης και επεξεργασίας προσωπικών δεδομένων

επιδιώκει την ενίσχυση της προστασίας των δεδομένων προσωπικού χαρακτήρα, αναθεωρώντας τις υποχρεώσεις όλων όσων επεξεργάζονται δεδομένα, καθώς πλέον, οι επονομαζόμενοι υπεύθυνοι επεξεργασίας δεδομένων, αλλά και οι εκτελούντες την επεξεργασία, για λογαριασμό των «Υπευθύνων», οφείλουν να αποδεικνύουν τη συμμόρφωση στις διατάξεις του Κανονισμού

αναδιαμορφώνει και ενισχύει τα δικαιώματα των υποκειμένων, γεγονός στο οποίο οφείλουν να προσαρμοστούν οι υπεύθυνοι επεξεργασίας, αλλά και οι εκτελούντες την επεξεργασία, για λογαριασμό των «Υπευθύνων», και συνεπώς να μεταβάλλουν τη δράση και τις αποφάσεις τους.

Συνεπώς, ο Κανονισμός εφαρμόζεται σε κάθε υπεύθυνο επεξεργασίας ή εκτελούντα που διενεργεί επεξεργασία δεδομένων στο πλαίσιο των αρμοδιοτήτων και δραστηριοτήτων, ο οποίος είναι εγκατεστημένος στην Ευρωπαϊκή Ένωση. Επίσης, εφαρμόζεται σε κάθε υπεύθυνο η εκτελούντα ανεξαρτήτως έδρας και τόπου, ο οποίος επεξεργάζεται δεδομένα φυσικών ανθρώπων που διαμένουν στην Ευρωπαϊκή Ένωση. Η εγκατάσταση νοείται πραγματικά και όχι νομικά, ως ύπαρξη επίσημης έδρας ενός κράτους μέλους.

Παρά την ευρωπαϊκή ταυτότητα του Κανονισμού, η εφαρμογή του δεν περιορίζεται απαραίτητα εντός των ορίων της Ευρωπαϊκής Ένωσης, καθώς υφίσταται η διεθνοποίηση της οικονομίας , η ύπαρξη συμφερόντων που αναπτύσσονται εντός των ευρωπαϊκών συνόρων  και η ανάγκη για τη διασυνοριακή ροή πληροφοριών χωρίς να παρεμποδίζεται το επιθυμητό επίπεδο προστασίας τους.

Επιπλέον, με σκοπό την αποτελεσματικότερη προστασία των προσωπικών δεδομένων απαραίτητη κρίνεται η συμμετοχή της αρμόδιας ανεξάρτητης εποπτικής αρχής, η οποία να είναι ικανή να εφαρμόζει τη σχετική νομοθεσία και παράλληλα να ελέγχει την επεξεργασία από τους υπεύθυνους επεξεργασίας και εκτελούντες την επεξεργασία, προληπτικά, με συστάσεις και ελέγχους, αλλά και κατασταλτικά, μέσα από κυρώσεις και παρατηρήσεις. Στην Ελλάδα, ο ρόλος αυτός έχει αποδοθεί στην

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), με αντίστοιχες εθνικές αρχές στα υπόλοιπα κράτη μέλη.

Τέλος, ο Κανονισμός προβλέπει τη σύσταση του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (ΕΣΠΔ) ως οργάνου αποτελούμενου από τους προϊσταμένους όλων των ευρωπαϊκών εποπτικών αρχών και τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων. Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων επιφορτίζεται με το καθήκον της συνεκτικής εφαρμογής του Κανονισμού, ώστε να εξασφαλίζεται η ασφάλεια δικαίου, ταχύτητα στις συναλλαγές με τις εποπτικές αρχές και η ασφαλής διασυνοριακή ροή δεδομένων.

**Οι καινοτομίες του Κανονισμού σε λέξεις-κλειδιά**

| | |
|---|---|
| ✓ Ενίσχυση δικαιωμάτων υποκειμένων | ✓ Αυστηριοποίηση κυρώσεων |
| ✓ Ενίσχυση δικαιώματος στη λήθη | ✓ Σύσταση Ευρωπαϊκού Συμβούλιου Προστασίας Δεδομένων |
| ✓ Θέσπιση δικαιώματος στη φορητότητα | ✓ Θέσπιση μηχανισμού συνεκτικότητας |
| ✓ Μεταφορά βάρους απόδειξης στους Υπευθύνους Επεξεργασίας (Λογοδοσία) | ✓ Θεσμοθέτηση της Αρχής της Διαφάνειας |

Πηγή: http://www.sev.org.gr/Uploads/Documents/51628/meleti_sev_GDPR_final.pdf

Εν συντομία, ο Κανονισμός αποτελεί ένα κοινό πλαίσιο ρυθμίσεων για τον τρόπο με τον οποίο συλλέγονται, επεξεργάζονται, φυλάσσονται, διακινούνται, αξιοποιούνται, αλλά και καταστρέφονται, δεδομένα προσωπικού χαρακτήρα των πολιτών της ΕΕ, ανεξαρτήτως του τόπου διαμονής τους, τόσο σε ηλεκτρονική όσο και σε φυσική μορφή.

## 3.4 ΣΥΝΘΗΚΕΣ ΠΟΥ ΟΔΗΓΗΣΑΝ ΣΤΟ ΝΕΟ ΚΑΝΟΝΙΣΜΟ

Η ανάγκη προστασίας των προσωπικών δεδομένων και το κανονιστικό πλαίσιο που τη διασφαλίζει, συνιστούσε προβληματισμό για την Ευρωπαϊκή Ένωση, αλλά και τη χώρα μας. Ήδη από το 1995 ο Ευρωπαίος νομοθέτης εισήγαγε σημαντικές υποχρεώσεις στα κράτη μέλη, όπως ήταν η Οδηγία 95/46/ΕΚ, διασφαλίζοντας αφενός την προστασία των πολιτών έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και αφετέρου την εξασφάλιση της ελεύθερης κυκλοφορίας των δεδομένων αυτών, ως μέσο επίτευξης οικονομικής και κοινωνικής προόδου.

Από το 1995 και έπειτα, βρισκόταν σε ισχύ η Οδηγία «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών», η οποία ενσωματώθηκε στο εθνικό δίκαιο βάσει του Νόμου 2472/1997 «για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα».

Αργότερα και κατά την προετοιμασία του Κανονισμού (ΕΕ) 2016/679 διαπιστώθηκε ότι η Οδηγία δεν κατάφερε να αναπτύξει αποτελεσματικά την εφαρμογή της προστασίας των δεδομένων των φυσικών προσώπων σε ολόκληρη την Ένωση. Ήδη από την εισαγωγή του Κανονισμού είχε φανεί πως όλες οι προσπάθειες που είχαν γίνει στο παρελθόν για ένα συνεκτικό και ομοιογενές θεσμικό πλαίσιο στις χώρες της Ευρωπαϊκής Ένωσης είχαν μόνο μερικώς κατορθωθεί. Τελικώς, τον Ιανουάριο του 2012 η Ευρωπαϊκή Επιτροπή υπέβαλε την πρότασή της, καθώς έκρινε απαραίτητη την ριζική αναθεώρηση της Οδηγίας.

Στις 27 Απριλίου 2016 τέθηκε σε εφαρμογή ο Κανονισμός, Γενικός Κανονισμός για την Προστασία Δεδομένων, του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της Οδηγίας 95/46/ΕΚ».

Συνοψίζοντας, οι δύο καθοριστικές παράμετροι που κατέστησαν αναγκαία τη μεταρρύθμιση του κανονιστικού πλαισίου, όπως αυτή εκφράστηκε με τον νέο Κανονισμό, καθώς τα μέτρα πολιτικής, που ίσχυσαν μέχρι τη δημιουργία του, εξάντλησαν την όποια ενδεχόμενη αποτελεσματικότητά τους, είναι οι εξής:

- Η πρώτη αφορά στις ραγδαίες τεχνολογικές εξελίξεις που έλαβαν χώρα, αλλάζοντας τον κόσμο και καθιστώντας την Οδηγία 95/46/ΕΚ παρωχημένη. Η τεχνολογική πρόοδος βοήθησε στην αύξηση της έκτασης και έντασης της συλλογής, ανταλλαγής και επεξεργασίας προσωπικών δεδομένων και πληροφοριών. Καθώς, όμως, οι πληροφορίες αποκτούσαν μεγαλύτερη αξία, σημειωνόταν και αύξηση περιπτώσεων παραβίασης της ασφάλειας των δεδομένων προσωπικού χαρακτήρα.
- Η δεύτερη αφορά στην ασυμμετρία εφαρμογής της Οδηγίας 95/46/ΕΚ από τα κράτη μέλη, αλλά και στο έλλειμμα προστασίας της ιδιωτικότητας των φυσικών προσώπων που διαπιστώθηκε στην πράξη. Γεγονός συνιστά η ύπαρξη ανασφάλειας δικαίου, εξαιτίας των αποκλίσεων κατά την εκτέλεση και εφαρμογή της Οδηγίας. Οι εν λόγω διαφορές στο επίπεδο προστασίας των πολιτών της Ευρώπης έναντι της επεξεργασίας των προσωπικών δεδομένων,

όχι μόνο δεν κατάφεραν να προστατεύσουν ενιαία την ιδιωτικότητα των φυσικών προσώπων, αλλά θεωρήθηκαν και ως εμπόδιο στην ψηφιακή επανάσταση. Επιπλέον, παρατηρήθηκε στρέβλωση του ανταγωνισμού. Οι διάσπαρτες διατάξεις και οι διαφορετικές ερμηνείες και πρακτικές δημιούργησαν μια διαδεδομένη αντίληψη στους πολίτες ότι υπάρχουν σημαντικοί κίνδυνοι για την προστασία των προσωπικών τους δεδομένων, ιδίως όσον αφορά την ηλεκτρονική δραστηριότητα.

Τέλος, στην παρακάτω εικόνα παρουσιάζεται η εξέλιξη του προσδιορισμού των προσωπικών δεδομένων που χρήζουν προστασίας και την ανάγκη για αναθεώρηση της νομοθεσίας που προϋπήρχε για την επίτευξη της προστασίας των προσωπικών δεδομένων των φυσικών προσώπων. Από τη δημιουργία της Οδηγίας 95/46/ΕΚ του 1995 για την προστασία δεδομένων, η συλλογή προσωπικών και ψηφιακών δεδομένων φαίνεται να είχε αλλάξει για πάντα. Με την αύξηση του εύρους των πληροφοριών των πελατών που είναι διαθέσιμες στις επιχειρήσεις , καθώς και τη δημοτικότητα των κοινωνικών μέσων και των ιστοσελίδων διαδικτύου που μπορούν να παρακολουθούν και να καταγράφουν δεδομένα για τη χρήση τρίτων, η ασφάλεια των προσωπικών δεδομένων φαίνεται να είναι ελλιπής. Μία από τις μεγαλύτερες αλλαγές που έφερε ο Κανονισμός είναι οι κατηγορίες που συνιστούν προσωπικά δεδομένα που χρήζουν προστασίας. Το παρακάτω διάγραμμα απεικονίζει την εκτεταμένη εξήγηση για το τι συνιστούν πλέον προσωπικά δεδομένα, σύμφωνα με τον Κανονισμό Γενικής Προστασίας Δεδομένων.

| Items That Constitute Personal Data | Data Protection Directive (1995) | General Data Protection Regulations (2018) |
|---|---|---|
| Name | ✓ | ✓ |
| Photo | ✓ | ✓ |
| E-mail Address | ✓ | ✓ |
| Phone Number | ✓ | ✓ |
| Address | ✓ | ✓ |
| Personal Identification Numbers | ✓ | ✓ |
| IP Addresses | ✗ | ✓ |
| Mobile Device Identifiers | ✗ | ✓ |
| Geo-Location | ✗ | ✓ |
| Biometric Data | ✗ | ✓ |
| Psychological Identity | ✗ | ✓ |
| Generic Identity | ✗ | ✓ |
| Economic Status | ✗ | ✓ |
| Cultural Identity | ✗ | ✓ |
| Social Identity | ✗ | ✓ |

Πηγή: https://coinaccord.io/blog/three-ways-data-protection-laws-will-affect-blockchain-organizations

# ΚΕΦΑΛΑΙΟ 4: ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (GDPR)

## 4.1 ΈΝΝΟΙΑ ΚΑΙ ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Όλοι οι οργανισμοί και οι επιχειρήσεις, τόσο του ιδιωτικού όσο και του δημόσιου τομέα, που βρίσκονται εγκατεστημένοι στην Ευρωπαϊκή Ένωση, ή που είναι εγκατεστημένοι εκτός Ευρωπαϊκής Ένωσης και χειρίζονται προσωπικά δεδομένα τα οποία αφορούν σε άτομα που βρίσκονται εντός της Ευρωπαϊκής Ένωσης, είναι υποχρεωμένοι να συμμορφωθούν πλήρως στις επιταγές του νέου Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR), ο οποίος τέθηκε σε εφαρμογή την 25η Μαΐου 2018.

Ο Κανονισμός (ΕΕ) 2016/679, καταργώντας την Οδηγία 95/46/ΕΚ, αποτελεί μια κανονιστική εξέλιξη στο ρυθμιστικό περιβάλλον. Έτσι, προκύπτει η εξισορρόπηση μεταξύ του δικαιώματος της προστασίας των δεδομένων προσωπικού χαρακτήρα από τη μία πλευρά και του δικαιώματος στην πληροφόρηση, διαφάνεια και δημόσια ασφάλεια από την άλλη, με τρόπο που να προάγει την ελεύθερη και ανεμπόδιστη οικονομική ανάπτυξη και επιχειρηματική δραστηριότητα. Ωστόσο, ο Κανονισμός εκφράζει μια χαρακτηριστική περίπτωση εκ των υστέρων ρύθμισης, όπου ο νομοθέτης έρχεται να θεραπεύσει και όχι να προλάβει, καθώς η τεχνολογία προπορεύεται κατά πολύ του δικαίου, αλλά και ίσως της ηθικής.

Ο Γενικός Κανονισμός Προστασίας των Προσωπικών Δεδομένων (GDPR), κρίνεται ως μία αναγκαία μεταρρύθμιση του υφιστάμενου πλαισίου προστασίας προσωπικών δεδομένων, το οποίο, όπως προαναφέρθηκε, είχε ξεπεραστεί από τις τεχνολογικές εξελίξεις και από την αποτυχία ενιαίου τρόπου εφαρμογής των διατάξεων για την προστασία των προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση, με αρνητικές συνέπειες στην ενιαία αγορά και τον ανταγωνισμό. Ωστόσο, το περιεχόμενο του αποτέλεσε, αντικείμενο έντονων και πολυετών διαπραγματεύσεων, με αποτέλεσμα να είναι ένα κείμενο «συμβιβασμού» διαφορετικών προσεγγίσεων. Πρόκειται για ένα εκτεταμένο Κανονισμό, 5 φορές μεγαλύτερο από την Οδηγία 95/46/ΕΚ, με 99 άρθρα, εκ των οποίων τα 28 αφήνουν περιθώριο παρέκκλισης.

Συνοπτικά, ο σκοπός του νέου Κανονισμού είναι να ανταπεξέλθει στις προκλήσεις της ψηφιακής εποχής, εισάγοντας δύο ουσιώδεις διαφοροποιήσεις. Πρώτον, εισάγει την αρχή της λογοδοσίας, καθώς μετατοπίζει το βάρος για την απόδειξη της συμμόρφωσης από τον ρυθμιστή / ελεγκτή στον ρυθμιζόμενο / ελεγχόμενο. Πλέον, οι επονομαζόμενοι «Υπεύθυνοι Επεξεργασίας» πρέπει να είναι σε θέση να αποδείξουν ότι έχουν λάβει όλα τα απαραίτητα μέτρα για την προστασία των προσωπικών δεδομένων, με την εποπτική Αρχή να αναλαμβάνει ρόλο και δράση σε δεύτερο

χρόνο, με την έννοια ότι στο παρελθόν ήταν εκείνη που είχε την πρωτοβουλία για την εποπτεία και τον έλεγχο συμμόρφωσης. Δεύτερον, ανανεώνει τα δικαιώματα των υποκειμένων των δεδομένων. Δηλαδή, οι ιδιοκτήτες των προσωπικών δεδομένων έχουν ενισχυμένα δικαιώματα, γεγονός στο οποίο οι επιχειρήσεις-υπεύθυνοι επεξεργασίας οφείλουν να λάβουν υπόψιν και συνεπώς να προσαρμόσουν ανάλογα τη λειτουργία και τις αποφάσεις τους

**Σημαντικοί λόγοι που οδήγησαν στο GDPR:**

- Αλόγιστη μεταβίβαση προσωπικών δεδομένων σε τρίτους.
- Παράνομη πώληση προσωπικών δεδομένων
- Επικοινωνία με τον πελάτη χωρίς την προηγούμενη ενημέρωση ή συναίνεσή του
- Απόκρυψη περιστατικών παραβίασης
- Μεγάλες διαφορές στη νομοθεσία των κρατών μελών
- Ανεπάρκεια του προηγουμένου νομοθετικού πλαισίου
- Ραγδαίες τεχνολογικές εξελίξεις
- Μη τήρηση βασικών αρχών και έλλειψη μέτρων ασφαλείας

Ο Κανονισμός 2016/679 έχει εφαρμογή σε όλους τους φορείς, όπως ιδιωτικές και δημόσιες επιχειρήσεις, κρατικές αρχές, συλλόγους, οι οποίοι διαχειρίζονται, επεξεργάζονται, αποθηκεύουν, και διακινούν δεδομένα προσωπικού χαρακτήρα είτε έχουν έδρα και δραστηριότητα σε χώρα της Ευρωπαϊκής Ένωσης είτε όχι, εφόσον τα δεδομένα αφορούν Ευρωπαίους πολίτες ή σχετίζονται με οποιουδήποτε είδους υπηρεσίες και αγαθά προς Ευρωπαίους πολίτες.

