Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Οικονομικών Επιστημών και Διοίκησης

Μεταπτυχιακό Πρόγραμμα Σπουδών: Διοίκηση, Τεχνολογία και Ποιότητα

Μεταπτυχιακή Διατριβή

<<Προστασία Προσωπικών Δεδομένων και Ηλεκτρονικός Φάκελος Υγείας>>

Κυριάκος Κωνσταντίνου

Επιβλέπων Καθηγητής

Στέφανος Γκρίτζαλης

2023

Ανοιχτό Πανεπιστήμιο Κύπρου

Σχολή Οικονομικών Επιστημών και Διοίκησης

Μεταπτυχιακό Πρόγραμμα Σπουδών: Διοίκηση, Τεχνολογία και Ποιότητα

Μεταπτυχιακή Διατριβή

<<Προστασία Προσωπικών Δεδομένων Και Ηλεκτρονικός Φάκελος Υγείας>>

Κυριάκος Κωνσταντίνου

Επιβλέπων Καθηγητής

Στέφανος Γκρίτζαλης

Η παρούσα διατριβή υποβλήθηκε προς μερικής εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών

στη ……

από τη **Σχολή Οικονομικών Επιστημών και Διοίκησης**

Του Ανοικτού Πανεπιστημίου Κύπρου

12/2023

Περίληψη

Με το άνοιγμα ενός λογαριασμού ή με το άνοιγμα μιας ιστοσελίδας, τα προσωπικά δεδομένα χρειάζονται, χρησιμοποιούνται και αποθηκεύονται. Ένας άνθρωπος είναι καλό να γνωρίζει τι πρέπει να κάνει σε τέτοιες στιγμές, τι δικαιώματα και τι υποχρεώσεις έχει. Πρέπει να ξέρει τι επιλογές έχει και τι είναι τι συνέπειες έχει η κάθε επιλογή του. Τα προσωπικά δεδομένα του καθενός μπορεί να χρησιμοποιηθούν και να επεξεργαστούν από ένα οργανισμό με οποιονδήποτε τρόπο θέλει εφόσον δίνεται η συγκατάθεση του ατόμου. Τις περισσότερες φορές συμφωνούμε στην επιλογή «ναι» για τα cookies χωρίς να ξέρουμε τις συνέπειες και τι κακό μπορεί να μας κάνουν. Όπως είπε κάποιος φιλόσοφος ο Φράνσις Μπέικον, η γνώση είναι δύναμη δηλαδή μέσω του κατακερματισμού της γνώσης οδηγούμαστε στην εύρεση του νοήματος πίσω από τα φαινόμενα.

Αρχικά θα μιλήσω για τα προσωπικά δεδομένα γενικά (σημασία, συλλογή, ανάλυση, επεξεργασία) και ποια η επίδραση τους στην καθημερινή μας ζωή. Θα μπω σε διάφορες ιστοσελίδες που αφορούν κλινικές, νοσοκομεία, φαρμακεία, ιδιωτικά ιατρικά γραφεία (γιατρούς) και πως αυτά τα προσωπικά δεδομένα διαχειρίζονται από αυτούς τους οργανισμούς και τι πρέπει να προσέχει ο καθένας που είτε επισκέπτεται τις ιστοσελίδες τους είτε γίνεται χρήστης τους μέσω της εγγραφής στην ιστοσελίδα τους. Σκοπός είναι να ρωτήσω τους οργανισμούς που διαχειρίζονται τα προσωπικά δεδομένα μέσω ηλεκτρονικών μηνυμάτων ή και κατ' ιδίαν, έτσι ώστε να βοηθηθούν άτομα που δεν γνωρίζουν τον σκοπό των «προσωπικών δεδομένων». Καταληκτικά, θα αναφέρω και τις δύο πλευρές, πλεονεκτήματα και μειονεκτήματα, έτσι ώστε να βγει ένα σωστό αποτέλεσμα.

Καταληκτικά, θα μπορείτε να γνωρίζετε σε τι πρέπει να δίνουμε σημασία και σε τι όχι. Θεωρώ τα προσωπικά δεδομένα πάρα πολύ σημαντικά στη ζωή μας λόγω της αυξημένης ψηφιοποίησης και τεχνολογίας τα οποία οδηγούν σε παραβίαση προσωπικών δεδομένων επί καθημερινής βάσης και θεωρώ καθήκον μου σαν ένας επιμελής πολίτης να ενημερώσω τους άλλους συμπολίτες μου για ένα τέτοιο άκρως σημαντικό θέμα.

Summary

Personal data is required, utilized, and kept when creating an account or launching a website. It is beneficial for a person to understand what he should do in such situations, as well as his rights and duties. He must understand his options and the ramifications of his decision. An organization can use and use an individual's personal data in any way it wishes as long as the subject consents. Most of the time, we accept to the "yes" choice for cookies without considering the repercussions and potential harm. According to philosopher Francis Bacon, knowledge is power; that is, we are guided to the truth via the fragmentation of knowledge.

First, I'll discuss the relevance of personal data in general (gathering, analysis, and processing) and how it affects our daily lives. I will look at numerous websites for clinics, hospitals, pharmacies, and private medical offices (doctors) and how these institutions manage personal data and what everyone who visits their websites or becomes a user through registration should be aware of. The goal is to contact companies that manage personal data by e-mail or in person in order to assist those who are unfamiliar with the term "personal data." Finally, I will discuss both sides, benefits and negatives, in order to get the best possible outcome.

You will eventually be able to tell what to pay attention to and what not to pay attention to. Personal data is very crucial in our lives because of rising digitalization and technology, which leads to personal data breaches on a regular basis, and I believe it is my obligation as a responsible citizen to tell my fellow citizens about such a critical issue.

Ευχαριστίες

Θέλω να ευχαριστήσω θερμά επιβλέπων καθηγητή Στέφανο Γκρίτζαλη για την καθοδήγησή, επίβλεψη και βοήθεια ολοκλήρωσης της διπλωματικής.

Θα ήθελα επίσης να ευχαριστήσω τον DPO της εταιρείας στην οποία δουλεύω, τον κ. Νίκο ο οποίος εγκάρδια μου έδωσε πληροφορίες για τα προσωπικά δεδομένα που αφορούν την εταιρεία μου και έτσι μπόρεσα να δω πως επεξεργάζεται μια εταιρία τα προσωπικά δεδομένα και επιπρόσθετα πως μπορούν να επηρεάσουν τρίτα άτομα αυτές οι πληροφορίες.

Ευχαριστίες στην μητέρα μου Νίκη η οποία μου έδωσε τις δικές της πληροφορίες όσον αφορά τα προσωπικά δεδομένα που αφορούν τη δική της εργασία στην Τράπεζα που δουλεύει. Ήταν αρκετά χρήσιμες πληροφορίες για να εμπλουτίσω την διατριβή που με τέτοιο τρόπο μπόρεσα να πάρω μια ιδέα με ποιο τρόπο χρησιμοποιούν τα προσωπικά δεδομένα σε μία εταιρία.

Ευχαριστώ όλους τους φίλους μου που με τον τρόπο τους με στήριξαν και με εμψύχωσαν στο να τελειώσω το πρώτο μέρος της διατριβής μου.

Τέλος, θα ήθελα να ευχαριστήσω τον εαυτό μου που δεν σταμάτησε ποτέ να εργάζεται μέχρι να φτάσει στο τέλος αυτού του έργου.

Περιεχόμενα

Πίνακας Σχεδιαγραμμάτων και Πινάκων

Κεφάλαιο 1

Εισαγωγή

Ο όρος «Προσωπικά Δεδομένα» είναι οποιαδήποτε πληροφορία ταυτοποιημένου ή ταυτοποιήσιμου φυσικού προσώπου το οποίο καλείται «Υποκείμενο Δεδομένων». Ταυτοποίηση φυσικού προσώπου εννοούμε την ταυτότητα που μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας. Το εύρος των δεδομένων είναι πάρα πολύ μεγάλο και περιλαμβάνει πλέον κάθε αναγνωριστικό στοιχείο όπως όνομα, ταυτότητα, δεδομένα τοποθεσίας, Ψηφιακές Διευθύνσεις/Ονόματα (IP Address/Ηλεκτρονική Διεύθυνση/Username) όπως και σε άλλους συγκεκριμένους παράγοντες π.χ. σωματικής, ψυχολογικής οικονομικής, πολιτικής ή κοινωνικής ταυτότητας αυτού του φυσικού προσώπου.

Τα τελευταία χρόνια μαζί με την ανάπτυξη της τεχνολογίας υπήρχαν παραβιάσεις από μεγάλες και μικρές εταιρίες για την συλλογή αυτών των δεδομένων και η Ευρωπαϊκή Ένωση έθεσε σε εφαρμογή κανόνες για την προστασία των πολιτών.

Ο GDPR (General Data Protection Regulation – Γενικός Κανονισμός Προστασίας Δεδομένων) ο σημαντικότερος αλλά και ο πιο αυστηρός κανονισμός, προστατεύει τα προσωπικά δεδομένα του κάθε πολίτη της ευρωπαϊκής ένωσης, ανεξαρτήτου του τρόπου συλλογής τους. Αυτό που έχει σημασία δεν είναι ο τρόπος αποθήκευσης τους ή ο τρόπος επεξεργασίας τους αλλά η συμμόρφωση με τις απαιτήσεις προστασίας που ορίζει ο GDPR.

Ο νέος Γενικός κανονισμός προστασίας δεδομένων GDPR (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 της ελεύθερης κυκλοφορίας των δεδομένων αυτών, καταργεί την Οδηγία 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία των Δεδομένων). Θεωρείται η μεγαλύτερη αλλαγή σε νομοθεσία τα τελευταία 20 χρόνια και γι' αυτό θα πρέπει να δοθεί η δέουσα σημασία και βαρύτητα στην συμμόρφωση του.

