ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ
ΕΠΙΣΤΗΜΩΝ & ΔΙΟΙΚΗΣΗΣ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ
«ΠΟΛΙΤΙΚΗ ΥΓΕΙΑΣ &
ΣΧΕΔΙΑΣΜΟΣ ΥΠΗΡΕΣΙΩΝ ΥΓΕΙΑΣ»

ΔΙΑΤΡΙΒΗ ΕΠΙΠΕΔΟΥ ΜΑΣΤΕΡ

Ο νέος ευρωπαϊκός κανονισμός GDPR με αναφορά στον αντίστοιχο αμερικάνικο (HIPAA). Πώς ένα ελληνικό ιδιωτικό νοσοκομείο προετοιμάζεται και τελικά προσαρμόζεται στον κανονισμό GDPR. Από τον σχεδιασμό μέχρι την τελική προσαρμογή.

Βασιλική Δημ. Ρούμπου

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: Δ. Κουτσούρης

ΛΕΥΚΩΣΙΑ, ΝΟΕΜΒΡΙΟΣ, 2018

ΑΝΟΙΚΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ
ΕΠΙΣΤΗΜΩΝ & ΔΙΟΙΚΗΣΗΣ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ
«ΠΟΛΙΤΙΚΗ ΥΓΕΙΑΣ &
ΣΧΕΔΙΑΣΜΟΣ ΥΠΗΡΕΣΙΩΝ ΥΓΕΙΑΣ»

ΔΙΑΤΡΙΒΗ ΕΠΙΠΕΔΟΥ ΜΑΣΤΕΡ

Ο νέος ευρωπαϊκός κανονισμός GDPR με αναφορά στον αντίστοιχο αμερικάνικο (HIPAA). Πώς ένα ελληνικό ιδιωτικό νοσοκομείο προετοιμάζεται και τελικά προσαρμόζεται στον κανονισμό GDPR. Από τον σχεδιασμό μέχρι την τελική προσαρμογή.

Βασιλική Δημ. Ρούμπου

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: Δ.Δ.Κουτσούρης

ΛΕΥΚΩΣΙΑ, ΝΟΕΜΒΡΙΟΣ, 2018

Πίνακας περιεχομένων

ΕΥΧΑΡΙΣΤΙΕΣ

Είναι γεγονός ότι, χωρίς την συμπαράσταση και υποστήριξη ορισμένων ανθρώπων, η υλοποίηση της συγκεκριμένης διατριβής και γενικότερα, η ολοκλήρωση αυτού του μεταπτυχιακού προγράμματος, δεν θα ήταν δυνατόν να πραγματοποιηθεί.

Πρώτα από όλα θα ήθελα να ευχαριστήσω τον επιβλέποντα Καθηγητή μου, κ. Δημήτριο Κουτσούρη και την συνεργάτιδα του κ. Μαριλένα Ταρούση για την επιστημονική υποστήριξη που μου παρείχαν καθ' όλη την διάρκεια της εκπόνησης της διατριβής.

Σε ένδειξη ευγνωμοσύνης, θα ήθελα να ευχαριστήσω τους συνεργάτες μου, στο Mediterraneo Hospital, για την κατανόηση τους στην προσπάθεια μου να ολοκληρώσω το μεταπτυχιακό πρόγραμμα και την διατριβή, παράλληλα με τα καθήκοντα μου. Ιδιαιτέρως, ευχαριστώ την κ. Δραγίνη Γεωργία, την κ. Σιάπκα Βασιλική και τον κ. Στεργιόπουλο Κων/νο, για την συνολική τους στήριξη στην προσπάθεια μου αυτή.

Ως ένδειξη φιλίας, θα ήθελα να ευχαριστήσω την Μαργαρίτα Παναγιωτοπούλου και τον Τάσο Τριανταφύλλου για την συμπαράσταση και υποστήριξη τους σε ευχάριστες και δυσάρεστες στιγμές. Την Κέλη Καραγιάννη για την συνεργασία και την αλληλοϋποστήριξη μας όλο αυτό το διάστημα. Την Λίνα Σκάρπου και την Μαριέτα Ράμφου για τις εποικοδομητικές συζητήσεις μας, που πάντα με βοηθούν να προχωρώ.

Στην συνέχεια, θα ήθελα να ευχαριστήσω την οικογένεια μου, με ιδιαίτερη μνεία στον πατέρα μου, Δημήτριο Ρούμπο για όσα μου προσφέρει όλα τα χρόνια της ζωής μου.

Τέλος, ευχαριστώ τον σύντροφο της ζωής μου και σύζυγο μου, Ιωάννη Φιλιππάκη, για την ανιδιοτελή ηθική υποστήριξη με εμψυχωτική, πάντα, διάθεση που μου παρέχει από την πρώτη στιγμή.

ΠΕΡΙΛΗΨΗ

Σκοπός της συγκεκριμένης διατριβής είναι αναλυθούν τόσο ο νέος ευρωπαϊκός κανονισμός GDPR όσο και ο αντίστοιχος αμερικάνικος (HIPAA) και να παρουσιαστεί ο τρόπος με τον οποίο ένα ελληνικό ιδιωτικό νοσοκομείο προετοιμάζεται και τελικά προσαρμόζεται στον κανονισμό GDPR. Στόχος της παρούσας εργασίας είναι να αποτελέσει βάση για περαιτέρω μελέτη και εξέλιξη των διεργασιών στον τομέα της Υγείας, με βασικό γνώμονα την προστασία των προσωπικών δεδομένων των εμπλεκομένων φυσικών προσώπων.

Εν γένει, η παρούσα διατριβή, κινείται σε τρεις βασικούς άξονες:

Ο πρώτος άξονας περιλαμβάνει εκείνες τις έννοιες που πρέπει να γνωρίζει κάποιος που ενδιαφέρεται να εντρυφήσει στην προστασία προσωπικών δεδομένων. Εδώ εξηγούνται οι όροι που χρησιμοποιούνται στους Νόμους, τους Κανονισμούς ή τις Οδηγίες που θεσπίζονται από την Ευρωπαϊκή Ένωση (ΕΕ) ή τα Κράτη. Στη συνέχεια, διαχωρίζονται τα προσωπικά δεδομένα σε κατηγορίες και εξηγείται τι θεωρείται επεξεργασία αυτών. Επίσης, γίνεται πλήρης αναδρομή στα βασικότερα κανονιστικά πλαίσια στην Ελλάδα και διεθνώς (πριν την θέσπιση του GDPR) με αναφορές σε άλλα Κράτη και στις δικές τους νομοθεσίες.

Ο δεύτερος άξονας αποτελεί τον πυλώνα της παρούσας διατριβής, καθώς περιλαμβάνει την ανάλυση του κανονισμού GDPR και του αμερικάνικου νόμου HIPAA. Γίνεται προσέγγιση άρθρο προς άρθρο, εξηγούνται νέες έννοιες και ορισμοί που έρχονται στο προσκήνιο μέσω του κανονισμού GDPR, όπως είναι ο ρόλος του Data Protection Officer. Στη διατριβή γίνεται αντιστοίχιση του κανονισμού GDPR με το HIPAA, τονίζοντας τις ομοιότητες και τις διαφορές τους, αλλά και τις δυσκολίες που προκύπτουν για τις ΗΠΑ με την έναρξη ισχύος του GDPR.

Ο τρίτος άξονας της εργασίας αυτής, περιλαμβάνει τα βήματα που ακολουθήθηκαν από ένα γενικό ιδιωτικό ελληνικό Νοσοκομείο, με σκοπό την εναρμόνιση του με το νέο κανονιστικό πλαίσιο για την προστασία των προσωπικών δεδομένων των πελατών, των συνεργατών, των ασθενών, των εργαζομένων και όλων των άλλων φυσικών προσώπων, που τίθενται σε επεξεργασία υπό την δική του ευθύνη.

Τέλος, κατά την ανάπτυξη την εργασίας, επιλέχθηκε να μην περιοριστεί η ανάλυση των Κανονισμών, των Νόμων και των Οδηγιών που αναφέρονται, στον τομέα της Υγείας, αλλά να αναφερθούν ως έχουν, στο σύνολο τους ώστε να μπορέσει να γίνει καλύτερη και

πληρέστερη αποτύπωση του κανονισμού GDPR. Για τις ανάγκες ολοκλήρωσης της εν λόγω διατριβής, χρησιμοποιήθηκαν φύλλα εφημερίδων των Κυβερνήσεων και της ΕΕ, επιστημονικά άρθρα, βιβλιογραφικές παραπομπές και προσωπική εμπειρία στο προαναφερόμενο ιδιωτικό Νοσοκομείο.

ABSTRACT

The purpose of this thesis is to analyze, both, General Data Protection Regulation (GDPR) and HIPAA law, and to present how a general private Greek Hospital is being prepared and eventually adapted to GDPR. The main goal of this thesis is to provide as a base for further study and development of healthcare processes, with the basic aim the privacy protection of involved individuals.

In general, this thesis is based on three main axes:

The first includes those concepts that someone, who is interested to study about personal data protection, in depth, should know. Are explained terms that used in the Laws, the Regulations or the Directives adopted by the EU or the United States. Are separated the different kinds of personal data and are explained what considered as personal data processing. A full review is made of the key regulatory frameworks in Greece and internationally (before GDPR) with references to other countries and their own legislation.

The second is the pillar of this thesis, as it includes the analysis of the GDPR and the American law, HIPAA. An article-by-article approach is explained, new concepts and definitions that come to the fore by the GDPR Regulation, such as the role of the Data Protection Officer. GDPR Regulation compares with HIPAA, highlighting their similarities and differences, as well as the difficulties that arise for the US with the entry into force of the GDPR.

The third part of this thesis includes the steps taken by a general private Greek Hospital to follow the new regulatory framework for the protection of personal data of clients, associates, patients, employees and all other individuals who let the Hospital manage their personal data, under their own responsibility.

In the preparation of this thesis, it has been chosen not to limit the analysis of the Regulations, Laws and Directives mentioned only in the health sector but to be analyzed as such in their entirety so as to give a better and fuller picture of main subject of this thesis, which is the Regulation GDPR.

For the purposes of completing the present thesis, government and EU newspapers have been used, scientific articles, bibliographical references and personal experience in the aforementioned private hospital.

1. ΕΙΣΑΓΩΓΗ

Σε κάθε δημοκρατική κοινωνία, η προστασία και ο σεβασμός ως προς την ιδιωτική ζωή και την ελευθερία του ατόμου, αποτελούν βασικό στόχο. Έχοντας κατά νου την μεγάλη και συνεχή πρόοδο και ανάπτυξη της τεχνολογίας, την μετάβαση από τις παραδοσιακές συναλλαγές στις ηλεκτρονικές, την ανάγκη για οργάνωση των κρατικών και ιδιωτικών μηχανισμών μέσω των ηλεκτρονικών συστημάτων, είναι αυτονόητο ότι υπάρχει μεγάλη αύξηση της ζήτησης για προσωπικά δεδομένα από τους διάφορους φορείς και παρόχους υπηρεσιών, τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα.

Η διατριβή αυτή ξεκίνησε σε μία χρονική περίοδο όπου επιχειρήσεις και οργανισμοί της Ευρωπαϊκής Ένωσης, προσπαθούσαν να μεταφράσουν και να κατανοήσουν με ακρίβεια τις αποφάσεις που ορίζονται μέσω του Κανονισμού 2016/679 GDPR για την προστασία δεδομένων προσωπικού χαρακτήρα και την ελεύθερη διακίνηση τους.
Με αφορμή τον Κανονισμό 2016/679, οι πιο ενημερωμένες επιχειρήσεις και οργανισμοί, είχαν αρχίσει να οργανώνουν, μετά την 27^{η} Απριλίου 2016, μικρές αλλαγές στις διαδικασίες τους, ώστε να προλάβουν να τις εναρμονίσουν με τις απαιτήσεις του Κανονισμού αυτού και να είναι πλήρως προετοιμασμένες κατά την έναρξη ισχύος του, την 25^{η} Μαΐου 2018.
Είναι γεγονός ότι στον χώρο της υγείας, η προστασία των προσωπικών δεδομένων έχει επιπλέον δυσκολίες, λόγω της φύσης των περιεχομένων τους. Αυτό οδηγεί τα Νοσοκομεία, τις Κλινικές και γενικά τους Επαγγελματίες Υγείας, να αναζητούν πιο εξελιγμένους τρόπους επεξεργασίας και αποθήκευσης προσωπικών δεδομένων, όχι μόνο των ασθενών, αλλά και των συνεργατών τους.

Αξιοσημείωτο είναι ότι, ο Κανονισμός GDPR, θα μπορούσε να αποτελέσει αρωγό στην προσπάθεια πολλών Κρατών για εξέλιξη των παρεχόμενων υπηρεσιών των οργανισμών και επιχειρήσεων τους με χαρακτηριστικό παράδειγμα, τις μονάδες υγείας που διατηρούν,ακόμη, Ιατρικό Φάκελο Ασθενούς σε φυσική μορφή. Τέτοιες μονάδες υγείας, εκμεταλλευόμενες τα εργαλεία που παρέχονται πλέον, θα μπορούσαν να αδράξουν την ευκαιρία και να μεταβούν στον Ηλεκτρονικό Ιατρικό Φάκελο, ενισχύοντας τα συστήματα ασφαλείας τους, ώστε να τηρούνται και όλες οι προϋποθέσεις που ορίζονται από την ευρωπαϊκή και την εθνική τους νομοθεσία.

Αντικείμενο της συγκεκριμένης διατριβής είναι η αποτύπωση των κανονιστικών πλαισίων στην Ελλάδα και διεθνώς, μέχρι και σήμερα. Πρωταγωνιστικό ρόλο στην ανάλυση, κατέχει η

θέσπιση του ευρωπαϊκού Κανονισμού 2016/679 (GDPR) για την προστασία προσωπικών δεδομένων και την ελεύθερη κυκλοφορία αυτών με σαφείς αναφορές σε αντίστοιχο νόμο των ΗΠΑ (HIPAA). Η προσέγγιση του θέματος έγινε προσεγγίζοντας τον Κανονισμό ανά άρθρο και σε αντιστοιχία με το HIPAA, τονίζοντας κοινά σημεία τους αλλά και βασικές διαφορές.

Είναι σημαντικό να γίνει κατανοητή η ανάγκη που υπήρξε για την θέσπιση ενός Κανονισμού που θα συμπεριελάμβανε, όχι μόνο τυπικούς κανόνες για την προστασία προσωπικών δεδομένων, ως γενική έννοια, ως είθισται μέχρι τώρα, αλλά και κανόνες που αφορούν κατηγορίες που δεν θίγονται, σε βάθος, μέσω άλλων νομοθετικών διατάξεων. Με την ραγδαία εξέλιξη της τεχνολογίας και την παγκοσμιοποίηση, οι κίνδυνοι για έκθεση των προσωπικών δεδομένων των φυσικών προσώπων ολοένα και αυξάνονται. Μέσω του GDPR, γίνεται η πρώτη σημαντική προσπάθεια από την πλευρά της Ευρωπαϊκής Ένωσης, να καλύψει το συνεχές χάσμα που δημιουργείται από το ταχέως εξελισσόμενο ψηφιακό περιβάλλον και όχι μόνο. Ορίζει ως σημαντικότατη απαίτηση, την απόλυτη διαφάνεια στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα και υποχρεώνει τους εκτελούντες την επεξεργασία, να είναι σε θέση να τεκμηριώνουν τα χαρακτηριστικά της επεξεργασίας που εκτελούν (διάρκεια, σκοπό, περιεχόμενα, χρησιμοποιούμενα μέτρα ασφαλείας, κτλ).

Δεν είναι τυχαίο ότι η προστασία των προσωπικών δεδομένων, αποτελεί για την ΕΕ, μια από τις θεμελιώδεις ελευθερίες των ατόμων, σύμφωνα με τον Χάρτη των θεμελιωδών δικαιωμάτων. Το GDPR καταφέρνει να ενισχύσει την προστασία των δεδομένων αυτών και να υπενθυμίσει στους εμπλεκόμενους οργανισμούς και επιχειρήσεις την σημαντικότητα της.
Τέλος, ενισχύει τον ρόλο του υποκειμένου των δεδομένων, καθώς αυξάνει σημαντικά τα δικαιώματα του, ενδυναμώνει τον ρόλο των εποπτικών Αρχών και τονίζει την σημασία της τήρησης του Κανονισμού, μέσω των, πολύ, υψηλών προστίμων των οποίων ορίζει μέσα από τα άρθρα του.

2.ΟΡΙΣΜΟΙ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

2.1. Τι είναι τα δεδομένα προσωπικού χαρακτήρα (κοινά ή απλά)

Σύμφωνα με την Ευρωπαϊκή Επιτροπή, ως προσωπικά δεδομένα ορίζονται οι «πληροφορίες που αφορούν ένα ταυτοποιημένο ή ταυτοποιήσιμο εν ζωή άτομο». (Ευρωπαϊκή Επιτροπή, 2018a).

Σε αυτές συμπεριλαμβάνονται και πληροφορίες οι οποίες υπάρχουν διάσπαρτες αλλά αν συγκεντρωθούν οδηγούν σε ένα συγκεκριμένο άτομο ή, ακόμη, έχουν ανωνυμοποιηθεί, κρυπτογραφηθεί ή αντικατασταθεί με ψευδώνυμα, οι οποίες όμως μπορούν να οδηγήσουν σε ταυτοποίηση ενός προσώπου. (Ευρωπαϊκή Επιτροπή, 2018a).

Τα δεδομένα για να μην αποτελούν δεδομένα προσωπικού χαρακτήρα θα πρέπει να έχουν κρυπτογραφηθεί ή ανωνυμοποιηθεί με τέτοιο τρόπο ώστε σε καμία περίπτωση να μην μπορεί αυτή η πληροφορία να ταυτοποιηθεί με ένα άτομο (Ευρωπαϊκή Επιτροπή, 2018a).

2.2. Ποια είναι τα κοινά ή απλά δεδομένα προσωπικού χαρακτήρα

Δεδομένα προσωπικού χαρακτήρα μπορούν να θεωρηθούν τα:

- Όνομα και επώνυμο
- Διεύθυνση Κατοικίας
- Προσωπικό ή Εταιρικό Email (που περιλαμβάνει στοιχεία όπως ονοματεπώνυμο, π.χ. name.lastname@company.gr)
- Αναγνωριστικός αριθμός κάρτας (π.χ. αριθμός δελτίου ταυτότητας, αριθμός διαβατηρίου, αριθμός διπλώματος οδήγησης)
- Δεδομένα τοποθεσίας
- IPaddressprotocol
- Cookie
- Ιατρικά δεδομένα (Φάκελος Υγείας Ασθενή – Ιατρικός Φάκελος). (Ευρωπαϊκή Επιτροπή, 2018a).

Δεδομένα προσωπικού χαρακτήρα δεν μπορούν να θεωρηθούν τα:

- Αριθμός μητρώου σε εταιρεία
- Email τύπου info@company.gr
- Ανώνυμα (με μη αναστρέψιμο τρόπο) δεδομένα. (Ευρωπαϊκή Επιτροπή, 2018a).

2.3. Τι είναι τα ευαίσθητα προσωπικά δεδομένα

Ως ευαίσθητα προσωπικά δεδομένα, θεωρούνται τα δεδομένα εκείνα που μπορεί να φανερώσουν καταγωγή ατόμου (φυλετική ή θρησκευτική), πολιτικές, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, πρότερη συμμετοχή σε συνδικαλιστικήοργάνωση, γενετικά ή βιομετρικά δεδομένα, πληροφορίες υγείας, δεδομένα σχετικά με την σεξουαλική ζωή ή τον γενετήσιο προσανατολισμό του ατόμου, ποινικές διώξεις ή καταδίκες του. Ως παράδειγμα μπορεί να αναφερθεί η συμμετοχή ενός συγγραφέα σε συνδικαλιστική οργάνωση. (ΑΠΔΠΧ, 2018a, Ευρ. Επιτροπή, 2018b).

2.4.Τι είναι η επεξεργασία προσωπικών δεδομένων

Επεξεργασία προσωπικών δεδομένων πραγματοποιείται με οποιαδήποτε από τις κάτωθι ενέργειες (μεμονωμένα ή σε συνδυασμό):

- Συλλογή
- Καταχώρηση
- Οργάνωση
- Αποθήκευση
- Διάρθρωση
- Προσαρμογή ή αλλαγή
- Ανάκτηση
- Αναζήτηση πληροφοριών
- Χρήση
- Κοινοποίηση με διαβίβαση
- Διάδοση
- Οποιασδήποτε μορφής συσχέτιση/συνδυασμός
- Περιορισμός
- Διαγραφή/καταστροφή. (ΑΠΔΠΧ, 2018a, Ευρ. Επιτροπή, 2018c).

Ενδεικτικά αναφέρονται παραδείγματα επεξεργασίας δεδομένων προσωπικού χαρακτήρα, (Ευρ. Επιτροπή, 2018c)[4]:

- Μισθοδοσία προσωπικού
- Αναζήτηση στοιχείων σε βάση δεδομένων επαφών
- Δημοσίευση φωτογραφιών ατόμου σε ιστότοπο
- Μαγνητοσκόπηση (κλειστό κύκλωμα)

2.5. Χρήσιμοι ορισμοί:

- Το άτομο στο οποίο αναφέρονται τα προσωπικά δεδομένα καλείται ως *υποκείμενο των δεδομένων.*

- Κάθε νομικό ή φυσικό πρόσωπο που επεξεργάζεται προσωπικά δεδομένα καλείται ως *υπεύθυνος επεξεργασίας.*

- Κάθε νομικό ή φυσικό πρόσωπο που επεξεργάζεται προσωπικά δεδομένα κατ' εντολή του υπευθύνου επεξεργασίας καλείται ως *εκτελών την επεξεργασία.*

- Κάθε νομικό ή φυσικό πρόσωπο, δημόσια αρχή, υπηρεσία ή άλλος φορέας, εξουσιοδοτημένος από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα, να επεξεργάζεται τα δεδομένα, ονομάζεται *τρίτος.*

- Ως *αποδέκτης*, ονομάζεται κάθε νομικό ή φυσικό πρόσωπο, δημόσια αρχή, υπηρεσία ή άλλος φορέας, στον οποία ανακοινώνονται τα δεδομένα.

- Κάθε ρητή δήλωση προσώπου που επιτρέπει την οποιαδήποτε επεξεργασία των δεδομένων του, ονομάζεται *συγκατάθεση.* (Ευρωπαϊκό Κοινοβούλιο, 1995).

3.Η ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΜΕΣΩ ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΚΑΙ ΤΗΣ ΔΙΕΘΝΟΥΣ ΝΟΜΟΘΕΣΙΑΣ (εκτός GDPR)

Στο κεφάλαιο αυτό γίνεται αναφορά στην ευρωπαϊκή και ελληνική νομοθεσία για την προστασία προσωπικών δεδομένων. Διαφαίνεται ο τρόπος με τον οποίο η Ελλάδα ενστερνίζεται και ενσωματώνει την ευρωπαϊκή νομοθεσία. Περιλαμβάνεται συνοπτική παρουσίαση αντίστοιχων νομοθεσιών άλλων ευρωπαϊκών χωρών και τέλος, γίνεται αναφορά στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και στην σύσταση της.

3.1. Διεθνής νομοθεσία σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα

3.1.1. Η ευρωπαϊκή σύμβαση για τα δικαιώματα του ανθρώπου

Η ανάγκη για προστασία της ιδιωτικότητας του ατόμου εκφράζεται αρχικά σε διεθνές επίπεδο. Συγκεκριμένα, στην Σύμβαση της Ρώμης (4 Νοεμβρίου 1950), διατυπώνεται η προστασία των ανθρώπινων δικαιωμάτων. Στο άρθρο 8 της Σύμβασης ορίζεται το δικαίωμα του ατόμου να γίνεται σεβαστή η ιδιωτική και οικογενειακή του ζωή, η κατοικία και η αλληλογραφία του. Δεν επιτρέπεται να παρέμβει κανείς εκτός κι αν η παρέμβαση καλύπτεται από τον νόμο και είναι αναγκαία για την εθνική και δημόσια ασφάλεια, την οικονομική ευημερία του κράτους, την πρόληψη ποινικών παραβάσεων, την προστασία της ηθικής και της υγείας, την προστασία και την ελευθερία των δικαιωμάτων άλλων ατόμων και την προάσπιση της τάξης. (ΕΔΑΔ, 2010).

Μία ακόμη απόφαση που εντοπίζεται ανάμεσα στις πρώτες σε σχέση με την προστασία των προσωπικών δεδομένων είναι η απόφαση 2450/19.12.1968 της Γενικής Συνέλευσης των Ηνωμένων Εθνών. Σε αυτήν αναφέρονται τα προβλήματα που προκύπτουν από την ανάπτυξη της τεχνολογίας και συγκεκριμένα από την χρήση ηλεκτρονικών μέσων. (Καρέτσου Α., 1997).

Αξίζει να σημειωθεί το γεγονός ότι το πεδίο της προστασίας προσωπικών δεδομένων, απασχόλησε και δημιούργησε νομοθετικές αντιδράσεις πρώτα σε διεθνές κι έπειτα σε εθνικό επίπεδο. Η έναρξη ανταλλαγής και μεταφοράς πληροφορίας, μέσω της ραγδαίας εξέλιξης της τεχνολογίας, σε διασυνοριακό επίπεδο οδήγησε στην ανάγκη για την προστασία των δεδομένων μέσω κανονιστικών διατάξεων.

3.1.2. Οι κατευθυντήριες οδηγίες του ΟΟΣΑ σε σχέση με την ιδιωτικότητα και τις διασυνοριακές ροές των προσωπικών δεδομένων

Σε διεθνές επίπεδο, ο ΟΟΣΑ το 1980, μέσα από τις «Κατευθυντήριες Αρχές που διέπουν την προστασία τις ιδιωτικότητας και τις διασυνοριακές ροές προσωπικών δεδομένων», ασχολήθηκε με την προστασία των προσωπικών δεδομένων.

Παρακάτω παρουσιάζονται οι κατευθυντήριες αρχές που ορίζονται από τον ΟΟΣΑ, οι οποίες αν και δεν είχανδεσμευτικό χαρακτήρα στόχευαν στο να φέρουν το θέμα της ιδιωτικότητας στο προσκήνιο και να τονίσουν την ανάγκη για δημιουργία συντονιστικών διατάξεων ώστε να μην δημιουργούνται προβλήματα στην ροή της πληροφορίας, λόγω των πολλών διαφορετικών εθνικών νομοθεσιών (OECD, 1980):

- Αρχή της περιορισμένης συγκέντρωσης και συλλογής δεδομένων (Collection Limitation Principle)
- Αρχή της ποιότητας των δεδομένων (Data Quality Principle)
- Αρχή του προσδιορισμένου σκοπού (Purpose Specification Principle)
- Αρχή της περιορισμένης χρήσης των προσωπικών δεδομένων (Use Limitation Principle)
- Αρχή των μέτρων ασφαλείας των προσωπικών δεδομένων (Security Safeguards Principle)
- Αρχή της διαφάνειας (Openness Principle)
- Αρχή της συμμετοχής του ατόμου (Individual Participation Principle)
- Αρχή της ευθύνης (Accountability Principle).

3.1.3. Η σύμβαση 108/28.1.1981

Η σύμβαση 108/28.1/1981 από το Συμβούλιο της Ευρώπης που έλαβε χώρα στο Στρασβούργο, αποτελεί την πρώτη διεθνή νομοθετική πράξη με δεσμευτικό χαρακτήρα και προστατεύει το πρόσωπο από τους κινδύνους που μπορεί να προκληθούν από την αυτοματοποιημένη συλλογή και επεξεργασία των προσωπικών του δεδομένων. Με την σύμβαση αυτή, απαγορεύεται η επεξεργασία των ευαίσθητων προσωπικών δεδομένων χωρίς όλες τις απαραίτητες νόμιμες εγγυήσεις. Επίσης, το άτομο έχει το δικαίωμα να γνωρίζει ότι τα δεδομένα του αποθηκεύονται και να επεμβαίνει ζητώντας διορθώσεις. Όπως και στην Σύμβαση της Ρώμης, τα δικαιώματα μπορούν να περιοριστούν όταν η πρόσβαση ή επεξεργασία αφορά την εθνική ασφάλεια ή άμυνα και η μη πρόσβαση ή επεξεργασία ελλοχεύει κινδύνους. (Council of Europe, 2001).

3.1.4. Οδηγία 95/46/ΕΚ

Η οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της Ευρωπαϊκής Ένωσης της 24ης Οκτωβρίου 1995 είχε δύο στόχους, (Ευρωπαϊκό Κοινοβούλιο, 1995):

1) «Την προστασία των θεμελιωδών ελευθεριών και δικαιωμάτων των φυσικών προσώπων, και ιδίως της ιδιωτικής ζωής, έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα».

2) Την ελεύθερη κυκλοφορία των προσωπικών δεδομένων με την εξασφάλιση της προστασίας όπως αναφέρεται στον πρώτο στόχο της οδηγίας.

Η συγκεκριμένη οδηγία αποτέλεσε το σημαντικότερο νομοθετικό πλαίσιο της Ευρωπαϊκής Ένωσης για την προστασία των προσωπικών δεδομένων μέχρι τον Μάιο του 2018 που καταργείται με την έναρξη ισχύος του GDPR 2016/679, όπως θα αναφερθεί σε επόμενα κεφάλαια.

Η 95/46/ΕΚ προσανατολίζεται στην ενδυνάμωση της αγοράς και την προώθηση της ροής της πληροφορίας και επιδιώκει την ομαλή λειτουργία των ευρωπαϊκών νομοθεσιών. (Ευρωπαϊκό Κοινοβούλιο, 1995).