**Με την συμμόρφωση μας στον GDPR πετυχαίνουμε:**

- Ανταγωνιστικό προβάδισμα στην αγορά
- Ψηφιακό μετασχηματισμό
- Χτίζουμε την σχέση μας με τον πελάτη επί του σεβασμού των δικαιωμάτων του
- Εξασφαλίζουμε την εμπιστοσύνη των εν δυνάμει πελατών μας
- Εξασφαλίζουμε τη φήμη μας
- Αλλάζουμε την κουλτούρα μας προς το καλύτερο: ενίσχυση της διαφάνειας και της ασφάλειας του πελάτη

Η χρησιμότητα ύπαρξης και εφαρμογής του Κανονισμού (ΕΕ) 2016/679 μπορεί να γίνει εύκολα αντιληπτή, παραθέτοντας τα παρακάτω παραδείγματα πραγματικών γεγονότων υποκλοπής δεδομένων:


Σύμφωνα με τους New York Times, η εταιρεία συλλογής δεδομένων Cambridge Analytica υπεξαίρεσε προσωπικά στοιχεία πάνω από 50 εκατομμυρίων χρηστών του Facebook το 2014, με σκοπό να ενισχυθεί η υποψηφιότητα Trump έναντι αυτής της Η. Clinton, αναπτύσσοντας ποικίλες τεχνικές προσέγγισης.

Η Facebook, μετά την αποκάλυψη του περιστατικού, ανακοίνωσε ότι διέκοψε οποιαδήποτε συνεργασία με την εν λόγω εταιρεία καθώς δεν είχε καμία αρμοδιότητα πάνω σε αυτά τα στοιχεία.

Η ομάδα Trump φέρεται μέσω των στοιχείων να πραγματοποιούσε profiling, ώστε να εντοπίζει συγκεκριμένους ψηφοφόρους στους οποίους προωθούσε στοχευμένες πολιτικές διαφημίσεις και μηνύματα υπέρ της υποψηφιότητας Trump.


Το 2016 η Τράπεζα Tesco έπεσε θύμα κυβερνο-επίθεσης. Παραβιάστηκαν 40.000 τραπεζικοί λογαριασμοί και οι δράστες υπέκλεψαν χρήματα από 20.000 εξ αυτών. Η Τράπεζα υποσχέθηκε ότι θα καλύψει την οικονομική απώλεια των πελατών της

Αν το περιστατικό συνέβαινε μετά τις 25/05/2018, το πρόστιμο που θα επιβαλλόταν θα μπορούσε να αγγίξει τις 1,9 εκατομμύρια λίρες βάσει του παγκόσμιου τζίρου του Ομίλου.


Επιβλήθηκε πρόστιμο 10.000 ευρώ από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα σε ελληνική Τράπεζα για τη μη ικανοποίηση δικαιώματος πρόσβασης του υποκειμένου στα δεδομένα των καταγεγραμμένων συνομιλιών τους.

Παράλληλα η Αρχή επέβαλε στην Τράπεζα, η οποία ήταν υπεύθυνος επεξεργασίας, να ικανοποιήσει το δικαίωμα των υποκειμένων να έχουν πρόσβαση στα δεδομένα των καταγεγραμμένων συνομιλιών τους καθώς και ότι πρέπει να ενημερώσει τα στελέχη και τους υπαλλήλους της για την εν λόγω υποχρέωση της, δηλαδή την άνευ ετέρου ικανοποίηση του δικαιώματος του υποκειμένου να έχει πρόσβαση στα δεδομένα του (καταγεγραμμένη συνομιλία), χωρίς την ανάγκη επίκλησης έννομου προς τούτο συμφέροντος της Τράπεζας και χωρίς δυνατότητα ελέγχου της συνδρομής ή μη τούτου στο πρόσωπο του ασκούντος το δικαίωμα αυτό υποκειμένου.

## 4.2 ΒΑΣΙΚΕΣ ΑΡΧΕΣ

Ο Κανονισμός επαναπροσδιορίζει τις θεμελιώδεις αρχές που υπήρχαν στην Οδηγία 95/46/ΕΚ και τις ενισχύει. Βασιζόμενοι στην αρχή της λογοδοσίας, κατά την επεξεργασία των προσωπικών δεδομένων, οι Υπεύθυνοι Επεξεργασίας και οι Εκτελούντες αυτήν, σύμφωνα με το άρθρο 5 του Κανονισμού, πρέπει να φροντίζουν να τηρούνται οι εξής βασικές αρχές:

**Η αρχή της νόμιμης, αντικειμενικής και διαφανούς επεξεργασίας** που καθιστά αναγκαία την σύννομη, θεμιτή και με διαφανή τρόπο επεξεργασία αναφορικά με το υποκείμενο των δεδομένων.

Η νομιμότητα της επεξεργασίας επισφραγίζεται και διασφαλίζεται στις περιπτώσεις στις οποίες, πρώτον, έχει ληφθεί η προηγούμενη συναίνεση του υποκειμένου στην επεξεργασία των δεδομένων του για έναν ή περισσότερους συγκεκριμένους σκοπούς, δεύτερον, η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης ή για τη συμμόρφωση με έννομη υποχρέωση του Υπευθύνου Επεξεργασίας που

απορρέει από άλλο κανόνα δικαίου, τρίτον, η επεξεργασία είναι αναγκαία για την διαφύλαξη ζωτικού συμφέροντος ή για την εκπλήρωση καθήκοντος προς το δημόσιο συμφέρον ή για την άσκηση δημόσιας εξουσίας ανατεθειμένης στον Υπεύθυνο Επεξεργασίας και τέλος, η επεξεργασία είναι απαραίτητη για τους σκοπούς των εννόμων συμφερόντων που επιδιώκει ο Υπεύθυνος Επεξεργασίας εκτός αν υποκείμενο δεν είναι ενήλικος, περίπτωση στην οποία υπερισχύει το έννομο συμφέρον προστασίας του τέκνου.

Η διαφάνεια εξασφαλίζεται μέσω της παροχής κάθε πληροφορίας και ανακοίνωσης όσον αφορά στην επεξεργασία με διαφανή και κατανοητό τρόπο σε εύκολα προσβάσιμη μορφή. Για την παροχή πληροφόρησης ή την διατύπωση της ανακοίνωσης πρέπει να γίνεται χρήση σαφούς, συνοπτικής και απλής διατύπωσης, ειδικά εάν πρόκειται για ενημέρωση ανηλίκων. Η πληροφορία πρέπει να δίνεται στο υποκείμενο των δικαιωμάτων εντός προθεσμίας ενός μήνα από την παραλαβή του σχετικού αιτήματός του (με δυνατότητα παράτασης για δύο μήνες), ενώ στην περίπτωση που η παροχή της πληροφορίας δεν είναι εφικτή, ο Υπεύθυνος Επεξεργασίας οφείλει να ενημερώσει το υποκείμενο για την αδυναμία αυτή, καθώς και για τη δυνατότητα υποβολής καταγγελίας στην αρμόδια εποπτική αρχή και άσκησης δικαστικής προσφυγής.

**Η αρχή του περιορισμού του σκοπού** εκπληρώνεται όταν η συλλογή και η επεξεργασία γίνονται με στόχο σαφή και καθορισμένο, ούτως ώστε να μην επιτρέπεται η υποβολή των δεδομένων σε περαιτέρω επεξεργασία. Μοναδική εξαίρεση αποτελεί η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης που εξυπηρετούν το δημόσιο συμφέρον ή στατιστικούς σκοπούς ή για σκοπούς επιστημονικής ή ιστορικής έρευνας, υπό τον όρο ότι μέσω των χρησιμοποιούμενων μεθόδων δε γίνεται εφικτή η ταυτοποίηση των υποκειμένων των δεδομένων, παρέχοντας τις κατάλληλες εγγυήσεις για την προστασία των δεδομένων τους.

**Η αρχή ελαχιστοποίησης των δεδομένων** εφαρμόζεται τόσο στον όγκο των δεδομένων όσο και στη διάρκεια διατήρησης αυτών. Βάσει αυτής, τα δεδομένα που τηρούνται πρέπει να είναι κατάλληλα, συναφή και περιορισμένα στα απολύτως απαραίτητα, σύμφωνα με τους σκοπούς για τους οποίους εκτελείται η επεξεργασία.

**Η αρχή της ακρίβειας**, μέσω της οποίας τονίζεται η αναγκαιότητα των δεδομένων να είναι ακριβή και, όταν χρειάζεται, να είναι επίκαιρα, ενώ ταυτόχρονα το υποκείμενο θα πρέπει να έχει επίγνωση ως προς τα προσωπικά του δεδομένα που υφίστανται επεξεργασία. Παράλληλα, πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την

άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή και μη σχετικά, όσον αφορά στους σκοπούς της επεξεργασίας αυτών.

**Η αρχή του περιορισμού της περιόδου αποθήκευσης**, δηλαδή την τήρηση των αρχείων των δεδομένων μόνο για το απαραίτητο χρονικό διάστημα, μέχρις ότου επιτευχθεί ο σκοπός της επεξεργασίας. Εξαίρεση συνιστά η περίπτωση κατά την οποία η επεξεργασία γίνεται για σκοπούς αρχειοθέτησης που αφορούν το δημόσιο συμφέρον ή στατιστικούς σκοπούς ή σκοπούς επιστημονικής ή ιστορικής έρευνας, με την προϋπόθεση της λήψης κατάλληλων οργανωτικά μέτρα για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων.

**Η αρχή της ακεραιότητας και εμπιστευτικότητας** αφορά στην υποβολή των προς επεξεργασία δεδομένων κατά τρόπο ώστε να εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων.

**Η αρχή της αναλογικότητας** αναφέρεται στη συνάφεια ανάμεσα στα δεδομένα που τηρούνται και το σκοπό για τον οποίο αυτά συλλέγονται, τα δεδομένα αυτά πρέπει να είναι πρόσφορα και αναγκαία για την εκπλήρωση του σκοπού αυτού. Τοιουτοτρόπως, η αρχή της αναλογικότητας συμβάλλει στην ελαχιστοποίηση των τηρούμενων δεδομένων, δεδομένου ότι η επεξεργασία δεν αφορά στο σύνολο των δεδομένων που συλλέγονται από τον Υπεύθυνο Επεξεργασίας ή τον Εκτελούντα αυτή.

Τέλος, σύμφωνα με **την αρχή της λογοδοσίας**, ο Υπεύθυνος Επεξεργασίας και ο Εκτελών αυτήν, οφείλουν να αποδείξουν τόσο την συμμόρφωση στις υποχρεώσεις που θέτει ο Κανονισμός, όσο και την ετοιμότητά τους να συμμορφωθούν. Οι υποχρεώσεις τους διαμορφώνονται ανάλογα με τον κίνδυνο που ενδέχεται να προκύψει από την επεξεργασία, όπως αυτός εκτιμάται πριν την έναρξη της επεξεργασίας, βάσει της Εκτίμησης Αντικτύπου.

## 4.3 ΔΙΚΑΙΩΜΑΤΑ ΤΟΥ ΥΠΟΚΕΙΜΕΝΟΥ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Μία από τις πιο ουσιαστικές τομές που έφερε ο Κανονισμός (ΕΕ) 2016/679 είναι τα δικαιώματα που παρέχονται στο υποκείμενο των δεδομένων. Η Ευρωπαϊκή Επιτροπή έθεσε ως βασική της προτεραιότητα την ενίσχυση των δικαιωμάτων των φυσικών προσώπων στην πρότασή της για το νέο νομοθετικό πλαίσιο. Για το λόγο αυτό, η παραβίαση των δικαιωμάτων που ορίζονται μέσω του Κανονισμού, επισύρει υψηλά πρόστιμα.

Τα δικαιώματα που εξασφαλίστηκαν από το νέο νομοθετικό πλαίσιο ενδυναμώνουν τον ρόλο του υποκειμένου, προσφέροντάς του τη δυνατότητα να ελέγχει πιο αποτελεσματικά και ουσιαστικά τον βαθμό έκθεσης της ιδιωτικής του ζωής. Συν τοις άλλοις, η ικανοποίηση των δικαιωμάτων των υποκειμένων απαιτεί από τις επιχειρήσεις να τροποποιήσουν ακόμη και βασικές επιχειρησιακές λειτουργίες προκειμένου να ανταποκριθούν.

**Δικαίωμα Ενημέρωσης**

Όπως έχει προαναφερθεί, κάθε επικοινωνία προς το φυσικό πρόσωπο, όσον αφορά στην επεξεργασία των προσωπικών του δεδομένων, διέπεται από την αρχή της διαφάνειας. Όταν το υποκείμενο διαθέτει σαφή και επαρκή πληροφόρηση, είναι σε θέση να ελέγχει και να επηρεάζει την επεξεργασία των δεδομένων του. Αυτό σημαίνει ότι ο υπεύθυνος της επεξεργασίας είναι υποχρεωμένος να διασφαλίζει την απαραίτητη πληροφόρηση του υποκειμένου.

Ο υπεύθυνος επεξεργασίας οφείλει να χρησιμοποιεί απλή, ξεκάθαρη και καθημερινή γλώσσα , μη επιδεχόμενη παρερμηνείας, ώστε να γίνεται κατανοητή από οποιονδήποτε, ιδιαίτερα στις περιπτώσεις που οι αποδέκτες είναι παιδιά είτε άτομα χαμηλού μορφωτικού επιπέδου είτε μεγάλης ηλικίας. Ο Κανονισμός δεν απαιτεί τη χρήση συγκεκριμένης μορφής επικοινωνίας. Προκειμένου, όμως, να εξυπηρετηθεί ο σκοπός της ενημέρωσης με εύληπτη μορφή, δίνεται η δυνατότητα να παρέχεται είτε γραπτώς είτε ηλεκτρονικώς ή άλλο μέσο. Ο υπεύθυνος επεξεργασίας, όταν η πηγή είναι το ίδιο το υποκείμενο, πρέπει να το ενημερώνει κατά τη λήψη των δεδομένων του και πριν  την επεξεργασίας τους. Ωστόσο, όταν τα δεδομένα του υποκειμένου συλλέγονται από διαφορετική πηγή, η ενημέρωση πρέπει να γίνεται το αργότερο εντός ενός μήνα. Επιπλέον, το υποκείμενο πρέπει να ενημερώνεται κατά την πρώτη γνωστοποίηση των δεδομένων του σε άλλον αποδέκτη και σαφώς πριν την επεξεργασία τους, εφόσον ο σκοπός επεξεργασίας παύει να είναι ο αρχικός σκοπός συλλογής τους. Τέλος, σχετικά με το περιεχόμενο της ενημέρωσης, ο υπεύθυνος επεξεργασίας είναι υποχρεωμένος να παρέχει όλες τις λεπτομέρειες για την

σκοπούμενη επεξεργασία, για τα δικαιώματα του υποκειμένου, καθώς και τον τρόπο άσκησής τους.

Στην περίπτωση δέσμευσης του υπεύθυνου επεξεργασίας από επαγγελματικό ή ιατρικό απόρρητο, ο Κανονισμός προβλέπει τη μη ενημέρωση των υποκειμένων. Συγκεκριμένα, αν στο πλαίσιο της εξέτασης ενός ασθενούς, ο γιατρός λάβει γνώση δεδομένων υγείας των συγγενών του, δεν υποχρεούται να ενημερώσει σχετικά τους εν λόγω συγγενείς, καθώς δεσμεύεται από το ιατρικό απόρρητο.

**Δικαίωμα Πρόσβασης**

Στο υποκείμενο παραχωρείται το δικαίωμα να αποκτά πρόσβαση στα προσωπικά δεδομένα του. Με τον τρόπο αυτό, ενισχύεται η αρχή της αντικειμενικότητας και της διαφάνειας, καθώς παρέχεται στο υποκείμενο η δυνατότητα να επιβεβαιώσει τη νομιμότητα της επεξεργασίας των δεδομένων του. Κατά συνέπεια, μπορεί να ασκήσει με αποτελεσματικότητα τα λοιπά δικαιώματα που του επιτρέπει ο Κανονισμός.

Το δικαίωμα της πρόσβασης περιλαμβάνει δύο στάδια. Στο πρώτο στάδιο, το υποκείμενο των δεδομένων έχει τη δυνατότητα να επιβεβαιώσει αν τα δεδομένα του τυγχάνουν επεξεργασίας. Εφόσον λάβει θετική απάντηση από τον υπεύθυνο επεξεργασίας, ακολουθεί το δεύτερο στάδιο. Παρέχεται στο υποκείμενο η πρόσβαση στα δεδομένα του, ενημερώνοντας το με λεπτομέρειες για το σκοπό της επεξεργασίας τους και ταυτόχρονα γνωστοποιώντας του τα δικαιώματά του.