Με λίγα λόγια ο GDPR είναι μια σειρά κανονισμών σχεδιασμένος για να δίνει στους κατοίκους της Ευρωπαϊκής Ένωσης περισσότερη εξουσιοδότηση στο τι γίνεται στα προσωπικά τους δεδομένα και πως επεξεργάζονται. Σκοπεύει στο να απλοποιήσει το κανονιστικό περιβάλλον για τις επιχειρήσεις έτσι ώστε και οι πολίτες αλλά και οι επιχειρήσεις μέσα στην Ευρωπαϊκή Ένωση να επωφελούνται πλήρως της ψηφιακής οικονομίας.

Λόγω της ανέλιξης της τεχνολογίας τα τελευταία χρονιά δημιουργήθηκε και επιβάλλεται από την ευρωπαϊκή ένωση ο νομός του GDPR. Είναι ένας νόμος που έχει να κάνει με τα ανθρώπινα δικαιώματα οποιουδήποτε πολίτη (π.χ. πελάτες, εργαζόμενοι , συνεργάτες , προμηθευτές κτλ.) και αφορά κάθε οργανισμό και πολίτη που δραστηριοποιείται εντός και εκτός της Ευρωπαϊκής Ένωσης (Ε.Ε.).

Γενικός Κανονισμός Προστασίας Δεδομένων

Σε γενικές γραμμές Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) είναι ένας κανονισμός της Ευρωπαϊκής Ένωσης (ΕΕ) που εγκρίθηκε τον Απρίλιο του 2016 και τέθηκε σε ισχύ στις 25 Μαΐου 2018. Αντικαθιστά την Οδηγία της ΕΕ για την Προστασία Δεδομένων του 1995. Ο GDPR ενισχύει τους κανόνες προστασίας δεδομένων της ΕΕ παρέχοντας στα άτομα περισσότερο έλεγχο των προσωπικών τους δεδομένων και του τρόπου συλλογής, χρήσης

και διακίνηση τους. Ισχύει για κάθε οργανισμό που δραστηριοποιείται εντός της ΕΕ, καθώς και για κάθε οργανισμό εκτός ΕΕ που επεξεργάζεται τα προσωπικά δεδομένα πολιτών της ΕΕ. Οι οργανισμοί που δεν συμμορφώνονται με τον GDPR μπορούν να τιμωρηθούν με πρόστιμο έως και 20 εκατομμύρια ευρώ ή το 4% των ετήσιων παγκόσμιων εσόδων τους, όποιο από τα δύο είναι υψηλότερο.

Οι Νόμοι περί Επεξεργασίας Προσωπικών Δεδομένων (Προστασίας του Ατόμου) τέθηκαν σε ισχύ με τους όρους του Ν. 125(Ι)/2018 παράλληλα με τον πιο πάνω κανονισμό στην Κύπρο.

Νόμος 125(Ι)/2018 (Ο περί της Προστασίας των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και της Ελεύθερης Κυκλοφορίας των Δεδομένων αυτών Νόμος του 2018)

Δημοσιεύθηκε στην Επίσημη Εφημερίδα της Κυπριακής Δημοκρατίας στις 31 Ιουλίου 2018 ο Νόμος του 2018 για την Προστασία των Φυσικών Προσώπων από την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα και την Ελεύθερη Διακίνηση Δεδομένων Προσωπικού Χαρακτήρα (Ν. 125(Ι)/2018.

Στις 27 Απριλίου 2016, ψηφίστηκε ο νόμος «Κανονισμός (ΕΕ) 2016/679» του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων - 'data subject' από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την ελεύθερη διακίνηση τέτοιων δεδομένων και για την κατάργηση της Οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός Προστασίας Δεδομένων) με στόχο την αποτελεσματική εφαρμογή ορισμένων διατάξεων της πράξης της Ευρωπαϊκής Ένωσης.

Η έννοια της μυστικότητας (privacy) έχει εξελιχθεί με την πάροδο του χρόνου και ποικίλλει μεταξύ των πολιτισμών και των κοινωνιών. Στους αρχαίους πολιτισμούς, η προστασία της ιδιωτικής ζωής δεν ήταν ευρέως αναγνωρισμένη έννοια, καθώς οι άνθρωποι συχνά ζούσαν σε μικρές, σφιχτοδεμένες κοινότητες όπου η ιδιωτικότητα δεν εκτιμήθηκε ιδιαίτερα. Τον 18ο και τον 19ο αιώνα, η Βιομηχανική Επανάσταση και η αστικοποίηση οδήγησαν σε μια αυξανόμενη επιθυμία για ιδιωτικότητα, καθώς οι άνθρωποι προσπαθούσαν να διαχωρίσουν την προσωπική και τη δημόσια ζωή τους.

Στον 20ο αιώνα, οι τεχνολογικές εξελίξεις, όπως το τηλέφωνο και το διαδίκτυο, άλλαξαν σε μεγάλο βαθμό τον τρόπο που σκεφτόμαστε την ιδιωτικότητα. Με την άνοδο των μέσων κοινωνικής δικτύωσης και τον αυξανόμενο όγκο προσωπικών πληροφοριών που μοιράζονται στο διαδίκτυο, οι ανησυχίες για το απόρρητο έχουν γίνει πιο εμφανείς και σε αυξανόμενο βαθμό. Ως απάντηση, οι κυβερνήσεις και οι οργανισμοί έχουν αναπτύξει νόμους και κανονισμούς για την προστασία των προσωπικών πληροφοριών και του απορρήτου, όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) στην Ευρωπαϊκή Ένωση και ο νόμος περί απορρήτου των καταναλωτών της Καλιφόρνια (CCPA) στις Ηνωμένες Πολιτείες. Με άλλα λόγια, ο GDPR και ο CCPA απαιτούν τη συλλογή και χρήση ορισμένων πληροφοριών με συγκεκριμένους τρόπους.

Σημαντικό είναι να αναφερθεί πως και οι δύο κανονισμοί έχουν κάποιες διάφορες μεταξύ τους. Το βασικότερο είναι πως ο κανονισμός του GDPR βασίζεται στην συγκατάθεση 'opt in'του 'data subject' που είναι το φυσικό πρόσωπο πριν οποιαδήποτε διεργασία των προσωπικών δεδομένων ενώ στο CCPA βασίζεται στο δικαίωμα του πολίτη να 'opt out' προχωρήσει στην διεργασία των προσωπικών του δεδομένων

Στην συγκεκριμένη διατριβή θα δοθεί περισσότερή βαρύτητα στον Γενικό Κανονισμό του GDPR που δίνει έμφαση σε ένα ευρύτερο φάσμα προσωπικών δεδομένων που σχετίζεται με την ταυτοποίηση του φυσικού προσώπου για την Ευρωζώνη.

Συνολικά, κάθε χώρα στον κόσμο έχει διαφορετικά επίπεδα νομοθεσίας περί απορρήτου. Ορισμένα έθνη, όπως η Ευρώπη και η Αμερική, έχουν πολύ σταθερούς κανόνες που προστατεύουν τα προσωπικά στοιχεία των ατόμων. Απεναντίας στην Αφρική και ορισμένα τμήματα της Νότιας Αμερικής, υπάρχει σχετικά περιορισμένη νομοθεσία

όσο αφορά την προστασία δεδομένων. (Burgess Matt. (2020). What is GDPR? The summary guide to GDPR compliance in the UK | WIRED UK. https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018).

GDPR Countries 2023

The GDPR has been implemented in the following EU countries:

- Austria
- Belgium
- Bulgaria
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- The Netherlands
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden
- United Kingdom*

* The United Kingdom is an outlier.

Although the UK has departed from the EU as of January 2021, the GDPR was enacted before its withdrawal and is therefore considered a valid UK law.

Πίνακας1: Οι χώρες που έχουν εφαρμόσει επίσημα τον κανονισμό του GDPR (The Complete Guide to UK-GDPR,Phil Strattor-Founder, https://www.gdpradvisor.co.uk/gdpr-countries)

List of Non-GDPR European Countries

The countries listed here are in Europe but have not implemented the GDPR regulation:

- **Albania**
- **Belarus**
- **Bosnia and Herzegovina**
- **Kosovo**
- **Moldovia**
- **Montenegro**
- **North Macedonia**
- **Russia**
- **Serbia**
- **Turkey**
- **Ukraine**

Any organization in these countries that collects data in EU/UK member states is subject to the GDPR, even though they haven't implemented the GDPR regulation.

Πίνακας 2 Οι χώρες που ΔΕΝ έχουν βάλει σε εφαρμογή επίσημα τον κανονισμό του GDPR (The Complete Guide to UK-GDPR,Phil Strattor-Founder, https://www.gdpradvisor.co.uk/gdpr-countries)

1.2 Σκοπός του Κανονισμού

Ο σκοπός αναβάθμισης του κανονισμού ήταν:

- Ανεπαρκή κενά στην προηγούμενη έκδοση του, όπως π.χ. νομικές ασάφειες.
- Ενδυνάμωση της αξιοπιστίας στο σύστημα και των δικαιωμάτων του κάθε φυσικού προσώπου.

Όπως αναφέρει και η νομοθεσία ο σκοπός δημιουργίας του κανονισμού ήταν << Οι αρχές και οι κανόνες για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα τους θα πρέπει, ανεξάρτητα από την ιθαγένεια ή τον τόπο διαμονής τους, να σέβονται τα θεμελιώδη δικαιώματα και τις ελευθερίες τους, ιδίως το δικαίωμά τους στην προστασία των δεδομένων προσωπικού χαρακτήρα. Ο παρών κανονισμός σκοπεύει να συμβάλλει στην επίτευξη ενός χώρου ελευθερίας, ασφάλειας και δικαιοσύνης και μιας οικονομικής ένωσης, στην οικονομική και κοινωνική πρόοδο, στην ενίσχυση και σύγκλιση των οικονομιών εντός της εσωτερικής αγοράς και στην ευημερία των φυσικών προσώπων>>.