Μέσω της οδηγίας 95/46/ΕΚ, ορίζονται τα δικαιώματα των φυσικών προσώπων, τα δεδομένα των οποίων υπόκεινται επεξεργασία από τρίτους, καθορίζει του κανόνες σχετικά με την επεξεργασία των δεδομένων αυτών και περιλαμβάνει την θέσπιση ανεξάρτητων εποπτικών αρχών. Η επεξεργασία επιτρέπεται αποκλειστικά με την ρητή συγκατάθεση του ατόμου και εφόσον έχει ενημερωθεί εκ των προτέρων για την επεξεργασία των προσωπικών του δεδομένων. (Ευρωπαϊκό Κοινοβούλιο, 1995).

Στο άρθρο 28 της συγκεκριμένης οδηγίας περιγράφεται και η Αρχή Ελέγχου. Πρόκειται για μία ή περισσότερες δημόσιες αρχές που ως βασική αρμοδιότητα, πέρα από πλήθος άλλων αρμοδιοτήτων, θα έχει τον έλεγχο της εφαρμογής των εθνικών διατάξεων που έχουν θεσπιστεί για την εφαρμογή της παρούσας οδηγίας, από τα κράτη μέλη. Στην Αρχή δίδεται πλήρης ανεξαρτησία σχετικά με τα καθήκοντα που της έχουν ανατεθεί.

Η οδηγία 95/46/ΕΚ μεταφέρθηκε στην ελληνική τάξη με τον νόμο 2472/97 και καταργήθηκε με τον κανονισμό 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016, όπως αναλύεται σε επόμενες παραγράφους.

3.1.5. Οδηγία 97/66/ΕΚ και Οδηγία 2002/58/ΕΚ

Στο κανονιστικό πλαίσιο της Ευρωπαϊκής Κοινότητας προστίθεται, το 1997, η οδηγία 97/66/ΕΚ. Η οδηγία 97/66/ΕΚ αφορά την προστασία των προσωπικών δεδομένων και ελευθεριών των χρηστών και των συνδρομητών των τεχνολογιών ηλεκτρονικών επικοινωνιών. Η συγκεκριμένη οδηγία ενσωματώθηκε στην ελληνική νομοθεσία με τον νόμο 2774/99. (Ευρωπαϊκό Κοινοβούλιο, 1998).

Η οδηγία 97/66/ΕΚ αντικαταστάθηκε από την οδηγία 2002/58/ΕΚ. Η έκδοση της οδηγίας 2002/58/ΕΚ αφορούσε την προσαρμογή της προηγούμενης στις εξελίξεις της τεχνολογίας των υπηρεσιών των ηλεκτρονικών επικοινωνιών και των αγορών. (Ευρωπαϊκό Κοινοβούλιο, 2002).

Στόχος της 2002/58/ΕΚ ήταν, η διασφάλιση ενός ισοδύναμου επιπέδου στην προστασία των θεμελιωδών δικαιωμάτων και των ελευθεριών για όλους τους χρήστες, με ιδιαίτερη μνεία στην ιδιωτική ζωή του ατόμου. Επίσης, στόχευε στην διασφάλιση της ελεύθερης ροής των πληροφοριών αλλά και του εξοπλισμού και των υπηρεσιών των τηλεπικοινωνιών εντός της Ευρωπαϊκής Κοινότητας. Η εισαγωγή της συγκεκριμένης οδηγίας στην ελληνική νομοθεσία έγινε μέσω του ν. 3471/2006. (Ευρωπαϊκό Κοινοβούλιο, 2002).

3.1.6. Απόφαση πλαίσιο 2008/977/ΔΕΥ

Η απόφαση πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου για την προστασία των προσωπικών δεδομένων που τυγχάνουν επεξεργασίας στα πλαίσια αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις, ήρθε συμπληρωματικά για να καλύψει ένα τομέα που δεν είχε περιληφθεί στην 95/46/ΕΚ. Αφορά δεδομένα, μόνο αστυνομικά και δικαστικά, που διακινούνται μεταξύ των κρατών μελών και των διασυνδεδεμένων αρχών της ΕΕ. Δεν καλύπτει επεξεργασία προσωπικών δεδομένων σε εγχώριο επίπεδο. Σκοπός της είναι η διασφάλιση των θεμελιωδών δικαιωμάτων και ελευθεριών του προσώπου σε συνδυασμό με την κατοχύρωση υψηλού επιπέδου δημόσιας ασφάλειας. Η συγκεκριμένη απόφαση καταργήθηκε με την 680/2016 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27^{ης} Απριλίου. Η οδηγία 680/2016 αφορά, εκτός από την κατάργηση της συγκεκριμένης απόφασης πλαισίου, την προστασία των φυσικών προσώπων σε σχέση με την επεξεργασία προσωπικών δεδομένων από αρμόδιες αρχές για σκοπούς πρόληψης, διερεύνησης, ανίχνευσης, ποινικής δίωξης ή εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. (Council of the European Union, 2008).

3.1.7. Χάρτης Θεμελιωδών δικαιωμάτων της Ε.Ε. (2000/C 364/01)

Στον Χάρτη Θεμελιωδών δικαιωμάτων της ΕΕ, το άρθρο 8 αναφέρεται στην προστασία των δεδομένων προσωπικού χαρακτήρα. Η προστασία των προσωπικών δεδομένων εδώ κατατάσσεται στις Ελευθερίες που ορίζονται από τον Χάρτη, μαζί με άλλες, όπως είναι η Ελευθερία της έκφρασης, της ασφάλειας, ο σεβασμός της ιδιωτικής ζωής κ.α. (Κεφάλαιο ΙΙ).

Συγκεκριμένα, ορίζεται ότι, το κάθε άτομο έχει δικαίωμα στην προστασία των προσωπικών δεδομένων που το αφορούν (άρθρο 8, παρ. 1). Η επεξεργασία αυτών μπορεί να γίνεται έπειτα από δική του συγκατάθεση, νομίμως και για συγκεκριμένους σκοπούς. Εδώ δίδεται και το δικαίωμα στο υποκείμενο της επεξεργασίας να έχει πρόσβαση στα δεδομένα που το αφορούν και να τα διορθώνει εάν το επιθυμεί (άρθρο 8, παρ. 2). Τέλος, ορίζει ως αρμόδια, ανεξάρτητη Αρχή, για τον έλεγχο και τον σεβασμό των ανωτέρω (άρθρο 8, παρ. 3). (Ευρωπαϊκή Ένωση, 2000).

3.1.8. Συνθήκη για την λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ)

Στον Τίτλο Ι, της Συνθήκης (ΣΛΕΕ), για τις Κατηγορίες και τους Τομείς Αρμοδιοτήτων της ΕΕ, στο άρθρο 16, αναφέρεται το δικαίωμα του κάθε προσώπου για προστασία των προσωπικών του δεδομένων (άρθρο 16, παρ. 1). Εδώ ορίζεται το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, ως υπεύθυνο για την θέσπιση κανόνων για την προστασία των δεδομένων προσωπικού χαρακτήρα των φυσικών προσώπων αλλά και για την ελεύθερη κυκλοφορία αυτών των δεδομένων. Ο έλεγχος της τήρησης των σχετικών κανόνων γίνεται από ανεξάρτητες Αρχές. (Ευρωπαϊκή Ένωση, 2012).

3.2 Ελληνική νομοθεσία σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα

3.2.1 Σύνταγμα της Ελλάδος

Κατά την αναθεώρηση του Συντάγματος το 2001 κατοχυρώθηκε συνταγματικά, με σαφήνεια το δικαίωμα προστασίας του φυσικού προσώπου από την συλλογή, επεξεργασία και χρήση των προσωπικών του δεδομένων (άρθρο $9^{α}$). (Βουλή των Ελλήνων, 2008).

Άρθρο $9^{α}$ του ελληνικού Συντάγματος: «Καθένας έχει δικαίωμα προστασίας από την συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει». Ουσιαστικά, στο

άρθρο αυτό κατοχυρώνεται η προστασία της προσωπικότητας σε σχέση με την πληροφόρηση, όπως αναφέρεται στο άρθρο 5^{α}. (Βουλή των Ελλήνων, 2008).

Πριν ακόμη από την ανωτέρω αναθεώρηση, το δικαίωμα αυτό περιλαμβανόταν, έμμεσα, στα παρακάτω άρθρα του Συντάγματος, (Βουλή των Ελλήνων, 2001a):

Στο άρθρο 2, παρ. 1, αναφέρεται ότι η Πολιτεία οφείλει να δείχνει σεβασμό και να προστατεύει τον άνθρωπο και να μην τον υποβαθμίζει ως οντότητα.

Στο άρθρο 5, παρ. 1, αναφέρεται ότι ο καθένας δικαιούται να αναπτύσσει την προσωπικότητα του μέσα στην χώρα, αρκεί να μην προσβάλλει δικαιώματα τρίτων, να τηρεί τα ήθη και το Σύνταγμα.

Στο άρθρο 9, παρ. 1, περιλαμβάνεται η απαγόρευση παραβίασης της ζωής άλλου ατόμου.

Τέλος, στο άρθρο 19, παρ. 1, αναφέρεται το απόρρητο της επικοινωνίας, με όποιο τρόπο κι αν συμβαίνει. Εξαιρεί δε, τις περιπτώσεις απειλής της εθνικής ασφάλειας, οι οποίες ορίζονται μέσω νόμου.

3.2.2 Ελληνικό δίκαιο σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα

3.2.2.1 Νόμος 2472/1997 – Προστασία του ατόμου από επεξεργασία προσωπικών δεδομένων

Ο Ν.2472/1997 αποτελεί την μεταφορά και ενσωμάτωση της κοινοτικής οδηγίας 95/46/ΕΚ, όπως αυτή αναφέρεται στην παράγραφο 2.1.4, στην ελληνική νομοθεσία.

Αντικείμενο του νόμου είναι «η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής». Ο νομοθέτης, με τον ν.2472/1997 ρυθμίζει την κίνηση των προσωπικών δεδομένων σε κρατικό, κοινωνικό και οικονομικό επίπεδο. Ο δημόσιος και ο ιδιωτικός τομέας αντιμετωπίζονται ως ισοδύναμες πηγές μέσω των οποίων διακινδυνεύονται τα δικαιώματα των υποκειμένων προσώπων. (Ευρωπαϊκό Κοινοβούλιο, 1995, Βουλή των Ελλήνων, 1997).

Στις παραγράφους 1.1. και 1.3. του παρόντος, επεξηγούνται οι έννοιες απλά και ευαίσθητα προσωπικά δεδομένα. Ο ν. 2472/1997, διακρίνει τα προσωπικά δεδομένα σε αυτές τις δύο κατηγορίες (άρθρο 2). Ως ευαίσθητα προσωπικά δεδομένα χαρακτηρίζονται όλες οι κατοχυρωμένες, από το Σύνταγμα, ελευθερίες. (Ευρωπαϊκό Κοινοβούλιο, 1995, Βουλή των Ελλήνων, 1997).

Μέσω του 2472/1997, καθορίζονται τα χαρακτηριστικά προσωπικών δεδομένων για να τύχουν επεξεργασίας και ως υπεύθυνος για την τήρηση όσων αναφέρονται (άρθρο 4), ορίζεται ο υπεύθυνος επεξεργασίας. (Ευρωπαϊκό Κοινοβούλιο, 1995, Βουλή των Ελλήνων, 1997)

Συγκεκριμένα, στο άρθρο 4, διευκρινίζεται ότι η συλλογή και επεξεργασία των δεδομένων θα πρέπει να γίνεται με νόμιμο και θεμιτό τρόπο για σαφείς, καθορισμένους και νόμιμους σκοπούς. Θα πρέπει τα συλλεχθέντα προσωπικά δεδομένα να είναι τα ελάχιστα απαραίτητα και όχι περισσότερα από όσα απαιτούνται για τους σκοπούς που έχουν οριστεί. Να υπόκεινται στις απαραίτητες ενημερώσεις και να είναι ακριβή. Τέλος, να αποτελούν ταυτοποιήσιμο υλικό σε σχέση με την ταυτότητα του υποκειμένου μόνο κατά την διάρκεια που απαιτείται για την ολοκλήρωση των σκοπών της συλλογής και επεξεργασίας τους. Μετά το πέρας της ολοκλήρωσης των σκοπών, μόνο η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, με αιτιολογημένη της απόφαση μπορεί να επιτρέψει την διατήρηση των δεδομένων για λόγους ιστορικούς, επιστημονικούς ή στατιστικούς, εφόσον δεν θίγονται τα δικαιώματα του υποκειμένου ή τρίτων. (Ευρωπαϊκό Κοινοβούλιο, 1995, Βουλή των Ελλήνων, 1997)

Στον νόμο 2472/1997 ορίζεται ως μοναδική προϋπόθεση για την επεξεργασία των απλών προσωπικών δεδομένων (άρθρο 5), η συγκατάθεση του υποκειμένου. Κατ' εξαίρεση, επιτρέπει την επεξεργασία δεδομένων προσωπικού χαρακτήρα και με την απουσία της συγκατάθεσης όταν συντρέχει ένα από του κάτωθι λόγους:

- Αν η επεξεργασία απαιτείται για την σύναψη ή εκτέλεση σύμβασης στην οποία το υποκείμενο είναι συμβαλλόμενο μέρος ή για την εκτέλεση προσυμβατικών μέτρων.
- Αν η επεξεργασία είναι υποχρεωτική για τον υπεύθυνο επεξεργασίας από τον νόμο.
- Αν είναι απαραίτητη για την διαφύλαξη ζωτικού συμφέροντος του υποκειμένου.
- Αν είναι απαραίτητη για την επίτευξη έργου δημοσίων συμφερόντων ή σχετίζονται με την άσκηση δημοσίας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας ή σε τρίτο πρόσωπο στο οποίο ανακοινώνονται τα αποτελέσματα.
- Αν είναι απαραίτητη για την επίτευξη έννομου συμφέροντος από τον υπεύθυνο επεξεργασίας ή τους τρίτους, με την προϋπόθεση ότι δεν ακυρώνεται ο βασικός στόχος της παρούσας οδηγίας όπως αναφέρεται στο άρθρο 1, παράγραφο 1.

Αντιστοίχως, στην κοινοτική οδηγία, στο άρθρο 7, παρουσιάζονται όλες μαζί οι ανωτέρω καταστάσεις (6 συνολικά, συμπεριλαμβανομένης και της ρητής συγκατάθεσης), και γίνεται σαφές ότι αρκεί να ισχύει μία εκ των έξι κάθε φορά.(Ευρωπαϊκό Κοινοβούλιο, 1995, Βουλή των Ελλήνων, 1997)

Η επεξεργασία των προσωπικών δεδομένων επιτρέπεται σύμφωνα με τον συγκεκριμένο νόμο, μόνο αν το υποκείμενο έχει δώσει την ρητή συγκατάθεση του και αφού έχει ενημερωθεί για τον σκοπό που απαιτεί την επεξεργασία των στοιχείων του, τους αποδέκτες των δεδομένων αυτών και τα στοιχεία του υπευθύνου για την επεξεργασία. Ουσιαστικά, το υποκείμενο της επεξεργασίας έχει το δικαίωμα να αποφασίσει ελεύθερα και αυτοβούλως, αν θα διαθέσει τα προσωπικά του δεδομένα προς επεξεργασία. Υπό προϋποθέσεις, όπως αυτές παρουσιάζονται αναλυτικά παραπάνω, μπορεί να απουσιάζει η ρητή συγκατάθεση, (Βάρκα Α., 2005).

Ομοίως, στο άρθρο 7 του ν. 2472/1997, ορίζονται οι προϋποθέσεις για την επεξεργασία των ευαίσθητων προσωπικών δεδομένων. Συγκεκριμένα, ο νόμος απαγορεύει την συλλογή και επεξεργασία τους και την επιτρέπει μόνο με άδεια από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, σε περιπτώσεις όπως όταν το υποκείμενο έχει παραχωρήσει ρητή συγκατάθεση, με εξαίρεση περιπτώσεις όπου η συγκατάθεση έχει αποσπαστεί με τρόπο παράνομο ή ανήθικο, όταν η επεξεργασία αφορά θέματα υγείας και η εκτέλεση της γίνεται από πρόσωπο που υπόκειται σε καθήκον εχεμύθειας (π.χ. Θεράπων Ιατρός), όταν η επεξεργασία είναι απαραίτητη για την εθνική ασφάλεια και εκτελείται από Δημόσια Αρχή, κ.α..

Στο κεφάλαιο Γ του νόμου, αναλύονται τα δικαιώματα του υποκειμένου των προσωπικών δεδομένων που υπόκεινται σε επεξεργασία, σχετικά με την ενημέρωση (άρθρο 11), την πρόσβαση (άρθρο 12), την αντίρρηση (άρθρο 13) και την προσωρινή δικαστική προστασία (άρθρο 14).

Τροποποιήσεις του Ν. 2472/1997 περιλαμβάνονται στους παρακάτω νόμους:

- Ν.2623/1998 «Προσθήκη και αντικατάσταση διατάξεων που αφορούν την ΑΠΔΠΧ» (άρθρο 11), (Βουλή των Ελλήνων, 1998)
- Ν. 2703/1999 «Ρύθμιση διαφόρων θεμάτων» (άρθρο 13), (Βουλή των Ελλήνων, 1999a)
- Ν. 2721/1999 «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα» (άρθρο 47), (Βουλή των Ελλήνων, 1999b)

- Ν. 2819/2000 «Τροποποίηση διατάξεων του ν.2472/1997 και του Κώδικα Πολιτικής Δικονομίας» (άρθρο 8), (Βουλή των Ελλήνων, 2000)
- Ν. 2915/2001 (άρθρο 34), (Βουλή των Ελλήνων, 2001b)
- Ν. 3090/2002 (άρθρο 10), (Βουλή των Ελλήνων, 2002a)
- Ν.3068/2002 (άρθρο 14), (Βουλή των Ελλήνων, 2002b)
- Ν.3051/2002«Τελικές και μεταβατικές διατάξεις» (άρθρο 5), (Βουλή των Ελλήνων, 2002c)
- Ν. 3156/2003 «Φορολογικές και άλλες ρυθμίσεις» (άρθρο 26), (Βουλή των Ελλήνων, 2003)
- Ν. 3471/2006 (Κεφάλαιο δεύτερο, άρθρα 18 έως 30), (Βουλή των Ελλήνων, 2006)
- Ν. 3625/2007(άρθρο 8), (Βουλή των Ελλήνων, 2007)
- Ν. 3783/2009 (άρθρο 12), (Βουλή των Ελλήνων, 2009)
- Ν. 3917/2011 «Τροποποιήσεις του Ν.2472/1997» (άρθρο 15), (Βουλή των Ελλήνων, 2011a)
- Ν. 4024/2011«Ρυθμίσεις θεμάτων Υπουργείου Οικονομικών» (άρθρο 39), (Βουλή των Ελλήνων, 2011b)
- Ν. 4152/2013 (άρθρο 126), (Βουλή των Ελλήνων, 2013)

3.2.2.2. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΔΠΔΧ)

Η ΑΠΔΠΧ είναι ανεξάρτητη και συνταγματικά κατοχυρωμένη Αρχή με βασικό αντικείμενο την διαφύλαξη και προστασία των δεδομένων προσωπικού χαρακτήρα. Ιδρύθηκε με τον νόμο 2472/1997 και έγινε ευρύτερα γνωστή με την θέσπιση του Κανονισμού GDPR2016/679, ως η αρμόδια εποπτική Αρχή για την προστασία των προσωπικών δεδομένων. Πρόκειται για 7μελή επιτροπή, συμπεριλαμβανομένου και του Προέδρου. (Βουλή των Ελλήνων, 1997, ΑΠΔΠΧ, 2018b).

Ο νομοθέτης όρισε την Αρχή, ως αρμόδια για την πρόληψη και τον κατασταλτικό έλεγχο της ορθής εφαρμογής του νόμου. Πρόκειται για ανεξάρτητη δημόσια αρχή, της οποίας η κατοχύρωση λαμβάνει χώρα και μέσω του Συντάγματος, με την αναθεώρηση του το 2001 (άρθρο 101^{A}).

Η αποστολή της ΑΠΔΠΧ είναι η προστασία των πολιτών από παράνομη επεξεργασία των προσωπικών του δεδομένων αλλά και η βοήθεια προς αυτούς, σε κάθε διαπιστωμένη σχετική παράβαση σύμφωνα με τους νόμους 2472/97 και 3471/06, όπως αυτοί αναλύονται. (ΑΠΔΠΧ,

2018b). Με την κατάργηση του ν. 2472/97, η παράβαση διαπιστώνεται σύμφωνα με το 2016/679.

Οι βασικές δραστηριότητες της ΑΠΔΠΧ αφορούν στην παραλαβή και στον έλεγχο αρχείων και επεξεργασιών στον δημόσιο και ιδιωτικό τομέα και της τήρησης των αρχείων αυτών, στην εξέταση σχετικών προσφυγών, στην ενημέρωση των υποκειμένων και των υπευθύνων επεξεργασίας. Πιο συγκεκριμένα, οι αρμοδιότητες της ΑΠΔΠΧ διακρίνονται σε τρεις τομείς:

- **Διοικητικές – Ελεγκτικές**(ΑΠΔΠΧ, 2018d)
    1. Αρχείο γνωστοποιήσεων – έκδοση αδειών: Ο υπεύθυνος επεξεργασίας είναι υποχρεωμένος να υποβάλλει, στην Αρχή, γνωστοποίηση για την σύσταση και την λειτουργία σχετικού αρχείου. Ανάλογα με την νομοθεσία και όπου απαιτείται, η Αρχή μπορεί να εκδίδει άδειες για την συλλογή ή/και επεξεργασία προσωπικών δεδομένων, την διακίνηση δεδομένων εκτός ΕΕ, υπό όρους.
    2. Διενέργεια διοικητικών ελέγχων: ΑΠΔΠΧ μπορεί να διενεργεί ελέγχους, αυτεπαγγέλτως ή έπειτα από σχετικά καταγγελία, σε αρχεία φορέων τόσο ιδιωτικών συμφερόντων, όσο και δημοσιών.
    3. Εξέταση προσφυγών, καταγγελιών και ερωτημάτων: Εξετάζει ερωτήματα σχετικά με την εφαρμογή του νόμου και με το αν τα προσωπικά δικαιώματα των αιτούντων θίγονται από την επεξεργασία που επιδέχονται.
- **Κανονιστικές – Συμβουλευτικές** (ΑΠΔΠΧ, 2018e)
    1. Εκδίδει οδηγίες με σκοπό την ενιαία εφαρμογή των ρυθμίσεων σχετικά με την επεξεργασία προσωπικών δεδομένων και κανονιστικές πράξεις για την ρύθμιση διαφόρων τεχνικών, ειδικών και λεπτομερειακών θεμάτων.
    2. Πραγματοποιεί συστάσεις και υποδείξεις στους υπευθύνους επεξεργασίας όταν κρίνεται απαραίτητο
    3. Γνωμοδοτεί για κάθε ρύθμιση σχετικά με την επεξεργασία και προστασία προσωπικών δεδομένων.
- **Απολογισμού – Δημοσιοποίησης –Συνεργασιών** (ΑΠΔΠΧ, 2018f)

Με σκοπό την ενημέρωση των υποκειμένων και των υπευθύνων επεξεργασίας προσωπικών δεδομένων σε σχέση με τα δικαιώματα και τις υποχρεώσεις τους, η ΑΠΔΠΧ:

1. Ετησίως συντάσσει έκθεση για την εκτέλεση της αποστολής της, κατά το περασμένο έτος.

2. Γνωστοποιεί στην Βουλή παραβάσεις των ρυθμίσεων.
3. Συνεργάζεται με τις ΑΠΔΠΧ άλλων κρατών-μελών της ΕΕ σχετικά με την εκτέλεση των καθηκόντων της.

Παραδείγματα κανονιστικών πράξεων της ΑΠΔΠΧ είναι οι: 408/1998 (ενημέρωση των υποκειμένων επεξεργασίας προσωπικών δεδομένων δια του Τύπου), Γ/ΕΞ/6220-13/07/2018 (Ενημέρωση για τον χειρισμό παλαιών υποθέσεων). (ΑΠΔΠΧ, 2018e).

3.2.2.3. Νόμος 3471/06

Ο Ν.3471/06 (Προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες και τροποποίηση του ν. 2472/97), ενσωματώνει στην ελληνικό δίκαιο την οδηγία 2002/58/ΕΚ, η οποία αναφέρεται στην §2.1.5 του παρόντος. Σκοπός του συγκεκριμένου νόμου (άρθρα 1 έως 17) είναι να προστατεύσει τα θεμελιώδη δικαιώματα και κυρίως την ιδιωτική ζωή του ατόμου, να θεσπίσει προϋποθέσεις για την προστασία των δεδομένων του και να διασφαλίσει το απόρρητο των επικοινωνιών σχετικά με τις ηλεκτρονικές επικοινωνίες. (Βουλή των Ελλήνων, 2006).

Ο Ν.3471/06, που κατοχυρώνει τα δικαιώματα των συνδρομητών τηλεπικοινωνιών, μαζί με τον Ν.3917/2011 που αφορά την διατήρηση δεδομένων που παράγονται ή τίθενται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων προς το κοινό υπηρεσιών ηλεκτρονικών ή δημοσίου δικαίου επικοινωνιών, συμπλήρωσαν με τις ρυθμίσεις τους, εκείνες του Ν.2472/97. (Βουλή των Ελλήνων, 2006).

Στο άρθρο 2 εμφανίζονται οι έννοιες και οι ορισμοί συνδρομητής, χρήστης, δεδομένα κίνησης, δεδομένα θέσης, επικοινωνία, υπηρεσία προστιθέμενης αξίας, ηλεκτρονικό ταχυδρομείο, υπηρεσίες ηλεκτρονικών επικοινωνιών, δημόσιο δίκτυο επικοινωνιών, διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών και παραβίαση δεδομένων προσωπικού χαρακτήρα. Κάποιοι από αυτούς τους ορισμούς αποτελούν αποτέλεσμα αντικατάστασης ή τροποποίησης, που προήλθε μέσα από το άρθρο 168, του Ν.4070/2012.

Ο συγκεκριμένος νόμος, μεταξύ άλλων διατάξεων, περιλαμβάνει άρθρα σχετικά με το απόρρητο των επικοινωνιών, τα δεδομένα κίνησης και θέσης, την αναλυτική χρέωση, την αυτόματη προώθηση κλήσεων και τους καταλόγους συνδρομητών. (Βουλή των Ελλήνων, 2006).

Ιδιαίτερη μνεία αξίζει να γίνει στο άρθρο 11 το οποίο αφορά την μη ζητηθείσα επικοινωνία. Ως μη ζητηθείσα επικοινωνία ορίζεται η πραγματοποίηση επικοινωνίας με ή και χωρίς ανθρώπινη παρέμβαση, με σκοπό την απευθείας προώθηση προϊόντων και υπηρεσιών για εμπορικούς ή άλλου είδους σκοπούς, χωρίς ρητή συγκατάθεση του ατόμου που λαμβάνει την επικοινωνία. (Βουλή των Ελλήνων, 2006).

Το άρθρο 11, μέχρι την διαγραφή του «ή με» που βρίσκεται στην πρώτη παράγραφο του, δεν επέτρεπε κανενός είδους ηλεκτρονική επικοινωνία (αυτοματοποιημένη ή μη), χωρίς την συγκατάθεση του ατόμου. Η διαγραφή του «ή με» πραγματοποιήθηκε με το άρθρο 16 του Ν. 3917/2011. Μετά την διαγραφή του «ή με», επιτρέπεται η χρησιμοποίηση αυτοματοποιημένων συστημάτων κλήσης (π.χ. φαξ), μόνο με ρητή συγκατάθεση, ενώ μη αυτοματοποιημένη επικοινωνία (π.χ. τηλεφωνικές κλήσεις), απαγορεύονται μόνο αν ο συνδρομητής έχει δηλώσει προς τον καλούντα φορέα, πως δεν επιθυμεί να δέχεται κλήσεις. (Βουλή των Ελλήνων, 2006).

Η επαφή μέσω ηλεκτρονικού ταχυδρομείου, εφόσον τα στοιχεία αποκτήθηκαν με νόμιμο τρόπο, δεν απαιτεί πρότερη συγκατάθεση, υπό την προϋπόθεση να παρέχεται η επιλογή απεγγραφής από την υπηρεσία με τρόπο δωρεάν, σαφή και ευδιάκριτο. Επίσης, η επαφή μέσω ηλεκτρονικού ταχυδρομείου, απαιτεί να είναι ευδιάκριτη και σαφής η ταυτότητα του αποστολέα, με μέρος της ευθύνης να βαραίνει τους παρόχους ηλεκτρονικού ταχυδρομείου, ώστε να αποφευχθεί μη ζητηθείσα επικοινωνία. (Βουλή των Ελλήνων, 2006).

Ως ελεγκτικά όργανα από τον νόμο αυτός ορίζονται η ΑΠΔΠΧ και η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ). Οι αρμοδιότητες της ΑΠΔΠΧ ορίζονται αναλυτικά στον Ν. 2472/1997, ενώ της ΑΔΑΕ στον Ν. 3115/2003.

Τροποποιήσεις του Ν. 3471/2006

- ΦΕΚ 889/Β/19.5.2011 «Οδηγία 2/2011 Ηλεκτρονική συγκατάθεση στα πλαίσια του άρθρου 11 του Ν.3471/2006», (ΑΠΔΠΧ, 2011).
- Ν.4070/2012 «Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων, και άλλες διατάξεις», (Βουλή των Ελλήνων, 2012).
- Ν. 3917/2011 « Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών, χρήση συστημάτων

επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις», (Βουλή των Ελλήνων, 2011a).

3.3. Εθνικές νομοθεσίες άλλων χωρών (πριν τους ΕΚ 2016/679 και Ευρ. Οδηγίας 2016/680)

Μεγάλη Βρετανία: Στην Μεγ. Βρετανία, λόγω μη ύπαρξης Συντάγματος, τα προσωπικά δεδομένα προστατεύονται μέσω του Νόμου 1998 (Data Protection Act, 1998). (TSO, 1998).