Στην περίπτωση που το υποκείμενο επιθυμεί να λάβει γνώση και να επηρεάσει την επεξεργασία των δεδομένων του, ο Κανονισμός παρέχει τη δυνατότητα άσκησης των δικαιωμάτων του. Το υποκείμενο μπορεί να υποβάλει αίτημα προς τον υπεύθυνο επεξεργασίας, εγγράφως είτε σε φυσική είτε σε ηλεκτρονική μορφή, για την ικανοποίηση των δικαιωμάτων του. Ο Κανονισμός ορίζει στον υπεύθυνο επεξεργασίας την υποχρέωση να γνωστοποιεί στο υποκείμενο κάθε ενέργεια που γίνεται εκ μέρους του και να δρα εντός των καθορισμένων χρονικών ορίων. Ο υπεύθυνος επεξεργασίας οφείλει να απαντήσει στο αίτημα του υποκειμένου εντός ενός μήνα από την παραλαβή του. Να σημειωθεί ότι αν ο υπεύθυνος επεξεργασίας δεν επιθυμεί την ικανοποίηση του αιτήματος του υποκειμένου, τότε θα πρέπει να γνωστοποιήσει την απόφασή του αυτή εντός ενός μήνα. Ταυτόχρονα, πρέπει να ενημερώνει το υποκείμενο για τη δυνατότητα που έχει να υποβάλει καταγγελία στην Αρχή και να προσφύγει+ στο αρμόδιο δικαστήριο.

**Δικαιώματα Διόρθωσης, Διαγραφής και Περιορισμού**

Ο Κανονισμός παρέχει στο υποκείμενο την δυνατότητα να ελέγξει ή να επηρεάσει την επεξεργασία που διενεργεί ο υπεύθυνος επεξεργασίας στα δεδομένα του, μέσω της άσκησης των δικαιωμάτων της διόρθωσης, της διαγραφής ή του περιορισμού της επεξεργασίας τους.

Το δικαίωμα της πρόσβασης βασίζεται στην αρχή της ακρίβειας. Μέσω της οποίας θα πρέπει να διασφαλίζεται η αποτύπωση της πραγματικής κατάστασης του υποκειμένου. Το υποκείμενο μπορεί να υποβάλει αίτημα στον υπεύθυνο επεξεργασία, ως προς τη διόρθωση ανακριβών ή ελλιπών δεδομένων του. Την ευθύνη για απόδειξη της επικαλούμενης ανακρίβειας ή έλλειψης φέρει το ίδιο το υποκείμενο, προσκομίζοντας τα απαραίτητα σχετικά και αποδεικτικά έγγραφα.

Το δικαίωμα της διαγραφής, ιδίως των ψηφιακών δεδομένων, δημιουργεί αρκετά προβλήματα, καθώς τα υποστηρικτικά τεχνολογικά και πληροφοριακά συστήματα και μέσα της επιχειρηματικής δραστηριότητας δεν υποστηρίζουν ή δεν παρέχουν τη επιλογή της διαγραφής δεδομένων. Στην περίπτωση αυτή, τα δεδομένα θα πρέπει να καταστούν μη επεξεργάσιμα, εμποδίζοντας τον τρόπο χρήσης τους από τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία ή οποιονδήποτε τρίτο. Η ικανοποίηση του δικαιώματος αυτού απαιτεί από το υποκείμενο την απόδειξη της ύπαρξης ενός σοβαρού λόγου, τον οποίο να έχει προβλέψει ο Κανονισμός.

Το δικαίωμα του περιορισμού της επεξεργασίας συνιστά τη συμβιβαστική λύση μεταξύ των δικαιωμάτων του υπεύθυνου επεξεργασίας, για συνέχιση της επεξεργασίας δεδομένων, και του υποκειμένου, για διόρθωση ή διαγραφή τους. Ο υπεύθυνος επεξεργασίας πρέπει να περιορίσει την επεξεργασία των δεδομένων εφόσον αιτηθεί το υποκείμενο, για όσο χρονικό διάστημα ορίζει ο Κανονισμός. Μετά την εφαρμογή του περιορισμού στην επεξεργασία των δεδομένων του υποκειμένου, ο υπεύθυνος επεξεργασίας είναι υποχρεωμένος να απέχει από οποιαδήποτε επεξεργασία, πέραν της αποθήκευσης, εκτός κι αν το υποκείμενο παράσχει την συναίνεση του ή το δημόσιο συμφέρον ή δικαιώματα άλλων φυσικών προσώπων χρήζουν προστασίας. Σε όλες τις περιπτώσεις, ο υπεύθυνος επεξεργασίας οφείλει να ενημερώσει το υποκείμενο, προτού άρει τον περιορισμό της επεξεργασίας.

Τέλος, στις περιπτώσεις διόρθωσης,  διαγραφής ή περιορισμού της επεξεργασίας, ο υπεύθυνος επεξεργασίας επωμίζεται την ευθύνη ενημέρωσης προς τους αποδέκτες των δεδομένων ή προς τους υπόλοιπους υπευθύνους επεξεργασίας.

**Δικαίωμα Φορητότητας**

Το δικαίωμα της φορητότητας αποτελεί νέο δικαίωμα, το οποίο προσφέρει στο υποκείμενο τη δυνατότητα ανεξαρτησίας και αυτενέργειας στον ψηφιακό κόσμο. Δίνεται η δυνατότητα στο υποκείμενο να λαμβάνει από τον υπεύθυνο επεξεργασίας τα δεδομένα του, σε δομημένο και κοινώς χρησιμοποιούμενο από τα μηχανήματα μορφότυπο, και να μεταφέρει σε άλλον υπεύθυνο επεξεργασίας. Η φορητότητα μπορεί να πραγματοποιηθεί απευθείας από τον υπεύθυνο επεξεργασίας αν και εφόσον είναι τεχνικά εφικτό. Ο υπεύθυνος επεξεργασίας πρέπει να ικανοποιήσει το δικαίωμα αυτό του υποκειμένου, όταν η επεξεργασία των δεδομένων γίνεται με αυτοματοποιημένα μέσα και βασίζεται στη νομική βάση της συναίνεσης του υποκειμένου. Επομένως, δεν επιτρέπεται η φορητότητα των δεδομένων σε φυσικά αρχεία αν αυτά δεν έχουν μετατραπεί σε ψηφιακά.

**Δικαίωμα Εναντίωσης**

Με το δικαίωμα αυτό το υποκείμενο μπορεί να εναντιωθεί στην επεξεργασία των δεδομένων του, ανεξάρτητα από το αν έχει ξεκινήσει η επεξεργασία ή όχι, συμπεριλαμβανομένης της κατάρτισης προφίλ. Συγκεκριμένα, το υποκείμενο έχει τη δυνατότητα να ασκήσει το δικαίωμα εναντίωσης για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, όταν η επεξεργασία, συμπεριλαμβανομένης της κατάρτισης προφίλ, βασίζεται στο έννομο συμφέρον του υπεύθυνου επεξεργασίας ή στο δημόσιο συμφέρον. Εντούτοις, ο υπεύθυνος επεξεργασίας μπορεί να αρνηθεί την ικανοποίηση του αιτήματος του υποκειμένου, στην περίπτωση που αποδείξει ότι συντρέχουν επιτακτικοί και νόμιμοι λόγοι, οι οποίοι υπερισχύουν της προστασίας των ελευθεριών και δικαιωμάτων του φυσικού προσώπου.

**Δικαίωμα στην Ανθρώπινη Παρέμβαση**

Με τη χρήση του δικαιώματος αυτού, δίνεται το δικαίωμα στο υποκείμενο να μην υπόκειται σε απόφαση που λαμβάνεται αυτοματοποιημένα, συμπεριλαμβάνοντας και την κατάρτιση προφίλ. Να επισημανθεί ότι οι αυτοματοποιημένες αποφάσεις μπορούν να λαμβάνονται με ή χωρίς κατάρτιση προφίλ, όπως η κατάρτιση προφίλ μπορεί να γίνεται χωρίς την αυτοματοποιημένη διαδικασία λήψης απόφασης. Δεν αποκλείεται, όμως, η απόφαση να ληφθεί αυτοματοποιημένα, έχοντας βασιστεί σε προηγούμενη ενέργεια κατάρτισης προφίλ του υποκειμένου. Τέλος, ο νομοθέτης έχει ως βασικό σκοπό να εμποδίσει να λαμβάνονται αποφάσεις για τα υποκείμενα από μηχανές, οι οποίες ενδέχεται να επιφέρουν στα δεδομένα αρνητικές ή θετικές νομικές συνέπειες ή θα μπορούσαν να επηρεάσουν τη ζωή τους ανάλογα.

## 4.4 ΥΠΕΥΘΥΝΟΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΚΑΙ ΕΚΤΕΛΩΝ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ

Σύμφωνα με τον Κανονισμό, Υπεύθυνος Επεξεργασίας είναι κάθε επιχείρηση ή οργανισμός ανεξαρτήτως μεγέθους που συλλέγει και επεξεργάζεται προσωπικά δεδομένα. Στην περίπτωση που η επεξεργασία γίνεται από κάποιο τρίτο μέρος για λογαριασμό της, το μέρος αυτό (φυσικό ή νομικό πρόσωπο) είναι ο Εκτελών την επεξεργασία, προς τον οποίο ο Υπεύθυνος Επεξεργασίας οφείλει να περιγράψει το σκοπό και τον τρόπο σύμφωνα με τον οποίο επιθυμεί να εκτελείται η επεξεργασία. Το τρίτο μέρος δεν αποτελεί μέρος του οργανισμού του Υπεύθυνου επεξεργασίας.

Η ευθύνη του Υπεύθυνου Επεξεργασίας προβλεπόταν ήδη στην Οδηγία, δεν συμπεριλάμβανε όμως και τον Εκτελούντα την επεξεργασία, που πλέον κάνει ο Κανονισμός και επεκτείνει την ευθύνη προς το μέρος αυτό. Προβλέπει δε την πλήρη ευθύνη του για αποζημίωση, αλλά και επιβολή κυρώσεων, στις περιπτώσεις που δεν ανταποκρίνεται στις υποχρεώσεις του Κανονισμού, δεν ενεργεί σύμφωνα με τις νόμιμες εντολές του υπευθύνου επεξεργασίας.

Ο Υπεύθυνος Επεξεργασίας φέρει την αποκλειστική ευθύνη τήρησης του Κανονισμού, έχει την υποχρέωση να χρησιμοποιεί μόνο Εκτελούντες την επεξεργασία που εφαρμόζουν κατάλληλες τεχνικές και οργανωτικά μέτρα, έτσι ώστε η επεξεργασία να πληροί τις απαιτήσεις του Κανονισμού και να διασφαλίζεται η προστασία των δικαιωμάτων του υποκειμένου των δεδομένων. Ωστόσο, ο Υπεύθυνος Επεξεργασίας οφείλει να ασκεί εποπτεία επί των εκτελούντων στους οποίους έχει αναθέσει την επεξεργασία, για να διασφαλίζεται το σύννομο των ενεργειών τους.

**Βάσει της Οδηγίας, για την επιβολή κυρώσεων και επιδίκαση αποζημίωσης στον υπεύθυνο επεξεργασίας απαιτούνται να συντρέχουν σωρευτικά τα ακόλουθα:**

- πράξη ή παράλειψη που παραβιάζει τις διατάξεις του Νόμου 2472/1997 ή/και των κατ' εξουσιοδότηση αυτού κανονιστικών πράξεων της Αρχής
- ηθική βλάβη
- αιτιώδη συνάφεια μεταξύ της συμπεριφοράς και της ηθικής βλάβης» και
- υπαιτιότητα, ήτοι γνώση ή υπαίτια άγνοια, αφενός των περιστατικών που συνιστούν την παράβαση και αφετέρου της πιθανότητας να επέλθει η ηθική βλάβη.

Να σημειωθεί ότι πρακτικά ο Υπεύθυνος Επεξεργασίας εφόσον μπορεί να αποδείξει ότι δεν ευθύνεται για το ζημιογόνο γεγονός που έθεσε σε κίνδυνο προσωπικά

δεδομένα μπορεί να απαλλαχθεί. Αντίθετα, τα στοιχεία του δόλου ή της αμέλειας συνυπολογίζονται μεν κατά τον υπολογισμό του προστίμου, εντούτοις δεν συνιστούν προϋπόθεση για την επιβολή κυρώσεων εκ μέρους της εποπτικής Αρχής.

Η μεταφορά ευθύνης για την τήρηση των διατάξεων καταλογίζεται από την Αρχή στο πρόσωπο του υπεύθυνου επεξεργασίας και του εκτελούντα αυτήν. Δημιουργείται μία νέα σχέση μεταξύ της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και του υπεύθυνου επεξεργασίας, ο οποίος έχει την υποχρέωση να αναλάβει πρωτοβουλίες για την τήρηση των υποχρεώσεών του, να ορίσει υπεύθυνο προστασίας προσωπικών δεδομένων και να προβεί σε συγκεκριμένες διαδικασίες που εξασφαλίζουν τη συμμόρφωση. Παράλληλα, ο Υπεύθυνος Επεξεργασίας πρέπει να είναι σε θέση να αποδεικνύει τη συμμόρφωση των δραστηριοτήτων του με τον Κανονισμό.

Ο Υπεύθυνος Επεξεργασίας είναι αποκλειστικός υπεύθυνος για την έγκαιρη γνωστοποίηση στην Αρχή ενός περιστατικού απώλειας της εμπιστευτικότητας ή διαθεσιμότητας δεδομένων, που ενδέχεται να υποβάλει σε κίνδυνο τα δικαιώματα του υποκειμένου. Παρακολουθεί διαρκώς τις διαδικασίες, τα πρωτόκολλα και τις ροές των δεδομένων που τηρεί και αναφέρει οποιοδήποτε σχετικό συμβάν στην Αρχή εντός 72 ωρών από την στιγμή που λάβει γνώση. Σε περιπτώσεις παραβάσεων, ο Κανονισμός απαιτεί όχι μόνο την ενημέρωση της Αρχής, αλλά και την εκπόνηση μιας εκτίμησης του κινδύνου που ενδέχεται να επέλθει από την επεξεργασία.

Επιπρόσθετα, ο Υπεύθυνος Επεξεργασίας οφείλει να ορίζει χρονικές προθεσμίες για τη διαγραφή των δεδομένων και την περιοδική επανεξέτασή τους προκειμένου να διασφαλίσει ότι δε διατηρούνται περισσότερο από όσο είναι αναγκαίο. Η επεξεργασία των δεδομένων θα πρέπει να γίνεται από εξουσιοδοτημένους χρήστες για να αποτρέπεται κάθε ανεξουσιοδότητη πρόσβαση σε αυτά και πρέπει να γίνεται αναφορά στον εξοπλισμό που χρησιμοποιείται για την επεξεργασία τους, με τρόπο που να διασφαλίζει την ενδεδειγμένη προστασία και εμπιστευτικότητα τους.

Ο Εκτελών την επεξεργασία είναι υπεύθυνος να εξασφαλίσει επαρκές επίπεδο προστασίας των δεδομένων που επεξεργάζεται για λογαριασμό του υπευθύνου επεξεργασίας. Εντούτοις, έχει τη δυνατότητα να επιλέξει ποια μέτρα ασφαλείας θα χρησιμοποιήσει και θα εφαρμόσει για τον σκοπό αυτό. Σε κάθε περίπτωση, θα πρέπει να λαμβάνει υπόψη τους κίνδυνους που προκύπτουν από την επεξεργασία των δεδομένων, όπως η απώλεια, παράνομη καταστροφή, μεταβολή, ανεξουσιοδότητη γνωστοποίηση ή πρόσβαση. Μετά το πέρας της επεξεργασίας, ο

Εκτελών αυτήν υποχρεούται να διαγράφει ή να επιστρέφει τα αρχεία, δεδομένα και σχετικά έγγραφα που επεξεργάστηκε στον υπεύθυνο επεξεργασίας.

Να επισημανθεί ότι ο Εκτελών την επεξεργασία δεν χρειάζεται να εκτιμήσει την πιθανότητα κινδύνου, αρκεί μόνο να ειδοποιήσει χωρίς καθυστέρηση τον υπεύθυνο επεξεργασίας τη στιγμή που θα αντιληφθεί ότι έχει πραγματοποιηθεί παραβίαση δεδομένων. Αν και ο Κανονισμός δεν προβλέπει ακριβές χρονικό όριο εντός του οποίου ο Εκτελών την επεξεργασία οφείλει να ενημερώσει τον υπεύθυνο επεξεργασίας, συνιστάται να αναφέρεται εντός της σύμβασης ότι πρέπει να ενημερώσει άμεσα.

## 4.5 ΥΠΕΥΘΥΝΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Η φιλοσοφία του νέου Κανονισμού εισάγει την αρχή της λογοδοσίας και μεταθέτει την ευθύνη για την τήρηση και επεξεργασία των δεδομένων στον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία. Επιδίωξη του νομοθέτη αποτέλεσε η μείωση των γραφειοκρατικών διαδικασιών γνωστοποίησης της επεξεργασίας δεδομένων προς τις εποπτικές αρχές. Για το λόγο αυτό, δημιουργήθηκε ο θεσμός του Υπευθύνου Προστασίας Δεδομένων (Data Protection Officer - DPO), μέσω του οποίου διασφαλίζεται η αρχή της λογοδοσίας, που προβλέπεται από τον Κανονισμό, και προσδίδεται ανταγωνιστικό πλεονέκτημα στους οργανισμούς που υιοθετούν αυτό το πρόσωπο. Ειδικότερα, ορίζεται ότι υπό συγκεκριμένες προϋποθέσεις, ορισμένοι υπεύθυνοι αλλά και εκτελούντες την επεξεργασία υποχρεούνται να ορίζουν υπεύθυνο προστασίας δεδομένων.

Μέχρι την παρουσίαση του όρου Υπεύθυνος Προστασίας Δεδομένων, τα κράτη μέλη ως επί το πλείστων δεν είχαν γνώση για την υποχρέωση διορισμού του συγκεκριμένου ρόλου. Ωστόσο, τον υποχρεωτικό διορισμό του για την προστασία δεδομένων είχε προβλέψει ο γερμανικός νόμος, για περισσότερα από 30 χρόνια, ο οποίος και λειτουργούσε με επιτυχία.