Επιβάλλετο να υπάρχει μία ομοιομορφία όσον αφορά τα νομικά πλαίσια σε όλα τα κράτη μέλη έτσι ώστε να υπάρχει το ίδιο νομικό πλαίσιο σε όποια χώρα και αν βρεθείς. (Chapter 1 – General provisions - General Data Protection Regulation (GDPR). (n.d.), from https://gdpr-info.eu/chapter-1/).

1.3. Τι είναι Προσωπικά Δεδομένα

Τα πιο κάτω μπορούν να θεωρηθούν ως προσωπικά δεδομένα:

- Στοιχεία αναγνώρισης όπως ταυτότητα διαβατήριο, φορολογικό μητρώο, όνομα ,ηλικία κατοικία κτλ.

- Φυσικά χαρακτηριστικά του προσώπου, η εκπαίδευση του ατόμου , η εργασία και η συμπεριφορά του σε αυτήν.
- Οικονομική κατάσταση όπως εισοδήματα, κινητή και ακίνητη περιουσία, τραπεζικούς λογαριασμούς.
- Τα ενδιαφέροντα και οι δραστηριότητες του.
- IP Διεύθυνσης όπως email, cookies.

Ως γενικό συμπέρασμα του τι μπορεί να θεωρηθεί προσωπικά δεδομένα μπορεί να λεχθεί μέσα σε αυτή την μικρή πρόταση: “Προσωπικά δεδομένα είναι Οτιδήποτε μπορεί να ταυτοποιήσει ένα φυσικό πρόσωπο”.

1.4. Κατηγοριοποίηση Προσωπικών Δεδομένων

Υπάρχουν 2 κατηγορίες δεδομένων, τα προσωπικά και τα ειδικά κατηγοριοποιημένα δεδομένα.

Τα προσωπικά δεδομένα περιέχουν πληροφορίες όπως:

- Όνομα.
- Ημερά Γεν.
- Διεύθυνση διαμονής.
- Τηλέφωνο επικοινωνίας.
- Αριθμός Διαβατήριου/Ταυτότητα/Άδειας οδήγησης.
- Ηλεκτρονικό ταχυδρομείο.
- Αριθμός της τραπεζικής κάρτας ή και διεθνής τραπεζικός λογαριασμός.
- Δεδομένα που διατηρούνται από νοσοκομεία και γιατρούς.

Your Europe. (2022). GDPR | Προσωπικά δεδομένα & ΓΚΠΔ - Your Europe. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm

Ειδικές κατηγορίες δεδομένων όπως (δεν επιτρέπεται η επεξεργασία προσωπικών δεδομένων σχετικά με τα εξής χαρακτηριστικά ενός προσώπου:

- Πολίτικες απόψεις.
- Φυλή.
- Βιομετρικές πληροφορίες (αποτύπωμα δαχτύλου).
- Κατάσταση υγείας.
- Θρησκεία ή τα πιστεύω σε αυτή.
- Σεξουαλικός προσανατολισμός.
- Γενετικά δεδομένα όπως(DNA etc.).
- Προσωπικά δεδομένα που σχετίζονται με ποινικές καταδίκες και αδικήματα.

GDPR Greece - Τι είναι το GDPR και πως επηρεάζει τις επιχειρήσεις;(2019). from https://www.gdprgreece.com/article/5/gdpr

1.5 Ιστορική Αναδρομή του GDPR

Αρχικά να αναφέρουμε πως ο νόμος του GDPR υπήρχε από παλιά αλλά έγινε αναγκαστικός από όλα τα κράτη μέλη της Ε.Ε από το 2018.

Ο Γενικός κανονισμός Προστασίας Δεδομένων είναι ένα μεγάλο κίνημα προστασίας δεδομένων, κανόνας εντός όλων των μελών της ΕΕ. Τέθηκε σε εφαρμογή στις 25 Μάιου το 2018. Οποιαδήποτε εταιρία που προσφέρει υπηρεσίες ή αγαθά σε οποιονδήποτε πολίτη που κατοικεί στην ΕΕ πρέπει να συμμορφώνεται με το κανονισμό. Επιπρόσθετα εάν ο πολίτης μιας χώρας που είναι ενεργός στην ΕΕ, επισκέπτεται άλλη χώρα που δεν είναι μέσα στην ΕΕ, παραμένει προστατευμένος δια μέσου αυτού του Κανονισμού.

Μια γρήγορη ματιά στο χρονοδιάγραμμα του GDPR.

Χρονολογία	**Ιστορική Αναδρομή**
1890	Όλα άρχισαν μεταξύ 2 Αμερικάνων δικηγορών των Samuel D. Warren and Louis Brandeis για το <<δικαίωμα στο να είσαι μόνος>> μια φράση που χρησιμοποιήσαν.
1940	Υιοθετείται η Οικουμενική Διακήρυξη των Ανθρωπίνων Δικαιωμάτων, συμπεριλαμβανομένου του 12ου θεμελιώδους δικαιώματος, δηλαδή το Δικαίωμα στην μυστικότητα.
1950	Σειρά θεμελιωδών δικαιωμάτων της Σύμβασης της ΕΕ για τα Ανθρώπινα Δικαιώματα τροποποιείται, με τα άρθρα να εμφανίζονται πλέον με διαφορετική σειρά.
1967	Ο Νόμος για την Ελευθερία της Πληροφορίας (FOIA – Freedom of Information Act) τίθεται σε εφαρμογή στην Αμερική. Δικαίωμα στο να ζητάς δεδομένα και να έχεις πρόσβαση για τα δικά σου δεδομένα από τις κρατικούς φορείς. Αρκετές χώρες ακολουθούν το παράδειγμα αυτό.
1980	(OECD – Organisation For Economic Co-operation and Development) Ο οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης ανακοινώνει κατευθυντήριες οδηγίες για τα προσωπικά δεδομένα λόγω της αύξησης της χρήσης των ηλεκτρονικών υπολογιστών περί την διαχείριση επιχειρηματικών συναλλαγών.
1981	Υπογράφτηκε από το Συμβούλιο της Ευρώπης η συμφωνία σχετικά με την προστασία των προσωπικών δεδομένων και την παροχή αυτόματης επεξεργασίας τους και τέθηκε σε ισχύ την 1 Οκτωβρίου το 1985. Όλα τα μέλη της Ευρωπαϊκής ένωσης είχαν επικυρώσει τη συνθήκη εκτός από την Τουρκία.
1983	Το Ομοσπονδιακό Συνταγματικό Δικαστήριο της Γερμανίας καταλήγει σε πρωταρχική απόφαση σχετικά με την απόφαση της απογραφής. Η ετυμηγορία θεωρείται γεγονός στην ιστορία για την προστασία των δεδομένων.
1995	Πρωτοβγήκε η πρώτη νομοθεσία για τα προσωπικά δεδομένα.
1998	Πρώτη Κίνηση για δημιουργία νομοθεσίας μέσω Βουλής περί προστασίας προσωπικών δεδομένων, το Data Protection Act 1998.
2000	Υπογράφτηκε συμφωνία μεταξύ της Ευρωπαϊκής Ένωσης και της Αμερικής μέσα από την οποία επιτρεπόταν σε χιλιάδες εταιρείες να μεταφέρουν ευρωπαϊκά προσωπικά δεδομένα ευρωπαίων πολιτών στην Αμερική εάν εγγυούνταν ότι θα υπήρχε αρκετή προστασία όσον αφορά τα προσωπικά δεδομένα όπως παρατίθονταν στην εν λόγω συμφωνία. (Google, safe harbor launched in 2000).
2002	Η Ευρωπαϊκή Ένωση θέτει σαν οδηγία την προστασία προσωπικών δεδομένων σε ηλεκτρονικές επικοινωνίες

2006	Εγκρίνεται η οδηγία της Ευρωπαϊκής Ένωσης για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία μέσω της παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών.
2009	Έγινε η Πρώτη Διαβούλευση (First Consultation) σε ότι αφορά ενημέρωση των Ευρωπαϊκών Νόμων επί της προστασίας προσωπικών δεδομένων.
2011	Ο Ευρωπαίος Επόπτης Της Προστασίας Δεδομένων δημοσιεύει γνώμη σχετικά με την ανακοίνωση της Ευρωπαϊκής Επιτροπής.
2012	Η Ευρωπαϊκή επιτροπή εισηγείται να ενδυναμωθούν τα διαδικτυακά απόρρητα και τα δικαιώματα στην ψηφιακή οικονομία. Εδώ είναι που έγινε οι εισήγηση στην αλλαγή του προηγούμενου κανονισμού (1995 the Data Protection Directive) στην νέο τώρα κανονισμό του GDPR.
2013	Η έκδοση του κανονισμού 611/2013 από την Ευρωπαϊκή επιτροπή για τα μέτρα που ισχύουν για την κοινοποίηση παραβιάσεων προσωπικών δεδομένων βάση της οδηγίας που 2002/58/ΕΚ.
2014	Δικαστική απόφαση της Ευρωπαϊκής ένωσης ενημερώνει ότι η η ευρωπαϊκή νομοθεσία δίνει στους χρήστες το δικαίωμα να ζητούν από μηχανές αναζήτησης όπως η Google να αφαιρέσουν αποτελέσματα από ερωτήματα που περιλαμβάνουν το όνομά τους. «The right to be forgotten». <<The right to be forgotten>> είναι μια νομική έννοια που προήλθε από απόφαση του 2014 του Δικαστηρίου της Ευρωπαϊκής Ένωσης (ΔΕΕ). Σε εκείνη την περίπτωση, η Google Spain κατά AEPD και ο Mario Costeja González, το ΔΕΕ έκρινε ότι τα άτομα έχουν το δικαίωμα να ζητήσουν από τις μηχανές αναζήτησης όπως. Αυτό το δικαίωμα βασίζεται στην ιδέα ότι τα άτομα έχουν δικαίωμα να ελέγχουν τα προσωπικά τους δεδομένα και το απόρρητο των διαδικτυακών τους πληροφοριών.
2015	Στις 6 Οκτωβρίου 2015, Το Δικαστήριο της Δικαιοσύνης της Ευρωπαϊκής Ένωσης (Court of Justice of the European Union (CJEU)) δήλωσε τη δομή που βρίσκεται η ΕΕ-ΗΠΑ (EU-US Safe Harbor framework) άκυρη και ως ένα μηχανισμό για να μεταφέρει νόμιμα προσωπικά δεδομένα μεταξύ των ΕΕ και ΗΠΑ.
2016	Θετήθηκε ο κανόνας του GDPR. Έγκρισή για την εφαρμογή του κανονισμού από την Ευρωπαϊκή Ένωση μετά από 4 χρόνια.
25/5/2018	Έγινε εφαρμογή του GDPR παγκοσμίως ανεξαρτήτου εάν έχουν την έδρα τους στην Ε.Ε ή όχι΄. Αντικαταστόντας το Νόμο<< Data Protection Act>>