Γερμανία: Στην Γερμανία, η πρώτη απόπειρα για νομοθετική κατοχύρωση της προστασίας προσωπικών δεδομένων, γίνεται το 1970 μέσω νόμου από το κρατίδιο της Hessen. Μέχρι και την θέσπιση του Ν. 2016/679, εφαρμοζόταν η οδηγία 95/46/ΕΚ. Ομοίως συνέβαινε σε Ελβετία, Αυστρία και Κάτω Χώρες. (Ευρωπαϊκό Κοινοβούλιο, 1995).

Σουηδία:Η Σουηδία, ξεχωρίζει ανάμεσα στις υπόλοιπες χώρες, καθώς, στο Σύνταγμα του 1975, περιλαμβάνει διατάξεις για την προστασία των προσωπικών δεδομένων. (Καραγιαννίδου Χ., χ.χ.).

Γαλλία: Το γαλλικό Σύνταγμα δεν περιέχει διατάξεις σχετικές με την προστασία προσωπικών δεδομένων, όμως η Γαλλία είχε θεσπίσει σχετικούς νόμους (Νόμος 78-17, 6/1/1978). (Legifrance, 1978).

4. ΚΑΝΟΝΙΣΜΟΣ ΕΕ 2016/679 – GENERAL DATA PROTECTION REGULATION (GDPR)

Ο GDPR τέθηκε σε ισχύ, αρχικά, στις 24 Μαΐου 2016 και εφαρμόστηκε, υποχρεωτικά, στις 25 Μαΐου 2018. Από εκείνη την ημερομηνία και μετά θα πρέπει κάθε υπεύθυνος επεξεργασίας προσωπικών δεδομένων να συμμορφώνεται στον συγκεκριμένο Κανονισμό της ΕΕ.

Στόχος του GDPR, σύμφωνα με το άρθρο 1, είναι η προστασία φυσικών προσώπων σε σχέση με την επεξεργασία των προσωπικών τους δεδομένων και την ελεύθερη διακίνηση αυτών και η προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων. (Ευρωπαϊκή Ένωση, 2016a).

Με την θέσπιση του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR), γίνεται προσπάθεια για κάλυψη διαφόρων νομικών ασαφειών που υπήρχαν από προηγούμενες νομοθετικές διατάξεις, με αποτέλεσμα να δημιουργείται ανασφάλεια σχετικά με την προστασία των δικαιωμάτων των φυσικών προσώπων.

4.1. Ορισμοί

Εκτός από τους ορισμούς που εξηγούνται στο Κεφάλαιο 1 της παρούσας, στο άρθρο 4 του νέου Κανονισμού αναλύονται και κάποιες επιπλέον έννοιες, που θα αναφερθούν παρακάτω. Μερικές από αυτές είναι οι, (Ευρωπαϊκή Ένωση, 2016b):

- **«Ψευδωνυμοποίηση»**: Αφορά την επεξεργασία προσωπικών δεδομένων, που γίνεται με τέτοιο τρόπο, όπου τα δεδομένα δεν μπορούν να ταυτοποιηθούν με συγκεκριμένο υποκείμενο, χωρίς να γίνεται χρήση επιπλέον πληροφοριών, οι οποίες πληροφορίες διατηρούνται σε διαφορετικό σημείο και για τις οποίες έχουν παρθεί μέτρα που δεν επιτρέπουν την ταυτοποίηση τους με συγκεκριμένο φυσικό πρόσωπο.Η ψευδωνυμοποίηση βοηθά στην μείωση της δυνατότητας σύνδεσης των δεδομένων προσωπικού χαρακτήρα με το υποκείμενο επεξεργασίας.
- **«Δεδομένα που αφορούν την υγεία»:** Πρόκειται για προσωπικά δεδομένα που αφορούν την κατάσταση της φυσικής ή ψυχικής υγείας του φυσικού προσώπου, περιλαμβάνοντας την παροχή υπηρεσιών υγείας και τα οποία αποκαλύπτουν στοιχεία για την κατάσταση της υγείας τους.

- **«Βιομετρικά δεδομένα»:** Πρόκειται για δεδομένα προσωπικού χαρακτήρα που συνδέονται που μπορεί να προκύψουν από ειδική επεξεργασία που συνδέεται με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά του φυσικού προσώπου και τα οποία μπορούν να επιβεβαιώσουν αδιαμφισβήτητα την ταυτοποίηση με το φυσικό πρόσωπο (π.χ. φωτογραφία προσώπου).
- **«Γενετικά δεδομένα»:**Αφορά χαρακτηριστικά του φυσικού προσώπου που είτε κληρονομήθηκαν (γενετικά), είτε αποκτήθηκαν και τα οποία αποκαλύπτουν στοιχεία σχετικά με την φυσιολογία ή την υγεία του ατόμου.
- **«Παραβίαση δεδομένων προσωπικού χαρακτήρα»:** Πρόκειται για την παραβίαση (τυχαία ή σκοπίμως), των συστημάτων ασφαλείας με αποτέλεσμα την πρόσβαση και ως εκ τούτου την δυνατότητα έκθεσης των δεδομένων σε καταστροφή, απώλεια, μεταβολή, διαγραφή ή κοινολόγηση χωρίς συγκατάθεση.
- **«Περιορισμός της επεξεργασίας»:** Η επισήμανση αποθηκευμένων προσωπικών δεδομένων, με σκοπό τον περιορισμό μελλοντικής επεξεργασίας τους.
- **«Σύστημα αρχειοθέτησης»:** Πρόκειται για σύνολο προσωπικών δεδομένων, στα οποία υπάρχει πρόσβαση μέσω συγκεκριμένων κριτηρίων, τα οποία είναι είτε συγκεντρωμένα σε ένα σημείο, είτε αποκεντρωμένα, είτε κατανεμημένα σε λειτουργική ή γεωγραφική βάση.
- **«Δεσμευτικοί εταιρικοί κανόνες»:** Πρόκειται για την πολιτική προστασίας προσωπικών δεδομένων, σύμφωνα με την οποία λειτουργεί ο εκάστοτε υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία. Ο υπεύθυνος ή ο εκτελών επεξεργασία βρίσκεται εγκατεστημένος εντός της ΕΕ και πραγματοποιεί διαβιβάσεις ή σύνολο διαβιβάσεων προσωπικών δεδομένων σε αντίστοιχο υπεύθυνο ή εκτελούνται επεξεργασία σε μία ή επιπλέον χώρες του ομίλου επιχειρήσεων που ανήκει ή που συνεργάζεται ως προς την οικονομική δραστηριότητα.
- **«Εποπτική Αρχή»:** Πρόκειται για ανεξάρτητη δημόσια αρχή, η οποία θεσπίζεται σε κάθε Κράτος Μέλος της ΕΕ και έχει ως κύρια δραστηριότητα την επόπτευση της εφαρμογής του Κανονισμού GDPR (Ευρωπαϊκή Ένωση, 2016c).
- **«Ενδιαφερόμενη Εποπτική Αρχή»:** Πρόκειται για εποπτική αρχή την οποία αφορά η επεξεργασία των δεδομένων καθώς είτε ο υπεύθυνος επεξεργασίας βρίσκεται εγκατεστημένος στο έδαφος ευθύνης της, είτε το υποκείμενο των δεδομένων αυτών διαμένει στο έδαφος ευθύνης της, είτε έχει προηγηθεί καταγγελία στην συγκεκριμένη εποπτική αρχή.

4.2. Τι είναι το GDPR και που εφαρμόζεται

Η Ευρωπαϊκή Ένωση, στην προσπάθεια της να καλύψει προβλήματα που δεν καλύπτονται από την οδηγία 95/46/ΕΚ, θέσπισε τον Κανονισμό 2016/679 (έναρξη 25/05/2018), γνωστό και ως GDPR, που αποτελεί την μεγαλύτερη αλλαγή νομοθεσίας τα τελευταία 20 έτη στην Ευρωπαϊκή Ένωση.Στις διατάξεις του, έχουν ληφθεί υπόψη οι τεχνολογικές, κοινωνικές, οικονομικές και πολιτικές αλλαγές. Το GDPR, ουσιαστικά, ρυθμίζει την επεξεργασία (αυτοματοποιημένη ή μη) δεδομένων προσωπικού χαρακτήρα από φυσικό ή νομικό πρόσωπο, για φυσικά πρόσωπα που βρίσκονται εντός Ευρωπαϊκής Ένωσης, χωρίς να περιλαμβάνει τα προσωπικά δεδομένων αποθανόντων και νομικών προσώπων. (Ευρωπαϊκή Ένωση, 2016d, Ευρωπαϊκή Ένωση, 2016e).

Ο κανονισμός, δεν αφορά επεξεργασία δεδομένων για προσωπική χρήση που δεν συνδέεται με εμπορικής ή επαγγελματική δραστηριότητα. (Ευρωπαϊκή Ένωση, 2016d).

Το GDPR, απευθύνεται τόσο στον ιδιωτικό, όσο και στον δημόσιο τομέα, περιλαμβάνοντας επιχειρήσεις, κρατικούς φορείς, συλλόγους, οργανισμούς, κτλ που σχετίζονται με κάποιο τρόπο με προσωπικά δεδομένα φυσικών προσώπων (μέσω της επεξεργασίας, συλλογής και αποθήκευσης ή και διακίνησης τους). Η έδρα των οποίων δεν περιορίζεται εντός της Ευρωπαϊκής Ένωσης απαραίτητα. Κριτήριο αποτελεί η έδρα του φυσικού προσώπου που γίνεται αντικείμενο της επεξεργασίας και όχι του υποκειμένου. (Ευρωπαϊκή Ένωση, 2016f, Ευρωπαϊκή Ένωση, 2016g).

Ο Κανονισμός εφαρμόζεται στην Ευρωπαϊκή Ένωση, στο Λιχτενστάιν, στην Ιρλανδία και στην Νορβηγία. Επίσης, δεν αφορά υπευθύνους επεξεργασίας που είναι υποχρεωτικά εγκατεστημένοι στην ΕΕ, αλλά και εκτός ΕΕ, αν οι υπηρεσίες και τα αγαθά που παρέχουν ή τα υποκείμενα επεξεργασίας τους, βρίσκονται εντός ΕΕ. (Gazzetta team, 2018).

Μεταξύ άλλων παραγόντων, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της ΕΕ, δημιούργησαν τον Κανονισμό 2016/679, αναγνωρίζοντας την προστασία των προσωπικών δεδομένων, πρώτον, ως θεμελιώδες δικαίωμα, όπως αναφέρεται και στον Χάρτη των θεμελιωδών δικαιωμάτων της ΕΕ, αλλά λαμβάνοντας, επίσης, υπόψη, την κοινωνικοοικονομική ολοκλήρωση, που προέκυψε από την λειτουργία της εσωτερικής αγοράς. Η λειτουργία, αυτή, οδήγησε στην αύξηση της ροής προσωπικών δεδομένων με

διασυνοριακό χαρακτήρα. Τέλος, δεν αγνοήθηκε, η ραγδαία τεχνολογική εξέλιξη και η παγκοσμιοποίηση. (Ευρωπαϊκή Ένωση, 2016g).

Τα κράτη μέλη, εάν το επιθυμούν, μπορούν να ενσωματώσουν με εθνική διάταξη, τον Κανονισμό, στο εθνικό τους δίκαιο. Σκοπός αυτής της δυνατότητας είναι η κατανόηση των όσων ορίζονται στον Κανονισμό, από τα πρόσωπα που αφορά. (Ευρωπαϊκή Ένωση, 201i).

4.2.1. Σημαντικές αλλαγές που προκύπτουν από το GDPR

Ο Κανονισμός, με την θέσπιση του επιφέρει σημαντικές αλλαγές, σε σχέση με τις προηγούμενες νομοθεσίες που ίσχυαν. Τα πεδία που επηρεάζονται αφορούν κυρίως τα δικαιώματα των φυσικών προσώπων, τα δεδομένα των οποίων τίθενται σε επεξεργασία. Σε επόμενη παράγραφο αναλύονται τα δικαιώματα των φυσικών προσώπων, τα οποία είναι σαφώς αυξημένα πλέον. Ενισχύεται η προστασία των δεδομένων των παιδιών, καθώς ορίζεται αυστηρότερο πλαίσιο για την συγκατάθεση για επεξεργασία των δεδομένων τους, με τα παιδιά να τοποθετούνται σε μία νέα κατηγορία που ονομάζεται «ευάλωτα φυσικά πρόσωπα». Γίνεται υποχρεωτική η γνωστοποίηση της παραβίασης των δεδομένων, αναγκάζοντας τον υπεύθυνο επεξεργασίας να ενημερώσει την αρμόδιο Αρχή, εντός συγκεκριμένου χρονικού ορίου, όπως αναλύεται σε επόμενη παράγραφο. Η συγκατάθεση από την πλευρά του υποκειμένου γίνεται υπό αυστηρότερες προϋποθέσεις, καθώς πλέον πρέπει να είναι ρητή και αποδεδειγμένα, πλήρως κατανοητή από την πλευρά του υποκειμένου που συναινεί. Με το GDPR, κάθε υπεύθυνος επεξεργασίας οφείλει να τηρεί αρχείο των δραστηριοτήτων ευθύνης του. Τέλος, με την θέσπιση του GDPR, ορίζεται η θέση του Υπευθύνου Προστασίας Δεδομένων – Data Protection Officer. (Ευρωπαϊκή Ένωση, 2016j)

Μέσω του Κανονισμού GDPR, καταργείται η οδηγία 95/46/ΕΚ, κάνει σαφή την σχέση του με την οδηγία 2002/58/ΕΚ. (Ευρωπαϊκή Ένωση, 2016j)

4.3. Συγκατάθεση φυσικού προσώπου

Η συγκατάθεση αποτελεί την μία εκ των 6 νόμιμων βάσεων για σύννομη επεξεργασία δεδομένων προσωπικού χαρακτήρα, σύμφωνα με το άρθρο 6 του Κανονισμού 2016/679. (Lawspot, 2018).

Η συγκατάθεση του φυσικού προσώπου για επεξεργασία των προσωπικών του δεδομένων, θα πρέπει να δίνεται ελεύθερα, να είναι συγκεκριμένη, ρητή και με πλήρη επίγνωση. Παραδείγματα μεθόδων συγκατάθεσης αποτελούν τα: ένα τετραγωνίδιο με δυνατότητα συμπλήρωσης σε μία ιστοσελίδα, η υπογεγραμμένη δήλωση του φυσικού προσώπου σε

γραπτή ενημέρωση σχετικά με την αποδοχή της πρότασης για επεξεργασία των προσωπικών του δεδομένων.

Η συγκατάθεση που παρέχει το φυσικό πρόσωπο θα πρέπει να καλύπτει όλους τους σκοπούς για τους οποίους συγκατατίθεται και όχι μέρος αυτών. Εξαίρεση αποτελεί η συγκατάθεση για σκοπούς επιστημονικής έρευνας, καθώς μπορεί τα υποκείμενα να συγκαταθέσουν για μέρος των σκοπών που θα χρησιμοποιηθούν τα προσωπικά τους δεδομένα, με την προϋπόθεση ότι ακολουθούνται όλα τα αναγνωρισμένα πρότυπα δεοντολογίας. (Ευρωπαϊκή Ένωση, 2016m, Ευρωπαϊκή Ένωση, 2016n).

Γίνεται σαφές ότι, προσυμπληρωμένα πεδία και ελλιπής ή καθόλου ενημέρωση, δεν μπορούν να ληφθούν ως συγκατάθεση του φυσικού προσώπου.

Τα φυσικά πρόσωπα θα πρέπει να ενημερώνονται σε γλώσσα απλή, σαφή και κατανοητή, ώστε να διασφαλίζεται ότι κατανοούν πλήρως τους λόγους και τους σκοπούς για τους οποίους συλλέγονται, χρησιμοποιούνται ή υποβάλλονται σε οποιουδήποτε είδους επεξεργασία, τα προσωπικά τους δεδομένα. Η ενημέρωση αυτή, προς τα φυσικά πρόσωπα, θα πρέπει να περιλαμβάνει τους πιθανούς κινδύνους, τους κανόνες, τις εγγυήσεις και τα δικαιώματα σε σχέση με την επεξεργασία των προσωπικών τους δεδομένων, αλλά και τον τρόπο με τον οποίο μπορούν να ασκήσουν τα δικαιώματα αυτά. Τονίζεται ότι τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να είναι τα απολύτως αναγκαία που απαιτούνται για την εξυπηρέτηση του σκοπού που προορίζονται και όχι περισσότερα. Επίσης, θα πρέπει ο υπεύθυνος επεξεργασίας, να ορίζει συγκεκριμένες προθεσμίες για την διαγραφή ή τον επαναπροσδιορισμό του διαστήματος διατήρησης τους. (Ευρωπαϊκή Ένωση, 2016m, Ευρωπαϊκή Ένωση, 2016n).

Η συγκατάθεση του υποκειμένου των προσωπικών δεδομένων, θα πρέπει να αποδεικνύεται, ότι έχει δοθεί ελεύθερα. Μπορεί να θεωρηθεί ότι δεν έχει δοθεί ελεύθερα, όταν δεν δίνεται η επιλογή, στο υποκείμενο, να παρέχει συγκαταθέσεις για διαφορετικές πράξεις της επεξεργασίας των δεδομένων.

Οι προϋποθέσεις για συγκατάθεση αναλύονται στα άρθρο 7 και 8 του παρόντος Κανονισμού. Σύμφωνα με το άρθρο 7, όταν η επεξεργασία των δεδομένων πραγματοποιείται με συγκατάθεση του υποκειμένου, θα πρέπει ο υπεύθυνος επεξεργασίας να είναι σε θέση να το αποδείξει. Όταν η γραπτή η δήλωση του υποκειμένου, περιλαμβάνει και άλλα θέματα, εκτός από την συγκατάθεση για επεξεργασία δεδομένων προσωπικού χαρακτήρα, τότε θα πρέπει το

μέρος που αφορά την συγκατάθεση να είναι διακριτό με σαφήνεια, σε σχέση με τα υπόλοιπα θέματα που περιλαμβάνονται στην δήλωση. Επίσης, η ανάκληση της συγκατάθεσης για επεξεργασία, θα πρέπει να γίνεται με εξίσου εύκολο τρόπο, όπως και η συγκατάθεση. Στο άρθρο θίγεται και η εκτίμηση για το κατά πόσο η αναφερόμενη συγκατάθεση δίδεται με απόλυτη ελευθερία ή όχι. (Ευρωπαϊκή Ένωση, 2016k, Ευρωπαϊκή Ένωση, 2016l).

Συμπληρωματικά στα ανωτέρω, το άρθρο 8, θίγει τις προϋποθέσεις που ισχύουν όσον αφορά την συγκατάθεση παιδιού, ως προς τις υπηρεσίες πληροφορικής. Ένα παιδί μπορεί να συναινέσει, από την ηλικία των 16 (με δυνατότητα να ισχύει από την ηλικία των 13, με εθνική νομοθεσία, από τα κράτη – μέλη), ενώ για ηλικία μικρότερη των 16, η επεξεργασία θεωρείται σύννομη, όταν παρέχεται συγκατάθεση από το φυσικό πρόσωπο που έχει υπό την γονική του μέριμνα το παιδί. (Ευρωπαϊκή Ένωση, 2016k, Ευρωπαϊκή Ένωση, 2016l).

Στις περιπτώσεις συγκατάθεσης που αφορούν παιδιά, ο υπεύθυνος επεξεργασίας, θα πρέπει να καταβάλει σημαντική προσπάθεια, ώστε να διασφαλίσει ότι η συγκατάθεση προκύπτει από το φυσικό πρόσωπο όπως ορίζεται στο άρθρο 8.

4.3.1. Επεξεργασία δεδομένων ειδικών κατηγοριών

Υπάρχουν δεδομένα τα οποία είναι εκ φύσεως ευαίσθητα σχετικά με τα θεμελιώδη δικαιώματα του ατόμου και τις ελευθερίες. Αυτά τα δεδομένα έχουν ανάγκη από ειδική προστασία, ώστε να μην υπάρξει σύγκρουση, κατά την επεξεργασία τους, με τα θεμελιώδη δικαιώματα και τις ελευθερίες του υποκειμένου. Τέτοια δεδομένα περιλαμβάνουν στοιχεία που αποκαλύπτουν καταγωγή (φυλετική ή εθνοτική), πολιτικές, θρησκευτικές, φιλοσοφικές πεποιθήσεις, συμμετοχή σε συνδικαλιστική οργάνωση, γενετικά ή βιομετρικά δεδομένα, δεδομένα που αφορούν την σεξουαλική ζωή του υποκειμένου ή τον γενετήσιο προσανατολισμό του. Η επεξεργασία φωτογραφιών, δεν περιλαμβάνεται πάντοτε σε αυτή την κατηγορία δεδομένων. (Ευρωπαϊκή Ένωση, 2016o, Ευρωπαϊκή Ένωση, 2016p).

Τα δεδομένα ειδικών κατηγοριών, δεν θα πρέπει να υπόκεινται σε επεξεργασία, με εξαίρεση περιπτώσεις που προβλέπονται μέσω του Κανονισμού 2016/679. Για παράδειγμα, επιτρέπεται η επεξεργασία τέτοιων δεδομένων όταν προβλέπεται από το δίκαιο της ΕΕ ή του κράτους – μέλους και περιλαμβάνει τις κατάλληλες προϋποθέσεις και εγγυήσεις για την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών του υποκειμένου επεξεργασίας. Η επεξεργασία τέτοιων δεδομένων, επιτρέπεται όταν το φυσικό πρόσωπο έχει δώσει ρητή συγκατάθεση, εκτός αν το δίκαιο της ΕΕ ή του κράτους – μέλους, προβλέπει ότι η απαγόρευση επεξεργασίας δεν μπορεί να αναιρεθεί ούτε από το ίδιο το υποκείμενο. Στο άρθρο 9 του

Κανονισμού, εκτός από την άρση της απαγόρευσης με ρητή συγκατάθεση του υποκειμένου, παρουσιάζονται συνολικά άλλες εννέα περιπτώσεις κατά τις οποίες η απαγόρευση της επεξεργασίας των προσωπικών δεδομένων που ανήκουν στην ειδική κατηγορία, μπορεί να αρθεί. (Ευρωπαϊκή Ένωση, 2016ο, Ευρωπαϊκή Ένωση, 2016ρ).

Δύο από αυτές αφορούν τον τομέα την υγείας:

1. Όταν η επεξεργασία των δεδομένων είναι απαραίτητη για την εξυπηρέτηση σκοπών που αφορούν προληπτική ή επαγγελματική Ιατρική, εκτίμηση της ικανότητας εργαζομένου να εργαστεί, ιατρική διάγνωσης, δυνατότητα παροχής περίθαλψης, θεραπείας ή για την διαχείριση συστημάτων και υπηρεσιών, κοινωνικών και υγειονομικών.
2. Όταν η επεξεργασία καθίσταται απαραίτητη για την διαφύλαξη τη δημόσιας υγείας.

Τα δεδομένα ειδικών κατηγοριών που έχουν ανάγκη από υψηλότερη προστασία κατά την υποβολή τους σε επεξεργασία, είναι αυτά που προορίζονται για σκοπούς σχετικούς με την υγεία. Ειδικότερα, όταν οι συγκεκριμένοι σκοποί θα έχουν όφελος ως προς το υποκείμενο της επεξεργασίας και την κοινωνία γενικότερα. Το δίκαιο της ΕΕ και των κρατών – μελών, θα πρέπει να έχει προβλέψει, ώστε να προστατεύονται τα θεμελιώδη δικαιώματα και οι ελευθερίες των ατόμων, μέσω κατάλληλων μέτρων, όπως αναφέρεται και σε προηγούμενη παράγραφο. (Ευρωπαϊκή Ένωση, 2016οΕυρωπαϊκή Ένωση, 2016ρ).

Τονίζεται ότι, η επεξεργασία προσωπικών δεδομένων ειδικών κατηγοριών, μπορεί να υφίσταται ακόμη και χωρίς την συναίνεση του φυσικού προσώπου στο οποίο ανήκουν τα δεδομένα. Αυτό μπορεί να συμβεί σε περιπτώσεις που πρόκειται για λόγους δημοσίου συμφέροντος σε τομέα της δημόσιας υγείας. Και σε αυτή την περίπτωση δεν θα πρέπει να παραβλέπεται η αναγκαία ύπαρξη κατάλληλων μέτρων, ώστε να διασφαλίζεται η προστασία των δικαιωμάτων και των ελευθεριών των υποκειμένων επεξεργασίας. Επομένως, αυτή η επεξεργασία δεν θα πρέπει σε καμία περίπτωση να οδηγεί σε επεξεργασία των δεδομένων για διαφορετικούς σκοπούς από τρίτους (π.χ. ασφαλιστικές εταιρείες, εργοδότες, κτλ). (Ευρωπαϊκή Ένωση, 2016ο, Ευρωπαϊκή Ένωση, 2016ρ).

Ως λόγους δημοσίου συμφέροντος, ο Κανονισμός αναγνωρίζει, επίσης, την επεξεργασία προσωπικών δεδομένων σχετικά με πολιτικές πεποιθήσεις, από πολιτικά κόμματα, στα πλαίσια εκλογικών δραστηριοτήτων.

4.4. Αρχές της επεξεργασίας προσωπικών δεδομένων

Σύμφωνα με το άρθρο 5 του Κανονισμού 2016/679, η υποβολή των προσωπικών δεδομένων σε σύννομη και θεμιτή επεξεργασία, γίνεται με απόλυτη διαφάνεια ως προς το υποκείμενο της επεξεργασίας. Η συλλογή τους γίνεται για καθορισμένους, ρητούς και νόμιμους σκοπούς. Τα δεδομένα προσωπικού χαρακτήρα, που χρησιμοποιούνται, είναι τα ελάχιστα απαραίτητα , είναι κατάλληλα και συναφή με τον σκοπό επεξεργασίας για τον οποίο προορίζονται. Για το διάστημα επεξεργασίας τους, παραμένουν σε μορφή ταυτοποιήσιμη ως προς το υποκείμενο επεξεργασίας και τέλος, η επεξεργασία στην οποία υποβάλλονται, πραγματοποιείται με τρόπο που διασφαλίζει την προστασία τους από παράνομη ή χωρίς συγκατάθεση επεξεργασία τους ή ακόμη και από απώλεια τους. (Ευρωπαϊκή Ένωση, 2016q, Lawspot, 2018).

Συνοπτικά, τα ανωτέρω παρουσιάζονται στο άρθρο 5, παράγραφο 1, ως εξής:

1. «Νομιμότητα, αντικειμενικότητα και διαφάνεια»
2. «Περιορισμός του σκοπού»
3. «Ελαχιστοποίηση των δεδομένων»
4. «Ακρίβεια»
5. «Περιορισμός της περιόδου αποθήκευσης»
6. «Ακεραιότητα και εμπιστευτικότητα»

Στην παράγραφο 2 του ιδίου άρθρου, καλείται ο υπεύθυνος επεξεργασίας να μπορεί να αποδείξει ότι τα προσωπικά δεδομένα που επεξεργάζεται, τα επεξεργάζεται με διαφάνεια ως προς το φυσικό πρόσωπο που αφορούν («λογοδοσία»). (Ευρωπαϊκή Ένωση, 2016q).

Στο άρθρο 12, του Κανονισμού, γίνεται εκτενέστερη αναφορά, ως προς την διαφάνεια και τα στάδια της επεξεργασίας των προσωπικών δεδομένων, στα οποία εφαρμόζεται. Συγκεκριμένα, θα πρέπει πριν από την έναρξη της συλλογής ή επεξεργασίας των προσωπικών δεδομένων και κατά την διάρκεια, να παρέχονται τα κατάλληλα μέσα από τον υπεύθυνο επεξεργασίας ώστε το υποκείμενο επεξεργασίας να γνωρίζει μέσα από συνοπτική, διαφανή, κατανοητή, εύκολα πρόσβάσιμη, απλή και σαφή περιγραφή, πληροφορίες όπως αναφέρονται στα άρθρα 13 - 14 και ρυθμίσεις της άσκησης των δικαιωμάτων του υποκειμένου, όπως αναφέρονται στα άρθρα 15 έως 22. Δίνεται ιδιαίτερη σημασία στην απαίτηση για απλή και σαφή περιγραφή, όταν απευθύνεται σε παιδιά. Οι πληροφορίες θα πρέπει να δίνονται γραπτώς ή ηλεκτρονικώς, εφόσον ενδείκνυται, εκτός κι αν ζητηθεί από το υποκείμενο να

δοθούν προφορικά. Τέλος, η παροχή πληροφοριών, σύμφωνα με την παράγραφο 5 του άρθρου, γίνεται δωρεάν. (Ευρωπαϊκή Ένωση, 2016r).

Στον Κανονισμό 2016/679, δεν δίνεται σαφής ορισμός για την διαφάνεια, όμως στην αιτιολογική παράγραφο 39, δίνονται πληροφορίες που μπορούν να θεωρηθούν σχετικές με την έννοια της. Στην συγκεκριμένη παράγραφο, αναφέρεται η αναγκαιότητα για σαφήνεια ως προς το υποκείμενο επεξεργασίας σχετικά με τα προσωπικά του δεδομένα, τους σκοπούς συλλογής, χρήσης, επεξεργασίας, μέσα από απλή και κατανοητή γλώσσα. (Ευρωπαϊκή Ένωση, 2016r).

4.5. Κριτήρια νομιμότητας της επεξεργασίας προσωπικών δεδομένων

Ο Κανονισμός 2016/679, μέσω του άρθρου 6, ορίζει έξι νόμιμες βάσεις, σύμφωνα με τις οποίες η επεξεργασία των δεδομένων προσωπικού χαρακτήρα έχει σύννομο χαρακτήρα, όταν ισχύει τουλάχιστον μία εκ των έξι. (Ευρωπαϊκή Ένωση, 2016n).