Ο υπεύθυνος προστασίας δεδομένων αποτελεί το φυσικό ή νομικό πρόσωπό, το οποίο ορίζεται από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και αναλαμβάνει συγκεκριμένα καθήκοντα, ώστε να εξασφαλιστεί η συμμόρφωση στον Κανονισμό. Είναι ένας ηγετικός ρόλος στον τομέα της ασφάλειας και είναι αρμόδιος για την επίβλεψη της στρατηγικής και της εφαρμογής της προστασίας των προσωπικών δεδομένων, προκειμένου να διασφαλιστεί η ορθή εφαρμογή του Κανονισμού στις επιχειρήσεις και οργανισμούς. Συνομιλεί και συνεργάζεται

απευθείας με την Αρχή, αντικαθιστώντας τον υπεύθυνο επεξεργασίας όσον αφορά στην αρμοδιότητά του αυτή, ενεργώντας όχι μόνο ως σημείο επικοινωνίας από την πλευρά του υπεύθυνου επεξεργασίας, αλλά και εξυπηρετώντας τους σκοπούς τήρησης της υποχρέωσης προηγούμενης διαβούλευσης με την Αρχή.

Τα υποκείμενα των δεδομένων μπορούν να επικοινωνούν μαζί του για κάθε ζήτημα σχετικό με την επεξεργασία των δεδομένων τους και με την άσκηση των δικαιωμάτων τους. Επομένως, είναι ευνόητο ότι ο Υπεύθυνος Προστασίας Δεδομένων δεσμεύεται από την τήρηση του απορρήτου ή εμπιστευτικότητας σχετικά με την εκτέλεση των καθηκόντων του, σύμφωνα με το δίκαιο της Ένωσης ή του κράτους μέλους.

Ο ρόλος του είναι συμβουλευτικός και είναι απόλυτα εναρμονισμένος με την πρωτοβουλία του ενωσιακού νομοθέτη για τη δημιουργία ενός αποτελεσματικού νομοθετικού πλαισίου, κεντρικό άξονα του οποίου αποτελεί η πρόληψη και η αποτροπή των φαινομένων παραβίασης της ιδιωτικότητας των υποκειμένων. Το πρόσωπο αυτό είναι η φωνή της συνείδησης της επιχείρησης, καθώς ενημερώνει και συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία. Λογοδοτεί απευθείας στην ανώτατη διοίκηση, αλλά και το προσωπικό του οργανισμού σχετικά με τις υποχρεώσεις τους για την προστασία των προσωπικών δεδομένων.

Ο Υπεύθυνος Επεξεργασίας και/ή ο Εκτελών  την επεξεργασία, πρέπει να διασφαλίζουν ότι ο υπεύθυνος προστασίας δεδομένων συμμετέχει σε όλα τα ζητήματα που σχετίζονται με την προστασία δεδομένων. Παράδειγμα αποτελεί η συμμετοχή σε συσκέψεις ανώτερων και μεσαίων στελεχών της διοίκησης και κατά τη λήψη αποφάσεων, η ελεύθερη πρόσβαση σε δεδομένα και πράξεις επεξεργασίας, η συμμετοχή σε συναντήσεις εργασίας και η ενημέρωση για όλες τις νέες δραστηριότητες, προϊόντα και υπηρεσίες. Επιπλέον, οφείλουν να του παρέχουν τους απαραίτητους πόρους (οικονομικούς και ανθρώπινους) για την άσκηση των καθηκόντων του και τη διατήρηση υψηλού επιπέδου τεχνογνωσίας.

Ακόμη, ο Υπεύθυνος Προστασίας Δεδομένων παρακολουθεί τη συμμόρφωση των πολιτικών που επιλέγει ο υπεύθυνος ή ο Εκτελών  την επεξεργασία και ελέγχει τη συμβατότητά τους με το σύνολο της ισχύουσας νομοθεσίας, σχετικά με την προστασία των προσωπικών δεδομένων. Τέλος, παρέχει συμβουλές σχετικά με την υποχρέωση εκτίμησης αντικτύπου και παρακολουθεί την υλοποίησή της.

Ο Κανονισμός επισημαίνει συγκεκριμένες περιπτώσεις, στις οποίες ο Υπεύθυνος Επεξεργασίας ή ο Εκτελών  την επεξεργασία υποχρεούται να ορίσει υπεύθυνο

προστασίας δεδομένων. Η μη συμμόρφωση στην υποχρέωση επισύρει χαμηλά πρόστιμα.

**Η υποχρέωση ορισμού Υπευθύνου Προστασίας Δεδομένων ισχύει εφόσον συντρέχουν συγκεκριμένες προϋποθέσεις:**

- Ο Υπεύθυνος Επεξεργασίας είναι Δημόσια αρχή ή φορέας, εξαιρουμένων των δικαστηρίων όταν αυτά ενεργούν υπό τη δικαιοδοτική τους αρμοδιότητα. Ο Κανονισμός δεν περιλαμβάνει ορισμό της έννοιας της Δημόσιας αρχής ή του δημόσιου φορέα, αντίθετα καταλείπεται στην σφαίρα της πρωτοβουλίας του εκάστοτε κράτους μέλους να προβεί στον προσδιορισμό αυτό.
- Προβλέπεται από το δίκαιο ενός κράτους μέλους. Παρά το γεγονός ότι δεν υποχρεούται στον ορισμό Υπευθύνου Προστασίας Δεδομένων, μπορεί να επιλέξει να το πράξει εθελοντικά, αυτό ωστόσο δε σημαίνει μειωμένη ευθύνη απέναντι στις υποχρεώσεις που επιβάλλονται από τον Κανονισμό.
- Οι βασικές δραστηριότητες του υπευθύνου περιλαμβάνουν μεγάλης κλίμακας επεξεργασία ευαίσθητων προσωπικών δεδομένων ή δεδομένων σχετικών με ποινικές καταδίκες και αδικήματα.

Οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας συνιστούν επεξεργασία που απαιτεί την τακτική και συστηματική παρακολούθηση των δεδομένων σε μεγάλη κλίμακα.

«Βασικές δραστηριότητες» αποτελούν αναπόσπαστο κομμάτι για την επίτευξη των στόχων του υπευθύνου επεξεργασίας ή εκτελούντα την επεξεργασία. Παράδειγμα αποτελεί η συλλογή ευαίσθητων δεδομένων από τα νοσοκομεία, καθώς η διαδικασία αυτή συνιστά αναπόσπαστο μέρος της βασικής τους δραστηριότητας. Αντιθέτως, η συλλογή των προσωπικών δεδομένων  του προσωπικού τους δεν αποτελεί βασική τους δραστηριότητα, αλλά παραπληρωματική και βοηθητική προς την επίτευξη της βασικής δραστηριότητας.

Η «τακτική και συστηματική παρακολούθηση» περιλαμβάνει όλες τις μορφές ανίχνευσης και κατάρτισης δεδομένων, όπως προφίλ στο διαδίκτυο, με σκοπό τη συμπεριφορική διαφήμιση, τη στοχευμένη επικοινωνία με email, το γεωεντοπισμό, τη χρήση κλειστών κυκλωμάτων παρακολούθησης και άλλες.

Η έννοια της «μεγάλης κλίμακας» ερμηνεύεται ως ο αριθμός των υποκειμένων των δεδομένων, είτε συγκεκριμένος αριθμός είτε ποσοστό του σχετικού πληθυσμού, ο όγκος των δεδομένων ή/και το εύρος των διαφόρων στοιχείων δεδομένων, η διάρκεια ή η μονιμότητα της δραστηριότητας επεξεργασίας και η γεωγραφική έκταση της

δραστηριότητας επεξεργασίας. Αδιάφορο είναι το μέγεθος της επιχείρησης που συλλέγει και επεξεργάζεται τα δεδομένα, όπως και η φύση τους (π.χ. ευαίσθητα). Επομένως, ο αριθμός των υποκειμένων τα οποία επηρεάζονται από την επεξεργασία καθώς και το γεωγραφικό εύρος αυτής καθιστούν την «μεγάλη κλίμακα».

Η ευθύνη του Υπεύθυνος Προστασίας Δεδομένων περιορίζεται σε θέματα πλημμελούς εκτέλεσης των υποχρεώσεών του έναντι του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία, επομένως δε φέρει ευθύνη έναντι του υποκειμένου των δεδομένων ή της Αρχής.

Για τον ορισμό του Υπεύθυνος Προστασίας Δεδομένων σε όμιλο επιχειρήσεων, ο Κανονισμός ορίζει ότι μπορεί να είναι το ίδιο πρόσωπο, ακόμα και σε ομίλους επιχειρήσεων με διασυνοριακή δραστηριότητα. Εντούτοις, για λόγους καλύτερης επικοινωνίας με την εκάστοτε αρμόδια τοπική Αρχή, αλλά και με τα υποκείμενα των δεδομένων, είναι προτιμότερο να ορίζεται και ένας τοπικά αρμόδιος Υπεύθυνος Προστασίας Δεδομένων.

Ο Κανονισμός ορίζει το ζήτημα πρακτικής εφαρμογής του καθεστώτος ανεξαρτησίας, το οποίο πρέπει να απολαμβάνει ο Υπεύθυνος Προστασίας Δεδομένων, και της δυνατότητας ρεαλιστικής υλοποίησης της απαίτησης αυτής, ειδικά στην περίπτωση που τη θέση αναλάβει ο διευθυντής της νομικής υπηρεσίας ή της υπηρεσίας πληροφοριακών συστημάτων του οργανισμού.

Στην περίπτωση του υπεύθυνου της υπηρεσίας πληροφοριακών συστημάτων, δεδομένου ότι συντρέχουν οι προϋποθέσεις σύγκρουσης συμφερόντων, δεν αποτελεί ορθή πρακτική η ταυτόχρονη ανάληψη καθηκόντων επικεφαλής IT και Υπεύθυνος Προστασίας Δεδομένων. Η άποψη σχετικά με την τοποθέτηση του δικηγόρου-επικεφαλή του νομικού τμήματος ως Υπεύθυνος Προστασίας Δεδομένων, ενώ βρίσκει υποστηρικτές, ταυτόχρονα υπάρχει προβληματισμός στο κατά πόσον ένας νομικός έχει το ιδανικό προφίλ για τη θέση αυτή. Καταλληλότερος για τη θέση κρίνεται ο Υπεύθυνος Κανονιστικής Συμμόρφωσης, ο οποίος διαθέτει μεγαλύτερη εμπειρία και εξοικείωση όσον αφορά σε τεχνικά και οργανωτικά θέματα του οργανισμού.

# ΚΕΦΑΛΑΙΟ 5: ΕΦΑΡΜΟΓΗ ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ

## 5.1 ΤΕΧΝΙΚΕΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

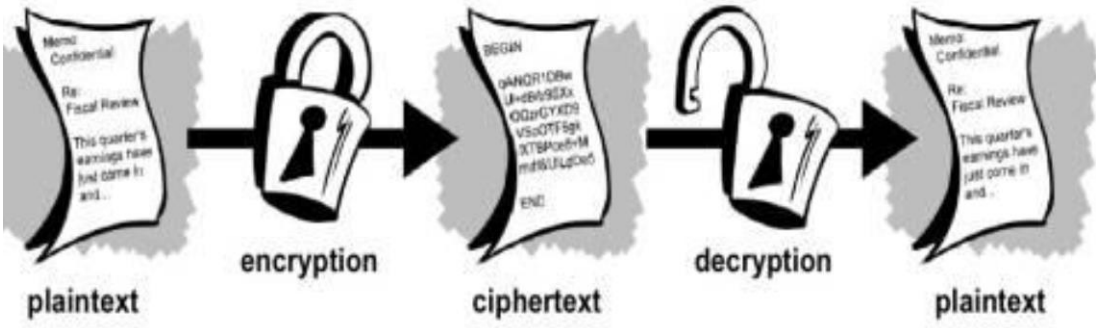
**Η κρυπτογράφηση και η ψευδωνυμοποίηση** ως προτεινόμενα ορίζονται ως τεχνικά μέτρα προστασίας στον Γενικό Κανονισμό Προστασίας Δεδομένων, καθώς μπορούν να μειώσουν σημαντικά τους κινδύνους που σχετίζονται με την επεξεργασία δεδομένων. Για τον λόγο αυτόν, μέσω του Κανονισμού, δημιουργούνται κίνητρα για τους υπεύθυνους επεξεργασίας ώστε να εφαρμόζουν τις τεχνικές αυτές στα προσωπικά δεδομένα που συλλέγουν, μέσω και της ελαστικοποίησης ορισμένων απαιτήσεων που τους αφορούν.

**Η κρυπτογράφηση** (encryption) είναι η επιστήμη, η οποία βασίζεται στα μαθηματικά, και αφορά στην κωδικοποίηση και αποκωδικοποίηση των δεδομένων. Μέσω της κρυπτογράφησης τα ευαίσθητα προσωπικά δεδομένα καθίστανται προσβάσιμα μόνο προς όσους είναι “κατάλληλα” εξουσιοδοτημένοι. Περιγράφεται ως η εφαρμογή μιας διαδικασίας μετασχηματισμού, μέσω κάποιου αλγορίθμου με τη χρήση «κλειδιών κρυπτογράφησης» (encryption keys), ενός συνόλου προσωπικών δεδομένων σε μία ακατανόητη μορφή, με σκοπό να μην μπορούν να αναγνωσθούν από κανέναν εκτός των νόμιμων ιδιοκτητών των κλειδιών κρυπτογράφησης. Με αυτόν τον τρόπο, εξασφαλίζουν το απόρρητο στις ψηφιακές επικοινωνίες, αλλά και στην αποθήκευση ευαίσθητων πληροφοριών. Επομένως, η κρυπτογράφηση αποτελεί μια μέθοδο παραλλαγής του απλού κειμένου (plaintext) σε μη αναγνωρίσιμη μορφή, χρησιμοποιώντας έναν αλγόριθμο κρυπτογράφησης. Κατά αυτόν τον τρόπο, οι πληροφορίες μετατρέπονται σε αλγόριθμο (ciphertext), γίνονται δυσανάγνωστες και μη κατανοητές, ώστε να μπορούν να διαβαστούν μόνο από αυτούς που κατέχουν την ειδική γνώση. Τη γνώση αυτήν έχουν εκείνοι που μεταδίδουν την πληροφορία.

Η διαδικασία της κρυπτογράφησης μπορεί να εκτελεστεί τόσο σε hardware, όσο και σε software.  Ενσωματώνοντας τις μεθόδους της κρυπτογραφίας σε hardware, επιταχύνεται σε μεγάλο βαθμό η πραγματοποίησή της. Εφόσον οι χρήστες δε γνωρίζουν ούτε αντιλαμβάνονται την παρουσία της, πραγματοποιούν ανενόχλητοι τις εργασίες τους. Έτσι, αυξάνεται η αποτελεσματικότητα του εργαλείου στην παρεχόμενη ασφάλεια. Ωστόσο, η κρυπτογραφία σε hardware έχει πολύ υψηλό κόστος, το οποίο δυσκολεύει την αγορά και διατήρηση των ειδικών μηχανημάτων που χρειάζονται για την εφαρμογή της. Η λογισμική κρυπτογραφία είναι πιο οικονομική, που την καθιστά ευρέως αποδεκτή και πραγματοποιήσιμη.

Τέλος, η αποκρυπτογράφηση (decryption) είναι η ανάκτηση του απλού κειμένου. Είναι η μέθοδος κατά την οποία το κρυπτογραφημένο - κωδικοποιημένο κείμενο

(ciphertext) που έχει δημιουργηθεί, επανέρχεται στην αρχική κατανοητή μορφή του, δηλαδή τα δεδομένα μετατρέπονται από κρυπτογραφημένος αλγόριθμος σε ευανάγνωστο κείμενο (plaintext). Αυτό επιτυγχάνεται μόνο χρησιμοποιώντας το επικαλούμενο κλειδί (decryption key), το οποίο είναι ένα κομμάτι πληροφορίας που υπολογίζει επακριβώς την έξοδο του αλγορίθμου. Χωρίς το κλειδί δεν υπάρχει αποτέλεσμα αποκρυπτογράφησης, καθώς αυτό δίνει το αποτέλεσμα στον αλγόριθμο και επιτρέπει την αλλαγή από κείμενο μορφής cipher text σε plaintext.




Πηγή: Βιβλίο Μιχαήλ Σφακιανάκης, «Εισαγωγή στην Πληροφορική Σκέψη»

Οι αλγόριθμοι διακρίνονται σε δύο κατηγορίες. Σε συμμετρικούς (symmetric), στους οποίους χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση, και σε ασύμμετρους (asymmetric), στους οποίους τα κλειδιά διαφέρουν, χωρίς να υπάρχει η δυνατότητα παραγωγής του κλειδιού αποκρυπτογράφησης από αυτό της κρυπτογράφησης. Το κλειδί που χρησιμοποιείται για την κρυπτογράφηση ονομάζεται δημόσιο (public), αφού επιτρέπεται να το χρησιμοποιούν διάφορα άτομα. Ωστόσο, μόνο οι παραλήπτες που διαθέτουν το ιδιωτικό (private) κλειδί μπορούν να αποκωδικοποιήσουν το μήνυμα. Οι ασύμμετροι αλγόριθμοι ονομάζονται και αλγόριθμοι δημοσίου κλειδιού (public-key algorithms).