Πίνακας 3 Ιστορική αναδρομή για το GDPR

Από το Μάιο του 2018 και μετά, κάθε Υπεύθυνος Διαχείρισης Προσωπικών Δεδομένων πρέπει να διασφαλίζει πως οι εταιρίες στις οποίες εργάζονται, έχουν στην κατοχή τους ξεκάθαρες και σαφείς διαδικασίες μέσω εκσυγχρονισμένων εφαρμογών π.χ. διαδικτυακές πύλες.

(The History of the General Data Protection Regulation | European Data Protection Supervisor. (n.d)from https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en)

(International Network Of Privacy Law Professionals. (2018). A brief history of data protection: How did it all start? | International Network of Privacy Law Professionals. https://inplp.com/latest-news/article/a-brief-history-of-data-protection-how-did-it-all-start/)

(Ernst Oliver Wilhelm, International Association of Privacy Professionals,2016, from https://iapp.org/about/person/0011a00000DlLyEAAV/).

1.6 Διαχειριστές Επεξεργασίας Προσωπικών Δεδομένων

Υπάρχουν 2 πλευρές όψεων όταν μιλάμε για προσωπικά δεδομένα, υπάρχει η μεριά του πελάτη/πολίτη και η μεριά των επιχειρήσεων που πρέπει με τον σωστό τρόπο να αποθηκεύουν και να επεξεργάζονται αυτά τα δεδομένα. Τα δεδομένα μόνα τους είναι άχρηστα εάν δεν γίνεται η σωστή διαχείρισή τους.

Μέχρι τώρα βλέπαμε την μεριά του πολίτη. Σε μία επιχείρηση τα δεδομένα είναι το κεντρικό σημείο.

Τα δεδομένα είναι σημαντικά για την ομαλή ροή και λειτουργία μιας επιχείρησης. Η κάθε επιχείρηση χρειάζεται ένα αποδοτικό μοντέλο στρατηγικής για την επίτευξή των στόχων της για την κατάλληλη χρήση των δεδομένων που θα έχει στην κατοχή της σε όλες τις αλυσίδες εφοδιασμού, τα δίκτυα εργαζομένων, τα οικοσυστήματα πελατών και εταίρων κτλ. (Τι είναι η διαχείριση δεδομένων; | Ορισμός, σημασία, & διαδικασίες | SAP Insights. (n.d), from https://www.sap.com/greece/products/technology-platform/what-is-data-management.html).

Ως συνήθως τα προσωπικά δεδομένα που συλλέγονται από έναν οργανισμό ή επιχείρηση ή άτομο, εξετάζονται και ελέγχονται πάντοτε από δύο άτομα, τον Υπεύθυνο Επεξεργασίας και τον Εκτελών Επεξεργασίας οι οποίοι είναι υποχρεωμένοι να λογοδοτήσουν απ' ευθείας στον GDPR:

1.6.1 Υπεύθυνος Επεξεργασίας

Είναι κάθε φυσικό ή νομικό πρόσωπο του δημόσιου ή ιδιωτικού τομέα που τηρεί και επεξεργάζεται προσωπικά δεδομένα σε μία εταιρία ή έναν οργανισμό. Είναι υπεύθυνος να κρίνει τον σκοπό και τον τρόπο επεξεργασίας των δεδομένων.

1.6.2 Εκτελών Επεξεργασίας

Είναι κάθε φυσικό ή νομικό πρόσωπο του δημοσίου ή ιδιωτικού τομέα που επεξεργάζεται δεδομένα για λογαριασμό κάποιου υπεύθυνου επεξεργασίας (δηλαδή τρίτο άτομο είτε από την ίδια την εταιρία είτε από κάποια άλλη) πάντα όμως κάτω από την διοίκηση του υπεύθυνου επεξεργασίας. Επιπρόσθετα έχει την ευθύνη για την επεξεργασία των προσωπικών δεδομένων για λογαριασμό του Υπεύθυνου επεξεργασίας.

(Lab Ground. (2021). GDPR DPO, Controller, Processor and Other Roles | Ground Labs. https://www.groundlabs.com/blog/gdpr-responsibility/)

1.6.3 Υπεύθυνος Προστασίας Δεδομένων/Data Protection Officer

Επιπρόσθετα η κάθε εταιρεία επιβάλλεται όπως τοποθετείται, δια νόμου, ένας υπεύθυνος για την πιστή τήρηση των πιο κάτω καθηκόντων:

- Να εκπροσωπεί την εταιρία έναντι των αρχών, εθνικών και ευρωπαϊκών.
- Να διασφαλίζει την εναρμόνιση της λειτουργίας της επιχείρησης σε ότι αφορά τις πολιτικές πρακτικές και μεθολογία επεξεργασίας, αποθήκευσης και μεταφοράς δεδομένων προσωπικού χαρακτήρα με το νέο αυστηρό νομοθετικό πλαίσιο.

- Είναι υπεύθυνος για την εκτίμηση επιπτώσεων που αφορούν την προστασία των δεδομένων (Data- Protection Impact Assessment-DPIA).
- Να προστατεύει την επιχείρηση από τους κινδύνους επιβολής των σημαντικότατων και βαρύτατων διοικητικών προστιμάτων που προβλέπει ο κανονισμός.

Επίσης μια εταιρία μπορεί να ορίσει σαν DPO κάποιον από τα στελέχη της, αλλά έχει και τη δυνατότητα να συνεργαστεί με άλλη εξειδικευμένη εταιρία που θα τις παρέχει τις υπηρεσίες του DPO.

Η ροή διαχείρισης τον δεδομένων περιέχει ευρύ φάσμα καθηκόντων όπως :

- Συλλογή, επεξεργασία, επιβεβαίωση , και αποθήκευση δεδομένων.
- Διαχωρισμός των δεδομένων που έχω συλλέξει από τις πηγές μου.
- Εγκυρότητα υψηλής διαθεσιμότητας δεδομένων σε περίπτωση καταστροφής.
- Εξασφάλιση των δεδομένων πως χρησιμοποιούνται και είναι προσβάσιμα από τα αρμόδια άτομα.
- Τέλος, διασφάλισή και προστασία των προσωπικών δεδομένων.

Βασισμένη σε αναφορά που έγινε από την 'Risk Based Security' το 2019 οι αριθμοί της κυβερνοασφαλειας είχαν αυξηθεί μέχρι και το 54% σε σύγκριση με το προηγούμενο έτος του 2018 σηματοδοτώντας έτσι το 2019 σαν το χειρότερο έτος. Χωρίς να μπούμε σε λεπτομέρειες, υπήρχαν παραβιάσεις στον επιχειρησιακό τομέα με ποσοστό 67%, στο κομμάτι τις υγείας με ποσοστό 14%, της κυβέρνησης με 12% και τέλος στο τομέα της εκπαίδευσης με 7%. Η κάθε εταιρία που αποθηκεύει τα εν λόγω προσωπικά δεδομένα, θέλει να προστατεύει τα προσωπικά δεδομένα της από αυτές τις επιθέσεις. Ο DPO πρέπει να είναι ενημερωμένος για τον κώδικα του GDPR και έχει άμεσο ρόλο μαζί του. (Breaches up 54% this year - Millgate Ltd, (2019) from https://millgate.co.uk/learn/breaches-up-50-this-year)

(https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page2b_en/page2b_en?opendocument)

(Rennie Stuart. (2019). ARMA-Magazine-2019-02-ARMA-QA_-GDPR-Regulations-and-Electronic-Records)

1.7 Ποιους Αφορά/Επηρεάζει

Όλοι οι νόμοι από κάθε Ε.Ε. μπορούν να τροποποιηθούν από το κάθε κράτος μέλος ελαχίστως πριν μπουν σε εφαρμογή. Αντιθέτως, ο συγκεκριμένος κανονισμός του GDPR πρέπει να τεθεί σε εφαρμογή χωρίς να υπάρχει η επιλογή της τροποποίησης δηλαδή να μπει σε εφαρμογή ακριβώς όπως τον αναθέτει η Ε.Ε.

Ο Γενικός Κανονισμός GDPR 2016/679 δεν θεωρείται Οδηγία/Directive έναντι της Οδηγίας του 1995 the Data Protection Directive η οποία είχε υιοθετηθεί όταν το διαδίκτυο ήταν στα αρχικά του στάδια. Δίνοντας την απαραίτητη έμφαση ο GDPR είχε αρχίσει σαν εισήγηση τον Ιανουάριο του 2012 από την Ευρωπαϊκή Ένωση και εγκρίθηκε επίσημα στις 27 Απρίλιου του 2016, και μπήκε σε πλήρη εφαρμογή από τις 25 Μάιου του 2018. Η διαφορά μεταξύ των δύο είναι ότι ως «Οδηγίες» το κάθε κράτος μέλος είχε το δικαίωμα να επιβάλει όπως θέλει τους εν λόγω κανονισμούς φτάνει να είχε τα επιθυμητά αποτελέσματα ενώ ως «Νομοθεσία» το κάθε κράτος μέλος έπρεπε να εφαρμόσει τους εν λόγω κανονισμούς όπως της δίνονταν χωρίς να τροποποιηθεί.