Οι βάσεις αυτές είναι:

1. Το φυσικό πρόσωπο έχει συναινέσει για έναν ή περισσότερους σκοπούς.
2. Η επεξεργασία είναι απαραίτητη για να μπορέσει να εκτελεστεί σύμβαση ή για σύναψη σύμβασης, στην οποία το φυσικό πρόσωπο που αφορούν τα δεδομένα, αποτελεί συμβαλλόμενο μέρος.
3. Η επεξεργασία σχετίζεται με υποχρέωση από τον νόμο, για τον υπεύθυνο επεξεργασίας.
4. Η επεξεργασία είναι ζωτικής σημασίας για το υποκείμενο της επεξεργασίας ή άλλο πρόσωπο.
5. Η επεξεργασία καθίσταται απαραίτητη για καθήκον που εκτελείται με σκοπό το δημόσιο συμφέρον.
6. Η επεξεργασία είναι απαραίτητη για την επίτευξη σκοπών με έννομο συμφέρον του υπευθύνου επεξεργασίας ή τρίτου. Εξαίρεση αποτελεί η υπερίσχυση του συμφέροντος και τα θεμελιώδη δικαιώματα και ελευθερίες του φυσικού προσώπου που αφορούν τα προσωπικά δεδομένα.

4.6. Ενημέρωση και πρόσβαση στα προσωπικά δεδομένα

Η πρόσβαση στα προσωπικά δεδομένα μπορεί να γίνει με δύο τρόπους. Ο ένας είναι, το ίδιο το υποκείμενο της επεξεργασίας, να παρέχει τα απαιτούμενα δεδομένα, στον υπεύθυνο

επεξεργασίας. Ο δεύτερος είναι, τα δεδομένα να μην ληφθούν από το ίδιο το φυσικό πρόσωπο. (Ευρωπαϊκή Ένωση, 2016r).

Ο υπεύθυνος επεξεργασίας σε κάθε περίπτωση, θα πρέπει να παρέχει ορισμένες πληροφορίες προς το υποκείμενο. Ορισμένες από τις πληροφορίες που θα πρέπει να λαμβάνει το υποκείμενο επεξεργασίας από τον υπεύθυνο, για λόγους διασφάλισης θεμιτής και διάφανης επεξεργασίας, είναι:

- Στοιχεία επικοινωνίας και ταυτότητα του υπευθύνου επεξεργασίας
- Στοιχεία επικοινωνίας του υπευθύνου προστασίας των δεδομένων, όπου χρειάζεται
- Σε ορισμένες περιπτώσεις, τα έννομα συμφέροντα που επιδιώκονται από τον υπεύθυνο επεξεργασίας
- Τους αποδέκτες των προσωπικών δεδομένων, όταν υπάρχουν
- Όταν υπάρχει, την πρόθεση του υπευθύνου επεξεργασίας, να διαβιβάσει τα δεδομένα σε τρίτη χώρα ή διεθνή οργανισμό.
- Το διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα
- Την ύπαρξη του δικαιώματος για μεταβολή, διαγραφή ή διόρθωση των δεδομένων
- Την ύπαρξη δικαιώματος άρσης της συγκατάθεσης
- Το δικαίωμα καταγγελίας σε αρμόδια Αρχή
- Την ενημέρωση για το κατά πόσο η παροχή των δεδομένων αποτελεί νομική ή όχι υποχρέωση

4.7. Δικαιώματα υποκειμένου επεξεργασίας

Ο Κανονισμός 2016/679 (GDPR), ενισχύει τα δικαιώματα του υποκειμένου επεξεργασίας. Τα δικαιώματα που προκύπτουν από την ανάλυση του Κανονισμού είναι:

- **Δικαίωμα άρσης της ήδη δοθείσης συγκατάθεσης – Άρθρο 7**: Στην παράγραφο 3 του άρθρου 7, παρουσιάζεται το δικαίωμα του υποκειμένου, για ανάκληση της συγκατάθεσης του ανά πάσα στιγμή. Τονίζεται δε, ότι το υποκείμενο, πριν την παροχή της συγκατάθεσης, πρέπει να έχει ενημερωθεί σχετικά με το δικαίωμα αυτό. (Ευρωπαϊκή Ένωση, 2016k).
- **Δικαίωμα στην ενημέρωση – Άρθρο 12:** Ο υπεύθυνος επεξεργασίας υποχρεούται να παρέχει κατάλληλη και πλήρη ενημέρωση στο υποκείμενο της επεξεργασίας δωρεάν, καθώς και να απαντά σε αίτηση του εντός συγκεκριμένης προθεσμίας. (Ευρωπαϊκή Ένωση, 2016j).

- **Δικαίωμα πρόσβασης στα δικαιώματα προσωπικού χαρακτήρα – Άρθρο 15:** Το υποκείμενο της επεξεργασίας, εφόσον το επιθυμεί, έχει δικαίωμα πρόσβασης στους σκοπούς της επεξεργασίας των δεδομένων του, στις σχετικές κατηγορίες δεδομένων, στους αποδέκτες των δεδομένων του, στο χρονικό διάστημα διατήρησης των, στο δικαίωμα διόρθωσης ή διαγραφής των δεδομένων, στο δικαίωμα καταγγελίας σε αρμόδια Αρχή, κ.α. Ο υπεύθυνος επεξεργασίας θα πρέπει να παρέχει αντίγραφο των δεδομένων που επεξεργάζεται. Αν το υποκείμενο ζητήσει επιπλέον αντίγραφα ο υπεύθυνος έχει δικαίωμα να ζητήσει την καταβολή τέλους για τα έξοδα που προκύπτουν. (Ευρωπαϊκή Ένωση, 2016s).
- **Δικαίωμα διόρθωσης των δεδομένων – Άρθρο 16:** Το υποκείμενο έχει δικαίωμα να ζητήσει διόρθωση σε δεδομένα που το αφορούν και είναι ανακριβή. Η διόρθωση θα πρέπει να γίνει άμεσα και χωρίς αδικαιολόγητη καθυστέρηση. Εκτός από διόρθωση, μπορεί να ζητηθεί συμπλήρωση ελλιπών στοιχείων. (Ευρωπαϊκή Ένωση, 2016t).
- **Δικαίωμα διαγραφής των δεδομένων/«Δικαίωμα στη λήθη» - Άρθρο 17:** Το φυσικό πρόσωπο έχει δικαίωμα στην απαίτηση για διαγραφή των δεδομένων του, χωρίς αδικαιολόγητη καθυστέρηση, όταν:
    - Τα δεδομένα δεν είναι πλέον απαραίτητα για την εκπλήρωση των σκοπών για τους οποίους συλλέχθηκαν.
    - Το υποκείμενο ανακαλεί την συγκατάθεση του, όπως περιγράφεται στο άρθρο 6 ή το άρθρο 9 και δεν υπάρχει νομική υποχρέωση για την επεξεργασία.
    - Το υποκείμενο αντιτίθεται στην επεξεργασία (άρθρο 21).
    - Η επεξεργασία των δεδομένων έγινε παράνομα.
    - Πρέπει να διαγραφούν, ώστε να υπάρχει τήρηση νομικής υποχρέωσης.
    - Έχουν συλλεχθεί για παροχή υπηρεσιών πληροφορικής (άρθρο 8).

  Επίσης, όταν τα δεδομένα έχουν κοινοποιηθεί και σε τρίτους, θα πρέπει ο υπεύθυνος επεξεργασίας, χρησιμοποιώντας τα διαθέσιμα μέσα και τεχνολογία, να τους ενημερώσει, ότι το υποκείμενο επεξεργασίας έχει ζητήσει διαγραφή.

  Σημειώνεται ότι, δύναται να μην εφαρμοστούν τα ανωτέρω υπό προϋποθέσεις, που αναλύονται στο άρθρο 17 και δεν επιτρέπουν στους υπευθύνους επεξεργασίας, την διαγραφή. Για παράδειγμα, ένα Νοσοκομείο που παρέχει δευτεροβάθμιες υπηρεσίας υγείας, υποχρεούται να διατηρεί τον Ιατρικό Φάκελο Ασθενούς από Νοσηλεία, για 20 έτη. (Λασκαρίδης Ε., 2005, Ευρωπαϊκή Ένωση, 2016u).

- **Δικαίωμα περιορισμού της επεξεργασίας των δεδομένων – Άρθρο 18:** Το φυσικό πρόσωπο μπορεί να εξασφαλίσει περιορισμό της επεξεργασίας των δεδομένων του υπό προϋποθέσεις. Συγκεκριμένα, όταν:
    - Υπάρχει αμφισβήτηση της ακρίβειας των δεδομένων. Ο περιορισμός λαμβάνει χώρα για διάστημα τόσο, όσο χρειάζεται ο υπεύθυνος για να επαληθεύσει την ακρίβεια τους.
    - Η επεξεργασία ενώ είναι παράνομη, το υποκείμενο αντιτάσσεται στην διαγραφή τους και ζητά περιορισμό.
    - Ο σκοπός επεξεργασίας έχει ολοκληρωθεί και δεν χρειάζονται πλέον, όμως το υποκείμενο για δικούς του σκοπούς ζητά τον περιορισμό και όχι την διαγραφή τους.
    - Το υποκείμενο έχει αμφιβολίες για τον σκοπό επεξεργασίας και ζητά επαλήθευση των νόμιμων λόγων που παρουσιάζονται από τον υπεύθυνο επεξεργασίας. (Ευρωπαϊκή Ένωση, 2016v).
- **Δικαίωμα φορητότητας των δεδομένων – Άρθρο 20:** Το φυσικό πρόσωπο έχει δικαίωμα να λάβει τα δεδομένα που παρείχε σε έναν υπεύθυνο επεξεργασίας και να τα διαβιβάσει σε άλλον, χωρίς αντίρρηση του δευτέρου όταν, η επεξεργασία στηρίζεται σε συγκατάθεση ή σύμβαση και όταν γίνεται με αυτοματοποιημένα μέσα. Η λήψη των δεδομένων από το υποκείμενο θα πρέπει να γίνεται με τρόπο αποδεκτό και ευκόλως χρησιμοποιούμενο ευρέως. Δίνεται δε, το δικαίωμα στο φυσικό πρόσωπο, να ζητήσει την απευθείας μεταφορά των δεδομένων του από τον πρώτο υπεύθυνο επεξεργασίας στον δεύτερο, όπου αυτό καθίσταται δυνατό. (Ευρωπαϊκή Ένωση, 2016w).
- **Δικαίωμα εναντίωσης – Άρθρο 21:** Το φυσικό πρόσωπο, σύμφωνα με το άρθρο 21, έχει δικαίωμα ανά πάσα στιγμή να αντιταχθεί στην επεξεργασία των δεδομένων του και ο υπεύθυνος επεξεργασίας θα πρέπει να παύσει την επεξεργασία των δεδομένων. Εξαίρεση αποτελούν οι περιπτώσεις όπου ο υπεύθυνος παρουσιάσει λόγους που επιτάσσουν την επεξεργασία οι οποίοι ξεπερνούν το δικαίωμα και τις ελευθερίες του υποκειμένου. Όταν η επεξεργασία των δεδομένων, αφορά εμπορική προώθηση, τότε και πάλι ανά πάσα στιγμή, το φυσικό πρόσωπο μπορεί να αντιταχθεί στην επεξεργασία, η οποία θα πρέπει να παύσει να υφίσταται για τους σκοπούς αυτούς. Σε περιπτώσεις που τα προσωπικά δεδομένα επεξεργάζονται για επιστημονικούς ή σκοπούς ιστορικής έρευνας, τα φυσικά πρόσωπα έχουν δικαίωμα να αντιταχθούν και

να διακοπεί η επεξεργασία, αρκεί να μην είναι απαραίτητη για λόγους δημοσίου συμφέροντος. (Ευρωπαϊκή Ένωση, 2016x).

4.8. Υπεύθυνος Επεξεργασίας / Εκτελών την επεξεργασία

Το Κεφάλαιο 4 του Κανονισμού (άρθρα 24-43), αναφέρεται στον υπεύθυνο επεξεργασίας (datacontroller) και στον εκτελούντα την επεξεργασία (dataprocessor). Η βασική τους διαφορά έγκειται στο γεγονός ότι ένας υπεύθυνος επεξεργασίας, θα προσδιορίσει τους λόγους για τους οποίους συλλέγονται προς επεξεργασία, τα δεδομένα προσωπικού χαρακτήρα, αλλά και τον τρόπο με τον οποίο θα πραγματοποιηθεί η επεξεργασία. Ο εκτελών την επεξεργασία, είναι εκείνος (φυσικό ή νομικό πρόσωπο), ο οποίος θα εκτελέσει την επεξεργασία των προσωπικών αυτών δεδομένων. Οι δύο αυτοί ρόλοι, έχουν την υποχρέωση να τηρούν όσα ορίζονται από τον Κανονισμό 2016/679. Η μεταξύ τους σχέση θα πρέπει να βασίζεται σε νομική δέσμευση, στην οποία αναφέρεται ρητά ότι ο εκτελών την επεξεργασία, δεν μπορεί να συμπεριλάβει επιπλέον άτομα στην επεξεργασία των συγκεκριμένων δεδομένων, εάν πρώτα δεν έχει συγκαταθέσει, ο υπεύθυνος επεξεργασίας. (Ευρωπαϊκή Ένωση, 2016y).

4.8.1.Υπεύθυνος Επεξεργασίας

Ευθύνη του Υπευθύνου Επεξεργασίας (Ευρωπαϊκή Ένωση, 2016z).:

Ο Υπεύθυνος Επεξεργασίας θα πρέπει να είναι σε θέση να αποδείξει, αν του ζητηθεί, ότι λαμβάνει όλα τα απαραίτητα μέτρα (τεχνικά και οργανωτικά), για την διασφάλιση της προστασίας των δεδομένων που συλλέγει προς επεξεργασία. Η διασφάλιση της προστασίας, γίνεται σύμφωνα με τις αρχές που ορίζονται στον Κανονισμό.

Προστασία των δεδομένων κατά τον σχεδιασμό (by design) και εξ'ορισμού (by default), (ΑΠΔΠΧ, 2018g, Ευρωπαϊκή Ένωση, 2016aa): Μία σημαντική αλλαγή που φέρνει ο Κανονισμός είναι η ιδιωτικότητα εξ ορισμού και κατά τον σχεδιασμό. Αυτό σημαίνει ότι οι επιχειρήσεις θα πρέπει να λαμβάνουν υπόψη τους την προστασία των δεδομένων από τα αρχικά στάδια ενός πλάνου – σχεδίου τους αλλά και σε όλη την διάρκεια της εκτέλεσης του.

Σύμφωνα με το GDPR, θα πρέπει να εφαρμόζονται υπηρεσίες ή προϊόντα, τα οποία είναι ειδικά σχεδιασμένα για την προστασία δεδομένων προσωπικού χαρακτήρα, ώστε να μπορεί ο χρήστης να επιλέγει ρυθμίσεις που θα προστατεύουν τα προσωπικά του δεδομένα περισσότερο. Αυτό αφορά στα τεχνικά και οργανωτικά μέτρα που χρησιμοποιεί ο υπεύθυνος επεξεργασίας, ώστε να διασφαλίζει την προστασία των δεδομένων κατά τον σχεδιασμό.

Αντίστοιχα, η προστασία των δεδομένων εξ' ορισμού, αφορά, στην επεξεργασία μόνο των απαραίτητων για τον σκοπό της επεξεργασίας, προσωπικών δεδομένων.

Συμπερασματικά, τα βασικά χαρακτηριστικά της προστασίας προσωπικών δεδομένων κατά τον σχεδιασμό όπως προκύπτουν είναι:

- Ο υπεύθυνος επεξεργασίας θα πρέπει να λαμβάνει μέριμνα εξ αρχής για την προστασία των δεδομένων και του απορρήτου τους.
- Προστασία των δεδομένων από τον σχεδιασμό των συστημάτων
- Να διασφαλίζεται η πλήρης λειτουργία του έργου χωρίς να αμελείται η προστασία των δεδομένων
- Να υπάρχει πλήρης διαφάνεια
- Να υπάρχει σεβασμός ως προς την προστατευμένη πλέον ιδιωτικότητα του χρήστη

Από κοινού Υπεύθυνοι επεξεργασίας (Ευρωπαϊκή Ένωση, 2016ab).: Στο συγκεκριμένο άρθρο, παρουσιάζεται η δυνατότητα ύπαρξης παραπάνω από ενός υπευθύνου επεξεργασίας. Ορίζεται ότι μεταξύ τους θα πρέπει να υπάρχει σαφής διαχωρισμός των ρόλων και απόλυτη διαφάνεια σε σχέση με τις ευθύνες τους. Σημειώνεται ότι, αν το υποκείμενο της επεξεργασίας επιθυμεί να ασκήσει τα δικαιώματα του με βάσει τον Κανονισμό 2016/679, μπορεί να το κάνει συνολικά ή και κατά καθενός υπευθύνου, ξεχωριστά.

4.8.2. Εκτελών την Επεξεργασία

Ο εκτελών την επεξεργασία προσωπικών δεδομένων, είναι το πρόσωπο (φυσικό ή νομικό), το οποίο πραγματοποιεί την επεξεργασία στην θέση του υπεύθυνου και το οποίο για να οριστεί ως εκτελών, θα πρέπει να μπορεί να διαβεβαιώσει ότι όλα τα μέτρα προστασίας προσωπικών δεδομένων, που λαμβάνει, πληρούν απολύτως τις απαιτήσεις του Κανονισμού. Ο εκτελών, όπως αναφέρεται παραπάνω, δεν έχει δικαίωμα να ορίσει ή να προσλάβει επιπλέον εκτελούντες, παρά μόνο με την άδεια του Υπευθύνου. (Ευρωπαϊκή Ένωση, 2016ac).

Η σχέση του Υπευθύνου και του Εκτελούντος την επεξεργασία, στηρίζεται σε μεταξύ τους σύμβαση, η οποία θα πρέπει μεταξύ άλλων, να περιλαμβάνει και τα κάτωθι:

- Ο εκτελών, επεξεργάζεται προσωπικά δεδομένα, υπό την πλήρη καθοδήγηση του Υπευθύνου, ο οποίος πρέπει να έχει ορίσει γραπτώς, εντολές σύμφωνα με τις οποίες θα πραγματοποιηθεί η επεξεργασία.

- Όλα τα εξουσιοδοτημένα πρόσωπα, για εκτέλεση της επεξεργασίας, θα πρέπει να έχουν δεσμευτεί σε τήρηση εμπιστευτικότητας

- Ο εκτελών, με επιλογή του Υπευθύνου, θα πρέπει να επιστρέφει ή να διαγράφει, δεδομένα μετά την ολοκλήρωση του σκοπού επεξεργασίας.

4.8.3. Αρχείο Δραστηριοτήτων

Κάθε επιχείρηση/οργανισμός, με προσωπικό > 250 ατόμων, οφείλει, σύμφωνα με το άρθρο 30 του Κανονισμού, να τηρεί «Αρχείο Δραστηριοτήτων», γραπτώς σε ηλεκτρονική μορφή. Το Αρχείο Δραστηριοτήτων, τηρείται από τον Υπεύθυνο Επεξεργασίας και τον Εκτελούντα την επεξεργασία ξεχωριστά και θα πρέπει να είναι στην διάθεση της αρμόδιας Εποπτικής Αρχής, εάν ζητηθεί μέσω αιτήματος. Οι οργανισμοί ή επιχειρήσεις, που απασχολούν λιγότερα από 250 άτομα, δεν υποχρεούνται να διατηρούν Αρχείο Δραστηριοτήτων, με την προϋπόθεση ότι η επεξεργασία, δεν μπορεί να εκθέσει σε κίνδυνο τα δικαιώματα ή και τις ελευθερίες του υποκειμένου. (Ευρωπαϊκή Ένωση, 2016ad, ΑΠΔΠΧ, 2018h).

Το Αρχείο Δραστηριοτήτων, αποτελεί ουσιαστικά, ένα αρχείο με συγκεκριμένα πεδία (όπως περιγράφονται παρακάτω), μέσω του οποίου περιγράφονται οι δραστηριότητες που σχετίζονται με την επεξεργασία των προσωπικών δεδομένων.

Οι ελάχιστες πληροφορίες που πρέπει να περιλαμβάνει το Αρχείο Δραστηριοτήτων του Υπευθύνου Επεξεργασίας είναι: το ονοματεπώνυμο και τα στοιχεία προς επικοινωνία του Υπευθύνου (ή του από κοινού υπευθύνου, του εκπροσώπου ή και του Υπευθύνου προστασίας δεδομένων, αναλόγως την περίπτωση), τον ή τους σκοπούς επεξεργασίας, την περιγραφή των κατηγοριών των υποκειμένων και των προσωπικών δεδομένων, τις κατηγορίες των αποδεκτών των προσωπικών δεδομένων, τις πιθανές διαβιβάσεις σε τρίτη χώρα ή διεθνή οργανισμό, τις πιθανές προθεσμίες για διαγραφή των δεδομένων (ανά κατηγορία) εάν καθίσταται εφικτό και τέλος, μία γενική περιγραφή των μέτρων ασφαλείας που λαμβάνονται, όπου είναι δυνατό. (Ευρωπαϊκή Ένωση, 2016ad, ΑΠΔΠΧ, 2018h).

Αντιστοίχως, οι ελάχιστες πληροφορίες που πρέπει να περιλαμβάνονται στο Αρχείο Δραστηριοτήτων του εκτελούντος την επεξεργασίας είναι: το ονοματεπώνυμο και τα στοιχεία προς επικοινωνία του Εκτελούντος και του Υπευθύνου (ή του από κοινού υπευθύνου, του εκπροσώπου ή και του Υπευθύνου προστασίας δεδομένων, αναλόγως την περίπτωση), τις κατηγορίες επεξεργασίας για λογαριασμό του Υπευθύνου, τις πιθανές διαβιβάσεις σε τρίτη

χώρα ή διεθνή οργανισμό και τέλος, μία γενική περιγραφή των μέτρων ασφαλείας που λαμβάνονται, όπου είναι δυνατό. (Ευρωπαϊκή Ένωση, 2016ad, ΑΠΔΠΧ, 2018h).

4.9.Ασφάλεια των προσωπικών δεδομένων

Το δεύτερο τμήμα του Κανονισμού GDPR, αρχής γενομένης με το άρθρο 32, γίνεται αναφορά στην ασφάλεια των προσωπικών δεδομένων. Συγκεκριμένα, στο άρθρο 32, καθίστανται σαφείς οι υποχρεώσεις του υπευθύνου, αλλά και του εκτελούντος την επεξεργασία, σχετικά με τα επίπεδα ασφαλείας για την μείωση ή και εξάλειψη των πιθανών κινδύνων. (Ευρωπαϊκή Ένωση, 2016ae).

Ως κατάλληλα μέτρα ασφαλείας προτείνονται, η ψευδωνυμοποίηση και κρυπτογράφηση των δεδομένων, η δυνατότητα διασφάλισης της ακεραιότητας, του απορρήτου, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων, η διασφάλιση της αποκατάστασης της διαθεσιμότητας και της προσβασιμότητας σε περίπτωση αστοχίας, ο τακτικός έλεγχος της λειτουργίας όλων των ανωτέρω. (Ευρωπαϊκή Ένωση, 2016ae).

Επιπλέον, ως ενδεδειγμένο μέτρο, παρουσιάζεται και η πιστοποίηση ως μηχανισμός για την απόδειξη της συμμόρφωσης στον Κανονισμό GDPR. (Ευρωπαϊκή Ένωση, 2016ae).

Σε συνέχεια όσων αναφέρονται στο άρθρο 32, έρχεται το άρθρο 33, όπου ορίζει την υποχρέωση γνωστοποίησης στην αρμόδια εποπτική αρχή, των συμβάντων παραβίασης των προσωπικών δεδομένων. (Ευρωπαϊκή Ένωση, 2016af).

Ο υπεύθυνος πρέπει, χωρίς να το αμελήσει, να γνωστοποιήσει στην εποπτική αρχή, εντός 72 ωρών, από την στιγμή που ενημερώνεται, το γεγονός της παραβίασης. Παραβιάσεις που δεν μπορούν να αποτελέσουν κίνδυνο για τα δικαιώματα ή τις ελευθερίες του υποκειμένου, δεν απαιτείται να γνωστοποιούνται. Επίσης, παραβιάσεις που δεν γνωστοποιούνται εντός του διαστήματος των 72 ωρών, πρέπει να συνοδεύονται και από αιτιολογία για την καθυστέρηση. (Ευρωπαϊκή Ένωση, 2016af, ΑΠΔΠΧ, 2018i).

Η προαναφερόμενη γνωστοποίηση παραβιάσεων, πρέπει να περιλαμβάνει τουλάχιστον τις κάτωθι πληροφορίες. (Ευρωπαϊκή Ένωση, 2016af, ΑΠΔΠΧ, 2018i).

- Φύση και, ήτοι δυνατόν, την έκταση της παραβίασης καθώς επίσης και τις κατηγορίες των υποκειμένων που πλήττονται από την παραβίαση
- Τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων
- Πιθανές συνέπειες ως προς τα υποκείμενα

- Τα, μέχρι εκείνη την στιγμή, μέτρα ασφαλείας που πάρθηκαν

Εκτός από την γνωστοποίηση στην εποπτική αρχή που είναι αρμόδια, ο Κανονισμός ορίζει ως υποχρεωτική και την ανακοίνωση της παραβίασης στο ή στα υποκείμενα των προσωπικών δεδομένων, από τον υπεύθυνο επεξεργασίας. (Ευρωπαϊκή Ένωση, 2016ag).

Στο ίδιο άρθρο, αναφέρονται οι περιπτώσεις κατά τις οποίες, η ανακοίνωση στο υποκείμενο δεν είναι υποχρεωτική. (Ευρωπαϊκή Ένωση, 2016ag).:

- Όταν έχουν εφαρμοστεί όλα εκείνα τα μέτρα ασφαλείας, που δεν επιτρέπουν να γίνουν κατανοητά τα δεδομένα, από οποιονδήποτε δεν έχει άδεια πρόσβασης σε αυτά.
- Όταν ο υπεύθυνος επεξεργασίας έλαβε, ακόμη και μετά την παραβίαση, μέτρα τέτοια, τα οποία δεν θα επιτρέψουν να διακινδυνεύσουν οι ελευθερίες ή τα δικαιώματα του υποκειμένου.
- Όταν για την ανακοίνωση απαιτούνται δυσανάλογες προσπάθειες. Σε τέτοια περίπτωση μπορεί να γίνει δημόσια ανακοίνωση, ώστε όλα τα υποκείμενα να ενημερωθούν με όμοιο τρόπο.

4.10. Υπεύθυνος Προστασίας Δεδομένων (Data Protection Officer – DPO)

Το GDPR, εισάγει για πρώτη φορά τον όρο του Υπευθύνου Προστασίας Δεδομένων, ή εν συντομία, DPO. Ο DPO, βοηθά τον Οργανισμό ή την Επιχείρηση, να παρακολουθεί την συμμόρφωση στην προστασία των προσωπικών δεδομένων, να ενημερώνεται για τις αλλαγές, συμβουλεύει για τις υποχρεώσεις που σχετίζονται με την προστασία προσωπικών δεδομένων, συμβουλεύει για τους πιθανούς κινδύνους και αποτελεί και το σημείο επαφής μεταξύ του υποκειμένου των δεδομένων και της αρμόδιας εποπτικής αρχής. (ICO, 2018, Ευρωπαϊκή Ένωση, 2016ah).

Ο ορισμός του DPO, γίνεται από τον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία όταν πρόκειται για δημόσια αρχή ή οργανισμό ή όταν διεξάγονται συγκεκριμένες μορφές επεξεργασίας. (ICO, 2018,Ευρωπαϊκή Ένωση, 2016ah).

Ο DPO, πρέπει να είναι ανεξάρτητος, ειδικός στην προστασία δεδομένων προσωπικού χαρακτήρα, να έχει στην διάθεση του τους απαραίτητους πόρους και να αναφέρεται στο ανώτατο διοικητικό επίπεδο. Δεν απαιτείται να είναι νέος υπάλληλος καθώς μπορεί να είναι υφιστάμενος εργαζόμενος ή και εξωτερικός συνεργάτης του οργανισμού, με την προϋπόθεση ότι οι υπόλοιπες υποχρεώσεις του δεν μπορούν να συνεπάγονται σύγκρουση συμφερόντων με

τον νέο του ρόλο, ως DPO. Εάν πρόκειται για όμιλο επιχειρήσεων, μπορεί να διοριστεί μόνο ένας DPO, με την προϋπόθεση ότι όλες οι επιμέρους επιχειρήσεις, έχουν εύκολη πρόσβαση προς εκείνον. (ICO, 2018,Ευρωπαϊκή Ένωση, 2016ah, LordN., 2018).

Τα στοιχεία επικοινωνίας τουDPO, θα πρέπει να γνωστοποιούνται από τον υπεύθυνο ή τον εκτελούντα επεξεργασία, στην αρμόδια εποπτική αρχή. (ICO, 2018, Ευρωπαϊκή Ένωση, 2016ah).

Αξίζει να σημειωθεί ότι ο Κανονισμός GDPR, στο άρθρο 38, προστατεύει τον DPO, καθώς ορίζεται ότι, ο υπεύθυνος ή ο εκτελών επεξεργασία, δεν μπορούν να απολύσουν τον DPO, επειδή εκτέλεσε τα καθήκοντα που περιγράφονται στην συγκεκριμένη θέση. (ICO, 2018, Ευρωπαϊκή Ένωση, 2016ah).

4.10.1. Καθήκοντα του Υπευθύνου Προστασίας Δεδομένων – DPO

Σύμφωνα με το άρθρο 39, του Κανονισμού GDPR, τα ελάχιστα καθήκοντα του DPO είναι. (Ευρωπαϊκή Ένωση, 2016ah, Lord N., 2018).