Συνεπώς, υπάρχουν δύο είδη κρυπτογραφίας η συμμετρική και η ασύμμετρη:

- Συμμετρική κρυπτογραφία, στην οποία χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση, όσο και για την αποκρυπτογράφηση. Το κλειδί αυτό είναι απαραίτητο να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη, Παράλληλα, απαιτείται ασφαλές μέσο για τη μετάδοσή του, όπως μία προσωπική συνάντηση κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται. Τα συστήματα συμμετρικής κρυπτογραφίας προϋποθέτουν την ύπαρξη ενός ασφαλούς καναλιού για την ανταλλαγή των μυστικών

κλειδιών (encryption keys). Τέλος, οι συμμετρικοί αλγόριθμοι χρειάζονται πολύ λιγότερο χρόνο για την κρυπτογράφηση ενός μηνύματος εν συγκρίσει με τους ασύμμετρους, παρουσιάζοντας ένα σοβαρό μειονέκτημα. Στην περίπτωση υποκλοπής του κλειδιού ενός συμμετρικού αλγόριθμου, μπορεί να πραγματοποιηθεί ανεμπόδιστα η αποκρυπτογράφηση των μηνυμάτων από μη εξουσιοδοτημένα άτομα.

- Ασύμμετρη Κρυπτογραφία, στην οποία χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση. Συνεπάγεται ότι είναι διαφορετικό το δημόσιο (public) και το ιδιωτικό (private) κλειδί αντίστοιχα. Τα κλειδιά αυτά παράγονται έτσι ώστε το μήνυμα το οποίο έχει κρυπτογραφηθεί με το δημόσιο κλειδί να είναι δυνατό να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί και αντίστροφα. Επιπλέον, το ένα κλειδί δεν μπορεί να προκύψει από το άλλο με απλό τρόπο. Οι ασύμμετροι αλγόριθμοι είναι αρκετά ασφαλείς, αλλά πολύ περισσότερο αργοί συγκρίνοντας με τους συμμετρικούς.

**Η ψευδωνυμοποίηση,** κατά τον Κανονισμό, είναι η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τέτοιο τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον αυτές οι πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Ωστόσο, υπάρχει ένας όρος που συχνά συγχέεται με την ψευδωνυμοποίηση στο πεδίο της ασφάλειας και της προστασίας των προσωπικών δεδομένων , ο οποίος είναι η ανωνυμοποίηση. Ουσιαστικά πρόκειται για δύο διαφορετικές τεχνικές προστασίας που πρέπει να διαχωρίζονται μεταξύ τους, δεδομένου ότι τα «ανωνυμοποιημένα δεδομένα» και τα «ψευδωνυποιημένα δεδομένα» αντιμετωπίζονται ως δύο εντελώς διαφορετικές κατηγορίες.

Πέραν της κρυπτογράφησης και της ψευδωνυμοποίησης δεν θα πρέπει να εξαιρεθεί από τα μέτρα προστασίας και η εφαρμογή της τεχνικής ανωνυμοποίησης στα προσωπικά δεδομένα που διατηρεί ένας υπεύθυνος επεξεργασίας.

Ως **ανωνυμοποίηση** ορίζεται η διαδικασία διαγραφής των αναγνωριστικών προσωπικού χαρακτήρα σε εγγραφές δεδομένων, έτσι ώστε να μην γίνεται η συσχέτιση των ανωνυμοποιημένων δεδομένων με το υποκείμενο των δεδομένων. Επομένως, πρόκειται για μία μέθοδο τροποποίησης των προσωπικών δεδομένων

που ακολουθείται, με σκοπό να μην είναι δυνατή η σύνδεση αυτών με κάποιο φυσικό πρόσωπο. Τα δεδομένα έπειτα από την διαδικασία αυτή καθίστανται ανώνυμα, δηλαδή δε σχετίζονται με κάποιο άτομο.

Η ανωνυμοποίηση μπορεί να επιτευχθεί μέσω ενός αριθμού τεχνικών, οι οποίες εμπίπτουν σε δύο κατηγορίες:

- Ψευδοτυχαία μεταβολή της ακρίβειας των δεδομένων, προκειμένου να εξαλειφθεί η ισχυρή σχέση μεταξύ των προσωπικών δεδομένων και του υποκειμένου. Εάν τα δεδομένα γίνουν επαρκώς αβέβαια, δε δύναται να αναφέρεται σε ένα συγκεκριμένο άτομο
- Γενίκευση των χαρακτηριστικών των υποκειμένων των δεδομένων, μέσω της τροποποίησης της αντίστοιχης κλίμακας ή της σειράς των δεδομένων

Η ανωνυμοποίηση μπορεί να θεωρηθεί από τον υπεύθυνο επεξεργασίας, ως μια στρατηγική επιλογή για την «αποδέσμευσή» του από τις διατάξεις του Γενικού Κανονισμού Προστασίας Δεδομένων, αλλά και από το αντίστοιχο νομοθετικό καθεστώς που προδιαγράφεται. Τα πλεονεκτήματα από μια τέτοια επιλογή μπορεί να είναι πολλαπλά, παρέχοντας κίνητρο για τους υπεύθυνους επεξεργασίας προσωπικών δεδομένων να υιοθετούν και να εφαρμόζουν τεχνικές και μεθόδους που ανωνυμοποιούν τα δεδομένα που έχουν στη διάθεσή τους. Εντούτοις, η ανωνυμοποίηση, δεδομένου ότι είναι μια μη αναστρέψιμη διαδικασία που καταργεί την ικανότητα αναγνώρισης των υποκειμένων των δεδομένων, ενδέχεται να έχει ως αποτέλεσμα την υποβάθμιση της χρησιμότητας και χρηστικότητας των ανωνυμοποιημένων δεδομένων και σε πολλές περιπτώσεις να τα καταστήσει μη εκμεταλλεύσιμα για σκοπούς επεξεργασίας. Κατά συνέπεια, η ανωνυμοποίηση δεν μπορεί να θεωρηθεί ότι αποτελεί μια τυπική επιλογή για όλους τους υπεύθυνους και να εφαρμοστεί σε όλες τις περιπτώσεις επεξεργασίας.

**Η χρήση ψευδωνύμων** ερμηνεύεται ως η επεξεργασία προσωπικών δεδομένων, κατά τρόπο ώστε τα προσωπικά δεδομένα να μην μπορούν πλέον να αποδίδονται σε συγκεκριμένα δεδομένα χωρίς τη χρήση πρόσθετων πληροφοριών. Η χρήση ψευδωνύμων μπορεί να επιτευχθεί με την αντικατάσταση του ονόματος ή άλλων χαρακτηριστικών με ορισμένους δείκτες. Η τήρηση των πρόσθετων πληροφοριών που επιτρέπουν την ταυτοποίηση πρέπει να γίνεται ξεχωριστά. Ταυτόχρονα, η τεχνική αυτή θα μπορούσε να ισχυροποιηθεί μέσω της κωδικοποίησης των πληροφοριών, περιορίζοντας τον αριθμό των ατόμων που έχουν πρόσβαση στα αντίστοιχα κλειδιά. Να επισημανθεί πως η χρήση ψευδωνύμων εμπίπτει στα πλαίσια εφαρμογής του Κανονισμού, σε αντίθεση με την ανωνυμοποίηση, καθώς ο κίνδυνος

προσδιορισμού του ατόμου είναι υψηλότερος με ψευδώνυμα δεδομένων παρά με ανώνυμα δεδομένα.

Από τους ορισμούς της ψευδωνυμοποίησης και της ανωνυμοποίησης προκύπτει ότι η χρήση της ανωνυμοποίησης έχει ως αποτέλεσμα την αδυναμία προσδιορισμού του υποκειμένου των δεδομένων, ενώ η ψευδωνυμοποίηση αντικαθιστά την ταυτότητα του υποκειμένου των δεδομένων με τέτοιο τρόπο, ώστε να απαιτούνται πρόσθετες πληροφορίες για την εκ νέου αναγνώριση του υποκειμένου των δεδομένων.

**Οι ψηφιακές υπογραφές** αποτελούν τη μέθοδο προστασίας, η οποία παρέχεται ως όφελος από την κρυπτογραφία δημόσιου κλειδιού. Οι ψηφιακές υπογραφές επιτρέπουν στον παραλήπτη να ελέγξει την αυθεντικότητα των πληροφοριών που λαμβάνει. Επομένως, προσφέρουν πιστοποίηση και ακεραιότητα των δεδομένων, καθώς και μη αποκήρυξη, με την έννοια ότι ο αποστολέας δεν μπορεί να ισχυριστεί ότι δεν έχουν σταλεί οι πληροφορίες. Μία ψηφιακή υπογραφή έχει ίση αξία με μια χειρόγραφη υπογραφή. Ενώ, όμως, η χειρόγραφη υπογραφή είναι εύκολο να πλαστογραφηθεί, οι ψηφιακές υπογραφές είναι ανώτερες και πιο ισχυρές επειδή μοιάζει αδύνατη η πλαστογράφησή τους. Για το λόγο αυτό, όλο και περισσότεροι χρήστες χρησιμοποιούν τις ψηφιακές υπογραφές, με σκοπό να προφυλάξουν τα προσωπικά δεδομένα τους.

**Τα Κρυπτογραφικά πρωτόκολλα** είναι εκείνα τα οποία υλοποιούνται με τη χρήση κρυπτογραφικών μηχανισμών. Ο βασικός σκοπός της κρυπτογραφίας είναι η προστασία των δεδομένων από τυχαίες ή εσκεμμένες τροποποιήσεις, προσπελάσεις και πλαστογραφήσεις. Βασικά παραδείγματα συστημάτων τα οποία εξασφαλίζουν τη μυστικότητα και την αυθεντικότητα των πληροφοριών αποτελούν τα κρυπτογραφικά συστήματα και τα συστήματα ψηφιακής υπογραφής. Εντούτοις, συνιστά απαραίτητη προϋπόθεση και στα δύο συστήματα η διανομή ενός μυστικού κλειδιού, κατά ασφαλή τρόπο, και όχι σε ένα περιβάλλον στο οποίο υπάρχει έλλειψη εμπιστοσύνης, με την έννοια ότι τα επιμέρους τμήματα δεν ακολουθούν το πρωτόκολλο.

Υπάρχουν τρία είδη κρυπτογραφικών πρωτοκόλλων και είναι τα εξής:

- Τα πρωτόκολλα ανταλλαγής κλειδιών που διανέμουν κατά ασφαλή τρόπο μυστικά κλειδιά στους χρήστες ενός πληροφοριακού συστήματος.
- Τα συστήματα διαμοίρασης ενός μυστικού κλειδιού που καθιστούν εφικτή τη διανομή τμημάτων του κλειδιού με τρόπο ώστε μόνο εξουσιοδοτημένες ομάδες χρηστών μπορούν να ανακατασκευάσουν το κλειδί από τα επιμέρους τμήματά του.

- Τα συστήματα ελάχιστης γνώσης που επιτρέπουν σε ένα χρήστη να αποδείξει ότι γνωρίζει ένα μυστικό κλειδί χωρίς να το αποκαλύψει.

Ο χρήστης ενός συστήματος αντιλαμβάνεται την ασφάλεια με τη μορφή των κρυπτογραφικών υπηρεσιών, εξασφαλίζοντας εμπιστευτικότητα, αυθεντικότητα και ακεραιότητα. Επιπλέον, οι κρυπτογραφικές υπηρεσίες προσφέρονται με την υλοποίηση των κρυπτογραφικών πράξεων, οι οποίες πρέπει να συνδυάζονται και να εκτελούνται με συγκεκριμένο τρόπο, προκειμένου να προσφέρουν τις επιθυμητές κρυπτογραφικές υπηρεσίες. Η περιγραφή με την οποία θα δράσουν οι κρυπτογραφικές πράξεις βρίσκεται στο κρυπτογραφικό πρωτόκολλο, το οποίο χαρακτηρίζεται από την αυστηρή περιγραφή του τρόπου λειτουργίας και δράσης των κρυπτογραφικών πράξεων.

Το κρυπτογραφικό πρωτόκολλο έχει τα ακόλουθα χαρακτηριστικά:

- Είναι καθορισμένο εκ των προτέρων, δηλαδή ο σχεδιασμός ενός πρωτοκόλλου έχει ολοκληρωθεί προτού το πρωτόκολλο χρησιμοποιηθεί
- Αμοιβαία συμφωνία, με την έννοια της συμφωνίας όλων των μελών για την εκτέλεση των βημάτων του πρωτοκόλλου με τη σειρά που υποδεικνύει το πρωτόκολλο.
- Σαφήνεια, δηλαδή η εκτέλεση όλων των βημάτων του πρωτοκόλλου να είναι σαφής, έτσι ώστε κανένα από τα μέλη να μην παρερμηνεύει τα βήματα που του αναλογούν.
- Πληρότητα, με την έννοια να υπάρχουν προκαθορισμένες ενέργειες για οποιαδήποτε κατάσταση που μπορεί να βρεθεί οποιοδήποτε μέλος.

**Η Κρυπτανάλυση** (cryptanalysis) είναι η μελέτη που γίνεται για την επινόηση μεθόδων οι οποίες εξασφαλίζουν την κατανόηση του νοήματος της κρυπτογραφημένης πληροφορίας, έχοντας ως άγνωστες ποσότητες τον κρυφό μετασχηματισμό, δηλαδή το κλειδί. Με βάση το κλειδί αυτός πραγματοποίησε και το κρυπτογραφημένο μήνυμα. Βασικός στόχος του κρυπταναλυτή - αναλυτή κρυπτοσυστημάτων είναι να βρει το κλειδί, το μήνυμα ή ένα ισοδύναμο αλγόριθμο που θα τον βοηθά να αναγνώσει το κρυφό μήνυμα. Στην περίπτωση που βρεθεί μία μέθοδος που μπορεί να βρει το μήνυμα ή το κλειδί με πολυπλοκότητα μικρότερη από την πολυπλοκότητα της επίθεσης ωμής βίας (brute force attack), σημαίνει ότι ο κρυπταλγόριθμος έχει σπάσει. Η πρώτη νύξη σχετικά με την κρυπτανάλυση έγινε από ένα Άραβα μαθηματικό τον 8ο αιώνα με την εργασία «Εγχειρίδιο των γραμματέων».

Η κρυπτανάλυση είναι ο ένας από τους δύο κλάδους της κρυπτολογίας (ο άλλος είναι η κρυπτογραφία), η οποία ασχολείται με τη μελέτη της ασφαλούς επικοινωνίας. Σήμερα η κρυπτολογία θεωρείται ένα διεπιστημονικό γνωστικό πεδίο, το οποίο μπορεί να μελετηθεί ως όψη των εφαρμοσμένων μαθηματικών, της θεωρητικής πληροφορικής ή της επιστήμης ηλεκτρονικού μηχανικού.

Κύριος σκοπός της κρυπτογραφίας είναι να εξασφαλίζει τη μυστικότητα του κειμένου και του κλειδιού κρυπτογράφησης. Αντίθετα, η κρυπτανάλυση έχει στόχο την εύρεση του αρχικού μηνύματος χωρίς τη γνώση του κλειδιού. Ο κρυπταναλυτής θέλει να βρει το αρχικό μήνυμα και το κλειδί κρυπτογράφησης. Επιπρόσθετα, ο κρυπταναλυτής προσπαθεί να βρει τις αδυναμίες του συστήματος, οι οποίες μπορούν να συμβάλλουν στο σκοπό του και θα του επιτρέψουν να προσποιηθεί έναν χρήστη ή να τροποποιήσει ένα μήνυμα ή ακόμα να πλαστογραφήσει μηνύματα.

Εφαρμογές της κρυπτογραφίας:

- Ασφαλής προσπέλαση: Στο πρόβλημα της ασφαλούς σύνδεσης εμπίπτουν οι περιπτώσεις των τραπεζικών μηχανών ATM, των συσκευών POS, της καλωδιακής τηλεόρασης και των καρτών τηλεφώνων. Σε αυτές τις περιπτώσεις το πλήθος των ανταλλασσόμενων πληροφοριών είναι μικρό η ζημιά που θα προκληθεί όμως είναι μεγάλη. Μια ασφαλής προσπέλαση μπορεί να επιτευχθεί με τη χρήση κρυπτογραφικών τεχνικών.
- Ψηφιακά διαβατήρια: Τα διαβατήρια είναι ένας τρόπος αναγνώρισης της ταυτότητας. Με τη βοήθεια των ηλεκτρονικών υπογραφών είναι δυνατό να δημιουργηθούν ασφαλή ψηφιακά διαβατήρια. Κάθε κράτος εκδίδει ένα ψηφιακό διαβατήριο το οποίο περιλαμβάνει μια υπογραφή της ταυτότητας του χρήστη. Έτσι όταν ο κάτοχος του διαβατηρίου θέλει να ταυτοποιηθεί το κάνει χρησιμοποιώντας ένα πρωτόκολλο μηδενικής γνώσης ότι γνωρίζει την υπογραφή χωρίς να την επιδείξει.
- Ηλεκτρονική μεταβίβαση δεδομένων: Οι πληροφορίες μορφοποιούνται βάση προκαθορισμένων προτύπων για να αναγνωρίζονται από τα υπολογιστικά συστήματα των εμπλεκόμενων μερών. Η όλη διαδικασία πραγματοποιείται σε ταχύτατους χρόνους, πολλές φορές με τη χρήση ψηφιακών υπογραφών, εξασφαλίζοντας γνησιότητα και εχεμύθεια των ανταλλασσόμενων πληροφοριών.