Οποιεσδήποτε επιχειρήσεις (ιδιωτικές και δημόσιες, κρατικές αρχές, μικρομεσαίες επιχειρήσεις, συλλόγους κ.α.) οι οποίες έχουν αποθηκευμένες πληροφορίες που αφορούν πολίτες της Ε.Ε. π.χ. όπως έχουμε αναφέρει πιο πάνω, πρέπει να τηρούν τον συγκεκριμένο κανονισμό.

Αφορά κάθε οργανισμό που δραστηριοποιείται εντός της Ε.Ε αλλά και εκείνες είτε με έδρα την ΕΕ και τόπο διεξαγωγής επεξεργασίας εκτός ΕΕ, είτε έδρα εκτός ΕΕ και τόπο διεξαγωγής επεξεργασίας εκτός Ε.Ε. Ο συγκεκριμένος κανονισμός αφορά ιδιώτες , επιχειρήσεις , κράτη μέλη κτλ., οπού έχουν την δυνατότητα πρόσβασης, επεξεργασίας και αποθήκευσης πληροφοριών όπου παρέχοντες υπηρεσίες στον πολίτη της Ευρωπαϊκής Ένωσης.

Μέσω της αναβάθμισης του έγινε πιο σαφής και κατανοητός προς τους πολίτες. (The History of the General Data Protection Regulation | European Data Protection Supervisor. (n.d.), from https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

1.8 Προϋποθέσεις (Requirements)

Υπάρχουν 10 απαραίτητες προϋποθέσεις προς πλήρη συμμόρφωση με τους κανόνες του GDPR και σας παρατίθενται πιο κάτω περιληπτικά :

LAWFUL, FAIRNESS, TRANSPARENT - (Νόμιμα, Δίκαια, Διαφανές)

Ένας οργανισμός θα πρέπει να είναι νομικά κατοχυρωμένος μέσω γραπτής εξουσιοδότησης έτσι ώστε οι πληροφορίες που του δίνονται να επεξεργάζονται, όσο επίσης και το υποκείμενο δεδομένων θα πρέπει να είναι γνώστης των τρόπων που αυτή η πληροφορία θα διοχετευτεί (πως θα χρησιμοποιηθεί και πως θα αποθηκευτεί). Κανένας δεν μπορεί να προχωρήσει σε συλλογή προσκοπικών δεδομένων τουλάχιστον μια νομική συγκατάθεσή εκ μέρους του ατόμου. Μερικά παραδείγματα από νομική συγκατάθεση από το άρθρο 6 του GDPR:

1) Εάν ο ίδιος έχει δώσει την συγκατάθεση για την συλλογή των δεδομένων του.

2) Για να εκπληρωθεί μία συμφωνία μεταξύ του υποκείμενου και του παρόχου.

3) Να συμμορφωθεί μαζί με τις υποχρεώσεις που έχει ορίσει ο υπεύθυνος επεξεργασίας δεδομένων.

(4) Να προστατέψει τα ενδιαφέροντα του υποκείμενου ή κάποιου τρίτου.

(5) Να εκτελέσει μια πράξη προς το κοινό συμφέρον ή μιας νομικής εξουσίας.

LIMITED FOR ITS PURPOSE/DATA MINIMISATION - (Περιοριστικά Για το Σκοπό του)

Τα δεδομένα που συλλέγονται θα πρέπει να αφορούν για συγκεκριμένο σκοπό και δεν θα πρέπει να χρησιμοποιηθούν με τέτοιον τρόπο που ο πολίτης δεν θα περίμενε.

DATA SUBJECT RIGHTS – (Δικαιώματα Πολιτών)

Πρέπει να είναι ξεκάθαρος ο λόγος συλλογής των πληροφοριών, για ποιον λόγο συλλέγονται και που θα χρησιμοποιηθούν. Οποιοδήποτε δεδομένο χωρίς σκοπό, δεν θα πρέπει να συλλέγεται. Επίσης μπορεί ο πολίτης να ρωτήσει τι πληροφορίες έχουν αποθηκευτεί γι' αυτόν από την συγκεκριμένη εταιρεία/οργανισμό ή άτομο και εάν θέλει έχει το δικαίωμα να ζητήσει όπως διορθωθούν, διαγραφούν ή να μην δοθούν σε τρίτα πρόσωπα.

CONSENT/ACCURACY - (Συγκατάθεση/Ακρίβεια)

Πρέπει να ληφθούν εύλογα μέτρα έτσι ώστε οι πληροφορίες να διατηρούνται ενημερωμένες και εάν είναι ανακριβείς να τροποποιούνται παίρνοντας πάντοτε τη συγκατάθεση του πολίτη. Σημαντικό δε, είναι η

συγκατάθεση που πρέπει να δίνεται από τους γονιούς/κηδεμόνες στις περιπτώσεις που αφορούν άτομα κάτω των 16.

NOT KEPT LONGER THAN NEEDED (PERSONAL DATA BREACHES) - (Παραβίαση Προσωπικών δεδομένων)

Τα προσωπικά δεδομένα δεν θα πρέπει να φυλάσσονται περισσότερο από ότι χρειάζονται και καταστρέφονται/διαγράφονται όταν δεν εξυπηρετούν κάποιο συγκεκριμένο σκοπό ή έχουν περάσει το χρονικό διάστημα αποθήκευσης. Παραβίαση μπορεί να θεωρηθεί επίσης εάν κάτι καταστραφεί παράνομα ή τυχαία, απωλεσθεί, αλλοιωθεί, αποκαλυφθεί χωρίς εξουσιοδότηση σε τρίτα άτομα. Βάσει νομοθεσίας, ο εκτελών ή ο υπεύθυνος επεξεργασίας θα πρέπει εντός 72 ωρών να ενημερώσει τον πολίτη και τον Νομοθέτη (regulator) για την παραβίαση.

PRIVACY BY DESIGN - (Πολιτική Απορρήτου στο Σχεδιασμό)

Οι εταιρίες πρέπει να έχουν τους απαραίτητους σχεδιασμούς και συστήματα έτσι ώστε η πολιτική απορρήτου και τα οποιαδήποτε θέματα προστασίας να διασφαλίζονται με προεπιλογή (by default).

DATA PROTECTION IMPACT ASSESSMENT - (Εκτίμηση Επιπτώσεων των Προσωπικών Δεδομένων)

Για την καλύτερη αξιολόγηση των οποιωνδήποτε επιπτώσεων πάνω σε αλλαγές ή νέες ενέργειες, πρέπει να ετοιμάζεται μία «Εκτίμηση Επιπτώσεων των Προσωπικών Δεδομένων». Η συγκεκριμένη εκτίμηση είναι μία διαδικασία η οποία χρειάζεται να γίνει όταν υπάρχουν οποιεσδήποτε αλλαγές ή νέες ενέργειες που αφορούν την επεξεργασία των προσωπικών δεδομένων.

DATA TRANSFERS - (Μεταφορά Δεδομένων)

Τα δεδομένα θα πρέπει να επεξεργάζονται με τέτοιον τρόπο που θα διασφαλίζεται η κατάλληλη ασφάλεια συμπεριλαμβανομένου της οποιασδήποτε μη εγκριμένης ή παράνομης επεξεργασίας, απώλειας, ζημιάς ή καταστροφής και θα πρέπει να αποθηκεύονται με πλήρη ασφάλεια.

DATA PROTECTION OFFICER - (Υπεύθυνος Προστασίας Δεδομένων)

Θα πρέπει να διασφαλίζει τη σωστή εκπαίδευση του προσωπικού σε θέματα GDPR και επίσης είναι υπεύθυνος να συμβουλεύει την εταιρεία στο πως να συμμορφώνεται με τις κανονιστικές απαιτήσεις του GDPR.

AWARENESS AND TRAINING - (Επίγνωση και Εκπαίδευση)

Οι οργανισμοί θα πρέπει να εκπαιδεύουν το προσωπικό τους σωστά έτσι ώστε να έχουν την επίγνωση σε θέματα GDPR και να διοργανώνει σεμινάρια και δραστηριότητες για να δοθεί η κατάλληλη έμφαση και βαρύτητα στο πόσο σημαντικό είναι η συμμόρφωση ολονών στις απαιτήσεις του GDPR και στο πόσο πρέπει να μην υπάρχει η οποιαδήποτε παραβίαση προσωπικών δεδομένων. Η σωστή εκπαίδευση γίνεται έτσι ώστε να αποφεύγονται περιπτώσεις όπως κλοπή, κίνδυνος και διάφορες απειλές που φέρουν η διαχείριση των δεδομένων αυτών.

Summary of the GDPR's 10 key requirements - IT Governance Blog, Luke Irwin,2021, Retrieved, from https://www.itgovernance.eu/blog/en/summary-of-the-gdprs-10-key-requirements.

Momen, N., Hatamian, M., & Fritsch, L. (2019). Did App Privacy Improve After the GDPR? IEEE Security Privacy, 17(6), 10–20. https://doi.org/10.1109/MSEC.2019.2938445

Kamleitner, B., & Mitchell, V. (2019). Your Data Is My Data: A Framework for Addressing Interdependent Privacy Infringements. Journal of Public Policy & Marketing, 38(4), 433–450. https://doi.org/10.1177/0743915619858924

1.9 Μη Συμμόρφωση με τις Προϋποθέσεις

Η μη τήρηση των κανόνων του GDPR μπορεί να επιφέρει υπέρογκα πρόστιμα τα οποία μπορεί να φτάσουν μέχρι και τα 20 εκ. ευρώ ή στο 4% του συνολικού κύκλου εργασιών (τζίρος) της εταιρείας για συγκεκριμένες παραβάσεις. Η Αρχή Προστασίας Δεδομένων μπορεί επίσης να επιβάλει επιπρόσθετα μέτρα προς διόρθωση π.χ. να διατάξει την διακοπή επεξεργασίας προσωπικών δεδομένων.