- Να εκπαιδεύσει την εταιρεία και τους εργαζομένους για τις σημαντικές απαιτήσεις του συμμόρφωσης στον Κανονισμό και σε άλλες σχετικές διατάξεις της ΕΕ.
- Να εκπαιδεύσει το προσωπικό που εμπλέκεται με την διαδικασία της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.
- Να διενεργεί ελέγχους για την διασφάλιση της συμμόρφωσης και την αντιμετώπιση πιθανών κινδύνων ως μέτρο πρόληψης.
- Να αποτελεί το σημείο επαφής μεταξύ της εταιρείας και των αρμόδιων εποπτικών αρχών.
- Να συμβουλεύει, όταν του ζητείται, σχετικά με την εκτίμηση του αντίκτυπου για την προστασία των προσωπικών δεδομένων.
- Να διατηρεί πλήρες αρχείο δραστηριοτήτων με την επεξεργασία προσωπικών δεδομένων της εταιρείας και να το κοινοποιεί στην εποπτική αρχή, όταν του ζητείται.
- Να επικοινωνεί με τα υποκείμενα της επεξεργασίας και να τα ενημερώνει σχετικά με τον σκοπό της επεξεργασίας, τα δικαιώματα τους για διαγραφή και όχι μόνο, αλλά και για τα μέτρα προστασίας που λαμβάνει η εταιρεία.

4.11. Κώδικες Δεοντολογίες και Πιστοποίηση

4.11.1. Κώδικες Δεοντολογίας

Οι κώδικες δεοντολογίες, παρουσιάζονται στα άρθρα 40 και 41 του Κανονισμού. Πρόκειται για κώδικες που ορίζονται, τροποποιούνται και επεκτείνονται από κατηγορίες υπευθύνων ή και εκτελούντων επεξεργασία. Αυτό σημαίνει ότι, δε πρόκειται για κώδικες δεοντολογίας που ορίζονται από μεμονωμένους υπευθύνους ή εκτελούντες την επεξεργασία, αλλά από ενώσεις ή φορείς που τους εκπροσωπούν ως σύνολο. (Ευρωπαϊκή Ένωση, 2016ai, ΑΠΔΠΧ, 2018j).

Πρόκειται για προαιρετικούς κώδικες, οι οποίοι όμως μπορούν να αποτελέσουν σύνολο καλών πρακτικών σύμφωνα με τα όσα ορίζονται από τον Κανονισμό.

Οι κώδικες αυτοί, πρέπει να υποβάλλονται προς την αρμόδια εποπτική αρχή, ώστε να γίνονται όλοι οι απαραίτητοι έλεγχοι, ότι τα όσα ορίζονται στους κώδικες συνάδουν με τα οριζόμενα από τον Κανονισμό και την τρέχουσα νομοθεσία σχετικά με την προστασία προσωπικών δεδομένων. Ο κώδικας δεοντολογίας που έχει εγκριθεί και δημοσιευθεί από την αρμόδια εποπτική αρχή, εφόσον διατηρείται από τον υπεύθυνο επεξεργασίας, μπορεί να αποτελέσει απόδειξη συμμόρφωσης. (Ευρωπαϊκή Ένωση, 2016ai, ΑΠΔΠΧ, 2018j).

Η παρακολούθηση των κωδίκων δεοντολογίας που έχουν εγκριθεί από την εποπτική αρχή, μπορεί να γίνεται από φορέα, με αποδεδειγμένη εμπειρία και με τις απαραίτητες διαπιστεύσεις από την εποπτική αρχή. (Ευρωπαϊκή Ένωση, 2016ai, ΑΠΔΠΧ, 2018j).

Η διαπίστευση του φορέα, μπορεί να γίνει όταν πρόκειται, αποδεδειγμένα, για ανεξάρτητο και έμπειρο φορέα σε σχέση με τον κώδικα δεοντολογίας που παρακολουθεί, σύμφωνα με κριτήρια της εποπτικής αρχής. Όταν έχει καθορισμένες διαδικασίες για την αντιμετώπιση αναφορών και καταγγελιών σχετικά με παραβάσεις ως προς τον κώδικα ή με τον τρόπο εφαρμογής του. Όταν έχει καθορίσει διαδικασίες για την εκτίμηση της επιλογής υπευθύνων και εκτελούντων επεξεργασίας για την εφαρμογή του κώδικα δεοντολογίας. Όταν δεν υπάρχει σύγκρουση συμφερόντων του φορέα με την εφαρμογή του κώδικα, σύμφωνα πάντα με την εποπτική αρχή που είναι αρμόδια. (Ευρωπαϊκή Ένωση, 2016ai, ΑΠΔΠΧ, 2018j).

Τέλος, όλα τα ανωτέρω σχετικά με φορέα για την παρακολούθηση των κωδίκων, δεν ισχύουν για επεξεργασία δεδομένων από δημόσια αρχή η δημόσιους φορείς. (Ευρωπαϊκή Ένωση, 2016ai, ΑΠΔΠΧ, 2018j).

4.11.2. Πιστοποίηση

Μέσω του Κανονισμού και του άρθρου 42, παροτρύνεται η θέσπιση πιστοποιήσεων για την προστασία δεδομένων, σημάτων και σφραγίδων, ώστε να αποδεικνύεται η συμμόρφωση ως προς αυτόν. Τονίζεται ότι, πρόκειται για προαιρετική και εθελοντική διαδικασία, η οποία σε καμία περίπτωση δεν μειώνει τις ευθύνες των υπευθύνων και των εκτελούντων την επεξεργασία και δεν εμπλέκει τα οριζόμενα καθήκοντα και τις υποχρεώσεις της αρμόδιας εποπτικής αρχής. (Ευρωπαϊκή Ένωση, 2016ak, ΑΠΔΠΧ, 2018k).

Η πιστοποίηση μπορεί να έχει θετικό αντίκρισμα όσον αφορά τα υποκείμενα της επεξεργασίας, τα οποία μπορούν να επιταχύνουν την διαδικασία αξιολόγησης σχετικά με την επεξεργασία των δεδομένων τους και να νιώθουν μεγαλύτερη ασφάλεια, καθώς η πιστοποίηση γίνεται μέσω διαφανούς και ανεπηρέαστης διαδικασίας. (Ευρωπαϊκή Ένωση, 2016ak, ΑΠΔΠΧ, 2018k).

Η πιστοποίηση δίδεται στους υπευθύνους ή και εκτελούντες την επεξεργασία, μπορεί να έχει μέγιστη διάρκεια τα τρία έτη με δυνατότητα ανανέωσης. Σημαντικό χαρακτηριστικό είναι ότι, αν και η πιστοποίηση χαρακτηρίζεται ως προαιρετική, λαμβάνεται σημαντικά υπόψη από την εποπτική αρχή, όταν προκύπτει κατάσταση επιβολής προστίμου. (Ευρωπαϊκή Ένωση, 2016ak, ΑΠΔΠΧ, 2018k).

Υπάρχει δυνατότητα ανάκλησης της πιστοποίησης όταν παύουν να τηρούνται τα κριτήρια της.

Τέλος, για να χορηγήσει κάποιος φορέας πιστοποίηση σε υπεύθυνο ή εκτελούντα την επεξεργασία, θα πρέπει πρώτα, ο ίδιος να είναι διαπιστευμένος από τον φορέα διαπίστευσης του Κράτους – Μέλους στο οποίο ανήκει. Στην Ελλάδα, ο φορέας διαπίστευσης είναι το Ε.ΣΥ.Δ. (Εθνικό Σύστημα Διαπίστευσης).

4.12. Ανεξάρτητη Εποπτική Αρχή

Το Κεφάλαιο VI του Κανονισμού GDPR, αναφέρεται εξ ολοκλήρου στις ανεξάρτητες εποπτικές αρχές. Κάθε Κράτος – Μέλος θα πρέπει να έχει ορίσει μία ή περισσότερες εποπτικές αρχές, για την παρακολούθηση της συμμόρφωσης ως προς τον Κανονισμό και την τρέχουσα νομοθεσία για την προστασία των θεμελιωδών ελευθεριών και δικαιωμάτων των υποκειμένων επεξεργασίας. Οι εποπτικές αρχές θα πρέπει να είναι ανεξάρτητες δημόσιες αρχές, κάθε μέλος τους θα πρέπει να εφαρμόζει και να εκτελεί τα καθήκοντα του, σύμφωνα με τον Κανονισμό, ανεπηρέαστο από εξωτερικές επεμβάσεις. (Ευρωπαϊκή Ένωση, 2016al).

Η ανώτερη εποπτική αρχή κάθε Κράτους – Μέλους, συνεργάζεται με εκείνες των υπολοίπων Κρατών – Μελών ώστε να διασφαλίζεται η εφαρμογή του Κανονισμού σε όλα τα επίπεδα σε όλη την ΕΕ. (Ευρωπαϊκή Ένωση, 2016al).

Η εποπτική αρχή κάθε Κράτους – Μέλους, υπόκειται σε ανεξάρτητους οικονομικούς ελέγχους, ώστε να διασφαλίζεται ότι δεν έχει επηρεαστεί η ανεξαρτησία της.

Τα μέλη της εποπτικής αρχής, διορίζονται με διαφανή διαδικασία. Κάθε μέλος θα πρέπει να χαρακτηρίζεται από εμπειρία και προσόντα που να σχετίζονται με την προστασία των προσωπικών δεδομένων για την εκτέλεση των καθηκόντων που θα αναλαμβάνουν. Μπορούν να απολυθούν μόνο αν συντρέχει σημαντικό παράπτωμα ή αν αποδεδειγμένα, δεν διαθέτουν πλέον τα χαρακτηριστικά που απαιτούνται για την θέση εργασίας τους. (Ευρωπαϊκή Ένωση, 2016al).

Στα άρθρα 55 έως και 57 του Κανονισμού, αναλύονται οι αρμοδιότητες, τα καθήκοντα και οι εξουσίες των εποπτικών αρχών.

Μεταξύ άλλων, στα καθήκοντα κάθε εποπτικής αρχής περιλαμβάνεται η παρακολούθηση και επιβολή της συμμόρφωσης προς τον Κανονισμό, η ευαισθητοποίηση του κοινού ως προς τους κινδύνους που ελλοχεύουν από την μη τήρηση του, την διαχείριση των καταγγελιών για παραβάσεις, την συνεργασία με τις υπόλοιπες εποπτικές αρχές, την διενέργεια ερευνών για την τήρηση του Κανονισμού και την ενθάρρυνση κατάρτισης κωδίκων δεοντολογίας. (Ευρωπαϊκή Ένωση, 2016al).

Αντίστοιχα, μέρος των εξουσιών που διαθέτουν οι εποπτικές αρχές είναι η προειδοποίηση προς τον υπεύθυνο ή εκτελούντα την επεξεργασία για υποψίες παράβασης του Κανονισμού, η πρόσβαση σε εγκαταστάσεις του υπευθύνου και εκτελούντος την επεξεργασία, η πρόσβαση σε όλα τα δεδομένα που επεξεργάζονται, η δυνατότητα να δίνουν εντολές και να απευθύνουν επιπλήξεις προς τους υπευθύνους και εκτελούντες επεξεργασία, να απαγορεύει προσωρινά ή οριστικά την επεξεργασία των δεδομένων. Στην Ελλάδα, η ανώτερη εποπτική Αρχή για την προστασία των προσωπικών δεδομένων είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, όπως αυτή αναλύεται στην παράγραφο 2.2.2.2. του παρόντος. (Ευρωπαϊκή Ένωση, 2016al).

4.13. Συνεργασία και Συνεκτικότητα

Σε περιπτώσεις που ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία, είναι εγκατεστημένος σε περισσότερα του ενός Κράτη – Μέλη της ΕΕ, θα πρέπει να δηλώσει την κύρια εγκατάσταση του, ώστε να καθοριστεί και η Εποπτική Αρχή στην οποία θα απευθύνεται. Σε αυτή την περίπτωση η Αρχή αυτή ονομάζεται επικεφαλής εποπτική Αρχή και θα πρέπει να συνεργάζεται με τις υπόλοιπες επιμέρους εποπτικές Αρχές, οι οποίες εμπλέκονται, σε περιπτώσεις υποθέσεων διευρωπαϊκού ενδιαφέροντος. Επίσης, με σκοπό την συνεκτική εφαρμογή του Κανονισμού, προβλέφθηκε ο μηχανισμός συνεκτικότητας, στον οποίο βασικό μέρος αποτελεί το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων μέσω των ιδιαίτερα δεσμευτικών αρμοδιοτήτων που έχει. Όλα όσα αναφέρονται στην παρούσα παράγραφο αναλύονται εκτενώς στο Κεφάλαιο VII του Κανονισμού GDPR. (Ευρωπαϊκή Ένωση, 2018am).

4.14. Μεταφορά δεδομένων εκτός της Ευρωπαϊκής Ένωσης

Ο Κανονισμός GDPR σε αυτή την κατηγορία δεν διαφέρει πολύ από τα όσα προβλέπονταν από την Οδηγία ΕΚ/95/46. (Ευρωπαϊκή Ένωση, 2016an).

Συγκεκριμένα, σύμφωνα με την Οδηγία, οι επιχειρήσεις απαγορευόταν να μεταφέρουν δεδομένα προσωπικού χαρακτήρα εκτός της ΕΕ (συμπεριλαμβανομένων των Λιχτενστάιν, Ιρλανδίας και Νορβηγίας), σε χώρες που δεν είχαν επαρκή προστασία των προσωπικών δεδομένων. Έδινε το δικαίωμα στην Ευρωπαϊκή Επιτροπή, να εγκρίνει τις χώρες που σύμφωνα με την εθνική τους νομοθεσία, κρίνονταν ως κατάλληλες, ώστε οι επιχειρήσεις να μπορούν να μεταφέρουν τέτοια δεδομένα. Επίσης, μέσω της Οδηγίας, επιτρεπόταν στις επιχειρήσεις να μοιραστούν δεδομένα προσωπικού χαρακτήρα, μέσω συγκεκριμένου μηχανισμού που παρείχε όλα τα απαραίτητα μέτρα προστασίας. (Ευρωπαϊκή Ένωση, 2016an).

Ο Κανονισμός GDPR, καθιστά σαφές ότι οι αποφάσεις για επάρκεια προστασίας σε τρίτες χώρες, δεν ισχύουν, απαραιτήτως, επ’ αόριστον. Ιδανικά, θα πρέπει η Ευρωπαϊκή Επιτροπή να επανεξετάζει μέσω συγκεκριμένων προδιαγραφών τέτοιες αποφάσεις, τουλάχιστον ανά τετραετία. Ο Κανονισμός GDPR, μέσα από αυτά τα άρθρα στην εισαγωγή νέων μηχανισμών σχετικά με τις μεταφορές δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες όπως είναι οι μεταφορές βάσει τυπικών κανόνων, που υιοθετούνται από την αρμόδια εποπτική Αρχή

προστασία δεδομένων, μεταφορές βάσει συγκεκριμένου κώδικα συμπεριφορά, μεταφορές μέσω εγκεκριμένου μηχανισμού πιστοποίησης, κ.α. (Ευρωπαϊκή Ένωση, 2016an).

4.15. Καταγγελίες, ευθύνες και κυρώσεις

Το κεφάλαιο VIII (άρθρα 77 έως 84), περιλαμβάνει αναλυτικά το δικαίωμα του υποκειμένου επεξεργασίας υποβολή καταγγελίας στην αρμόδια εποπτική αρχή, το δικαίωμα για δικαστική προσφυγή κατά της αρχής ελέγχου, τα δικαίωμα της δικαστικής προσφυγής κατά των υπευθύνων και εκτελούντων την επεξεργασία των προσωπικών του δεδομένων, την δυνατότητα εκπροσώπησης του υποκειμένου από ανεξάρτητο, μη κερδοσκοπικό φορέα, γενικών συμφερόντων, με δραστηριότητες σχετικές με την προστασία των προσωπικών δεδομένων, την αναστολή των διαδικασιών, όταν για παράδειγμα υπάρχει ενημέρωση ότι για τον ίδιο υπεύθυνο ή εκτελούντα επεξεργασία, εκκρεμούν διαδικασίες σε δικαστήριο άλλου Κράτους – Μέλους, για το ίδιο αντικείμενο επεξεργασίας. Επίσης, αναλύεται το δικαίωμα αποζημίωσης σε κάθε πρόσωπο που έχει υποστεί υλική ή μη υλική ζημία, από τον υπεύθυνο ή τον εκτελούντα επεξεργασία. Ο υπεύθυνος ή ο εκτελών, μπορούν να απαλλαγούν από την ευθύνη αυτή, αν αποδειχτεί ότι δεν οφείλεται σε δική τους αστοχία το γεγονός της ζημίας. (Ευρωπαϊκή Ένωση, 2016ao).

4.15.1. Επιβολή διοικητικών προστίμων

Η επιβολή προστίμων θα πρέπει να είναι αποτελεσματική, αποτρεπτική και αναλογική, για κάθε ξεχωριστή περίπτωση και η αρμόδια εποπτική Αρχή θα πρέπει να φροντίζει γι’ αυτό.

Για την επιβολή του προστίμου θα πρέπει να λαμβάνονται υπόψη:

- Η φύση, η βαρύτητα και η διάρκεια της παράβασης
- Αν πρόκειται για δόλο ή αμέλεια
- Τα μέτρα ασφαλείας που λάμβανε μέχρι τότε ο υπεύθυνος και ο εκτελών την επεξεργασία για την ελαχιστοποίηση του κινδύνου ζημίας
- Ο βαθμός ευθύνης τους
- Πιθανό βεβαρημένο παρελθόν τους σχετικά με παραβάσεις στην επεξεργασία
- Το αν ζητήθηκε βοήθεια και συνεργασία με την εποπτική Αρχή για την επανόρθωση της παράβασης
- Οι κατηγορίες στις οποίες ανήκουν τα εκτεθειμένα προσωπικά δεδομένα
- Ποιος κοινοποίησε στην Αρχή την παράβαση
- Η τήρηση εγκεκριμένων κωδίκων δεοντολογίας, αν υπάρχουν

- Ελαφρυντικά ή επιβαρυντικά στοιχεία (π.χ. αν υπήρχε οικονομικό όφελος ή ζημία προς την εταιρεία από την παράβαση)

Το ύψος των διοικητικών προστίμων μπορεί να είναι έως 10000000€, ή για επιχειρήσεις έως το 2% του παγκόσμιου τζίρου τους (επιλέγεται όποιο είναι μεγαλύτερο) όταν πρόκειται για παραβάσεις των υποχρεώσεων του υπευθύνου και εκτελούντος την επεξεργασία (άρθρα 25 έως 39, 8, 11 42, 43), των υποχρεώσεων του φορέα πιστοποίησης (άρθρα 42 και 43), των υποχρεώσεων του φορέα παρακολούθησης (άρθρο 41, παρ. 4). (Ευρωπαϊκή Ένωση, 2016ao).

Όταν δεν υπάρχει συμμόρφωση προς την αρμόδια εποπτική Αρχή αλλά και παραβάσεις ως προς τις βασικές αρχές επεξεργασίας (άρθρα 5, 6, 7, 9), ως προς τα δικαιώματα των υποκειμένων επεξεργασίας (άρθρα 12 έως 22), ως προς την διαβίβαση δεδομένων σε τρίτη χώρα ή διεθνή οργανισμό (άρθρα 44 έως 49), ως προς τις υποχρεώσεις που ορίζονται στο Κεφάλαιο IX του Κανονισμού και μη συμμόρφωση σε προσωρινό ή οριστικό περιορισμό της επεξεργασίας, το διοικητικό πρόστιμο μπορεί να είναι ως 20000000€ ή το 4% του παγκόσμιου τζίρου για επιχειρήσεις (επιλέγεται όποιο είναι μεγαλύτερο).(Ευρωπαϊκή Ένωση, 2016ao).

Τον Κανονισμό GDPR, συμπλήρωσαν αμέσως οι Οδηγίες 2016/680 (αναλύεται παρακάτω) και 2016/681.

4.16. Ευρωπαϊκή Οδηγία 2016/680

Η ευρωπαϊκή Οδηγία 2016/680, έρχεται συμπληρωματικά στον Κανονισμό GDPR 2016/679, με βασικούς στόχους πρώτον, την προστασία από όλα τα Κράτη – Μέλη της ΕΕ, των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων και πιο ειδικά το δικαίωμα τους στην προστασία των προσωπικών τους δεδομένων. Και δεύτερον, ότι δεν περιορίζεται ή απαγορεύεται η ανταλλαγή προσωπικών δεδομένων μεταξύ αρμόδιων αρχών εντός της ΕΕ, εφόσον η ανταλλαγή αυτή απαιτείται από το δίκαιο της ΕΕ ή ων Κρατών – Μελών. (Ευρωπαϊκή Ένωση, 2016am).

Στο πεδίο εφαρμογής της τονίζεται ότι δεν εφαρμόζεται όταν η επεξεργασία των προσωπικών δεδομένων γίνεται σε πλαίσια που δεν εμπίπτουν στην δικαιοδοσία του δικαίου της ΕΕ και δεν εφαρμόζεται από τα θεσμικά και άλλα όργανα της ΕΕ. (Ευρωπαϊκή Ένωση, 2016am).

Βασικός στόχος της Οδηγίας είναι η θέσπιση κανόνων και προϋποθέσεων επεξεργασίας για την πρόληψη, την διερεύνηση, την δίωξη ποινικών αδικημάτων ή την εκτέλεση κυρώσεων και την προστασία της δημόσιας ασφάλειας. (Ευρωπαϊκή Ένωση, 2016am).

Η παρούσα Οδηγία απευθύνεται στα Κράτη – Μέλη της ΕΕ και αρχίζει να ισχύει από τις 05/05/2016. Με την συγκεκριμένη οδηγία καταργείται η απόφαση – πλαίσιο 2008/977/ΔΕΥ για την προστασία των δεδομένων που υπόκεινται σε επεξεργασία στα πλαίσια της αστυνομικής και δικαστικής συνεργασίας για ποινικές υποθέσεις και την διασυνοριακή ανταλλαγή δεδομένων. Πλέον, το κάθε Κράτος – Μέλος καλείται να ενσωματώσει στην εθνική του νομοθεσία την συγκεκριμένη Οδηγία και να εφαρμόζει την ειδική νομοθεσία για την προστασία των προσωπικών δεδομένων όπως ορίζεται από την Οδηγία. (Ευρωπαϊκή Ένωση, 2016am).

Στα πλαίσια της Οδηγίας προβλέπεται η επεξεργασία των ευαίσθητων προσωπικών δεδομένων, οι υποχρεώσεις του υπευθύνου και του εκτελούντος την επεξεργασία, ο ορισμός Υπευθύνου Προστασίας Δεδομένων (DPO), καθώς και οι ανταλλαγές δεδομένων εκτός συνόρων. (Ευρωπαϊκή Ένωση, 2016am).

Κατηγορίες υποκειμένων επεξεργασίας που αφορά η Οδηγία 2016/680

- Υπόπτους για ήδη εκτελεσμένα ή μελλοντικά εγκλήματα
- Κατηγορούμενους
- Καταδικασμένους
- Θύματα και μάρτυρες (συμπεριλαμβανομένων και των προστατευμένων μαρτύρων)
- Τρίτα πρόσωπα που εμπλέκονται (πραγματογνώμονες, τεχνικούς, διερμηνείς, κτλ)(Ευρωπαϊκή Ένωση, 2016am, Τσολιάς Γ., 2016).

5. HIPAA – HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY

5.1. Τι είναι και που εφαρμόζεται το HIPAA

Ο HIPAA (1996), είναι νόμος των ΗΠΑ που δημιουργήθηκε για τον εκσυγχρονισμό της ροής των υγειονομικών πληροφοριών των φυσικών προσώπων, τον καθορισμό του τρόπου που διατηρούνται προσωπικά δεδομένα σε υγειονομικές μονάδες, την προστασία των ασφαλιστικών εταιρειών από παραβάσεις, όπως απάτες, και τέλος για να αντιμετωπίσει περιορισμούς στην ασφαλιστική κάλυψη για την υγεία, όπως η φορητότητα και η ασφάλιση ατόμων με προϋπάρχον ιστορικό. (HCS, 2018).

Παρά το γεγονός ότι το Κογκρέσο έχει θεσπίσει νόμους για το απόρρητο των πληροφοριών από το 1970, με το HIPAA εστιάζει στην ψηφιοποίηση των ιατρικών αρχείων και την διασφάλιση της προστασίας τους είτε είναι σε ηλεκτρονική μορφή είτε όχι. (HCS, 2018).

Κατά την εμφάνιση του HIPAA, προέκυψαν πολλές αλλαγές στις ασφαλιστικές βιομηχανίες για την υγειονομική περίθαλψη. Χρειάστηκε να εκδοθούν πρότυπα για την προστασία των πληροφοριών στην υγεία, με τα πρώτα να δημοσιεύονται το 1999. (HCS, 2018).

Οι συμμόρφωση με τον HIPAA ελέγχεται από το Γραφείο Πολιτικών Δικαιωμάτων (OCR) του Υπουργείου Υγείας και Ανθρωπίνων Υπηρεσιών (HSS) των ΗΠΑ. Εξουσία ωστόσο έχουν και οι γενικοί εισαγγελείς, οι οποίοι μπορούν, αν χρειαστεί, να λάβουν μέτρα και να επιβάλλουν οικονομικές κυρώσεις, κατά των Επιχειρηματικών Συνεργατών (BusinessAssociates – BA) και των καλυπτομένωνοντοτήτων (CoveredEntities – CE), οι οποίοι δεν συμμορφώνονται με τον HIPAA.(HCS, 2018, OCR, χ.χ.).

Αξίζει να σημειωθεί ότι δεν παρέχονται πιστοποιητικά για συμβατότητα ή συμμόρφωση με το HIPAA για φυσικά πρόσωπα ή εταιρείες, αλλά αντιθέτως, η συμμόρφωση αυτή απαιτεί συνεχή αγώνα και προσπάθεια.

Ο τρόπος εφαρμογής του HIPAAμεταβάλλεται συνεχώς, ώστε να μπορεί να συμβαδίζει με τις τεχνολογικές εξελίξεις και με τις αλλαγές στις εργασιακές πρακτικές, που μπορεί να εκθέσουν ευκολότερα την ιδιωτική ζωή των ασθενών (Ο HIPAA σχεδιάστηκε τουλάχιστον 8 χρόνια πριν την εμφάνιση του Facebook).Οι νέοι κανόνες και οι οδηγίες που εκδίδονται, συνεχώς, από το Γραφείο Πολιτικών Δικαιωμάτων, προσπαθούν να αντιμετωπίζουν θέματα όπως είναι το cloud computing, οι Bring Your Own Device πολιτικές (BYOD policies) και τα προγράμματα wellness workplace. (HCS, 2018).

Παρά της τροποποιήσεις που έχουν γίνει στον HIPAA, ο αρχικός του σκοπός και τα βασικά του στοιχεία δεν έχουν αλλάξει. Ο αρχικός σχεδιασμός του είχε γίνει με τέτοιο τρόπο που κάλυπτε μεγάλο εύρος διαφορετικών περιπτώσεων. Ο HIPAA δεν προωθεί κάποιον συγκεκριμένο τρόπο αντιμετώπισης του προβλήματος, με την προϋπόθεση πάντα ότι ο μηχανισμός που θα χρησιμοποιηθεί πραγματοποιεί αξιολόγηση κινδύνου. Τέλος, ο HIPAA συμβαδίζει με το Κρατικό Δίκαιο, με εξαίρεση τις περιπτώσεις όπου οι Κανονισμοί του Κράτους περί ιδιωτικότητας και ασφάλειας είναι ασθενέστεροι από αυτούς που ορίζονται από τον HIPAA. (HCS, 2018).

Ο HIPAA εφαρμόζεται σε όλους τους σχεδιασμούς για την υγεία, σε προμηθευτές υπηρεσιών υγείας, σε εταιρείας εκκαθάρισης υγειονομικών υπηρεσιών και κωδικοποιητές, αλλά και στους χορηγούς της εκπτωτικής κάρτας φαρμάκων, μέσω Medicare συνταγής. (HCS, 2018).

Η συμμόρφωση με το HIPAA απαιτείται από ένα μέρος εργοδοτών. Συγκεκριμένα, οι εταιρείες που χρησιμοποιούν προγράμματα (π.χ. Πρόγραμμα Βοηθείας Εργαζομένων) θα πρέπει να είναι συμβατές με το HIPAA. Αν απλώς, διατηρούν ιατρικά αρχεία για τους εργαζομένους τους, δεν απαιτείται να συμβαδίζουν με τις απαιτήσεις του HIPAA. Αντίστοιχα, οι BA θα πρέπει να συμμορφώνονταιμε το HIPAA καθώς επεξεργάζονται, διατηρούν, λαμβάνουν και ανταλλάσουν PHI. Επίσης, μπορεί να αναλάβουν κάποια δραστηριότητα ή να παρέχουν υπηρεσία για λογαριασμό εταιρείας CE. Σε αυτή την περίπτωση θα πρέπει να υπάρχει μεταξύ τους σύμβαση που να περιλαμβάνει και τα μέτρα προστασίας των PHI. (HCS, 2018).

5.1.1. Τα τμήματα του HIPAA

Το HIPAAδιακρίνεται σε 5 τμήματα δράσης που ονομάζονται τίτλοι:

- Τίτλος I: Εστίαση στην προσβασιμότητα, φορητότητα και ανανεωσιμότητα των ιατρικών δεδομένων και υπηρεσιών (“Focus on Healthcare Access, Portability and Renewability”)
- Τίτλος II: Πρόληψη της απάτης και κακομεταχείρισης των ιατρικών δεδομένων και υπηρεσιών, απλοποίηση διοικητικών διαδικασιών και μεταρρύθμιση της ιατρικής ευθύνης (“Preventing HealthCare Fraud and Abuse, Administrative Simplification, Medical Liability Reform")
- Τίτλος III: Φορολογικές διατάξεις σχετικές με λογαριασμούς ιατρικής αποταμίευσης (“Tax-related health provisions governing medical savings accounts”)

- Τίτλος IV: Εφαρμογή και επιβολή των απαιτήσεων ομαδικής ασφάλειας υγείας ("Application and enforcement of group health insurance requirements")
- Τίτλος V: Αντιστάθμιση εισοδήματος για φορολογικές εκπτώσεις προς τους εργοδότες ("Revenue offset governing tax deductions for employers"). (Edemekong, P., 2018).