13 Πρακτικές συμβουλές από τη Δίωξη Ηλεκτρονικού Εγκλήματος:


Πηγή: Εφημερίδα ΤΑ ΝΕΑ, Φύλλο 20-21/4/2019, «Χρυσές δουλειές με τα προσωπικά δεδομένα μας»

## 5.2 ΕΠΙΒΟΛΗ ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ

Σε σύγκριση με την Οδηγία 95/46/ΕΚ για την προστασία των δεδομένων, ο Γενικός Κανονισμός Προστασίας Δεδομένων - GDPR εισάγει εκτεταμένες αλλαγές, όσον αφορά στην αρμοδιότητα και τη συνεργασία των εθνικών εποπτικών αρχών. Κάθε κράτος μέλος της Ευρωπαϊκής Ένωσης διαθέτει δική του Εποπτική Αρχή, η οποία ως ανεξάρτητη δημόσια αρχή είναι υπεύθυνη για την παρακολούθηση της εφαρμογής του Κανονισμού. Στην αποστολή τους περιλαμβάνεται η προστασία των θεμελιωδών δικαιωμάτων και οι ελευθεριών των φυσικών προσώπων από την επεξεργασία των προσωπικών τους δεδομένων και η διευκόλυνση της νόμιμης ροής

προσωπικών δεδομένων εντός της Ένωσης. Συχνά παρατηρείται ότι η επεξεργασία των προσωπικών δεδομένων πραγματοποιείται σε παραπάνω από μία χώρες ή επηρεάζει άτομα τα οποία βρίσκονται σε διαφορετικές χώρες. Συνεπώς, παραπάνω από μια εποπτικές αρχές ενδέχεται να ασχοληθούν με μια μεμονωμένη περίπτωση.

Κατά τον Γενικό Κανονισμό Προστασίας Δεδομένων - GDPR, μία Εποπτική αρχή ενεργεί ως μοναδικό σημείο επαφής για τον Υπεύθυνο διαχείρισης ή Υπεύθυνο επεξεργασίας, των οποίων οι δραστηριότητες επεξεργασίας επηρεάζουν πολλά κράτη μέλη της Ευρωπαϊκής Ένωσης. Αποτελεί τον οργανισμό που αλληλοεπιδρά με το υπεύθυνο διαχείρισης ή υπεύθυνο επεξεργασίας εξ ονόματος όλων των εμπλεκομένων εθνικών εποπτικών αρχών. Η επιλογή αυτής της ενιαίας Εποπτικής Αρχής συνοδεύεται από μηχανισμούς συνεργασίας και συνέπειας, απλοποιώντας περαιτέρω την κατάσταση για τις υπόλοιπες εθνικές αρχές. Επίσης, αποτελεί μεγάλο πλεονέκτημα για τις επιχειρήσεις, οι οποίες γενικά αλληλοεπιδρούν μόνο με μια ενιαία Εποπτική Αρχή, καθώς δε χρειάζεται η αλληλεπίδραση με διαφορετικές αρχές.

Ωστόσο, σε ορισμένες περιπτώσεις, η τοπική αρμοδιότητα των εθνικών εποπτικών αρχών παραμένει σε ισχύ. Ακόμη και όταν έχει ορισθεί Εποπτική αρχή, οι συνεργαζόμενες εθνικές εποπτικές αρχές ενδέχεται να μην είναι σε θέση να καταλήξουν σε συμφωνία ως προς την τελική τους απόφαση για μια συγκεκριμένη περίσταση. Σε μια τέτοια περίπτωση, τα άτομα να αντιμετωπίζουν νομικές αβεβαιότητες έως ότου ληφθεί τελική απόφαση από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων.

Από την πλευρά των επιχειρήσεων είναι ιδιαίτερα σημαντικό, μέσω των Υπευθύνων Διαχείρισης ή Επεξεργασίας, να προσδιορίσουν το συντομότερο δυνατό την αρμόδια Εποπτική αρχή τους, με σκοπό την εμπρόθεσμη εκπλήρωση διαφόρων οργανωτικών απαιτήσεων στο πλαίσιο του Γενικού Κανονισμού Προστασίας Δεδομένων. Στην περίπτωση των πολυεθνικών επιχειρήσεων, με βάσεις σε διαφορετικές χώρες, κρίνεται αναγκαίο να επιλεχθεί η κύρια έδρα τους, προτού οριστεί μία Εποπτική Αρχή. Αυτό, ίσως παρουσιάζει κάποιες δυσκολίες όσον αφορά στο μη αυστηρό ορισμό της έννοιας “έδρα” στη νομοθεσία της Ευρωπαϊκής Ένωσης. Η ύπαρξη αυτής της έδρας, σε μια συγκεκριμένη χώρα, προσδιορίζεται με βάση συγκεκριμένα κριτήρια και συνθήκες.

Σύμφωνα με το άρθρο 4, κύρια βάση μιας εταιρίας μπορεί να αποτελέσει:

- Η τοποθεσία της κεντρικής διοίκησής της στην Ευρωπαϊκή Ένωση, εκτός εάν οι αποφάσεις σχετικά με τους σκοπούς και τα μέσα επεξεργασίας

προσωπικών δεδομένων για τον Υπεύθυνο Διαχείρισης λαμβάνονται σε διαφορετικό κράτος μέλος, και εάν η τελευταία αυτή τοποθεσία έχει την εξουσία να λάβει τέτοιες αποφάσεις, αυτή θεωρείται ως η κύρια εγκατάσταση.

- Η τοποθεσία της κεντρικής διαχείρισης ενός Υπευθύνου επεξεργασίας και σε περίπτωση που ο Υπεύθυνος Επεξεργασίας, δεν έχει ορίσει τοποθεσία, ορίζεται εκείνη όπου πραγματοποιούνται οι κύριες δραστηριότητες επεξεργασίας δεδομένων που υπάγονται στον Κανονισμό.

Επιπλέον, έχουν υλοποιηθεί διάφοροι μηχανισμοί που ορίζουν την επικοινωνία των εποπτικών αρχών με το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. Το Συμβούλιο αυτό αποτελεί ένα νέο ανεξάρτητο φορέα ελέγχου για την νομική προστασία δεδομένων προσωπικού χαρακτήρα σε επίπεδο Ευρωπαϊκής Ένωσης. Στα άρθρα 68-76 του Κανονισμού, ορίζονται οι κανόνες σχετικά με τα καθήκοντα και την οργάνωση του Συμβουλίου. Σύμφωνα με αυτά, το Συμβούλιο αποτελείται από τους επικεφαλείς της Εποπτικής Αρχής κάθε κράτους μέλους της Ευρωπαϊκής Ένωσης και τον Προϊστάμενο Προστασίας Ευρωπαϊκών Δεδομένων. Ο κύριος ρόλος του οργάνου είναι η λήψη τελικών αποφάσεων, στο πλαίσιο των μηχανισμών συνεργασίας και συνέπειας του Κανονισμού. Στόχο των μηχανισμών συνεργασίας συνιστά η αποτελεσματική ανταλλαγή πληροφοριών και την αμοιβαία συνδρομή από τις εθνικές εποπτικές αρχές προκειμένου να επιτευχθεί συναίνεση ως προς την απόφαση σε μια συγκεκριμένη περίπτωση. Αντίστοιχα, ο μηχανισμός συνέπειας ενεργοποιείται στη μοναδική περίπτωση που η συνεργασία των εποπτικών αρχών δεν μπορεί να οδηγήσει σε συναίνεση. Τέλος, το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων είναι το τελικό σημείο έκδοσης γνωμοδοτήσεων και δεσμευτικών αποφάσεων για την επίλυση διαφωνιών μεταξύ των ενδιαφερόμενων εποπτικών αρχών.

Με σκοπό την ορθή εκπλήρωση των νέων καθηκόντων των εποπτικών αρχών, περιγράφεται στον Κανονισμό λεπτομερώς η εξουσία ελέγχου που τους παραχωρείται. Καθώς ο Κανονισμός εφαρμόζεται σε όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης, η εξουσία αυτή είναι ευρέως συνεπής σε ολόκληρη την Ένωση. Η εν λόγω συνέπεια συμβάλει σ την επεξεργασία προσωπικών δεδομένων, λόγω του ότι οι επιχειρήσεις γνωρίζουν εκ των προτέρων το εύρος των ελέγχων και την δικαιοδοσία των Αρχών. Ωστόσο, στο άρθρο 58, περιέχεται ρήτρα που επιτρέπει σε κάθε κράτος μέλος της Ένωσης να εισαγάγει πρόσθετες εξουσίες στην εθνική του νομοθεσία.

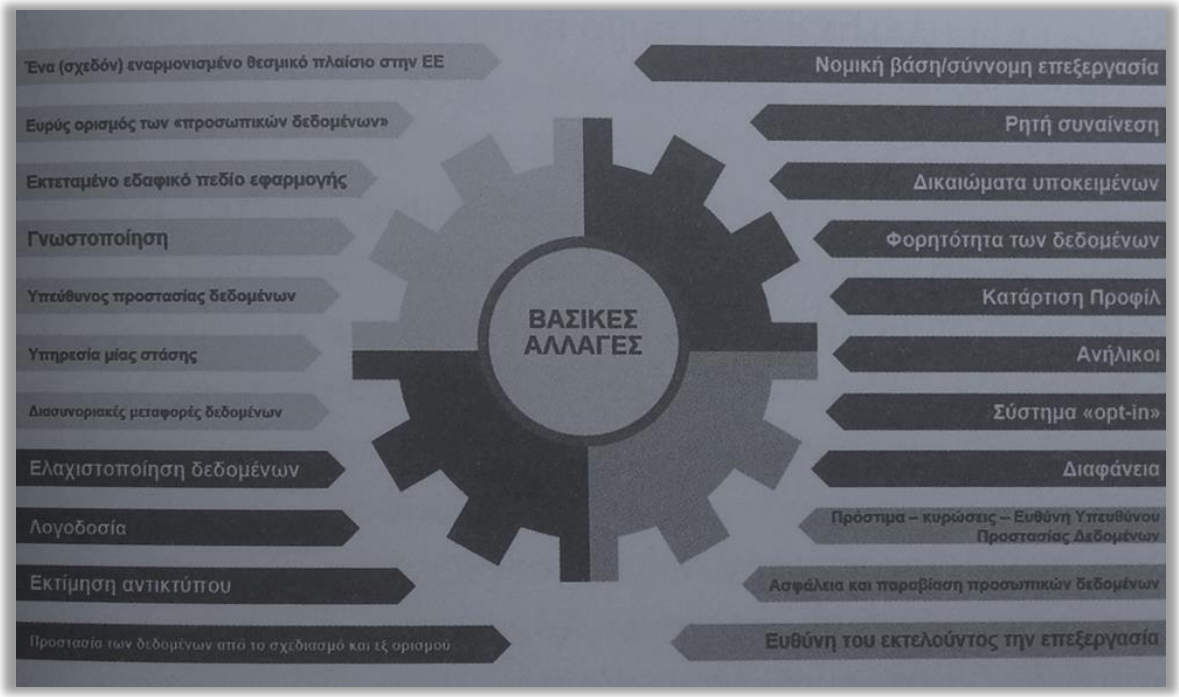
Σύμφωνα με το άρθρο 58 του Κανονισμού, η εξουσία ελέγχου που έχει κάθε εθνική Εποπτική αρχή περιλαμβάνει:

- Το δικαίωμα να απαιτήσει από τον Υπεύθυνο διαχείρισης, τον Υπεύθυνο επεξεργασίας, ή τον αντίστοιχο εκπρόσωπο στην Ευρωπαϊκή Ένωση, την παροχή των πληροφοριών που απαιτούνται για την εκτέλεση των καθηκόντων της Εποπτικής Αρχής. Αυτό συμβαδίζει με το άρθρο 31 και την γενικότερη απαίτηση προς τις επιχειρήσεις για συνεργασία.
- Το δικαίωμα της διεξαγωγής ερευνών με τη μορφή ελέγχων για την προστασία των προσωπικών δεδομένων. Οι Εποπτικές αρχές θα καθορίσουν το πεδίο εφαρμογής και τον λόγο για τον έλεγχο, δεδομένου ότι και τα δύο δεν προβλέπονται από το νόμο. Τέτοιοι έλεγχοι δύναται να διεξαχθεί στις εγκαταστάσεις του υπεύθυνου Διαχείρισης/ επεξεργασίας, μέσω της πρόσβασης στα συστήματα πληροφορικής της αντίστοιχης επιχείρησης ή μέσω συνολικών αιτήσεων για πληροφορίες.
- Το δικαίωμα να πραγματοποιήσει επιθεώρηση σχετικά με μια συγκεκριμένη Πιστοποίηση.
- Την υποχρέωση να κοινοποιεί στον Υπεύθυνο Διαχείρισης/ επεξεργασίας μια εικαζόμενη παράβαση του GDPR. Εάν κατά τον έλεγχο από τις εποπτικές αρχές, βρεθεί ένα συγκεκριμένου περιστατικό που έχει χαρακτηριστεί ως πιθανή παράβαση του GDPR, η επιχείρηση πρέπει να ειδοποιηθεί το συντομότερο δυνατόν.
- Την πρόσβαση σε όλα τα προσωπικά δεδομένα και σε όλες τις απαραίτητες πληροφορίες για την εκτέλεση των καθηκόντων της.
- Την πρόσβαση σε οποιαδήποτε εγκατάσταση του υπεύθυνο Διαχείρισης / επεξεργασίας, συμπεριλαμβανομένων όλων των εξοπλισμών και μέσων επεξεργασίας δεδομένων, σε συμφωνία με το δίκαιο των κρατών μελών. Η διάταξη αυτή παρέχει στις Εποπτικές Αρχές την εξουσία να διεξάγουν αιφνιδιαστικές επιτόπιες επιθεωρήσεις. Καθώς όμως, τα μέτρα της έρευνας πρέπει να είναι κατάλληλα, αναγκαία και αναλογικά των πιθανών παραβιάσεων, σε ορισμένες περιπτώσεις, μια ειδοποίηση θα πρέπει να υπάρξει πριν από την επιθεώρηση.

Ο Κανονισμός περιλαμβάνει το δικαίωμα αποζημίωσης των ατόμων για οποιαδήποτε ζημιά, υλική ή μη, την οποία υπέστησαν ως παράβασή του. Το δικαίωμα αυτό δεν περιορίζεται σε ορισμένες φάσεις επεξεργασίας δεδομένων ή ορισμένες διαδικασίες. Επιπλέον, η έννοια της παραβίασης του Γενικού Κανονισμού Προστασίας

Δεδομένων - GDPR, πρέπει να ερμηνεύεται με ένα ευρύ τρόπο και, συνεπώς, περιλαμβάνει την επεξεργασία που παραβιάζει τον Κανονισμό αλλά και την νομοθεσία των κρατών μελών. Υπό αυτό το πρίσμα, οι εταιρίες πρέπει να είναι σε εγρήγορση όσον αφορά την ύπαρξη εθνικών ιδιαιτεροτήτων στην επεξεργασία προσωπικών δεδομένων.

Οι κύριες αλλαγές του Κανονισμού:




Πηγή: Βιβλίο Ειρηνικός Πλατής. «Προσωπικά Δεδομένα - Προστασία GDPR»

## 5.3 ΣΥΣΤΗΜΑ ΚΥΡΩΣΕΩΝ

Η πρόβλεψη υψηλών προστίμων για τους υπεύθυνους επεξεργασίας, οι οποίοι παραβιάζουν τις διατάξεις του Κανονισμού αναζωογόνησε το ενδιαφέρον για την προστασία προσωπικών δεδομένων. Το σύστημα κυρώσεων που περιγράφεται, αποτελεί δομικό στοιχείο του Κανονισμού της πολιτικής συμμόρφωσης, που προβλέπει την αποτελεσματικότητα της εφαρμογής. Το ιδιαίτερα αυστηρό κυρωτικό πλαίσιο του Κανονισμού είναι ίσως ο κυριότερος λόγος για τη δημοσιότητα που έχει λάβει η εφαρμογή του, αλλά και η βασική αιτία για την τόσο γρήγορη διάχυση της πληροφορίας σχετικά με τις νέες υποχρεώσεις των υπεύθυνων επεξεργασίας και την ένταση με την οποία αυξήθηκαν οι δράσεις ενημέρωσης των υποκειμένων των δεδομένων. Ωστόσο, παρόλη την αναστάτωση που έχει επικρατήσει στην αγορά, πρέπει να σημειωθεί ότι σκοπός πρόληψης και μέριμνας του Κανονισμού, για την

προστασία των δεδομένων από την πλευρά των επιχειρήσεων, σε μεγάλο βαθμό έχει επιτευχθεί.

Σύμφωνα με την Οδηγία, οι αρμόδιες εποπτικές αρχές περιορίζονταν νομοθετικά ως προς το ύψος των επιβαλλόμενων προστίμων. Ως αποτέλεσμα η προληπτική διάσταση του θεσμικού πλαισίου ήταν άκρως περιορισμένη. Πλέον ο Κανονισμός προβλέπει ενιαίες, εξαιρετικά αυστηρές διοικητικές κυρώσεις. Η μόνη διακριτική ευχέρεια που παρέχεται στους εθνικούς νομοθέτες αφορά στη δυνατότητα που τους δίνει για τη θέσπιση ποινικών κυρώσεων. Στο άρθρο 83, προβλέπεται πρόστιμο για διοικητικές παραλείψεις έως και 10.000.000 €, ενώ για υπαίτιες παραβάσεις προβλέπεται η δυνατότητα επιβολής προστίμου έως 20.000.000 €. Στις περιπτώσεις επιχειρήσεων τα πρόστιμα μπορεί να είναι ακόμα υψηλότερα.