Πρέπει να τονιστεί ότι το λογισμικό κάθε εταιρείας θα πρέπει να είναι πάντα εκσυγχρονισμένο και αναβαθμισμένο έτσι ώστε να συμμορφώνεται με τους νέους κανονισμούς του GDPR. Αυτή τη συμμόρφωση είναι το πρώτο βήμα που επιβάλλεται σε κάθε οργανισμό έτσι ώστε να φτάνει το ελάχιστο των προσδοκιών. Η μη συμμόρφωση στα πιο πάνω λεγόμενα, μπορεί να επιφέρει αρκετά προβλήματα όπως π.χ. βραδύτητα στη συλλογή πληροφοριών (cookies etc), μη επαρκής έλεγχος στις παραβιάσεις των αποθηκευμένων δεδομένων κλπ.

1.10 Δικαιώματα Του Πολίτη Ως Προς Στα Προσωπικά Τους Δεδομένα

Δικαίωμα Της Ενημέρωσης (Right to Information)

Σύμφωνα με τον GDPR, ένα άτομο έχει το δικαίωμα να γνωρίζει ποια προσωπικά δεδομένα συλλέγονται γι' αυτόν, πώς χρησιμοποιούνται, σε ποιους κοινοποιούνται και για πόσο καιρό θα διατηρούνται.

Αυτό το δικαίωμα, το οποίο είναι μία από τις βασικές αρχές προστασίας δεδομένων που περιγράφονται στον GDPR, καλεί τους Υπεύθυνους Επεξεργασίας δεδομένων να παρέχουν στα άτομα σαφείς και ξεκάθαρες πληροφορίες σχετικά με τους τρόπους με τους οποίους χρησιμοποιούν τα προσωπικά τους δεδομένα. Είναι απαραίτητο να δοθούν αυτές οι πληροφορίες με σαφή, κατανοητό και προσιτό τρόπο.

Τα άτομα πρέπει να ενημερώνονται για την ταυτότητα και τα στοιχεία επικοινωνίας του Υπευθύνου Επεξεργασίας δεδομένων, τους λόγους επεξεργασίας των προσωπικών τους δεδομένων, τη νομική βάση για αυτή την επεξεργασία και τους παραλήπτες ή τις κατηγορίες αποδεκτών των προσωπικών τους δεδομένων.

Δικαίωμα Πρόσβασης (SAR- Subject Access Request/Right to Access)

Αίτημα πρόσβασης θεμάτων (SAR) είναι ένα αίτημα που υποβάλλεται από ένα άτομο σε μια εταιρεία ή οργανισμό, ζητώντας οποιεσδήποτε πληροφορίες κατέχουν σχετικά με αυτόν ή αυτήν. Σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) στην ΕΕ και τον Νόμο για την Προστασία Δεδομένων του 2018 στο Ηνωμένο Βασίλειο, τα άτομα έχουν το δικαίωμα να ζητήσουν πρόσβαση στα προσωπικά τους δεδομένα και σε κάθε πληροφορία που κατέχει ένας οργανισμός για αυτά.

Το πιο πάνω δικαίωμα είναι ένα αναφαίρετο δικαίωμα που έχει ο κάθε πολίτης στο να έχει πρόσβαση στα προσωπικά του δεδομένα που είναι αποθηκευμένα από την κάθε εταιρεία ή οργανισμό. Είναι πάρα πολύ σημαντικό ο κάθε οργανισμός να έχει την επίγνωση στο πως θα χειρίζεται το SAR έτσι ώστε να αποφεύγονται μεγάλα προστίματα.

Αυτό περιλαμβάνει πράγματα όπως:

- Στοιχεία επικοινωνίας.
- Μητρώα απασχόλησης.
- Οικονομικές Συναλλαγές.
- Προτιμήσεις μάρκετινγκ και επικοινωνίας.
- Πλάνα CCTV.
- Διευθύνσεις IP.
- Βιομετρικά δεδομένα (δακτυλικά αποτυπώματα, δεδομένα αναγνώρισης προσώπου).

Οι οργανισμοί είναι υποχρεωμένοι να ανταποκρίνονται στα SAR εντός ορισμένου χρονικού διαστήματος, συνήθως εντός ενός μηνός, και πρέπει να παρέχουν τις πληροφορίες σε μορφή που είναι εύκολα κατανοητή. Οφείλουν επίσης να επαληθεύσουν την ταυτότητα του προσώπου που υποβάλλει το αίτημα, προκειμένου να προστατεύσουν τα προσωπικά δεδομένα και να αποτρέψουν την αποκάλυψη σε μη εξουσιοδοτημένα μέρη.

- Να αναγνωριστεί το αίτημα.
- Να κατανοηθούν τα χρονικά πλαίσια μέσα στα οποία θα πρέπει να απαντήσεις.
- Χειρισμός πολύπλοκων και χωρίς βάσεις αιτημάτων.
- Αναγνώρισε, Ψάξε και μάζεψε την αιτούμενη πληροφορία.
- Μάθε ποια πληροφορία μπορείς να κατακρατήσεις μόνο για σένα.
- Ανάπτυξη και αποστολή απάντησης.

Ωστόσο, υπάρχουν ορισμένες εξαιρέσεις και όρια σε ό,τι μπορεί να αποκαλυφθεί βάσει ενός SAR, για παράδειγμα εάν θα μπορούσε να βλάψει την εθνική ασφάλεια ή εάν οι πληροφορίες σχετίζονται με μια εξελισσόμενη εγκληματική έρευνα ή εάν οι πληροφορίες αφορούν άλλα άτομα. (Franklin. (2018). GDPR subject access request (SAR) - 6 steps to deal with it. https://cybersmart.co.uk/blog/6-steps-to-deal-with-a-gdpr-subject-access-request-sar/).

Δικαίωμα Της Διόρθωσης (Right of Rectification)

Το δικαίωμα διόρθωσης είναι ένα από τα δικαιώματα του υποκειμένου των δεδομένων βάσει του GDPR που επιτρέπει στα άτομα να ζητούν τη διόρθωση ή την ενημέρωση των προσωπικών τους δεδομένων που κατέχει ένας Υπεύθυνος Επεξεργασίας δεδομένων. Αυτό αναφέρεται επίσης ως «Δικαίωμα στη διόρθωση».

Τα άτομα έχουν το δικαίωμα σύμφωνα με τον GDPR να ζητήσουν τη διόρθωση ή τη συμπλήρωση τυχόν ανακριβειών ή ελλιπών προσωπικών δεδομένων, το συντομότερο δυνατό. Αυτό το δικαίωμα είναι σημαντικό γιατί δίνει τη δυνατότητα στα άτομα να διασφαλίζουν ότι τα προσωπικά τους δεδομένα είναι ακριβή και ενημερωμένα, γεγονός που μπορεί να βοηθήσει στην αποφυγή τυχόν αρνητικών συνεπειών που μπορεί να προκύψουν από την κατοχή εσφαλμένων δεδομένων.

Εάν ένα άτομο ασκήσει το δικαίωμά του για διόρθωση, ο Υπεύθυνος Επεξεργασίας δεδομένων πρέπει να λάβει εύλογα μέτρα για τη διόρθωση των δεδομένων το συντομότερο δυνατό. Ο ίδιος ο Υπεύθυνος Επεξεργασίας φέρει την ευθύνη για τη συλλογή αυτών δεδομένων.

Δικαίωμα Αντίρρησης (Αντιτάξης) (Right to Object to Processing)

Ένα από τα δικαιώματα των υποκειμένων των δεδομένων βάσει του Γενικού Κανονισμού Προστασίας Δεδομένων είναι το δικαίωμα αντίρρησης (GDPR). Τα φυσικά πρόσωπα έχουν το δικαίωμα να αντιταχθούν στην επεξεργασία των προσωπικών τους δεδομένων για συγκεκριμένους σκοπούς βάσει του παρόντος νόμου.

Τα άτομα έχουν το δικαίωμα βάσει του GDPR να αντιταχθούν στην επεξεργασία των προσωπικών τους δεδομένων για τους ακόλουθους λόγους:

- εάν αυτή γίνεται για νόμιμους σκοπούς του Υπευθύνου Επεξεργασίας δεδομένων ή τρίτων ατόμων.
- Εάν αυτή γίνεται για σκοπούς άμεσου μάρκετινγκ.
- Εάν αυτή γίνεται για επιστημονική ή ιστορική έρευνα ή στατιστικούς σκοπούς.
- Επιπλέον, τα άτομα έχουν το δικαίωμα να αντιταχθούν στην επεξεργασία των προσωπικών τους δεδομένων όταν υφίστανται επεξεργασία για το έννομο συμφέρον του υπευθύνου επεξεργασίας δεδομένων ή τρίτου μέρους, εκτός εάν ο υπεύθυνος επεξεργασίας μπορεί να αποδείξει επιτακτικούς νόμιμους λόγους για την επεξεργασία που υπερτερούν των συμφερόντων, των δικαιωμάτων του ατόμου, και ελευθερίες.

Για την άσκηση αυτού του δικαιώματος, τα άτομα πρέπει να ειδοποιούν εγγράφως τον Υπεύθυνο Επεξεργασίας δεδομένων για την αντίρρησή τους στην επεξεργασία των προσωπικών τους δεδομένων. Ο υπεύθυνος επεξεργασίας δεδομένων πρέπει στη συνέχεια να σταματήσει την επεξεργασία των προσωπικών δεδομένων εκτός εάν μπορεί να αποδείξει επιτακτικούς νόμιμους λόγους για την επεξεργασία που υπερτερούν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του ατόμου ή εάν η επεξεργασία απαιτείται για τη θεμελίωση, άσκηση ή υπεράσπιση νομικών αξιώσεων.