5.2. Protected Health Information (PHI και ePHI)

Στον HIPAA ορίζονται δεκαοχτώ χαρακτηριστικά τα οποία ονομάζονται Προστατευμένες Πληροφορίες Υγείας (PHI) και ηλεκτρονικά Προστατευμένες Πληροφορίες (ePHI), όταν είναι σε ηλεκτρονική μορφή. Τα χαρακτηριστικά αυτά, θεωρείται ότι είναι αυτά που μπορούν να αποκαλύψουν πληροφορίες σχετικά με το υποκείμενο των στοιχείων, το ιατρικό ιστορικό του ή τα οικονομικά του στοιχεία και τις πληρωμές του. Σύμφωνα με το HIPAA, κάθε οργανισμός ή φυσικό πρόσωπο που έχει στα αρχεία του PHI, θα πρέπει να έχει λάβει τα κατάλληλα μέτρα για την διασφάλιση της προστασίας των δεδομένων προσωπικού χαρακτήρα. Κατά τον HIPAA, για να θεωρηθεί ότι υπάρχει παράβαση και μη συμμόρφωση, αρκεί να μην έχουν ληφθεί τα κατάλληλα μέτρα προστασίας, ακόμη κι αν δεν έχει προκύψει διαρροή των PHI. (HIPAA Journal, 2018).

<u>Προστατευμένες Πληροφορίες Υγείας:</u>

- Όνομα ή μέρος του ονόματος
- Οποιοδήποτε μοναδικό χαρακτηριστικό ταυτοποίησης
- Γεωγραφικά αναγνωριστικά
- Ημερομηνίες, άμεσα σχετιζόμενες με το φυσικό πρόσωπο
- Τηλέφωνο
- Αριθμός ΦΑΞ
- Στοιχεία email
- Λεπτομέρειες σχετικές με την κοινωνική του ασφάλιση
- Κωδικοί των ιατρικών του αρχείων
- Στοιχεία ασφάλισης υγείας των εξαρτώμενων μελών
- Λεπτομέρειες για τον λογαριασμό του
- Αριθμοί πιστοποιητικών ή αδειών του
- Πινακίδα οχήματος
- Αναγνωριστικά συσκευών και serial numbers

- Διευθύνσεις ιστοσελίδων
- IP address
- Δακτυλικά, φωνητικά ή οπτικά αποτυπώματα
- Πρόσωπο ή φωτογραφίες

5.3. Κανόνες HIPAA

Ο HIPAA αποτελείται από ένα σύνολο κανόνων οι οποίοι υπάρχουν για να διασφαλίζουν την εμπιστευτικότητα, την ακεραιότητα, αλλά και την διαθεσιμότητα των PHI:

- Κανόνας για την προστασίας των δεδομένων προσωπικού χαρακτήρα (HIPAA Privacy Rule): Ο συγκεκριμένος κανόνας ορίζει τον τρόπο, την χρονική περίοδο και τις συνθήκες υπό τις οποίες μπορεί να εκτεθεί ένα στοιχείο PHI.Μέσω του συγκεκριμένου Κανόνα, ορίζονται τα όρια για την επεξεργασία των στοιχείων ασθενών, χωρίς πρότερη συγκατάθεση του. Δίνει το δικαίωμα στους ασθενείς ή στους εκπροσώπους τους, να λαμβάνουν αντίγραφα των ιατρικών τους φακέλων και να ζητήσουν μεταβολές. Οι εμπλεκόμενοι φορείς θα πρέπει να απαντούν σχετικά αιτήματα εντός 30 ημερών. Ο συγκεκριμένος κανόνας, με την εμφάνιση του το 2003, αφορούσε όλους τους Οργανισμούς παροχής υπηρεσιών υγείας και τις επιχειρήσεις παροχής προγραμμάτων υγείας. Από το 2013 και μετά συμπεριέλαβε μέσω επέκτασης, και τους BA. (HHS, 2013a, OCR, χ.χ.).

- Κανόνας ασφαλείας (HIPAA Security Rule):Ο συγκεκριμένος Κανόνας, ορίζει ελάχιστα πρότυπα σχετικά με την πρόσβαση, την δημιουργία, την επεξεργασία και την μεταφορά των ePHI. Περιλαμβάνει φυσικές, διοικητικές και τεχνικές διασφαλίσεις. Οι φυσικές μπορεί να είναι για παράδειγμα, η διάταξη των οθονών εντός των σταθμών εργασίας (να μην είναι εκτεθειμένες οι οθόνες προς μη εξουσιοδοτημένα άτομα). Οι διοικητικές διασφαλίσεις αποτελούν την σύνδεση του συγκεκριμένου με τον προηγούμενο Κανόνα (HIPAA Privacy Rule). Στα πλαίσια των διοικητικών διασφαλίσεων απαιτείται ο ορισμός Υπευθύνου Ασφαλείας και Υπευθύνου Προστασίας Προσωπικών Δεδομένων οι οποίοι πρέπει να πραγματοποιούν ελέγχους για την συμμόρφωση και να κάνουν αξιολόγηση των κινδύνων. Τέλος, οι τεχνικές διασφαλίσεις μπορεί να είναι η κρυπτογράφηση σύμφωνα με τα πρότυπα NIST, όταν τα δεδομένα θα πρέπει να μεταφερθούν εκτός της ίδιας της εταιρείας. Τα μέτρα ασφαλείας ή διασφαλίσεις, όπως αναφέρονται σε

αυτόν τον Κανόνα διακρίνονται σε απαραίτητα και απευθυνόμενα. Ουσιαστικά όλα τα μέτρα είναι απαραίτητα, εκτός κι αν μπορεί να αιτιολογηθεί ο λόγος που δεν θα είναι. Παράδειγμα απευθυνόμενων μέτρων μπορεί να αποτελέσει η κρυπτογράφηση των email που περιέχων στοιχεία PHI. Η κρυπτογράφηση απαιτείται όταν τα email ανταλλάσσονται εκτός του εσωτερικού διακομιστή. Αν πρόκειται για εσωτερική επικοινωνία ή αν υπάρχει εξουσιοδότηση από το ίδιο το φυσικό πρόσωπο για αποστολή χωρίς κρυπτογράφηση τότε δεν πρόκειται για απαραίτητο μέτρο ασφαλείας. (HHS, 2013b).

- Κανόνας Ενημέρωσης για την Παράβαση (Breach Notification Rule): Εντός 60 ημερών, θα πρέπει να υπάρχει ενημέρωση προς το Υπουργείο Υγείας και Ανθρωπίνων Υπηρεσιών για την παράβαση που έχει εντοπιστεί. Σε περιπτώσεις που κρίνεται ότι η παράβαση επηρεάζει πληθυσμό μεγαλύτερο των 500 ασθενών, απαιτείται κι ενημέρωση των ΜΜΕ. (HHS, 2013c).

- Κανόνας Omnibus (Omnibus Rule): Μέσω αυτού του Κανόνα, έγιναν αλλαγές στο HIPAA που περιελάμβαναν την επέκταση του απέναντι στις CE, απαγορεύθηκε η χρήση στοιχείων που περιλαμβάνονται στην λίστα PHI για προωθητικούς σκοπούς ή για επικερδείς καταστάσεις χωρίς άδεια. Επίσης, με την εμφάνιση του συγκεκριμένου Κανόνα, αυξήθηκαν οι πόροι προς το Γραφείο Πολιτικών Δικαιωμάτων, ώστε να διεξάγει αυστηρότερους ελέγχους για πιθανές παραβάσεις ως προς το HIPAA και ορίζοντας νέα αυστηρότερα επίπεδα ποινών. (HHS, 2013d).

- Κανόνας Επιβολής (Enforcement Rule): Πρόκειται για τον Κανόνα που καθορίζει τον τρόπο με τον οποίο διεξάγονται οι έρευνες όταν εντοπίζεται παράβαση του HIPAA και έκθεση στοιχείων PHI. Μέσω αυτού, ορίζεται το επίπεδο αμέλειας των υπευθύνων και ορίζονται τα κατάλληλα πρόστιμα. Τα πρόστιμα για παράβαση από άγνοια μπορούν να είναι μέχρι και 50000$ ενώ για σκόπιμη παραμέληση των Κανόνων μπορεί να είναι 50000$ ανά παράβαση. (HHS, 2013e).

5.4. Απαιτήσεις HIPAA

5.4.1. Κρυπτογράφηση και Κωδικοί πρόσβασης

Η κρυπτογράφηση, όπως αναφέρεται και παραπάνω, είναι ένα από τα σημαντικότερα μέτρα ασφαλείας καθώς μπορεί να κάνει τα ηλεκτρονικά προσωπικά δεδομένα ακατανόητα ως προς τα μη εξουσιοδοτημένα πρόσωπα, αλλά ανιχνεύσιμα ως προς τα εξουσιοδοτημένα. Παρά την σημαντικότητα του συγκεκριμένου μέτρου, το HIPAAείναι αρκετά ελαστικό ως προς αυτό. Δίνει την δυνατότητα στον οργανισμό να χρησιμοποιεί κρυπτογράφηση μόνο όταν θεωρεί ότι είναι απαραίτητη λόγω μεταφοράς δεδομένων εκτός του εταιρικού δικτύου. Επιτρέπει στους ίδιους τους οργανισμούς να κάνουν εκτίμηση των κινδύνων και να επιλέξουν τις καταλληλότερες διασφαλίσεις για τις υπηρεσίες που παρέχουν. Βέβαια, σε περίπτωση μη χρήσης κρυπτογράφησης, θα πρέπει να υπάρχει τεκμηριωμένη θέση ως προς τους λόγους και τα εναλλακτικά μέτρα προστασίας που λαμβάνονται (HIPAA guide, χ.χ.).

Οι κωδικοί πρόσβασης, αν και αποτελούν βασική διασφάλιση για την αποτροπή εισόδου σε κλειδωμένα αρχεία, μη εξουσιοδοτημένων ατόμων, το HIPAA δεν τους περιγράφει με λεπτομέρεια. Παρά το γεγονός όμως, ότι δεν αναλύονται διεξοδικά, το HIPAA απαιτεί από τους οργανισμούς που καλύπτονται από το HIPAA, να αναπτύσσουν πολιτικές σχετικά με την δημιουργία κωδικών πρόσβασης προωθώντας τα πρότυπα NIST ως συμβούλους για την ανάπτυξη των κωδικών αυτών (HIPAA journal, 2018a).

Σύμφωνα με τις αναθεωρημένες συμβουλές των προτύπων NIST για την δημιουργία κωδικών πρόσβασης, αυτοί προτείνεται να είναι από 8 έως 64 χαρακτήρες, με μακρές φράσεις πρόσβασης παρά τυπικοί κωδικοί που μπορεί να ξεχαστούν και ίσως χρειαστεί να σημειωθούν κάπου, αποτελώντας κίνδυνο για έκθεση προσωπικών δεδομένων (NIST, 2017).

5.4.2. Διατήρηση ιατρικών αρχείων

Ο HIPAA στις απαιτήσεις του, δεν περιλαμβάνει συγκεκριμένα μέτρα σχετικά με την διατήρηση ιατρικών αρχείων, καθώς θεωρείται ότι αυτό καλύπτεται από την κρατική νομοθεσία, όπου απαιτείται και η ανάπτυξη κατάλληλων πολιτικών για την διατήρηση τους (MLN, 2012).

Η νομοθεσία διαφέρει από Πολιτεία σε Πολιτεία. Για παράδειγμα στην Πολιτεία της Νέας Υόρκης, τα ιατρικά αρχεία διατηρούνται για 6 έτη από τους Ιατρούς και από τα Νοσοκομεία. Εξαίρεση αποτελούν οι ανήλικοι ασθενείς για τους οποίους τα Νοσοκομεία διατηρούν τα ιατρικά τους αρχεία μέχρι τα 21 τους. Ως ημερομηνία έναρξης λαμβάνεται υπόψη, η

τελευταία επαφή του ασθενούς με τον Ιατρό ή το Νοσοκομείο, αντίστοιχα. Στην Πολιτεία της Βόρεια Καρολίνα, διατηρούνται για 11 έτη κατ' ελάχιστον, εκτός αν πρόκειται για ανήλικο ασθενή. Σε αυτή την περίπτωση διατηρούνται ως τα 30 του έτη. Στο Τέξας, οι Ιατροί διατηρούν τα αρχεία για 7 έτη, εκτός αν πρόκειται για ανήλικο ασθενή, όπου διατηρούνται ως τα 21 του έτη. Αντίστοιχα τα Νοσοκομεία στο Τέξας διατηρούν τα ιατρικά αρχεία για 10 έτη, εκτός αν πρόκειται για ανήλικο ασθενή, όπου διατηρούνται ως τα 20 του έτη (HealthInformation, 2016).

Όσον αφορά τις ασφαλιστικές εταιρείες, εκείνες μπορεί να υπόκεινται σε νόμους FINRA (FinancialIndustryRegulatoryAuthority), σχετικούς με την διατήρηση των αρχείων που περιέχουν δεδομένα της λίστας PHI (FINRA, χ.χ.).

5.4.3. Καταγγελία Παραβίασης δεδομένων PHI

Ως παραβίαση, κατά τον HIPAA, ορίζεται η χρήση ή η έκθεση προστατευόμενων πληροφοριών για την υγεία σύμφωνα με τον Κανόνα για την προστασία προσωπικών δεδομένων, όταν η χρήση ή η έκθεση αυτή, θέτει σε κίνδυνο την ασφάλεια ή το απόρρητο των πληροφοριών αυτών. (HIPAA Journal, 2017).

Η κοινοποίηση μπορεί να μην είναι υποχρεωτική, όταν ο φορέας που εμπλέκεται αποδείξει ότι υπάρχει χαμηλή επικινδυνότητα να έχει παραβιαστεί κάποιο από τα στοιχεία PHI. (HIPAA Journal, 2017).

Όταν η κοινοποίηση είναι απαραίτητη, πρέπει, χωρίς να περάσει η πάροδος των 60 ημερών, να ενημερώνονται οι ασθενείς και τα εμπλεκόμενα μέλη (για πληθυσμό άνω των 500 ατόμων, ενημερώνονται και τα ΜΜΕ) αλλά και το Υπουργείο Υγείας και Ανθρωπίνων Υπηρεσιών. Η κοινοποίηση θα πρέπει να είναι σύντομη περιγραφή της παραβίασης, του τύπου των εκτεθειμένων πληροφοριών, να περιλαμβάνει οδηγίες και μέτρα για τον περιορισμό της βλάβης. (HIPAA Journal, 2017).

5.4.4. Συχνές παραβάσεις του HIPAA

Συχνές παραβάσεις και μη συμμορφώσεις του HIPAAσχετίζονται με έλλειψη εκτίμησης κινδύνου, με έλλειψη ορθής και πλήρους εκπαίδευσης των εργαζομένων, με άγνοια του HIPAA, με παράλειψη αναφοράς της παράβασης εντός της καθορισμένης προθεσμίας. Η άγνοια φυσικά δεν γίνεται αποδεκτή ως αιτιολογία από το OCR, όμως δεν επιβάλλονται μεγάλες χρηματικές ποινές, αν δεν έχει διαρρεύσει κάποιο στοιχείο PHI. Συνήθως, επιβάλλει να υπάρξουν διορθωτικές ενέργειες. (Johnson J., 2016).

Πιο συγκεκριμένα:

Ανεπάρκεια εκτίμησης κινδύνου: Εδώ εντοπίζεται η αδυναμία πολλών οργανισμών να πραγματοποιήσουν ολοκληρωμένη εκτίμηση κινδύνων σχετικά με την προστασία, την ακεραιότητα, την διαθεσιμότητα και την εμπιστευτικότητα των προσωπικών δεδομένων PHI.

Ακατάλληλη η μη απαραίτητη διατήρηση και διάθεση των PHI:Σύμφωνα με το HIPAA, όταν κρίνεται ότι το PHI ή ePHI, δεν χρειάζεται πλέον, θα πρέπει να καταστρέφεται ή να απορρίπτεται με τέτοιο τρόπο, ώστε να διασφαλίζεται η δεν μπορεί να αναγνωστεί, να ταυτοποιηθεί ή να ανακατασκευαστεί. Συγκεκριμένα, τα έγχαρτα δεδομένα θα πρέπει να καταστρέφονται, τεμαχίζονται ή να καίγονται. Αντίστοιχα, τα ηλεκτρονικά δεδομένα θα πρέπει να διαγράφονται και να καταστρέφονται μη αφήνοντας ίχνη.

Αποκάλυψη στοιχείων PHI σε τρίτους:Η παροχή στοιχείων PHIπρος τρίτους, επιτρέπεται μόνο εφόσον έχει ληφθεί εξουσιοδότηση από το υποκείμενο των δεδομένων.

Παράλειψη παροχής δεδομένων με στοιχεία PHI προς τους ασθενείς: Όπως αναφέρεται σε προηγούμενες παραγράφους, οι ασθενείς έχουν το δικαίωμα να αιτηθούν να παραλάβουν αντίγραφα των προστατευμένων πληροφοριών υγείας τους και οι πάροχοι υποχρεούνται να τους τα παρέχουν εντός 30 ημερών από την παραλαβή της αίτησης.

5.5. Πλεονεκτήματα και Μειονεκτήματα HIPAA ως προς τους ασθενείς

Μέσω του HIPAA, είναι προφανές πως λόγω του γεγονότος ότι οι πληροφορίες υγείας αντιμετωπίζονται διαφορετικά, η πρόσβαση από τους ίδιους του παρόχους και τους προμηθευτές υγειονομικών υπηρεσιών γίνεται αποτελεσματικότερη, ασφαλέστερη και ταχύτερη, σε αντίθεση με τον κλασικό Ιατρικό Φάκελο που διατηρούσαν παλαιότερα. Ένα επιπλέον πλεονέκτημα, είναι ότι για πρώτη φορά, μέσω του HIPAA, μπορούν οι ασθενείς να ζητήσουν και να διορθώσουν τις προσωπικές ιατρικές τους πληροφορίες. Επίσης, επιτρέπει σε ασθενείς με προϋπάρχον ιστορικό να αλλάξουν εργασία χωρίς να ανησυχούν για την έκθεση του ιατρικού τους ιστορικού από τον νέο εργοδότη. (Andrews J., 2017).

Στον αντίποδα αυτού του γεγονότος, έρχεται ο περιορισμός της έρευνας που προκύπτει από τον συνεχή αγώνα για συμμόρφωση με το HIPAA. Οι φορείς υγειονομικής περίθαλψης, περιορίζουν την έρευνα ή επιβραδύνεται ο ρυθμός για την ολοκλήρωση της λόγω της περιορισμένης και ελεγχόμενης πρόσβασης σε στοιχεία PHI. Αυτό έχει ως αποτέλεσμα να υπάρχει καθυστέρηση στην μετάβαση σε ποιοτικότερες υπηρεσίες υγείας και

περίθαλψη.Επίσης, δυσκολεύει σε κάποιον βαθμό την επικοινωνία μεταξύ των θεραπόντων και των ασθενών. Υπάρχουν Ιατροί που αρνούνται να αποστείλουν ιατρικά αποτελέσματα στους ασθενείς και ζητούν από τους ίδιους ή εξουσιοδοτημένα πρόσωπα να παραλάβουν δια ζώσης. (Andrews J., 2017).

6. GDPR ΚΑΙ HIPAA

6.1. Συμμόρφωση HIPAAμε GDPR

Από την ανάλυση του ΚανονισμούGDPR και τουHIPAA, στα προηγούμενα κεφάλαια, προκύπτει ότι, Οργανισμοί και Υπηρεσίες υγειονομικής περίθαλψης στις ΗΠΑ, που διαχειρίζονται προστατευμένα προσωπικά δεδομένα (PHI) θα πρέπει να είναι συμβατοί με τοHIPAA. Αντίστοιχα, οργανισμοί και υπηρεσίες που διαχειρίζονται προσωπικά δεδομένα και ευαίσθητα προσωπικά δεδομένα εντός της ΕΕ, θα πρέπει να συμμορφώνονται με τον Κανονισμό GDPR. Εδώ γεννάται το ερώτημα, αν η επιχείρηση δεν διαχειρίζεται και επεξεργάζεται προσωπικά δεδομένα εντός της ΕΕ αλλά στις ΗΠΑ, αν θα πρέπει να συμμορφώνεται με το GDPR. Σε πρώτη ανάγνωση η απάντηση δεν είναι εύκολη. Επιχειρήσεις και οργανισμοί των ΗΠΑ που ασχολούνται με προγράμματα για τον Ιατρικό Τουρισμό και παρέχουν υγειονομικές υπηρεσίες σε διεθνές επίπεδο θα πρέπει να συμμορφώνονται με το GDPR, καθώς πρόκειται για διεθνή μετακίνηση για ιατρική περίθαλψη. (Ευρωπαϊκή Ένωση, 2016j, HCD, 2018, ZogBlog, 2018, Mooney G., 2018).

Όταν πρόκειται για κάτοικο της Ένωσης, που δέχεται υγειονομικές υπηρεσίες στις ΗΠΑ, ο Κανόνας για προστασία προσωπικών δεδομένων του HIPAA, τίθεται σε εφαρμογή, σε συνδυασμό με τον Κανόνα ασφαλείας. Ως εκ τούτου, τα απαραίτητα μέτρα θα πρέπει να εφαρμοστούν ανεξάρτητα από τον Κανονισμό GDPR. (Ευρωπαϊκή Ένωση, 2016j, HCD, 2018, ZogBlog, 2018).

Εδώ βέβαια, προκύπτει το ζήτημα, ότι κάποιος Οργανισμός των ΗΠΑ, συλλέγει προσωπικές πληροφορίες για κάποιον κάτοικο της Ένωσης. Αν τα δεδομένα συλλέγονται ενώ το φυσικό πρόσωπο βρίσκεται εντός ΕΕ, τότε θα πρέπει να ακολουθούνται οι Κανόνες του GDPR, αν όχι τότε, η επιχείρηση δεν υποχρεούται να το ακολουθήσει. Όταν οι πληροφορίες λαμβάνονται ηλεκτρονικά, και η θέση του ατόμου είναι αμφίβολη, τότε οι επιχειρήσεις προκειμένου να είναι ασφαλείς, τηρούν το GDPR. (Ευρωπαϊκή Ένωση, 2016j, HCD, 2018, ZogBlog, 2018).

6.2. Βασικές διαφορές και ομοιότητες μεταξύ HIPAA και GDPR

6.2.1. Υποκείμενα επεξεργασίας

Μία βασική διαφορά μεταξύ των δύο (GDPR και HIPAA) είναι το γεγονός ότι το GDPRείναι σχεδιασμένο με τρόπο τέτοιο ώστε να καλύπτει υποκείμενα επεξεργασίας που βρίσκονται εντός της Ένωσης, ανεξάρτητα από την ιδιότητα τους ως πολίτες. Αντιθέτως το HIPAA, προστατεύει συγκεκριμένα τα PHIκαι ePHI που χειρίζονται επιχειρήσεις και οργανισμοί στις Ηνωμένες Πολιτείες. (Ευρωπαϊκή Ένωση, 2016j, HCD, 2018, ZogBlog, 2018).

Ο HIPAA, είναι σαφές ότι έχει ως αντικείμενο αποκλειστικά την διαχείριση προσωπικών δεδομένων σχετικά με την παροχή υγειονομικής περίθαλψης και όχι στο σύνολο τους, όπως συμβαίνει με το GDPR. Αυτό σημαίνει πως, αν μια επιχείρηση ή οργανισμός, διατηρεί προσωπικά δεδομένα γενικά, τότε, θα πρέπει να συμμορφώνεται με το GDPR. Αν τα δεδομένα αυτά, εμπίπτουν και στην κατηγορία των PHI ή ePHI, (όπως περιγράφονται σε προηγούμενη παράγραφο), τότε θα πρέπει να υπάρχει και συμμόρφωση σύμφωνα με το HIPAA. (Ευρωπαϊκή Ένωση, 2016j, HCD, 2018, ZogBlog, 2018).

6.2.2. Απαίτηση για ρητή συγκατάθεση

Μία ακόμη σημαντική διαφορά που προκύπτει ανάμεσα στον Κανονισμό 2016/679 (GDPR) και στο HIPAA, είναι το γεγονός της ανάγκης για ρητή συγκατάθεση, ως συναίνεση, από το υποκείμενο της επεξεργασίας των δεδομένων. Κατά το GDPR, η ρητή συγκατάθεση απαιτεί πολύ σημαντική και απαραίτητη προϋπόθεση για την επεξεργασία/αποθήκευση/διαχείριση δεδομένων προσωπικού χαρακτήρα του υποκειμένου. Αντιθέτως, για το HIPAA, η ρητή συγκατάθεση δεν είναι υποχρεωτική. Το ίδιο ισχύει και όσον αφορά την επικοινωνία των επιχειρήσεων με τα άτομα. Κατά το GDPR, το άτομο θα πρέπει να παρέχει την ρητή του συγκατάθεση για τον τρόπο που επιθυμεί να γίνεται η επικοινωνία (μέσω email, τηλεφωνικά, καθόλου επικοινωνία, κτλ). (Ευρωπαϊκή Ένωση, 2016j, HCD, 2018, ZogBlog, 2018).

6.2.3. Δικαίωμα διαγραφής προσωπικών δεδομένων

Εδώ αξίζει να σημειωθεί το δικαίωμα για διαγραφή των δεδομένων των υποκειμένων επεξεργασίας. Σύμφωνα με τον Ευρωπαϊκό Κανονισμό GPDR, δίδεται το δικαίωμα στα υποκείμενα επεξεργασίας να ζητήσουν από μία επιχείρηση ή οργανισμό, να διαγράψουν ότι αφορά τα προσωπικά τους δεδομένα, μαζί με όλα τα αντίγραφα ασφαλείας που μπορεί να διατηρούν. Κατά το HIPAA, αυτό δεν καλύπτεται. Επιχειρήσεις ή οργανισμοί, λοιπόν, που δραστηριοποιούνται με πολίτες της ΕΕ, θα πρέπει να είναι σε θέση, αν τους ζητηθεί, να

διαγράψουν όλα τα δεδομένα τους και τα αντίγραφα αυτών, χωρίς να υπάρχει η υποχρέωση από την πλευρά του αιτούντος να αιτιολογήσει την απαίτηση του. (Ευρωπαϊκή Ένωση, 2016j, HCD, 2018, ZogBlog, 2018).

6.2.4. Αντιμετώπιση παραβιάσεων προσωπικών δεδομένων

Όσον αφορά τις παραβιάσεις, κατά το HIPAA, η αντίδραση που θα πρέπει να έχει όποιος εντοπίζει την παραβίαση σε έναν οργανισμό ή μία επιχείρηση (π.χ.ο υπεύθυνος προστασίας δεδομένων), εξαρτάται από το μέγεθος της παραβίασης. Αντιθέτως, κατά το GDPR, δεν ισχύει αυτό. Σύμφωνα με το άρθρο 33, θα πρέπει κάθε παραβίαση που εντοπίζεται, να κοινοποιείται στην αρμόδια εποπτική Αρχή εντός 72 ωρών, μαζί με όλα τα τεκμήρια που την στοιχειοθετούν. (Ευρωπαϊκή Ένωση, 2016j, HCD, 2018, ZogBlog, 2018).

6.2.5. Κρυπτογράφηση δεδομένων

Η κρυπτογράφηση των δεδομένων είναι απαραίτητη σύμφωνα και με τους δύο Κανονισμούς. Το HIPAA, όπως και το GDPR, έχουν ως απαίτηση την κρυπτογράφηση των δεδομένων, όμως είναι χαρακτηριστικό ότι στις ΗΠΑ, ακόμη υπάρχουν επιχειρήσεις που δεν μπορούν να ισχυριστούν με σιγουριά, ότι κρυπτογραφούν τα προσωπικά δεδομένα που διακινούν στο σύνολό τους. Αυτό σε μεγάλο βαθμό, οφείλεται σε έλλειψη εκπαίδευσης των εργαζομένων, αλλά και στην έλλειψη των κατάλληλων και εύχρηστων προγραμμάτων που βοηθούν στην κρυπτογράφηση. (Ευρωπαϊκή Ένωση, 2016j, HCD, 2018, ZogBlog, 2018).

7. ΒΑΣΙΚΑ ΒΗΜΑΤΑ ΕΝΑΡΜΟΝΙΣΗΣ ΜΕ ΤΟ GDPR – CASESTUDY

Το παράδειγμα αφορά στα βασικά βήματα που ακολούθησε ένα γενικό Ιδιωτικό Νοσοκομείο της Αθήνας, με δυναμικότητα 164 κλινών, για να εναρμονιστεί με τον Κανονισμό GDPR. Για τις ανάγκες της ανάλυσης παρακάτω, το Ιδιωτικό Νοσοκομείο θα αναφέρεται ως Νοσοκομείο Χ.

Το Νοσοκομείο Χ, εφαρμόζει Γενικό Σύστημα Ποιότητας και είναι πιστοποιημένο σύμφωνα με το ISO EN15224 και το ISO 9001:2015.