Ο Κανονισμός αλλάζει το καθεστώς των κυρώσεων και εξοπλίζει τις εθνικές εποπτικές αρχές με την αρμοδιότητα επιβολής δυο κατηγοριών προστίμων:

- Το χαμηλό επίπεδο προστίμων ανέρχεται μέχρι και τα 10.000.000 € ή το 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, όποιο είναι μεγαλύτερο. Στο χαμηλό επίπεδο εντάσσονται οι παραβάσεις, όπως οι υποχρεώσεις του υπεύθυνου επεξεργασίας και του εκτελούντος την επεξεργασία, οι υποχρεώσεις του φορέα πιστοποίησης και οι υποχρεώσεις του φορέα παρακολούθησης.
- Το υψηλό επίπεδο προστίμων ανέρχεται μέχρι τα 20.000.000 € ή το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, όποιο είναι μεγαλύτερο. Στο υψηλό επίπεδο συγκαταλέγονται συγκεκριμένες παραβάσεις. Οι παραβάσεις που σύμφωνα με τον Ευρωπαίο νομοθέτη αποτελούν σημαντική βλάβη στα δικαιώματα των υποκειμένων, αφορούν τις βασικές αρχές για την επεξεργασία, περιλαμβανομένων των όρων που ισχύουν για την έγκριση, τα βασικά δικαιώματα των υποκειμένων, τη διαβίβαση δεδομένων σε αποδέκτη σε τρίτη χώρα ή σε διεθνή οργανισμό και οποιεσδήποτε επιπλέον υποχρεώσεις του Κανονισμού, σύμφωνα με το δίκαιο του κράτους μέλους. Στη συνέχεια, περιλαμβάνεται και η μη συμμόρφωση προς εντολή ή προς προσωρινό ή οριστικό περιορισμό της επεξεργασίας ή προς αναστολή της κυκλοφορίας δεδομένων που επιβάλλει η εποπτική αρχή ή μη παροχή πρόσβασης στα δεδομένα και η μη συμμόρφωση προς εντολή της εποπτικής αρχής.

Τα παραπάνω πρόστιμα δεν επιβάλλονται αυτόματα, αλλά ακολουθούνται ορισμένες βασικές πρακτικές ως προς την αναγκαιότητα και το ύψος αυτού. Το πρόστιμο πρέπει να ακολουθεί την αρχή της αναλογικότητας, να είναι αναγκαίο, επαρκές ως προς την προληπτική του επίδραση και αναλογικό με την διαπιστωμένη παράβαση του Κανονισμού.

Ο Υπεύθυνος Διαχείρισης μπορεί να θεωρηθεί άμεσα υπαίτιος για παραβιάσεις των υποχρεώσεών του βάσει του Γενικού Κανονισμού Προστασίας Δεδομένων. Φέρει την ευθύνη για την παράνομη επεξεργασία και, ως εκ τούτου, πρέπει να αποζημιώσει τυχόν ζημίες που προκύπτουν από αυτή ανεξάρτητα από το αν προκάλεσε άμεσα τη ζημία ή όχι. Η ευθύνη προκύπτει από τον προσδιορισμό των σκοπών και των μέσων επεξεργασίας, καθώς και την εξουσία του να δίνει εντολές στους Υπεύθυνους Επεξεργασίας ως προς την διεξαγωγή της επεξεργασίας. Λαμβάνοντας υπόψιν το γεγονός ότι ο Υπεύθυνος Επεξεργασίας ενεργεί για λογαριασμό του υπεύθυνου διαχείρισης, η ευθύνη του πρώτου περιορίζεται στις ζημίες που απορρέουν από τις παραβιάσεις των δικών του υποχρεώσεων στο πλαίσιο του Κανονισμού ή όπου αυτός ενήργησε εκτός ή σε αντίθεση με τις νόμιμες οδηγίες του Υπεύθυνου διαχείρισης. Συνεπώς, ο υπεύθυνος επεξεργασίας είναι προνομιούχος, καθώς είναι υπεύθυνος μόνο σε περιορισμένες περιπτώσεις.

Ο Νέος Κανονισμός ορίζει αναλυτικά τις γενικές υποχρεώσεις που φέρουν οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία των προσωπικών δεδομένων για λογαριασμό αυτών. Και οι δύο έχουν την υποχρέωση τήρησης κατάλληλων μέτρων ασφαλείας, ανάλογα με τον κίνδυνο τον οποίον ενέχουν οι πράξεις επεξεργασίας δεδομένων τις οποίες εκτελούν. Οι υπεύθυνοι επεξεργασίας, σε ορισμένες περιπτώσεις, οφείλουν να κοινοποιούν τα περιστατικά παραβίασης δεδομένων προσωπικού χαρακτήρα εντός 72 ωρών από την ανακάλυψη του περιστατικού παραβίασης και απώλειας προσωπικών δεδομένων στις αρμόδιες αρχές και στα υποκείμενα των δεδομένων, αν η φύση των δεδομένων που χάθηκαν το απαιτεί.

Επιπλέον, η Αρχή μπορεί ακόμη να ειδοποιήσει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα αυτήν, για εικαζόμενη παράβαση, να του απευθύνει προειδοποιήσεις, επιπλήξεις και εντολές για συμμόρφωση με συγκεκριμένο τρόπο ή εντός ορισμένης προθεσμίας ή να επιβάλει προσωρινό ή οριστικό περιορισμό, περιλαμβανομένης της απαγόρευσης επεξεργασίας.

Σχετικά με τις εταιρείες και τις δημόσιες αρχές που εκτελούν πράξεις επεξεργασίας δεδομένων που ενέχουν κινδύνους, θα πρέπει να έχουν ορίσει υπεύθυνο

προστασίας δεδομένων. Για τους υπεύθυνους επεξεργασίας ή τους εκτελούντες την επεξεργασία δεδομένων, οι οποίοι παραβιάζουν τους κανόνες για την προστασία των δεδομένων, προβλέπονται πολύ αυστηρές κυρώσεις. Όσον αφορά στους υπευθύνους επεξεργασίας δεδομένων ενδέχεται να επιβληθεί πρόστιμο που μπορεί να ανέλθει σε 20.000.000 € ή στο 4% του συνολικού ετήσιου κύκλου εργασιών τους.

Κατά κύριο λόγο οι εποπτικές αρχές πριν από την επιβολή ενός προστίμου θα πρέπει να λαμβάνουν υπόψιν τους:

- Τη φύση, τη σοβαρότητα και τη διάρκεια της παράβασης
- Τον εκ προθέσεως χαρακτήρα της παράβασης
- Τα μέτρα που ελήφθησαν για τον μετριασμό της ζημίας που υπέστη
- Βαθμός ευθύνης ή τυχόν σχετικές προηγούμενες παραβάσεις
- Τον τρόπο με τον οποίο έγινε γνωστή η παράβαση στον εποπτικό φορέα
- Συμμόρφωση με τα μέτρα που διατάχθηκαν κατά του Υπεύθυνου διαχείρισης επεξεργασίας
- Τήρηση ενός Κώδικα δεοντολογίας

Επιπρόσθετα, η επιβολή των προστίμων χρειάζεται να λειτουργεί με ομοιόμορφο τρόπο σε όλα τα κράτη μέλη. Μέσω του μηχανισμού συνεκτικότητας, που προβλέπει ο Κανονισμός στο άρθρο 63, οι εθνικές εποπτικές αρχές οφείλουν να συντονίζουν τη δράση τους για την αντιμετώπιση των παραβάσεων του Κανονισμού, καθώς και τον τρόπο που τελικά επιβάλλουν τα σχετικά πρόστιμα. Στο άρθρο 84, δίνεται στα κράτη μέλη η δυνατότητα θέσπισης ποινικών κυρώσεων, επιλογή για την οποία η νομοπαρασκευαστική επιτροπή δέχθηκε αρνητική κριτική κατά τη δημόσια διαβούλευση του ελληνικού Σχεδίου Νόμου. Στο άρθρο 70, εξάντλησε τη διακριτική της ευχέρεια προβλέποντας τη δυνατότητα επιβολής ποινών φυλάκισης ή και κάθειρξης, καθώς και χρηματικές ποινές που μπορεί να φτάσουν τις 300.000 €. Όπως γίνεται αντιληπτό, το γεγονός ότι καταλείπεται αρκετά μεγάλη διακριτική ευχέρεια κατά την εφαρμογή του κυρωτικού πλαισίου, οδηγεί στη δημιουργία προβληματισμού ως προς την ορθή εφαρμογή των κυρωτικών διατάξεων από τις αρμόδιες εθνικές αρχές.

Στην παρακάτω εικονα απεικονίζονται τα βασικά χαραλτηριστικά που διαθέτει και εφαρμόζει ο Γενικός Κανονισμός Προστασίας Δεδομένων – GDPR:


Πηγή: https://www.orangehrm.com/resources/news/gdpr-readiness/

## 5.4 ΠΡΑΚΤΙΚΗ ΕΦΑΡΜΟΓΗ

Διανύοντας την εποχή της πληροφορίας, είναι αδιαμφισβήτητο πως τα προσωπικά δεδομένα των ατόμων έχουν πολύ μεγάλη αξία. Επομένως, η παράνομη πώληση των δεδομένων τους φέρει τεράστια κέρδη σε συνάρτηση με το είδος, τη ζήτηση και το μέγεθος. Το αντίτιμο πώλησης των δεδομένων προσωπικού χαρακτήρα ποικίλλει ανάλογα με το είδος των δεδομένων. Η εκτίμηση του επικεφαλή της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Κωνσταντίνου Μενουδάκη, μέσω των υποθέσεων που έχουν αντιμετωπιστεί, υποστηρίζει ότι «η αγοραπωλησία των δεδομένων φαίνεται να είναι αρκετά επικερδής διαδικασία». Στη συνέχεια, παραθέτει το παράδειγμα μιας εταιρεία, η οποία παρότι είχε ειδοποιηθεί για χρηματική ποινή της τάξεως των 75.000 €, συνέχιζε και έκανε διαφημίσεις, βομβαρδίζοντας με mail τους πολίτες. Συνεχίζοντας με αυτόν τον τρόπο την παραβατική δραστηριότητάς της, η εταιρεία αποδεικνύει πόσο μικρή είναι η απειλή του προστίμου, σε ορισμένες περιπτώσεις, σε σύγκριση με το κέρδος από το πελατολόγιο που αποσπά.

Ωστόσο, κατά την εφαρμογή του Κανονισμού, σημειώθηκαν πολλά περιστατικά διαρροής και υποκλοπής πρωσικών δεδομένων από νόμιμες λίστες. Εντός του έτους 2018, η Δίωξη Ηλεκτρονικού Εγκλήματος προχώρησε σε δύο συλλήψεις Ελλήνων, διότι είχαν καταρτίσει ψηφιακές λίστες με 1,5 εκατομμύριο εγγραφές πολιτών, καθώς και πωλούσαν τα δεδομένα αυτά σε τρίτους, μην αποτελώντας όμως τη μοναδική περίπτωση. Επιπροσθέτως, σύμφωνα με πληροφορίες των «ΝΕΩΝ», τα

αποτελέσματα από έλεγχο που διεξάχθηκε σε 65 ελληνικές ιστοσελίδες (τράπεζες, ασφαλιστικές εταιρείες, e-shops) με μεγάλη επισκεψιμότητα, έδειξαν ότι δεν υπάρχει καμία ενημέρωση προς τους πολίτες ή γίνεται ελλιπώς και σε πολύ χαμηλό βαθμό, όσον αφορά στον λόγο της επεξεργασίας των δεδομένων τους, τη διαβίβαση των στοιχείων τους σε τρίτους, σε ποιους και γιατί.

Η εφαρμογή του νέου Κανονισμού για τα προσωπικά δεδομένα, από το Μάιο του 2018, δημιούργησε ένα αυστηρότερο πλαίσιο λειτουργίας για τις επιχειρήσεις, προβλέποντας βαρύτατα πρόστιμα για τις εταιρείες που δεν έχουν εναρμονιστεί με όσα προβλέπονται. Στο πλαίσιο του Γενικού Κανονισμού Προστασίας Δεδομένων - GDPR, είχαν επιβληθεί πρόστιμα στην Αυστρία (4.800 ευρώ για παράνομο σύστημα βιντεοεπιτήρησης) και στην Πορτογαλία (400.000 ευρώ για ζητήματα που αφορούν στην πρόσβαση σε δεδομένα). Εντός του 2018, επήλθε και το πρώτο πρόστιμο στη γερμανική αρχή, το οποίο αποτέλεσε το τρίτο πρόστιμο για το GDPR σε ολόκληρη την Ευρωπαϊκή Ένωση.

Επιβλήθηκε το πρόστιμο ύψους 20.000 € στη γερμανική εταιρεία που λειτουργούσε μέσω κοινωνικής δικτύωσης (Knuddels.de), για παραβίαση της υποχρέωσής της να διασφαλίζει την ασφάλεια της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, σύμφωνα με το άρθρο 32 του GDPR (ψευδωνυμοποίηση και κρυπτογράφηση δεδομένων προσωπικού χαρακτήρα). Η εταιρεία είχε προχωρήσει σε γνωστοποίηση παραβίασης δεδομένων προς την LfDI, μετά από επίθεση κακόβουλων χρηστών, καθώς κλάπηκαν και δημοσιεύθηκαν κωδικοί πρόσβασης και διευθύνσεις ηλεκτρονικού ταχυδρομείου περίπου 330.000 χρηστών. Αποδείχθηκε ότι η εταιρεία δεν κρυπτογραφούσε τους κωδικούς πρόσβασης των πελατών της, αλλά τους αποθήκευε ως απλό κείμενο, εκθέτοντας έτσι σε κίνδυνο τα προσωπικά τους δεδομένα.

Επιπλέον, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα έχει επιβάλλει πρόστιμα σε τρεις εταιρείες για παραβιάσεις που αφορούν τα προσωπικά δεδομένα.

- Στην «Cosmote – Κινητές Τηλεπικοινωνίες Α.Ε» επιβλήθηκε το πρόστιμο των 150.000 € για παραβιάσεις, αρχικά λόγω πλήθους καταγγελιών αναφορικά με ανεπιθύμητες τηλεφωνικές κλήσεις που πραγματοποιούνται με ανθρώπινη παρέμβαση και με σκοπό την προώθηση προϊόντων ή υπηρεσιών της εταιρείας. Επίσης διαπιστώθηκε ότι δεν τηρείται συστηματικά κάποια συγκεκριμένη διαδικασία για την ικανοποίηση της ειδικής αντίρρησης των καλούμενων συνδρομητών και γίνεται μη ορθή ενημέρωση των καλούμενων συνδρομητών και μη ύπαρξη ορθής διαδικασίας για την τήρηση

συγκαταθέσεων και στοιχείων παλαιών συνδρομητών, τα οποία χρησιμοποιούνται για την εκ νέου προσέλκυσή τους στον όμιλο ΟΤΕ.

- Στη VODAFONE - ΠΑΝΑΦΟΝ Ανώνυμη Ελληνική Εταιρεία Τηλεπικοινωνιών, η Αρχή επέβαλε πρόστιμο 150.000 € για παραβιάσεις. Στην Αρχή είχε υποβληθεί πλήθος καταγγελιών αναφορικά με ανεπιθύμητες τηλεφωνικές κλήσεις που πραγματοποιούνται με ανθρώπινη παρέμβαση και με σκοπό την προώθηση προϊόντων ή υπηρεσιών της εταιρείας. Επισημαίνεται ότι η Vodafone δεν ελέγχει αποτελεσματικά τους συνεργάτες της ως προς την τήρηση του αρχείου.
- Στη WIND, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα επέβαλε τον Οκτώβριο του 2018 πρόστιμο 150.000 €.Ειδικότερα, διαπιστώθηκε ότι πραγματοποιήθηκαν πολυάριθμες κλήσεις σε τηλεφωνικούς αριθμούς, για τις οποίες δεν υπήρχε ειδική συγκατάθεση, δεν τηρείται ορθή διαδικασία για την ικανοποίηση της ειδικής αντίρρησης των καλούμενων συνδρομητών και δεν περιλαμβάνεται ενημέρωση για την ταυτότητα του εκπροσώπου της εταιρείας για λογαριασμό της οποίας γίνεται η κλήση, αλλά ούτε ενημέρωση σχετικά με τη δυνατότητα άσκησης του δικαιώματος πρόσβασης.