Δικαίωμα σε σχέση με την αυτοματοποιημένη λήψη Αποφάσεων και το Κατάρτιση Προφίλ (Να μην υποβάλλεται σε απόφασή που βασίζεται αποκλειστικά στην αυτοματοποιημένη επεξεργασία)(Right to Object to Automated Processing)

Τα άτομα έχουν το δικαίωμα σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) να αντιταχθούν στην αυτοματοποιημένη επεξεργασία των προσωπικών τους δεδομένων, συμπεριλαμβανομένης της δημιουργίας προφίλ.

Οποιαδήποτε επεξεργασία προσωπικών δεδομένων που εκτελείται από συστήματα υπολογιστών ή άλλα αυτοματοποιημένα μέσα χωρίς ανθρώπινη αλληλεπίδραση αναφέρεται ως αυτοματοποιημένη επεξεργασία.

Το προφίλ μπορεί να χρησιμοποιηθεί για να γίνουν αυτοματοποιημένες επιλογές που έχουν σημαντικό αντίκτυπο σε ένα άτομο, όπως η πιστοληπτική ικανότητα, η απασχολησιμότητα ή η καταλληλότητα για συγκεκριμένες υπηρεσίες ή παροχές. Αυτό σημαίνει ότι εάν μια εταιρεία χρησιμοποιεί αυτοματοποιημένες διαδικασίες ή αλγόριθμους για να κάνει επιλογές που σας επηρεάζουν σημαντικά, έχετε το δικαίωμα να διαμαρτυρηθείτε και να αναθεωρήσετε την απόφαση από ένα άτομο.

Για να ασκήσετε αυτό το δικαίωμα, επικοινωνήστε με τον οργανισμό και ζητήστε να σταματήσει να χρησιμοποιεί αυτοματοποιημένη επεξεργασία για τα δεδομένα σας. Ο οργανισμός πρέπει να απαντήσει στο αίτημά σας χωρίς αδικαιολόγητη καθυστέρηση και εάν αρνηθεί να συμμορφωθεί, θα πρέπει να σας αιτιολογήσει την απόφασή του.

Είναι σημαντικό να θυμάστε ότι αυτό το προνόμιο δεν είναι απόλυτο και μπορεί να υπόκειται σε περιορισμούς, όπως όταν απαιτείται αυτοματοποιημένη επεξεργασία για την εκτέλεση της σύμβασης ή επιτρέπεται από το νόμο.

Εάν ανησυχείτε για τον τρόπο χειρισμού των προσωπικών σας δεδομένων, θα πρέπει να ζητήσετε τη γνώμη ενός νομικού επαγγελματία ή ενός φορέα προστασίας δεδομένων.

Συμπερασματικά ,η αυτοματοποιημένη επεξεργασία μπορεί να είναι απίστευτα ωφέλιμη και αποτελεσματική, μπορεί επίσης να εγείρει ερωτήματα σχετικά με το απόρρητο, τη δικαιοσύνη και τη διαφάνεια. Αυτός είναι ο λόγος για τον οποίο ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) προβλέπει συγκεκριμένους νόμους και εγγυήσεις για την προστασία των δικαιωμάτων των ατόμων όταν τα προσωπικά τους δεδομένα υφίστανται αυτόματη επεξεργασία.

Δικαίωμα της Διαγραφής (Right to be Forgotten/Erased)

Τα άτομα έχουν το δικαίωμα στη διαγραφή και το μπλοκάρισμα, που μερικές φορές είναι γνωστό ως «Δικαίωμα στη Διαγράφη»(The right to be forgotten), σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR).

Τα άτομα έχουν το δικαίωμα βάσει του GDPR να ζητούν τη διαγραφή ή τον αποκλεισμό των προσωπικών τους δεδομένων βάσει των πιο κάτω:

- Όταν τα δεδομένα δεν απαιτούνται πλέον για τον σκοπό που συλλέχθηκαν ή υποβλήθηκαν σε επεξεργασία.
- Όταν ένα άτομο αποσύρει τη συγκατάθεσή του και δεν υπάρχει άλλη νομική βάση για την επεξεργασία των δεδομένων.
- Όταν ένα άτομο αντιτίθεται στην επεξεργασία των δεδομένων του και δεν υπάρχουν επιτακτικοί βάσιμοι λόγοι για να το πράξει.
- Όπου τα δεδομένα έχουν υποστεί ακατάλληλη επεξεργασία.
- Όταν απαιτείται διαγραφή για την εκπλήρωση νομικής υποχρέωσης.
- Εάν ένα άτομο ζητήσει διαγραφή ή αποκλεισμό.

Εάν το υποκείμενο ζητήσει τη διαγραφή ή τον αποκλεισμό των δεδομένων του, ο υπεύθυνος επεξεργασίας δεδομένων πρέπει να λάβει εύλογα μέτρα για να συμμορφωθεί, συμπεριλαμβανομένης της ειδοποίησης τρίτων στα οποία έχουν αποκαλυφθεί τα δεδομένα. Ωστόσο, το δικαίωμα διαγραφής δεν είναι απόλυτο και μπορεί να περιοριστεί σε ορισμένες περιπτώσεις, όπως όταν τα δεδομένα απαιτούνται για την άσκηση ελεύθερης έκφρασης ή για τη συμμόρφωση με νομική υποχρέωση.

Π.χ Να επιτρέπει στα άτομα να έχουν το δικαίωμα να διαγράψουν, να αφαιρέσουν ή και να τροποποιήσουν δεδομένα από μηχανές αναζήτησης/ιστοσελίδες που περιέχουν ανακριβείς, ανεπαρκείς, άσχετες ή ξεπερασμένες πληροφορίες. Μία μηχανή αναζήτησης (όπως το Google,Bing, Yahoo etc) πρέπει να αξιολογήσει εάν οι πληροφορίες πρέπει να αφαιρεθούν με βάση την ισορροπία μεταξύ του δικαιώματος στην ιδιωτική ζωή και του δικαιώματος του κοινού να έχει πρόσβαση στις πληροφορίες που θα αναφέρει. Εάν η μηχανή αναζήτησης κρίνει ότι οι πληροφορίες πρέπει να αφαιρεθούν, πρέπει να το κάνει με τρόπο που να συνάδει με τη νομοθεσία της ΕΕ για την προστασία δεδομένων.

Δικαίωμα στην Φορητότητα των δεδομένων (Right for Data Portability)

Το δικαίωμα GDPR στη φορητότητα δεδομένων αναφέρεται στο δικαίωμα του υποκειμένου των δεδομένων να λαμβάνει αντίγραφο των προσωπικών του δεδομένων σε δομημένη, κοινώς χρησιμοποιούμενη και μηχανικά αναγνώσιμη μορφή, καθώς και να διαβιβάζει αυτά τα δεδομένα σε άλλα δεδομένα ελεγκτή όπου είναι τεχνικά

εφικτό. Με άλλα λόγια, αυτό το δικαίωμα εξουσιοδοτεί τα άτομα να συλλέγουν και να επαναχρησιμοποιούν τα προσωπικά τους δεδομένα σε πολλούς παρόχους. Τα άτομα μπορούν επίσης να μετακινήσουν γρήγορα, να αντιγράψουν ή να μεταφέρουν τα προσωπικά τους δεδομένα από ένα περιβάλλον πληροφορικής σε άλλο με ασφαλή και εύκολο τρόπο. Το δικαίωμα στη φορητότητα δεδομένων ισχύει για δεδομένα προσωπικού χαρακτήρα που υποβάλλονται από ένα υποκείμενο δεδομένων σε υπεύθυνο επεξεργασίας και υποβάλλονται σε επεξεργασία βάσει άδειας ή σύμβασης. Δεν ισχύει για προσωπικές καταστάσεις.

Ο στόχος του δικαιώματος στη φορητότητα δεδομένων είναι να δώσει στα άτομα περισσότερο έλεγχο στα προσωπικά τους δεδομένα και να ενθαρρύνει τον ανταγωνισμό μεταξύ των παροχών υπηρεσιών.

Δικαίωμα Περιορισμού της Επεξεργασίας (Right to Restrict Processing)

Το Δικαίωμα Περιορισμού της Επεξεργασίας παρατίθεται στο άρθρο 18 του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR). Σύμφωνα με αυτό το άρθρο, οι υπόχρεοι επεξεργασίας πρέπει να ενημερώνουν τα άτομα σχετικά με το δικαίωμά τους να ζητήσουν τον περιορισμό της επεξεργασίας των προσωπικών τους δεδομένων κατά τη συλλογή τους. Επίσης, οι υπόχρεοι επεξεργασίας πρέπει να απαντούν σε αυτά τα αιτήματα εντός μιας μηνιαίας προθεσμίας.