7.1. Βήμα 1: Ορισμός ομάδας έργου για την υλοποίηση του έργου και ρόλοι μελών – Ορισμός DPO

Το Νοσοκομείο Χ, μετά την 27η Απριλίου 2016 και θέλοντας να προλάβει να εναρμονιστεί με τον Κανονισμό GDPR μέχρι την τελική προθεσμία που οριζόταν (25 Μαΐου 2018), όρισε μία ομάδα έργου για να αναλάβει να εναρμονίσει όλες τις διεργασίες που λαμβάνουν χώρα εντός της περιοχής ευθύνης του, και σχετίζονται με προσωπικά δεδομένα, με τον Κανονισμό 2016/679 (GDPR). Η ομάδα από την 25η Μαΐου 2018 και μετά, λειτουργεί υπό την μορφή 12μελούς Επιτροπής, η οποία ονομάζεται «Επιτροπή Ασφαλείας Προσωπικών Δεδομένων και Πληροφοριών» και έχει 3ετή θητεία. Η Επιτροπή αποτελείται από στελέχη με διαφορετικό πεδίο εργασίας εντός του Οργανισμού, ώστε να μπορούν να παρέχονται στον DPO, όλες οι απαραίτητες πληροφορίες που χρειάζεται σύμφωνα με τις αρμοδιότητες του.

Ορισμός DPO: Ο Υπεύθυνος Προστασίας Δεδομένων (DPO), συμβουλεύει τους Υπευθύνους ή Εκτελούντες επεξεργασία, σχετικά με την συμμόρφωση τους, ως προς το GDPR (ΑΠΔΠΧ, 2018l).

Παρακάτω η ομάδα έργου, για ευκολότερη κατανόηση της περιγραφής, αναφέρεται ως Επιτροπή, ανεξάρτητα αν οι ενέργειες που αναφέρονται έγιναν πριν την 25η Μαΐου 2018 όπου συστάθηκε ως Επιτροπή, ή πριν.

Συγκεκριμένα:

- Πρόεδρος: Γενικός Διευθυντής
- Μέλος: Data Protection Officer (DPO)
- Μέλος: Επιστημονικός Διευθυντής
- Μέλος: Επιχειρησιακός Διευθυντής (υποστηρίζει τον DPO ως προς τις υπηρεσίες Πληροφορικής)

- Μέλος: Διευθυντής Νοσηλευτικής Υπηρεσίας – Συντονιστής Ποιότητας (υποστηρίζει τον DPO ως προς τα θέματα της Ποιότητας)
- Μέλος: Διοικητικός Διευθυντής (υποστηρίζει τον DPO ως προς την Κανονιστική Συμμόρφωση)
- Μέλος: Υπεύθυνος Γραμματείας – Αναπληρωτής Συντονιστής Ποιότητας (Οργανώνει και ενημερώνει όλους τους εμπλεκομένους για την πορεία του έργου)
- Μέλος: Προϊστάμενος Μηχανογράφησης (Υπεύθυνος Ασφάλειας των Πληροφοριών)
- Μέλος: Στέλεχος τμήματος Επικοινωνίας και Ανάπτυξης
- Μέλος: Προϊστάμενος Κεντρικού Λογιστηρίου
- Μέλος: Υπεύθυνος Γραφείου Προσωπικού
- Μέλος:Γραμματέας Διοίκησης (Ενημερώνει τους Νομικούς Εκπροσώπους του Νοσοκομείου)

Στόχος του Νοσοκομείου Χ και της Γενικής Διεύθυνσης με τον ορισμό της Επιτροπής είναι να παρέχεται προς τον DPO, η κατάλληλη υποστήριξη σε σχέση με όλες τις διεργασίας που πραγματοποιούνται στο Νοσοκομείο και περιέχουν δεδομένα προσωπικού χαρακτήρα. Το κάθε μέλος επομένως, λειτουργεί υποστηρικτικά ως προς τον DPO ανάλογα με το πεδίο αρμοδιοτήτων του και όπως αυτό αναγράφεται στην Περιγραφή Θέσης Εργασίας του.

7.2. Βήμα 2: Εκπαίδευση μελών Επιτροπής στον Κανονισμό GDPR

Ως δεύτερο βήμα αναφέρεται η εκπαίδευση των μελών της Επιτροπής στον Κανονισμό GDPR και τις απαιτήσεις του. Το Νοσοκομείο Χ, παρείχε στα μέλη, όλα τα εργαλεία και το υλικό που χρειάζονταν για την ενημέρωση τους σχετικά με τον Κανονισμό. Επίσης, ο DPO μαζί με τον Επιχειρησιακό Διευθυντή συμμετείχαν σε εξειδικευμένο σεμινάριο για το GDPRκαι τις αρμοδιότητες του DPO, ώστε να αποκτήσουν την απαραίτητη τεχνογνωσία και να την μεταλαμπαδεύσουν και στα υπόλοιπα μέλη της Επιτροπής. Σημαντική είναι η συμμετοχή των Νομικών Συμβούλων του Νοσοκομείουστο έργο, οι οποίοι σε όλα τα στάδια καθοδηγούν και συμβουλεύουν την Επιτροπή σύμφωνα με όσα ορίζονται από τον Κανονισμό.

7.3. Βήμα 3: GAP Analysis & Compliance Plan (που είμαστε και που πρέπει να φτάσουμε)

Η Επιτροπή, πραγματοποίησε εσωτερική επιθεώρηση στο σύνολο του Οργανισμού και κατέγραψε όλα τα ευρήματα (ελλείψεις/αποκλίσεις) που έχρηζαν διορθωτικών ενεργειών

σύμφωνα με τον Κανονισμό GDPR. Για την αποτύπωση και τον σχεδιασμό δημιουργήθηκε ένα πλάνο με τα αποτελέσματα της επιθεώρησης, που περιελάμβανε ανά στήλη, τα ευρήματα (ελλείψεις/αποκλίσεις), τις προτεινόμενες ενέργειες συμμόρφωσης, τους υπευθύνους υλοποίησης (προϊστάμενοι & υπεύθυνοι τμημάτων), την προθεσμία υλοποίησης και τις σχετικές παρατηρήσεις. Για κάθε εύρημα έγινε συσχέτιση με το αντίστοιχο άρθρο ή αιτιολογική παράγραφο του Κανονισμού GDPR που αφορούσε. Το πλάνο αυτό είναι το GAP analysis & Compliance Plan της Επιτροπής και αποτελεί το βασικό αντικείμενο της για την έναρξη των εργασιών της.

Ορισμός GAP Analysis (Ανάλυση Ελλείψεων): Η ανάλυση των ελλείψεων σε σχέση με το GDPR, είναι η τεχνική μελέτη μέσω της οποίας συντάσσεται αναλυτική έκθεση σχετικά με τις ελλείψεις του Οργανισμού ως προς τις απαιτήσεις του Κανονισμού, αναφέρονται σχετικές καλές πρακτικές (best practices) και προτάσεις βελτίωσης με σκοπό την εναρμόνιση με το GDPR. (Καραλιβανός, 2017).

Ορισμός Compliance Plan (Σχέδιο Συμμόρφωσης): Πρόκειται για ένα πλάνο το οποί συντάσσεται μετά την ανάλυση ελλείψεων και περιλαμβάνει προτεραιοποιημένες και ανά κατηγορία, τις ενέργειες που πρέπει να γίνουν από την πλευρά του Οργανισμού, με σκοπό την συμμόρφωση με τον Κανονισμό. (Priority, 2018).

Παρατίθενται παραδείγματα ελλείψεων/αποκλίσεων του Νοσοκομείου Χ, σύμφωνα με τα ανωτέρω:

- Σε δείγματα που αποστέλλονταν για ανάλυση σε εξωτερικά εργαστήρια εντοπίστηκε ότι συνοδεύονταν από περισσότερα δεδομένα ασθενών από όσα ήταν απαραίτητα. Το Νοσοκομείο Χ για να είναι σύμφωνο με τον Κανονισμό θα έπρεπε να προχωρήσει σε απάλειψη ή κρυπτογράφηση των στοιχείων των ασθενών, με εξαίρεση τις περιπτώσεις που υπάρχει ρητή συγκατάθεση των ασθενών για μεταβίβαση επιπλέον, των ελαχίστων απαραιτήτων, στοιχείων. Το Νοσοκομείο Χ, μέσω της Επιτροπής και σε συνεργασία με την Διευθύντρια του Μικροβιολογικού Εργαστηρίου, προχώρησε άμεσα σε ψευδωνυμοποίηση των προαναφερόμενων στοιχείων.

- Κατά την εσωτερική επιθεώρηση, εντοπίστηκε ότι δεν υπήρχαν τοποθετημένοι καταστροφείς εγγράφων, σε κάθε σταθμό εργασίας, με αποτέλεσμα να μην διασφαλίζεται η καταστροφή των εγγράφων που περιείχαν προσωπικά δεδομένα. Αμέσως μετά την κατάρτιση

του GAP Analysis, παραγγέλθηκαν και τοποθετήθηκαν καταστροφείς εγγράφων σε κάθε τμήμα που διαχειρίζεται αρχεία με προσωπικά δεδομένα.

- Εντοπίστηκε ότι, οι κωδικοί πρόσβασης στο πληροφοριακό σύστημα του Νοσοκομείου δεν ήταν αρκετά περίπλοκοι και δεν υπήρχε οργανωμένο σύστημα αλλαγής των κωδικών σε τακτά χρονικά διαστήματα. Το κενό καλύφθηκε πολύ άμεσα με αλλαγή όλων των κωδικών και υποχρεωτική αλλαγή ανά εύλογο χρονικό διάστημα.

Για την οργάνωση των δραστηριοτήτων που απαιτούνται, το Νοσοκομείο Χ, έχει αναπτύξει σε συνεργασία με εταιρεία σχεδιασμού λογισμικών, ειδική πλατφόρμα διαχείρισης σύμφωνα με τις δικές του ανάγκες. Η συγκεκριμένη πλατφόρμα λειτουργεί μέσω intranet και δεν δίνει την δυνατότητα απομακρυσμένης χρήσης. Επίσης, η προσβασιμότητα δίνεται μέσω ατομικών κωδικών και με προκαθορισμένα δικαιώματα ανά χρήστη. Μέσω της συγκεκριμένης πλατφόρμας, υπάρχει πλήρης παρακολούθηση όλων των διεργασιών του έργου καθώς σε αυτό το στάδιο έγινε καταχώρηση του συνόλου του πλάνου.

7.4. Βήμα 4: Ενημέρωση όλου του εμπλεκόμενου προσωπικού σχετικά με τις απαιτήσεις του Κανονισμού GDPR

Για την ενημέρωση όλου του προσωπικού που μπορεί να διαχειριστεί, επεξεργαστεί, αποθηκεύσει δεδομένα προσωπικού χαρακτήρα, πραγματοποιήθηκαν ενδο-επιχειρησιακά σεμινάρια, με εισηγητές εξειδικευμένους εκπαιδευτές, αλλά και τον DPO του Νοσοκομείου. Τα σεμινάρια περιελάμβαναν την ανάλυση και επεξήγηση του κανονισμού GDPR. Επίσης, στα σεμινάρια αυτά, παρουσιάστηκε στο προσωπικό ο νέος ρόλος που ενσωματωνόταν πλέον στο Νοσοκομείο, αυτός του DPO. Δόθηκαν κατευθυντήριες οδηγίες ως προς τα κρίσιμα σημεία που πρέπει το προσωπικό να μην αμελεί και να τηρεί αλλά και ως προς την δυνατότητα επικοινωνίας, ανά πάσα στιγμή, με τον DPO για όσα σχετίζονται με τα προσωπικά δεδομένα. Τέλος, ενημερώθηκαν σχετικά με τα δικαιώματα τους ως φυσικά πρόσωπα που τα προσωπικά δεδομένα τους υπόκεινται σε οποιασδήποτε μορφής επεξεργασία.

Το υλικό των σεμιναρίων δόθηκε σε έντυπη και ηλεκτρονική μορφή στους συμμετέχοντες, μαζί με όλα τα στοιχεία επικοινωνίας με τον DPO του Νοσοκομείου.

7.5. Βήμα 5: Ορισμός υπευθύνων υλοποίησης ανά εύρημα

Η Επιτροπή, στην πρώτη της συνεδρίαση, μετά την ολοκλήρωση του πλάνου GAP Analysis, όρισε τους υπευθύνους υλοποίησης ανά εύρημα, σύμφωνα με την Περιγραφή Θέσης

Εργασίας του καθενός. Ορισμένα ευρήματα ορίστηκαν ως διατμηματικά. Για την οργάνωση και τον συντονισμό των διατμηματικών ευρημάτων, ο DPO, συμμετείχε στην υπό-ομάδα που οριζόταν για την υλοποίηση της ενέργειας συμμόρφωσης, ώστε να αποτελεί τον συνδετικό κρίκο μεταξύ των εμπλεκομένων.

Αν ο υπεύθυνος υλοποίησης μίας δράσης, για κάποιο λόγο αδυνατούσε να προχωρήσει στην ολοκλήρωση της, τότε ενημέρωνε τον DPO και την Επιτροπή, οι οποίοι αναλάμβαναν να βοηθήσουν τον υπεύθυνο υλοποίησης και να τον ενισχύσουν με τα απαραίτητα μέσα. Αν ο υπεύθυνος υλοποίησης που είχε οριστεί από την Επιτροπή, αποδείκνυε ότι, η συγκεκριμένη δράση δεν ενέπιπτε στο δικό του πεδίο αρμοδιοτήτων, τότε η Επιτροπή σε συνεργασία με τον DPO, αναλάμβανε να ορίσει νέο υπεύθυνο υλοποίησης.

7.6. Βήμα 6: Ενημέρωση υπευθύνων υλοποίησης

Η ενημέρωση όλων των υπευθύνων υλοποίησης των διορθωτικών ενεργειών, έγινε ηλεκτρονικά μέσω της ειδικά διαμορφωμένης πλατφόρμας που αναφέρθηκε σε προηγούμενο βήμα.

Η πλατφόρμα αυτή, παρέχει τη δυνατότητα στον χρήστη να καταχωρεί τον υπεύθυνο υλοποίησης ανά δράση και αυτόματα να του αποστέλλει όλη την ενημέρωση που χρειάζεται για να ξεκινήσει τις απαραίτητες δράσεις. Ο υπεύθυνος υλοποίησης λαμβάνει όλες τις πληροφορίες που τον αφορούν μέσω email. Με άξονα τις πληροφορίες του συγκεκριμένου email, ο υπεύθυνος υλοποίησης οργανώνει τις απαραίτητες εργασίες για την επίτευξη της Κανονιστικής συμμόρφωσης. Όταν οι εργασίες του ολοκληρωθούν, ενημερώνει τον DPO και την Επιτροπή και αποστέλλει τεκμηρίωση της ολοκλήρωσης της απαραίτητης δράσης, η οποία καταχωρείται στην πλατφόρμα και εξαιρεί την συγκεκριμένη έλλειψη ή απόκλιση από τις εκκρεμότητες για την εναρμόνιση του Νοσοκομείου Χ στον Κανονισμό GDPR. Στόχος είναι η ολοκλήρωση, με την απαραίτητη τεκμηρίωση, όλων των ελλείψεων/αποκλίσεων που έχουν συμπεριληφθεί στο πλάνο GAP Analysis και όλων όσων μπορεί να εντοπίζονται σε κάθε ανασκόπηση των εργασιών, ώστε το Νοσοκομείο Χ να λειτουργεί πάντα σύμφωνα με τον Κανονισμό GDPRκαι τις απαιτήσεις του, σε όλα τα επίπεδα των διεργασιών του.

7.7. Βήμα 7: Καθολική συμμετοχή του προσωπικού στην υλοποίηση του έργου και στην καθημερινή προστασία των δεδομένων προσωπικού χαρακτήρα

Η Επιτροπή Ασφαλείας Προσωπικών Δεδομένων και Πληροφοριών του Νοσοκομείου Χ και οι υπεύθυνοι υλοποίησης των επιμέρους ελλείψεων, για την ολοκλήρωση του έργου, πρέπει

να έχουν την υποστήριξη του συνόλου του προσωπικού. Για την ορθή λειτουργία του Νοσοκομείου Χ, σύμφωνα με τις απαιτήσεις του Κανονισμού GDPR, είναι απαραίτητη η συμμετοχή όλων των εμπλεκομένων στην διαχείριση δεδομένων προσωπικού χαρακτήρα. Για παράδειγμα, η Επιτροπή οφείλει να ενημερώσει την Διοίκηση του νοσοκομείου και το τμήμα Πληροφορικής για την ανάγκη κρυπτογράφησης των ηλεκτρονικών μηνυμάτων (email), η Διοίκηση με την σειρά της, θα πρέπει να παρέχει τα απαραίτητα μέσα για την κρυπτογράφηση τους. Όμως, αν οι χρήστες (αποστολείς), των email, δεν τηρούν τα όσα οι προηγούμενοι ορίζουν και παρέχουν, τότε το Νοσοκομείο Χ, μπορεί να βρεθεί να εκθέτει δεδομένα προσωπικού χαρακτήρα, αν και έχει λάβει όλα τα τυπικά απαραίτητα μέσα.

Η Επιτροπή, σε συνεργασία με την Διοίκηση του Νοσοκομείου Χ, εφάρμοσε τις αρχές του μοντέλου Διοίκησης Αλλαγών με τα 8 βήματα που προτείνονται από τον Kotter. Η τακτική αυτή δημιούργησε ένα έντονο αίσθημα ευθύνης από την πλευρά όλων των εργαζομένων και βοήθησε την Επιτροπή στο να διεκπεραιώνει τις εκκρεμότητες που είχε εξαρχής θέσεις, με σκοπό πάντα την εναρμόνιση του Νοσοκομείου με τον Κανονισμό GDPR για την προστασία των προσωπικών δεδομένων που επεξεργάζεται. (Kotter, 2018).

Παρακάτω αναλύεται βήμα προς βήμα, ο τρόπος με τον οποίο η Επιτροπή κατάφερε να ενσωματώσει το έντυπο Ενημέρωσης και Συγκατάθεσης των Ασθενών που εισέρχονται στο Νοσοκομείο για Νοσηλεία, σχετικά με την Προστασία των Δεδομένων Προσωπικού Χαρακτήρα. Το συγκεκριμένο έντυπο, διατίθεται από το Νοσοκομείο στα ελληνικά και στα αγγλικά, είναι ανηρτημένο σε όλους τους χώρους που εξυπηρετούνται νοσηλευόμενοι ή εισαχθέντες και μεταξύ άλλων περιλαμβάνει υποχρεώσεις και δικαιώματα των ίδιων των ασθενών, τους σκοπούς επεξεργασίας των δεδομένων τους από το Νοσοκομείο, συγκατάθεση ή άρνηση επικοινωνίας μέσω email, smsή εφαρμογών κινητού και τέλος όλα τα απαραίτητα στοιχεία επικοινωνίας με τον DPO (διεύθυνση, τηλέφωνο, email). (πίνακας 7.7.1)

ΕΝΣΩΜΑΤΩΣΗ ΕΝΤΥΠΟΥ ΕΝΗΜΕΡΩΣΗΣ ΚΑΙ ΣΥΓΚΑΤΑΘΕΣΗΣ ΑΣΘΕΝΩΝ ΠΟΥ ΚΑΝΟΥΝ ΕΙΣΑΓΩΓΗ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΤΟΥΣ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΤΗΝ ΔΙΑΧΕΙΡΙΣΗ ΑΥΤΩΝ, ΣΤΗΝ ΚΑΘΗΜΕΡΙΝΗ ΛΕΙΤΟΥΡΓΙΑ ΤΩΝ ΤΜΗΜΑΤΩΝ	**ΜΟΝΤΕΛΟ KOTTER**
Μέσω της εκπαίδευσης του συνόλου του προσωπικού,πραγματοποιήθηκε αναλυτική ενημέρωση σχετικά με την σπουδαιότητα και την αναγκαιότητα της ρητής συγκατάθεσης από την πλευρά του ασθενή για την επεξεργασία των προσωπικών του δεδομένων και την νομική υποχρέωση που είχε πλέον το Νοσοκομείο, να τον ενημερώνει με απλά κατανοητά λόγια για τα δικαιώματα του. Το προσωπικό ενημερώθηκε και κατανόησε πλήρως την πιθανότητα επιβολής προστίμων, σε περίπτωση που αποδειχθεί ότι δεν τηρεί τις απαιτήσεις του Κανονισμού GDPR, κατανοώντας την ανάγκη για άμεση προσαρμογή των ήδη υπαρχουσών διαδικασιών με σκοπό την συμμόρφωση προς τον Κανονισμό.	1. Δημιουργία αισθήματος επείγοντος
Η Επιτροπή, σε συνεργασία με τον DPO, αποτέλεσαν την ομάδα καθοδήγησης των εμπλεκομένων προσώπων.	2. Συγκρότηση ομάδας καθοδήγησης

Η Επιτροπή, γνωρίζοντας της απαιτήσεις του Κανονισμού σε σχέση με την ρητή συγκατάθεση του υποκειμένου επεξεργασίας (στο παράδειγμα: του ασθενή), αποφάσισε να αναπτύξει το Έντυπο Ενημέρωσης και Συγκατάθεσης Ασθενών, το οποίο υπογράφεται κατά την εισαγωγή κάθε ασθενή.	3. Ανάπτυξη οράματος
Ακολούθησε συγκεκριμένη ενημέρωση και ανάλυση του εντύπου προς τους Υπεύθυνους και τους Συντονιστές των Γραμματειών Εισαγωγής Ασθενών, οι οποίοι εκπαιδεύτηκαν και έλαβαν κατευθυντήριες οδηγίες σχετικά με τον τρόπο που πρέπει να επικοινωνούν τα περιεχόμενα του εντύπου προς τους ασθενείς. Η ενημέρωση έγινε από την Επιτροπή Ασφαλείας Προσωπικών Δεδομένων και Πληροφοριών του Νοσοκομείου.Οι Υπεύθυνοι και οι Συντονιστές των εμπλεκόμενωνΓραμματειών, ενημέρωσαν και εκπαίδευσαν με την σειρά τους, όλους τους Γραμματείς ευθύνης τους, αλλά και τα εμπλεκόμενα Νοσηλευτικά Τμήματα.	4. Μετάδοση του οράματος
Αποφασίστηκε για την αποφυγή αστοχιών, το έντυπο αμέσως μόλις υπογράφεται να σαρώνεται και να αποθηκεύεται στον Ηλεκτρονικό Ιατρικό Φάκελο του Ασθενούς από τον Γραμματέα Εισαγωγής και να παραδίδεται μαζί με όλα τα υπόλοιπα	5. Ενδυνάμωση και υποστήριξη του οράματος

απαραίτητα έγγραφα στην Υπεύθυνη Νοσηλεύτρια Εισαγωγής. Το έντυπο ορίστηκε ως απαραίτητο για τον Ιατρικό Φάκελο του Ασθενούς. Αυτό είχε ως αποτέλεσμα, η Νοσηλεύτρια Εισαγωγής που λαμβάνει όλα τα απαραίτητα έγγραφα του Φακέλου κατά την Εισαγωγή, να λειτουργεί ως δεύτερο επίπεδο ελέγχου, της ύπαρξης του Εντύπου. Το Νοσοκομείο Χ, λόγω της εφαρμογής Γενικού Συστήματος Ποιότητας, έχει αναπτύξει μία κουλτούρα συνεχούς παρακολούθησης της τήρησης των διαδικασιών και οδηγιών σε όλα του τα επίπεδα. Αυτό έχει ως αποτέλεσμα κάθε υπάλληλος να νιώθει πάντα ένα αίσθημα ευθύνης για την αποφυγή αστοχιών και ως εκ τούτου ελλείψεων μέσα στον Φάκελο του Ασθενούς. Τέλος, ο Γραμματέας εισαγωγής, καταχωρεί μία επιπλέον σήμανση στο Πληροφοριακό Σύστημα του Νοσοκομείου, σχετικά με την αποδοχή ή άρνηση για επικοινωνία από την πλευρά του υποκειμένου για την επεξεργασία των προσωπικών δεδομένων (ασθενή). Όλα τα προαναφερθέντα λειτουργούν υποστηρικτικά ως προς την επίτευξη της ενσωμάτωσης του εντύπου.	
Το προσωπικό ενημερώθηκε πολύ σύντομα για την επίτευξη της επιτυχούς και ολοκληρωτικής λειτουργίας του εντύπου και για τα αποτελέσματα ενός πρώτου ελέγχου, όπου δεν απουσίαζε	6. Δημιουργία βραχυπρόθεσμων επιτυχιών

κανένα έντυπο από Ιατρικό φάκελο Ασθενούς.	
Μετά την συμπλήρωση των πρώτων 6 μηνών λειτουργίας του εντύπου, η Επιτροπή σε συνεργασία με την Διοίκηση του Νοσοκομείου και το τμήμα Πληροφορικής, διερευνά την δυνατότητα ενσωμάτωσης νέων συστημάτων για την υλοποίηση της διαδικασίας εισαγωγής ασθενούς που να περιλαμβάνει την δυνατότητα ηλεκτρονικής υπογραφής, ώστε να μειωθεί ο απαιτούμενος χρόνος ολοκλήρωσης της διαδικασίας και να μην είναι πλέον απαραίτητη η σάρωση των εγγράφων και η χειροκίνητη καταχώρηση δεδομένων (π.χ. η άρνηση για επικοινωνία μέσω email) προς διευκόλυνση των εμπλεκομένων εργαζομένων.	7. Παγίωση των αλλαγών και καθορισμός νέων στόχων
Το έντυπο έχει ενσωματωθεί πλήρως στην συνείδηση των εμπλεκόμενων εργαζομένων και αποτελεί απαραίτητη προϋπόθεση για την εισαγωγή ασθενούς στο Νοσοκομείο Χ. Περιλαμβάνεται σε όλες τις οδηγίες και τις διαδικασίες που περιγράφουν την εισαγωγή ενός ασθενούς στο Νοσοκομείο. Πλέον, αποτελεί μία συνήθεια των εργαζομένων στις εισαγωγές ασθενών.	8. Ενσωμάτωση της αλλαγής στις αξίες και την κουλτούρα του Οργανισμού.

Πίνακας 7.7.1: Παράδειγμα εφαρμογής Διοίκησης Αλλαγών(μοντέλο Kotter)

7.8. Βήμα 8: Ανασκόπηση εργασιών και συνεχής παρακολούθηση

Στη λειτουργία της Επιτροπής Ασφαλείας Προσωπικών Δεδομένων και Πληροφοριών, έχει οριστεί η υποχρέωση για συνεδρίαση σε τακτά χρονικά διαστήματα. Συγκεκριμένα, λόγω της

σπουδαιότητας του αντικειμένου της, η Επιτροπή συνεδριάζει σε τακτική βάση μηνιαίως και σε έκτακτη, όποτε και αν παραστεί ανάγκη.

Με σκοπό την συνεχή παρακολούθηση των διεργασιών που έχουν μοιραστεί και ανατεθεί στους διάφορους υπεύθυνους υλοποίησης μέσα στο Νοσοκομείο, η Επιτροπή σε κάθε συνεδρίαση της, ανασκοπεί τις εκκρεμότητεςτου αρχικού GAP Analysis που είχε γίνει αλλά και τις εκκρεμότητες από τις νέες δράσεις που ορίζονται σε κάθε συνεδρίαση της. Η παρακολούθηση όλων των εκκρεμοτήτων γίνεται με τη βοήθεια της ειδικής πλατφόρμας που αναφέρθηκε σε προηγούμενη παράγραφο. Μία από τις δυνατότητες της πλατφόρμας είναι η εξαγωγή αποτελεσμάτων σε όποια μορφή επιθυμεί ο χρήστης (excel, pdf, κτλ) με αποτέλεσμα να τον βοηθά στην ταξινόμηση των εκκρεμοτήτων.

Σε κάθε συνεδρίαση ορίζονται επιπλέον νέες εκκρεμότητες που στηρίζονται στην τακτική του Νοσοκομείου Χ, να λειτουργεί προληπτικά και σύμφωνα με την αξιολόγηση κινδύνων που γίνεται στα πλαίσια της εφαρμογής του Γενικού Συστήματος Ποιότητας.

Αξίζει να σημειωθεί ότι, εκτός από τις τακτικές και έκτακτες συνεδριάσεις της Επιτροπής, όλα τα μέλη ενημερώνονται σε εβδομαδιαία βάση για το σύνολο των εκκρεμοτήτων, λαμβάνοντας τες σε μορφή excel. Επίσης, όλοι οι υπεύθυνοι υλοποίησης λαμβάνουν εξατομικευμένα αρχεία excel με τις δικές τους εκκρεμότητες, ως υπενθύμιση και ως προς διευκόλυνση τους, λόγω του πλήθους των ενημερώσεων στις οποίες εμπλέκονται. Τα εξατομικευμένα αρχεία excel που λαμβάνουν, αποτελούν, πάντα, την πιο ανανεωμένη μορφή των δικών τους εκκρεμοτήτων, συμπεριλαμβανομένων όλων των αλλαγών που γίνονται συνεχώς. Αυτή η ενημέρωση έχει ως σκοπό την αποσυμπίεση των εμπλεκομένων ως προς το άγχος της παρακολούθησης των εκκρεμοτήτων των διεργασιών.

ΣΥΜΠΕΡΑΣΜΑΤΑ – ΣΥΖΗΤΗΣΗ

Από όλα τα παραπάνω, είναι σαφές ότι ο Γενικός Κανονισμός Προστασίας Δεδομένων – GDPR, αφορά κάθε φυσικό πρόσωπο αλλά και μεγάλο μέρος των Οργανισμών και Επιχειρήσεων και δικαίως έχει βρεθεί στην επικαιρότητα από την δημοσίευση του, το 2016, ως σήμερα.

Είναι φανερό ότι, υπήρχαν σημαντικές ελλείψεις στην νομοθεσία της Ε.Ε. και των κρατών – μελών σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα και μέσω του GDPR γίνεται σημαντική προσπάθεια να καλυφθεί κάθε κενό. Αποσαφηνίζονται ορισμοί που δεν ήταν ξεκάθαροι, δημιουργούνται νέες ιδιότητες(π.χ.DPO), προστατεύονται ομάδες φυσικών προσώπων και αποκτούν σημαντικά δικαιώματα σε σχέση με τα προσωπικά τους δεδομένα. Η ρητή συγκατάθεση του φυσικού προσώπου σε καθετί που σχετίζεται με τα δεδομένα του, αποκτά άλλη βαρύτητα, λόγω των υπέρογκων προστίμων,και όχι μόνο, που επιφέρει η παράβλεψη του.