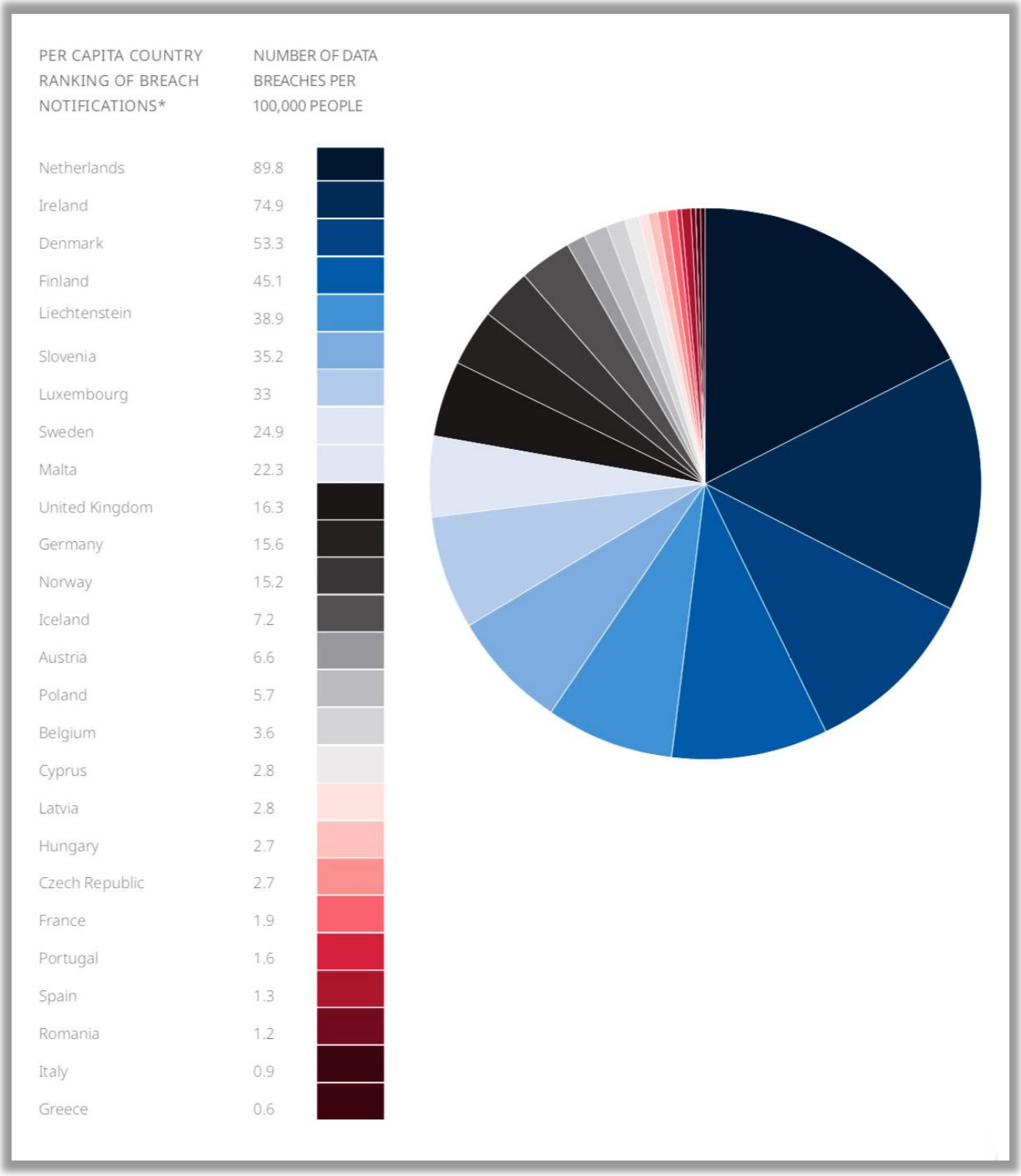

Πηγή: europa.eu/dataprotection – The European Data Protection Board

Μέχρι σήμερα έχουν αναφερθεί 91 πρόστιμα, τα οποία όμως δεν αφορούν όλες τις παραβιάσεις προσωπικών δεδομένων. Για παράδειγμα, το μαζικό πρόστιμο ύψους 50.000.000 €, που χορήγησε η γαλλική αρχή προστασίας δεδομένων στην Google, οφείλεται στην επιχείρηση που επεξεργάζεται τα προσωπικά δεδομένα για διαφημιστικούς σκοπούς χωρίς έγκυρη άδεια. Επίσης, οι γερμανικές αρχές προστασίας δεδομένων έχουν ήδη εκδώσει πάνω από 60 πρόστιμα, μικρά και μεγάλα, για διάφορες παραβιάσεις. Επιπλέον, είναι ενδιαφέρον ότι στη Μάλτα αναφέρθηκαν 17 πρόστιμα.

Ένας από τους βασικούς στόχους του Γενικού Κανονισμού για την Προστασία Δεδομένων - GDPR είναι να ενδυναμώσει τους πολίτες και να τους δώσει μεγαλύτερο έλεγχο σε έναν από τους πιο πολύτιμους πόρους στη σύγχρονη οικονομία, των δεδομένων τους. Ο μόνος τρόπος για να επιτευχθεί ο στόχος αυτός είναι να γνωρίζουν οι πολίτες τα δικαιώματά τους και τις συνέπειες των αποφάσεών τους.

Στους οκτώ μήνες μετά την έναρξη εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων - GDPR, το Μάιο του 2018, παρουσιάστηκαν τα θετικά αποτελέσματα των νέων κανόνων. Οι πολίτες έχουν συνειδητοποιήσει και κατανοήσει περισσότερο τη σημασία της προστασίας των δεδομένων και των δικαιωμάτων τους, ασκώντας πλέον τα δικαιώματα αυτά στην καθημερινή τους εργασία. Μέσα στους πρώτους πέντε μήνες από την εφαρμογή του Κανονισμού, σημειώθηκε ο αριθμός των 1.002 εταιρειών, οι οποίες δήλωσαν επισήμως ότι επεξεργάζονται δεδομένα προσωπικού χαρακτήρα.

Στο παρακάτω διάγραμμα παρουσιάζεται ο αριθμός παραβιάσεων των δεδομένων ανά 100.000 άτομα. Η Ευρωπαϊκή Επιτροπή (ΕΚ) δημοσίευσε πρόσφατα στατιστικά στοιχεία και πληροφορίες, σχετικά με τη συμμόρφωση και την εφαρμογή των κανόνων του GDPR. Αναφέρει ότι οι αρχές προστασίας δεδομένων σε ολόκληρη την Ευρώπη έλαβαν περισσότερες από 95.000 καταγγελίες από ιδιώτες ή οργανισμούς και περισσότερες από 41.000 ειδοποιήσεις παραβίασης δεδομένων από εταιρείες και ότι τα περισσότερα παράπονα σχετίζονται με τηλεμάρκετινγκ, διαφημιστικά μηνύματα ηλεκτρονικού ταχυδρομείου και παρακολούθηση βίντεο / CCTV. Οι αριθμοί αυτοί είναι συντηρητικοί, δεδομένου ότι βασίζονται στις εθελοντικές συνεισφορές των ρυθμιστικών αρχών προστασίας δεδομένων μόνο 21 από τα 28 κράτη μέλη της ΕΕ. Συν τοις άλλοις, εκτιμάται ότι υπήρξαν 59.430 αναφερόμενες παραβιάσεις δεδομένων κατά την ίδια περίοδο στην Ευρώπη και επισημαίνεται ότι αυτά τα στοιχεία κοινοποίησης παραβίασης αποτελούν «καλύτερες προσεγγίσεις», λόγω έλλειψης διαθέσιμων από το κοινό ή ελλιπών δεδομένων.




Πηγή: https://www.helpnetsecurity.com/2019/02/07/gdpr-numbers-january-2019/

# ΚΕΦΑΛΑΙΟ 6: ΣΥΜΠΕΡΑΣΜΑΤΑ

Είναι αλήθεια ότι η τεχνολογία και το δίκαιο βρίσκονται σε διαρκή σχέση έντασης. Καθώς η τεχνολογική εξέλιξη φαίνεται να προπορεύεται της χάραξης κανόνων, το δίκαιο καλείται να διαχειριστεί τα αρνητικά αποτελέσματα της τεχνολογίας. Το δίκαιο προστασίας δεδομένων έχει ως στόχο την προστασία των θεμελιωδών δικαιωμάτων της ιδιωτικής ζωής και του πληροφοριακού αυτοκαθορισμού. Στην αβεβαιότητα του σύγχρονου κόσμου, το δίκαιο έχει πρωταρχικό ρόλο και ευθύνη στη ρύθμιση της τεχνολογικής εξέλιξης προς την κατεύθυνση της κοινής ωφέλειας και του περιορισμού των τεχνολογικών κινδύνων.

Η οικονομική και κοινωνική ολοκλήρωση της Ευρωπαϊκής Ένωσης, με τη λειτουργία της εσωτερικής αγοράς έχει ως αποτέλεσμα τη σημαντική αύξηση των διασυνοριακών ροών δεδομένων προσωπικού χαρακτήρα. Ταυτόχρονα, η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι αναπόφευκτη και γίνεται με σκοπό να εξυπηρετεί τον άνθρωπο. Στα πλαίσια της ενιαίας ψηφιακής αγοράς, λειτουργεί ο Γενικός Κανονισμός Προστασίας Δεδομένων – GDPR, ο οποίος συμβάλει στην ενιαία ρύθμιση των όρων της επιχειρηματικής και οικονομικής δραστηριότητας, αίροντας εμπόδια και στρεβλώσεις για την απρόσκοπτη ροή πληροφορίας.

Δεδομένου ότι ο παρών Κανονισμός σέβεται όλα τα θεμελιώδη δικαιώματα των ατόμων και αποσκοπεί στο να ενισχύσει την ασφάλεια δικαίου, προβλέπει νέα δικαιώματα για τα υποκείμενα των δεδομένων προσωπικού χαρακτήρα στο σύγχρονο περιβάλλον των πολλαπλών προκλήσεων. Στην Ευρωπαϊκή Ένωση, η αποτελεσματική προστασία των προσωπικών δεδομένων, απαιτεί τον λεπτομερή καθορισμό των δικαιωμάτων των υποκειμένων, όπως και των υποχρεώσεων όσων εμπλέκονται στην επεξεργασία δεδομένων. Ο Γενικός Κανονισμός Προστασίας Δεδομένων – GDPR προβλέπει ένα σύνθετο πλέγμα δικαιωμάτων και υποχρεώσεων, του οποίου η παραβίαση επιφέρει σοβαρές κυρώσεις. Λαμβάνοντας υπόψιν ότι σε περίπτωση παραβίασης η επιβολή προστίμων είναι αυστηρότατη σε σύγκριση με το προγενέστερο καθεστώς, η Δημόσια Διοίκηση οφείλει να προετοιμαστεί συστηματικά και μεθοδικά, καθώς το οργανωτικό έλλειμμα συνιστά σημαντικό κίνδυνο για την παραβίαση των προσωπικών δεδομένων.

Συνοψίζοντας, ο Κανονισμός παρέχει το ίδιο επίπεδο προστασίας δεδομένων των Ευρωπαίων πολιτών, ανεξάρτητα από το αν βρίσκονται εντός ή εκτός των συνόρων της Ευρωπαϊκής Ένωσης. Επιπρόσθετα, αναφορικά με τις διασυνοριακές

διαβιβάσεις δεδομένων, προβλέπει ένα σύνολο διατάξεων το οποίο δεσμεύει υπευθύνους και εκτελούντες την επεξεργασία. Ο κύκλος υποχρεώσεων των υπεύθυνων και εκτελούντων την επεξεργασία περιλαμβάνει την καταγραφή των δεδομένων που βρίσκονται στην κατοχή τους, την περιγραφή του τρόπου επεξεργασίας των δεδομένων, τον έλεγχο περί αναγκαιότητας και περί αναλογικότητας της επιχειρούμενης επεξεργασίας, την επιμέτρηση του κινδύνου από την παραβίαση των προσωπικών δεδομένων, το σχεδιασμό των μέτρων αντιμετώπισης του κινδύνου και την καταγραφή και την επανεξέταση ολόκληρου του προηγούμενου κύκλου των ενεργειών.

Από την άλλη πλευρά, ρόλος του Υπεύθυνου Προστασίας Δεδομένων - DPO είναι καινούργιος, καθώς πρώτη φορά εμφανίζεται και λειτουργεί, μέσω της εφαρμογής του Κανονισμού, έχοντας ως προαπαιτούμενο αυξημένα προσόντα για τον διορισμό του. Απολαμβάνοντας καθεστώς ανεξαρτησίας, αναφέρεται άμεσα στο ανώτατο διοικητικό επίπεδο. Συνδράμει τον Υπεύθυνο Επεξεργασίας και τον Εκτελούντα, παρέχει συμβουλές αναφορικά με την εκτίμηση αντικτύπου και αποτελεί το σημείο επικοινωνίας με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Ωστόσο, η ισχύουσα νομοθεσία και οργανωτική κατάσταση, όσον αφορά στην εφαρμογή του Κανονισμού, χρήζει στενότερης συνεργασίας μεταξύ των δημόσιων φορέων και της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ιδιαίτερα κατά τη διαδικασία γνωστοποίησης περιστατικών παραβίασης προσωπικών δεδομένων.

Εν κατακλείδι, ο Γενικός Κανονισμός Προστασίας Δεδομένων διασφαλίζει ένα ιδιαίτερα υψηλό επίπεδο προστασίας δεδομένων, θέτοντας ένα παγκόσμιο πρότυπο το οποίο φαίνεται επαρκές ιδίως στον παρόντα χρόνο, ενώ δείχνει ικανό να καλύψει σημαντικά ακόμα και μελλοντικές προκλήσεις. Είναι όμως δεσπόζουσας σημασίας η συμμετοχή των πολιτών της Ευρωπαϊκής Ένωσης, στην ορθή εφαρμογή του Κανονισμού και στην αξιοποίησή του ως μέσο προστασίας της ιδιωτικότητας και της ελευθέριας τους.

# ΒΙΒΛΙΟΓΡΑΦΙΑ

## Ιστοσελίδες


1. https://stats.areppim.com/tech.htm
2. https://www.ssl2buy.com/wiki/gdpr-checklist-the-rigid-security-and-privacy-of-user-information
3. https://www.managementstudyhq.com/functions-of-management.html
4. https://www.cyberinsurancequote.gr/insurance/nomothesia/
5. http://www.privacy-regulation.eu/el/83.htm
6. https://dpoacademy.gr/_files/200000256-7e6f77f69f/SYNHGOROS%20LOUKAS.pdf
7. http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/4795/Nikitas.pdf?sequence=2&isAllowed=y
8. https://www.taxheaven.gr/laws/circular/view/id/27607
9. http://apothetirio.teiep.gr/xmlui/bitstream/handle/123456789/3278/ΠΤΥΧΙΑΚΗ%20ΕΡΓΑΣΙΑ%20ΞΗΡΟΥ%20ΚΩΝΣΤΑΝΤΙΝΑ.pdf?sequence=1
10. http://www.ekdd.gr/ekdda/images/seminaria/GDPR.pdf
11. https://eugdpr.org/the-regulation/
12. https://eugdpr.org/the-process/
13. https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en#background
14. https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en
15. https://www.commvault.com/solutions/by-topic/gdpr?utm_source=euGDPR&utm_medium=post&utm_campaign=GDPR&sfid=70140000000zBdL
16. https://www.barclaysimpson.com/blogs/gdpr-fines-the-story-so-far-83471310192
17. https://www.helpnetsecurity.com/2019/02/07/gdpr-numbers-january-2019/
18. https://www.niriis.gr/gdpr/prostima-450000-se-wind-vodafone-cosmote/
19. https://www.niriis.gr/gdpr/gdpr-%CF%84%CE%BF-%CF%80%CF%81%CF%8E%CF%84%CE%BF-%CF%80%CF%81%CF%8C%CF%83%CF%84%CE%B9%CE%BC%CE%BF-%CF%83%CF%84%CE%B7-%CE%B3%CE%B5%CF%81%CE%BC%CE%B1%CE%BD%CE%AF%CE%B1/
20. https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
21. https://el.wikipedia.org/wiki/Διαδίκτυο
22. https://el.wikipedia.org/wiki/Αρχή_Προστασίας_Δεδομένων_Προσωπικού_Χαρακτήρα
23. https://el.wikipedia.org/wiki/Προσωπικά_Δεδομένα#Υποκείμενο_των_δεδομένων
24. https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32016R0679
25. http://www.sev.org.gr/Uploads/Documents/51628/meleti_sev_GDPR_final.pdf
26. http://www.dpa.gr/portal/page?_pageid=33,19005&_dad=portal&_schema=PORTAL
27. https://www.statista.com/chartoftheday/

28. https://legal.heal-link.gr/index.php/sensitive-personal-data
29. https://stats.areppim.com/
30. https://en.wikipedia.org/wiki/Trojan_horse_(computing)
31. https://el.wikipedia.org/wiki/Σκουλήκι_υπολογιστή
32. https://en.wikipedia.org/wiki/Computer_worm
33. https://el.wikipedia.org/wiki/Ιός_υπολογιστή
34. https://en.wikipedia.org/wiki/Personal_data

## Συγγράμματα


35. Μιχαήλ Σφακιανάκης, «Εισαγωγή στην Πληροφορική Σκέψη», Εκδόσεις Κλειδάριθμος
36. Μιχαήλ Σφακιανάκης, «Προσομοίωση και Εφαρμογές», Εκδόσεις Πατάκη.
37. Π. Δόνος – Λ. Μήτρου – Φ. Μίτλεττον – Ε. Παπακωνσταντίνου, «Η αρχή της προστασίας προσωπικών δεδομένων και η επαύξηση της προστασίας των δικαιωμάτων», Εκδόσεις Σάκκουλα
38. Ειρηνικός Πλατής, «Προσωπικά Δεδομένα - Προστασία GDPR», Εκδόσεις Παπαδόπουλος


## Αρθρογραφία


39. Για μία αποτελεσματική δημόσια προστασία των προσωπικών δεδομένων: ο «θαυμαστός καινούργιος κόσμος» του Κανονισμού (ΕΕ) 679/2016 Γιώργου Δελλή, Αν. καθηγητή Νομικής Σχολής Πανεπιστημίου Αθηνών
40. Εφημερίδα ΤΑ ΝΕΑ, Φύλλο 20-21/4/2019, «Χρυσές δουλειές με τα προσωπικά δεδομένα μας»
41. Official Journal of the European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 27/4/2016


## Εθνικά κείμενα


42. Νόμος 3917/2011, ΦΕΚ 22/Α'/21.02.2011. Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις.
43. Νόμος 3471/2006, ΦΕΚ 133/Α'/28.6.2006. Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997.
44. Νόμος 3448/06, ΦΕΚ 57/Α'/15.03.2006. Για την περαιτέρω χρήση πληροφοριών του δημόσιου τομέα και τη ρύθμιση θεμάτων αρμοδιότητας Υπουργείου Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης.
45. Νόμος 2690/1999, ΦΕΚ 45/Α'/09.03.1999. Κύρωση του Κώδικα Διοικητικής Διαδικασίας και άλλες διατάξεις.
46. Νόμος 2472/1997, ΦΕΚ 50/Α'/10.04.1997. Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.
47. Προεδρικό Διάταγμα 28/2015 ΦΕΚ 34/Α'/23.03.2015. Κωδικοποίηση διατάξεων για την πρόσβαση σε δημόσια έγγραφα και στοιχεία.