Το GDPR, εκτός από τις Επιχειρήσεις και τους Οργανισμούς που δρουν εντός της Ε.Ε., καταφέρνει να θέσει όρια και στις προσβάσεις που έχουν αντίστοιχες Επιχειρήσεις και εκτός της Ε.Ε., σε σχέση με φυσικά πρόσωπα που βρίσκονται εντός της. Λόγω της ραγδαίας τεχνολογικής εξέλιξης και της παγκοσμιοποίησης πολλές εταιρείες δρουν απομακρυσμένα σε χώρες που βρίσκονται εντός της Ε.Ε. και επεξεργάζονται (διατηρούν, αποθηκεύουν, μεταφέρουν), δεδομένα προσωπικού χαρακτήρα.

Στην ανωτέρω ανάλυση, δεν παραλείπεται και η σχέση που προκύπτει μεταξύ του GDPR και του HIPAA, καθώς πρόκειται για νομοθετικές διατάξεις σε Ευρώπη και ΗΠΑ, αντιστοίχως. Η βασική του διαφορά έγκειται στα νομικά πρόσωπα που πρέπει να εναρμονίζονται στοGDPR ή το HIPAA, κατά περίπτωση. Το GDPR απευθύνεται σε κάθε Επιχείρηση ή Οργανισμό που επεξεργάζεται προσωπικά δεδομένα φυσικών προσώπων που βρίσκονται εντός της Ε.Ε. Το HIPAA απευθύνεται σε Οργανισμούς ή Υπηρεσίες υγειονομικής περίθαλψης, που επεξεργάζονται συγκεκριμένα προσωπικά δεδομένα (PHI ή ePHI) στις ΗΠΑ.

Από το Νοσοκομείο Χ (case study) και τον τρόπο που εργάστηκε για την εναρμόνιση του με τον Κανονισμό GDPR, γίνεται σαφής η ανάγκη για συνεχή έλεγχο των διεργασιών του και καθημερινή παρακολούθηση όλων των διαδικασιών, ώστε να μην βρεθεί ευάλωτο λόγω έκθεσης προσωπικών δεδομένων οποιασδήποτε κατηγορίας φυσικών προσώπων (προμηθευτών, εργαζομένων ή ασθενών).

Στην παρούσα διατριβή, προτείνεται, κάθε Οργανισμός ή Επιχείρηση,που επιθυμεί να εναρμονιστεί με τον Κανονισμό με οργάνωση και συνέπεια, να ξεκινήσει κάνοντας εσωτερική επιθεώρηση με σκοπό την σύνταξη ενός αναλυτικού GAP Analysis αλλά και Data Flow Mapping (μέσω συνεντεύξεων ή workshops) ώστε να γνωρίζει η Διοίκηση που βρίσκεται και που πρέπει να φτάσει σύμφωνα με τις απαιτήσεις του Κανονισμού GDPR. Στην συνέχεια, να δημιουργήσει μία ομάδα διαχείρισης ή μια Επιτροπή για το συγκεκριμένο έργο, με μέλη από διάφορα τμήματα του Οργανισμού και από διαφορετικά επίπεδα (π.χ. προϊστάμενοι, γραμματείς, διευθυντές). Με επικεφαλής τον DPO και τον Υπεύθυνο Ασφαλείας, όπως αυτοί θα οριστούν σύμφωνα με τον Κανονισμό, να μοιραστούν αρμοδιότητες σε κάθε μέλος. Τέλος, η ομάδα θα πρέπει να συνεδριάζει σε τακτά χρονικά διαστήματα, να επιβλέπονται οι δραστηριότητες και να θέτονται συνεχώς νέοι στόχοι (βραχυπρόθεσμοι και μακροπρόθεσμοι).

Είναι σημαντικό, κάθε εμπλεκόμενος Οργανισμός ή Επιχείρηση, να αντιληφθεί πως το GDPR είναι πλέον σε ισχύ και αποτελεί κανονιστική συμμόρφωση η οποία για να συμβεί απαιτεί, σε όλα τα επίπεδα, στρατηγική, νομική, τεχνολογική, τεχνική, πολιτική, και διοικητική υποστήριξη με συνεχή παρακολούθηση και αξιολόγηση.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. (2011). *Οδηγία 2/2011: Ηλεκτρονική συγκατάθεση στο πλαίσιο του άρθρου 11 του ν. 3471/2006.* (Τόμ. Β, Αρ. 889): Εφημερίδα της Κυβέρνησης.

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. (2018a) Διαθέσιμο σε: http://www.dpa.gr (Ανακτήθηκε 1 Ιουνίου, 2018).

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. (2018b) *Αποστολή της Αρχής.* Διαθέσιμο σε: http://www.dpa.gr/portal/page?_pageid=33,14970&_dad=portal&_schema=PORTAL (Ανακτήθηκε 12 Ιουλίου, 2018).

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. (2018c) *Προσωπικά Δεδομένα.* Διαθέσιμο σε: http://www.dpa.gr/portal/page?_pageid=33,213319&_dad=portal&_schema=PORTAL (Ανακτήθηκε 12 Ιουλίου, 2018).

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. (2018d). *Διοικητικές – ελεγκτικές αρμοδιότητες της Αρχής*. Διαθέσιμο σε: http://www.dpa.gr/portal/page?_pageid=33,23031&_dad=portal&_schema=PORTAL(Ανακτήθηκε 12 Ιουλίου, 2018).

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. (2018e). *Κανονιστικές – Συμβουλευτικές αρμοδιότητες της Αρχής.* Διαθέσιμο σε: http://www.dpa.gr/portal/page?_pageid=33,23220&_dad=portal&_schema=PORTAL (Ανακτήθηκε 12 Ιουλίου, 2018).

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. (2018f) *Αρμοδιότητες Απολογισμού – Δημοσιοποίησης - Συνεργασιών*. Διαθέσιμο σε: http://www.dpa.gr/portal/page?_pageid=33,23266&_dad=portal&_schema=PORTAL (Ανακτήθηκε 12 Ιουλίου, 2018).

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. (2018g). *Προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού*. Διαθέσιμο σε: http://www.dpa.gr/portal/page?_pageid=33,213228&_dad=portal&_schema=PORTAL (Ανακτήθηκε 12 Αυγούστου, 2018).

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (2018h). *Αρχεία δραστηριοτήτων επεξεργασίας.* Διαθέσιμο σε: http://www.dpa.gr/portal/page?_pageid=33,211400&_dad=portal&_schema=PORTAL(Ανακτήθηκε 12 Αυγούστου, 2018).

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. (2018i). *Γνωστοποίηση περιστατικών παραβίασης δεδομένων.* Διαθέσιμο σε: http://www.dpa.gr/portal/page?_pageid=33,211125&_dad=portal&_schema=PORTAL (Ανακτήθηκε 12 Αυγούστου, 2018).

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, (2018j). *Κώδικες Δεοντολογίας.* Διαθέσιμο σε: http://www.dpa.gr/portal/page?_pageid=33,211438&_dad=portal&_schema=PORTAL(Ανακτήθηκε 22 Σεπτεμβρίου, 2018).

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. (2018k). *Πιστοποίηση-Διαπίστευση.* Διαθέσιμο σε: http://www.dpa.gr/portal/page?_pageid=33,213183&_dad=portal&_schema=PORTAL(Ανακτήθηκε 22 Σεπτεμβρίου, 2018).

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. (2018l). *Υπεύθυνος Προστασίας Δεδομένων.* Διαθέσιμο σε: http://www.dpa.gr/portal/page?_pageid=33,211475&_dad=portal&_schema=PORTAL(Ανακτήθηκε 27Νοεμβρίου, 2018).

Βάρκα Αδάμη, Α. (2005). *Εισαγωγή στο αστικό δίκαιο*. Εκδόσεις Σακκουλά.

Βουλή των Ελλήνων. (1997). *Ν.2472/1997: Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα με ενσωματωμένες τις τροποποιήσεις.* (Τόμ. Α, Αρ. 50): Εφημερίδα της Κυβέρνησης.

Βουλή των Ελλήνων. (1998). *Ν.2623/1998: Ανασύνταξη των εκλογικών καταλόγων, οργάνωση και άσκηση του εκλογικού δικαιώματος των ετεροδημοτών, εκσυγχρονισμός της εκλογικής διαδικασίας και άλλες διατάξεις.* (Τόμ. Α, Αρ. 139): Εφημερίδα της Κυβέρνησης.

Βουλή των Ελλήνων. (1999a). *Ν.2703/1999: Αναπροσαρμογή συντάξεων συνταξιούχων μελών Δ.Ε.Π. των Α.Ε.Ι., Ε.Π. των Τ.Ε.Ι., γιατρών Ε.Σ.Υ. και διπλωματικών υπαλλήλων, ρύθμιση συνταξιοδοτικών θεμάτων και άλλες διατάξεις*. (Τόμ. Α, Αρ. 72): Εφημερίδα της Κυβέρνησης.

Βουλή των Ελλήνων. (1999b). *Ν.2721/1999:Τροποποίηση και αντικατάσταση διατάξεων των νόμων 1756/1988 (ΦΕΚ 35 Α'), 1729/1987 (ΦΕΚ 144 Α'), του Ποινικού Κώδικα, του Κώδικα Ποινικής Δικονομίας, του Κώδικα Πολιτικής Δικονομίας και άλλες διατάξεις.* (Τόμ. Α, Αρ. 112): Εφημερίδα της Κυβέρνησης.

Βουλή των Ελλήνων. (2000). *Ν.2819/2000:Ίδρυση εταιρείας «Ολυμπιακό Χωριό 2004 ΑΕ» προστασία Ολυμπιακών Συμβόλων και Σημάτων και άλλες διατάξεις.* (Τόμ. Α, Αρ. 84): Εφημερίδα της Κυβέρνησης.

Βουλή των Ελλήνων. (2001a). *Σύνταγμα της Ελλάδος, μετά την αναθεώρηση του*. (Τόμ. Α, Αρ. 85): Εφημερίδα της Κυβέρνησης.

Βουλή των Ελλήνων. (2001b). *Ν.2915/2001: Επιτάχυνση της τακτικής διαδικασίας ενώπιον των πολιτικών δικαστηρίων και λοιπές δικονομικές και συναφείς ρυθμίσεις.* (Τόμ. Α, Αρ. 109): Εφημερίδα της Κυβέρνησης.

Βουλή των Ελλήνων. (2002a). *Ν.3090/2002: Σύσταση σώματος επιθεώρησης και ελέγχου των καταστημάτων κράτησης και άλλες διατάξεις.* (Τόμ. Α, Αρ. 329): Εφημερίδα της Κυβέρνησης.

Βουλή των Ελλήνων. (2002b). *Ν.3068/2002: Συμμόρφωση της Διοίκησης προς τις δικαστικές αποφάσεις, προαγωγή των δικαστών των τακτικών διοικητικών δικαστηρίων στο βαθμό του συμβούλου Επικρατείας και άλλες διατάξεις.* (Τόμ. Α, Αρ. 274): Εφημερίδα της Κυβέρνησης.

Βουλή των Ελλήνων. (2002c). *Ν.3051/2002: Συνταγματικά κατοχυρωμένες ανεξάρτητες αρχές, τροποποίηση και συμπλήρωση του συστήματος προσλήψεων στο δημόσιο τομέα και συναφείς ρυθμίσεις.* (Τόμ. Α, Αρ. 220): Εφημερίδα της Κυβέρνησης.

Βουλή των Ελλήνων. (2003). *Ν.3156/2003: Ομολογιακά δάνεια, τιτλοποίηση απαιτήσεων και απαιτήσεων από ακίνητα και άλλες διατάξεις.* (Τόμ. Α, Αρ. 157): Εφημερίδα της Κυβέρνησης.

Βουλή των Ελλήνων. (2006). *Ν. 3471/2006: Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997*. (Τόμ. Α, Αρ. 133): Εφημερίδα της Κυβέρνησης.

Βουλή των Ελλήνων. (2007). *Ν.3625/2007 (άρθρο 8): Κύρωση, εφαρμογή του Προαιρετικού Πρωτοκόλλου στη Σύμβαση για τα Δικαιώματα του Παιδιού σχετικά με την εμπορία παιδιών, την παιδική πορνεία και παιδική πορνογραφία και άλλες διατάξεις*. (Τόμ. Α, Αρ. 50): Εφημερίδα της Κυβέρνησης.

Βουλή των Ελλήνων (2008). *Σύνταγμα της Ελλάδος, όπως αναθεωρήθηκε με το Ψήφισμα της 27ης Μαΐου 2008 της Η΄ Αναθεωρητικής Βουλής των Ελλήνων*. Διαθέσιμο σε: https://www.hellenicparliament.gr/UserFiles/8c3e9046-78fb-48f4-bd82-bbba28ca1ef5/SYNTAGMA.pdf (Ανακτήθηκε 10 Ιουλίου, 2018).

Βουλή των Ελλήνων. (2009). *Ν.3783/2009: Ταυτοποίηση των κατόχων και χρηστών εξοπλισμού και υπηρεσιών κινητής τηλεφωνίας και άλλες διατάξεις.* (Τόμ. Α, Αρ. 136): Εφημερίδα της Κυβέρνησης.

Βουλή των Ελλήνων. (2011a). *Ν.3917/2011: Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις.* (Τόμ. Α, Αρ. 22): Εφημερίδα της Κυβέρνησης.

Βουλή των Ελλήνων. (2011b). *Ν.4024/2011: Συνταξιοδοτικές ρυθμίσεις, ενιαίο μισθολόγιο - βαθμολόγιο, εργασιακή εφεδρεία και άλλες διατάξεις εφαρμογής του μεσοπρόθεσμου πλαισίου δημοσιονομικής στρατηγικής 2012-2015.* (Τόμ. Α, Αρ. 226): Εφημερίδα της Κυβέρνησης.

Βουλή των Ελλήνων. (2013). *Ν.4152/2013: Επείγοντα μέτρα εφαρμογής των νόμων 4046/2012, 4093/2012 και 4127/2013.* (Τόμ. Α, Αρ. 107): Εφημερίδα της Κυβέρνησης.

Βουλή των Ελλήνων. (2012). *Ν.4070/2012: Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις.* (Τόμ. Α, Αρ. 82): Εφημερίδα της Κυβέρνησης.

Ευρωπαϊκή Ένωση. (2000). *Χάρτης Θεμελιωδών δικαιωμάτων της Ευρωπαϊκής Ένωσης (Κεφάλαιο ΙΙ, άρθρο 8).* (Τόμ. C, Αρ. 364/1): Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων.

Ευρωπαϊκή Ένωση. (2012). *Ενοποιημένη απόδοση της Συνθήκης για την λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ), Τίτλος Ι, άρθρο 16.* (Τόμ. C, Αρ. 326/47). ΕΕ: Επίσημη Εφημερίδα της ΕΕ.

Ευρωπαϊκή Ένωση. (2016). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Αιτιολογικές παράγραφοι 1, 5 και 6)

Ευρωπαϊκή Ένωση. (2016a). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρο 1, παρ. 1 και 2).

Ευρωπαϊκή Ένωση. (2016b). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρο 4).

Ευρωπαϊκή Ένωση. (2016c). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρο 51).

Ευρωπαϊκή Ένωση. (2016d). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (αιτιολογικές παράγραφοι 14,18 και 27).

Ευρωπαϊκή Ένωση. (2016e). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρο 2, παρ. 1).

Ευρωπαϊκή Ένωση. (2016f). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (αιτιολογικές παράγραφοι 101).

Ευρωπαϊκή Ένωση. (2016g). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρο 3)

Ευρωπαϊκή Ένωση. (2016i). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Αιτιολογική παράγραφος 8).

Ευρωπαϊκή Ένωση. (2016j). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ.

Ευρωπαϊκή Ένωση. (2016k). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρο 7).

Ευρωπαϊκή Ένωση. (2016l). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την*

Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ). (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρο 8).

Ευρωπαϊκή Ένωση. (2016m). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Αιτιολογικές παράγραφοι 32,33,39,43).

Ευρωπαϊκή Ένωση. (2016n). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρο 6).

Ευρωπαϊκή Ένωση. (2016o). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Αιτιολογικές παράγραφοι 51,52,53,54,56).

Ευρωπαϊκή Ένωση. (2016p). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρο 9).

Ευρωπαϊκή Ένωση. (2016q). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρο 5, αιτιολογική παράγραφος 39).

Ευρωπαϊκή Ένωση. (2016r). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρο 13, 14).

Ευρωπαϊκή Ένωση. (2016s). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρο 15).

Ευρωπαϊκή Ένωση. (2016t). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρο 16).

Ευρωπαϊκή Ένωση. (2016u). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρο 17).

Ευρωπαϊκή Ένωση. (2016v). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρο 18).

Ευρωπαϊκή Ένωση. (2016w). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρο 20).

Ευρωπαϊκή Ένωση. (2016x). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρο 21).

Ευρωπαϊκή Ένωση. (2016y). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την*

Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ). (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. Κεφάλαιο IV (Τμήμα 1).

Ευρωπαϊκή Ένωση. (2016z). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρο 24).

Ευρωπαϊκή Ένωση. (2016aa). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρο 25 και αιτιολογική σκέψη 78).

Ευρωπαϊκή Ένωση. (2016ab). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρο 26).

Ευρωπαϊκή Ένωση. (2016ac). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρο 28).

Ευρωπαϊκή Ένωση. (2016ad). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρο 30).

Ευρωπαϊκή Ένωση. (2016ae). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρο 32).

Ευρωπαϊκή Ένωση. (2016af). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρο 33).

Ευρωπαϊκή Ένωση. (2016ag). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).*(Τόμ. L, Αρ. 119): ΕφημερίδατηςΕΕ. (Άρθρο 34).

Ευρωπαϊκή Ένωση. (2016ah). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).*(Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρα 37, 38, 39).

Ευρωπαϊκή Ένωση. (2016ai). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).*(Τόμ. L, Αρ. 119): Επίσημη ΕφημερίδατηςΕΕ. (Άρθρα40, 41).

Ευρωπαϊκή Ένωση. (2016ak). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Άρθρο 42).

Ευρωπαϊκή Ένωση. (2016al). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Κεφάλαιο VI).

Ευρωπαϊκή Ένωση. (2016am). *Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, 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 και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου. (Τόμ. L, Αρ. 119/89). [χ.τ.]: Επίσημη Εφημερίδα της ΕΕ.

Ευρωπαϊκή Ένωση. (2016an). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Επίσημη Εφημερίδα της ΕΕ. (Άρθρα 44 έως 50).

Ευρωπαϊκή Ένωση. (2016ao). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ).* (Τόμ. L, Αρ. 119): Εφημερίδα της ΕΕ. (Κεφάλαιο VIII, Άρθρα 77 έως 84).

Ευρωπαϊκή Επιτροπή, (2018a). Τι είναι τα δεδομένα προσωπικού χαρακτήρα;. Διαθέσιμο σε: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_el#answer (Ανακτήθηκε 1 Ιουνίου, 2018).

Ευρωπαϊκή Επιτροπή, (2018b). Ποια δεδομένα προσωπικού χαρακτήρα θεωρούνται ευαίσθητα;. Διαθέσιμο σε:

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_el (Ανακτήθηκε 1 Ιουνίου, 2018).

Ευρωπαϊκή Επιτροπή, (2018c). Τι αποτελεί επεξεργασία δεδομένων;. Διαθέσιμο σε: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_el (Ανακτήθηκε 1 Ιουνίου, 2018).

Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων (Council of Europe). (2010). *Σύμβαση για την Προστασία των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών. όπως τροποποιήθηκε από τα Πρωτόκολλα υπ' αριθ. 11 και 14 συνοδευόμενη από τα Πρωτόκολλα υπ' αριθ. 1, 4, 6, 7, 12 και 13*. Στρασβούργο: Γραμματεία του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου Ιούνιος 2010.

Ευρωπαϊκό Κοινοβούλιο, Συμβούλιο της Ευρωπαϊκής Ένωσης. (1995). *Προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ελεύθερη κυκλοφορία των δεδομένων αυτών*. Οδηγία 95/46/ΕΚ. (Τόμ. L, Αρ. 281). Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης.

Ευρωπαϊκό Κοινοβούλιο, Συμβούλιο της Ευρωπαϊκής Ένωσης. (1998). περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα. *Οδηγία 97/66/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του*

Συμβουλίου της 15ης Δεκεμβρίου 1997 περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα. (Τόμ. L, Αρ. 024). Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης.

Ευρωπαϊκό Κοινοβούλιο, Συμβούλιο της Ευρωπαϊκής Ένωσης. (2002). Σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες). *Οδηγία 2002/58/εκ του ευρωπαϊκού κοινοβουλίου και του συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες).* (Τόμ. L, Αρ. 201/37). Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης.

Καραγιαννίδου, Χ. *Το Σύνταγμα της Σουηδίας*. Διδακτορική διατριβή. Αθήνα: Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών Σχολή ΝΟΠΕ, Τμήμα Νομικής.

ΚαραλιβανόςΠ. (2017). *GDPRGAPAnalysis: Τι είναι και τι περιλαμβάνει μια ανάλυση ελλείψεων στο πλαίσιο του GDPR.*NiriisS.A. Διαθέσιμο σε: https://www.niriis.gr/gdpr/gdpr-gap-analysis-ti-einai/ (Ανακτήθηκε 27 Νοεμβρίου 2018)

Καρέτσου, Α. (1997). *"Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα".* Έκθεση στο σχέδιο νόμου: Βουλή των Ελλήνων, διεύθυνση επιστημονικών μελετών τμήμα νομοτεχνικής επεξεργασίας σχεδίων και προτάσεων νόμων.

Λασκαρίδης, Ε. (Ιούλιος 2005). Η υποχρέωση τήρησης ιατρικού αρχείου. *Digesta*. Γ:294-310.

Τσόλιας, Γ. (2016). *ΟΔΗΓΙΑ (ΕΕ) 680/2016 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 και την κατάργηση της απόφασης πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου.* Διαθέσιμο σε: http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/20YEARS/FILES%2020YEARS/%CE%A4%CE%A3%CE%9F%CE%9B%CE%99%CE%91%CE%A3.PDF (Ανακτήθηκε 23 Σεπτεμβρίου, 2018).

Andrews, J. (2017). What Are Some Pros & Cons of HIPAA?.Διαθέσιμο σε: https://healthfully.com/75368-pros-cons-hipaa.html (Ανακτήθηκε 10 Οκτωβρίου, 2018).
Council of Europe, (2001). *Convention on Information and Legal Co-operation concerning "Information Society Services".*Διαθέσιμοσε:

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/180 (Ανακτήθηκε 15 Ιουνίου, 2018).

Council of the European Union. (2008). Για την προστασία των δεδομένων προσωπικού χαρακτήρα που τυγχάνουν επεξεργασίας στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις. *Απόφαση πλαίσιο 2008/977/ΔΕΥ του συμβουλίου της 27ης*

Νοεμβρίου 2008. (Τόμ. L, Αρ. 350/60). Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης: Council of the European Union.

Edemekong, P. (2018). *Health Insurance Portability and Accountability Act (HIPAA).*Διαθέσιμοσε: https://www.ncbi.nlm.nih.gov/books/NBK500019/ (Ανακτήθηκε 17 Οκτωβρίου, 2018).

FINRA, Financial Industry Regulatory Authority. Διαθέσιμο σε: https://www.finra.org/(Ανακτήθηκε 10 Οκτωβρίου, 2018).

Gazzetta Team, (2018). *Τι άλλαξε με το GDPR. Η καθ. Δικαίου Πληροφορικής Ευγενία Αλεξανδροπούλου - Αιγυπτιάδου απαντά αν την Παρασκευή ο GDPR έδωσε στα χέρια μας τον έλεγχο των δεδομένων μας.* Διαθέσιμο σε:

http://www.gazzetta.gr/plus/texnologia/article/1234394/ti-allaxe-me-gdpr (Ανακτήθηκε 16 Σεπτεμβρίου, 2018).

HCS, (2018). *What is HIPAA.*Διαθέσιμοσε: https://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00WhatisHIPAA.aspx (Ανακτήθηκε 08 Οκτωβρίου, 2018).

Health Information and the Law, (2016). *Medical Record Retention Required of Health Care Providers: 50 State Comparison.*Διαθέσιμοσε: http://www.healthinfolaw.org/comparative-analysis/medical-record-retention-required-health-care-providers-50-state-comparison (Ανακτήθηκε 10 Οκτωβρίου, 2018).

HHS.gov. (2013a). *The HIPAA Privacy Rule.*Διαθέσιμοσε: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html (Ανακτήθηκε 08 Οκτωβρίου, 2018).

HHS.gov. (2013b). *The Security Rule.* Διαθέσιμο σε: https://www.hhs.gov/hipaa/for-professionals/security/index.html (Ανακτήθηκε 15 Οκτωβρίου, 2018).

HHS.gov. (2013c). *Breach Notification Rule.* Διαθέσιμο σε: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (Ανακτήθηκε 10 Οκτωβρίου, 2018).

HHS.gov.(2013d). *Omnibus HIPAA Rulemaking*. Διαθέσιμο σε: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/omnibus-hipaa-rulemaking/index.html (Ανακτήθηκε 10 Οκτωβρίου, 2018).

HHS.gov. (2013e). *The HIPAA Enforcement Rule*. Διαθέσιμο σε: https://www.hhs.gov/hipaa/for-professionals/special-topics/enforcement-rule/index.html(Ανακτήθηκε 15 Οκτωβρίου, 2018).

HIPAA Journal, (2018). *What is Protected Health Information?*Διαθέσιμο σε: https://www.hipaajournal.com/what-is-protected-health-information/ (Ανακτήθηκε 08 Οκτωβρίου, 2018).

HIPAA Journal, (2018a). *TheHIPAA Password Requirements and the Best Way to Comply With Them.*Διαθέσιμοσε: https://www.hipaajournal.com/hipaa-password-requirements/ (Ανακτήθηκε 10 Οκτωβρίου, 2018).

HIPAA Journal, (2017). What are the HIPAA Breach Notification Requirements? Διαθέσιμο σε: https://www.hipaajournal.com/hipaa-breach-notification-requirements/ (Ανακτήθηκε 10 Οκτωβρίου, 2018).

ICO-Information Commissioner's Office, (2018). *Data protection officers*. Διαθέσιμο σε: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/ (Ανακτήθηκε 14 Αυγούστου, 2018).

Johnson, J. (2016). Top 10 Most Common HIPAA Violations. Διαθέσιμο σε: http://www.grouponehealthsource.com/blog/top-10-most-common-hipaa-violations (Ανακτήθηκε 10 Οκτωβρίου, 2018).

Kotter. (2018). The *8-Step Process for leading change.* Διαθέσιμο σε: https://www.kotterinc.com/8-steps-process-for-leading-change/ (Ανακτήθηκε 25 Οκτωβρίου, 2018).

Lawspot.gr, (2018). *LawSpot: Η υποχρέωση της διαφάνειας στον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR).* Διαθέσιμο σε: https://www.lawspot.gr/nomika-nea/i-ypohreosi-tis-diafaneias-ston-geniko-kanonismo-gia-tin-prostasia-dedomenon-gdpr(Ανακτήθηκε 3 Αυγούστου, 2018).

Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés Version consolidée au 21 Novembre 2018. Διαθέσιμο σε: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460 (Ανακτήθηκε 1 Αυγούστου, 2018).

Lord, N. (2018). *What is a Data Protection Officer (DPO)? Learn About the New Role Required for GDPR Compliance.*Διαθέσιμοσε: https://digitalguardian.com/blog/what-data-protection-officer-dpo-learn-about-new-role-required-gdpr-compliance (Ανακτήθηκε 20 Σεπτεμβρίου, 2018).

MLNMatters® Number: SE1022. (2012). Medical Record Retention and Media Formats for Medical Records. CMS. (Φυλλάδιο). Διαθέσιμο σε: https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNMattersArticles/downloads/SE1022.pdf

Mooney, G. (2018). *Is HIPAA Compliant With The GDPR?* Διαθέσιμο σε: https://blog.ipswitch.com/is-hipaa-compliant-with-the-gdpr (Ανακτήθηκε 17 Οκτωβρίου, 2018).

NIST, (2017). *Password Guidance from NIST*. Διαθέσιμο σε: https://www.nist.gov/video/password-guidance-nist-0 (Ανακτήθηκε 09 Οκτωβρίου, 2018).

OCR Privacy Brief, Summary of the HIPAA Privacy Rule. Διαθέσιμοσε: https://repository.library.georgetown.edu/handle/10822/1000587 (Ανακτήθηκε 10 Οκτωβρίου, 2018).

OECD. (1980). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Διαθέσιμοσε: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm(Ανακτήθηκε 15 Ιουνίου, 2018).

Priority business intelligence, (2018). *General Data Protection Regulation*. Διαθέσιμοσε: https://www.priority.com.gr/gdpr/ (Ανακτήθηκε 27 Νοεμβρίου 2018).

The HIPAA Guide: Healthcare Compliance. *HIPAA Encryption Requirements*. Διαθέσιμοσε: https://www.hipaaguide.net/hipaa-encryption-requirements/ (Ανακτήθηκε 10 Νοεμβρίου, 2018).

The Zog Blog, (2018). *Does HIPAA Compliance Cover GDPR Data Security Regulations?*.Διαθέσιμο σε: https://www.zoginc.com/confusing-hipaa-and-gdpr/ (Ανακτήθηκε 20 Οκτωβρίου, 2018). (Ανακτήθηκε 10 Οκτωβρίου, 2018).

TSO (TheStationeryOffice), (1998). DataProtectionAct. Διαθέσιμοσε: http://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf (Ανακτήθηκε 1 Αυγούστου, 2018).