Τα άτομα έχουν το δικαίωμα να ζητήσουν από τον Υπεύθυνο Επεξεργασίας δεδομένων να περιορίσει την επεξεργασία των προσωπικών τους δεδομένων στις ακόλουθες περιπτώσεις:

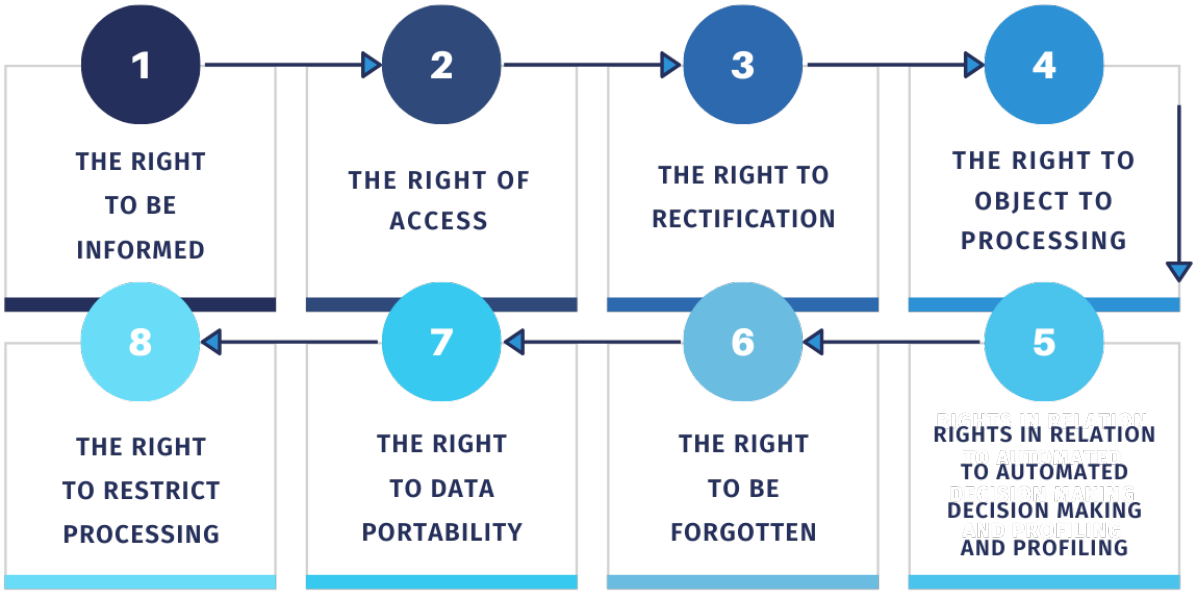
- Το υποκείμενο των δεδομένων αμφισβητεί την ακρίβεια των προσωπικών δεδομένων και η επεξεργασία περιορίζεται έως ότου επαληθευτεί η ακρίβεια των δεδομένων.
- Η επεξεργασία είναι παράνομη και το άτομο απορρίπτει τη διαγραφή προσωπικών δεδομένων, προτιμώντας αντ' αυτού να περιορίσει τη χρήση τους.
- Ο υπεύθυνος επεξεργασίας δεδομένων δεν απαιτεί πλέον τα προσωπικά δεδομένα για σκοπούς επεξεργασίας. Ο σκοπός για τον οποίο έχουν συλλεχθεί τα δεδομένα δεν είναι πλέον απαραίτητος.
- Το άτομο έχει αντιταχθεί στην επεξεργασία σύμφωνα με το άρθρο 21 παράγραφος 1 του GDPR και το θέμα εκκρεμεί επαλήθευση για το εάν οι νόμιμοι λόγοι του υπευθύνου επεξεργασίας υπερτερούν εκείνων του ατόμου.

Είναι καλό να σημειωθεί ότι η μοναδική διαφορά μεταξύ του 6 και του 8, είναι ότι το 8 είναι προσωρινό μέτρο ενώ η διαγραφή είναι μόνιμη.

Είναι σημαντικό να γνωρίζει κάποιος όλα τα δικαιώματα που έχει, όπως τα αναφέραμε πιο πάνω γιατί με το συνδυασμό όλων τον δικαιωμάτων ο πολίτης έχει το μεγαλύτερο έλεγχο τον προσωπικών του δεδομένων στο μέγιστο βαθμό βοηθώντας στον έτσι στην προστασία του ιδίου και στην μυστικότητα του.

Είναι αξιοσημείωτο ότι το δικαίωμα της διόρθωσης συσχετίζεται πολύ κοντά σε άλλα δικαιώματα του GDPR π.χ. δικαίωμα πρόσβασης και το δικαίωμα διαγραφής.

(Wolters, P. T. J. (2018). The Control by and Rights of the Data Subject Under the GDPR)



Πίνακας 4: Τα δικαιώματα του πολίτη μέσω του GDPR και η ροή τους (What are 8 Data Subject rights according to the GDPR – Data Privacy Manager. (2022). https://dataprivacymanager.net/what-are-data-subject-rights-according-to-the-gdpr/)

Κεφάλαιο 2

Ηλεκτρονικός Φάκελος Υγείας

Μαζί με την ραγδαία εξέλιξη της τεχνολογίας μας, επέφερε μαζί της και αρκετά ωφελήματα στην καθημερινότητα μας και ειδικά στο τομέα της υγείας**.** Εάν πάμε πίσω στο χρόνο που δεν υπήρχε η ευχέρεια σε κάθε εταιρία να υπήρχε ένας ηλεκτρονικός υπολογιστής, μπορούμε να πούμε πως η ζωή ήταν αρκετά δυσκολότερη. Σήμερα μαζί με την βοήθεια της τεχνολογίας μπορούμε να βελτιστοποιήσουμε την ζωή μας σε μεγάλο βαθμό. Οι άνθρωποι πλέον αποζητούν πιο ποιοτικές υπηρεσίες υγείας, απαιτούν την καλύτερη προσφερόμενη υπηρεσία και επιπρόσθετα επιζητούν να είναι ενημερωμένοι για οποιαδήποτε νεοφερμένη αλλαγή ενώ από την άλλη, το κράτος και οι μονάδες υγείας θα πρέπει να προσφέρουν την καλύτερη ποιότητα με τον καλύτερο αλάνθαστο, εάν γίνεται, τρόπο. Το χάσμα μεταξύ των δύο, γεφυρώνεται μέσω της υιοθέτησης του Ηλεκτρονικού Φακέλου Υγείας ή άλλως γνωστό ως ΗΦΥ ο οποίος είναι ένας τρόπος βελτιστοποίησης της καθημερινότητας μας στον τομέα υγείας.

Με το πέρασμα του χρόνου εμφανιστήκαν και διάφορες προκλήσεις για τον τρόπο διασφάλισης των προσωπικών δεδομένων προσωπικού χαρακτήρα για το τομέα της υγείας. Λόγω αυτής της ραγδαίας τεχνολογικής ανάπτυξης τα τελευταία χρόνια, έχει επέλθει μεγάλη αύξηση στην ανταλλαγή πληροφοριών σε ιδιωτικούς και κρατικούς οργανισμούς που αφορούν την εξυπηρέτηση των καθηκόντων τους.

Η προστασία των φυσικών προσώπων θα πρέπει να εφαρμόζεται τόσο στην επεξεργασία δεδομένων προσωπικού χαρακτήρα με αυτοματοποιημένα μέσα, όσο και στη χειροκίνητη επεξεργασία, εάν τα δεδομένα προσωπικού χαρακτήρα περιέχονται ή προορίζονται να περιληφθούν σε σύστημα αρχειοθέτησης. Τα αρχεία ή τα σύνολα αρχείων, καθώς και τα εξώφυλλά τους, τα οποία δεν είναι διορθωμένα σύμφωνα με συγκεκριμένα κριτήρια, δεν θα πρέπει να υπάγονται στο πεδίο εφαρμογής του παρόντος κανονισμού. (Kumar, M., Raj, H., Chaurasia, N., & Gill, S. S. (2023). Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0. Internet of Things and Cyber-Physical Systems, 3, 309–322. https://doi.org/10.1016/j.iotcps.2023.05.006).

2.1 Πρόλογος

Για να λειτουργήσει ομαλά ο ΗΦΥ (Ηλεκτρονικός Φάκελος Υγείας) και τα πληροφοριακά συστήματα του νοσοκομείου, παίζει τεράστια σημασία η διασφάλιση των ευαίσθητων ιατρικών δεδομένων που αφορούν την υγεία των ασθενών. Το νοσοκομείο θα πρέπει να εξασφαλίζει τεχνικές προδιαγραφές προκειμένου τα δεδομένα να ανταλλάσσονται με ασφαλή τρόπο και να υπάρχει ορθή συνεργασία μεταξύ των διάφορων συστημάτων.

Οι σωστές πληροφορίες και τα πρόσφατα αναθεωρημένα δεδομένα καθορίζουν τη δημιουργία ενός σωστού ιστορικού υγείας για τον κάθε πολίτη το οποίο θα οδηγήσει σε μια σωστή διάγνωση, ακόμη και σε μια σωστή θεραπεία. Άρα εάν υπάρχουν οι σωστές πληροφορίες σε μία βάση δεδομένων, τότε τα πάντα

μπορούν να επιτευχθούν. Δίνοντας έτσι βάση στα πιο πάνω, καταλήγουμε στο ότι οι πληροφορίες και τα δεδομένα για τον πολίτη είναι το κέντρο ενός ηλεκτρονικού φακέλου. Σίγουρα ο πελάτης/πολίτης δεν μπορεί πάντα να θυμάται σε κάθε συνάντηση ή ραντεβού τι είχε αναφερθεί, γι' αυτό ένας «Ηλεκτρονικός Φάκελος Υγείας» έρχεται για να δώσει επίλυση σε πολλά προβλήματα. (Kumar, M., Raj, H., Chaurasia, N., & Gill, S. S. (2023). Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0. Internet of Things and Cyber-Physical Systems, 3, 309–322. https://doi.org/10.1016/J.IOTCPS.2023.05.006).

2.2 Big Data

Στην σήμερον ημέρα λόγω του μεγάλου όγκου δεδομένων, είναι εύκολο για ένα γιατρό να γνωρίζει την ολική εικόνα του ασθενή για την επιλογή της καταλληλότερης θεραπείας που μπορεί να του παρέχει. Η χρήση των λεγόμενων <<big data – μεγάλα δεδομένα>> έχει χρησιμοποιηθεί στο κομμάτι της ιατρικής τα τελευταία χρόνια για την βελτίωση και μεταφορά μεγάλου βαθμού δεδομένων μεταξύ γιατρών και χωρών για διευκόλυνση του πελάτη.

Τα μεγάλα δεδομένα αναφέρονται σε μεγάλα και πολύπλοκα σύνολα δεδομένων που οι παραδοσιακές μέθοδοι επεξεργασίας δεδομένων δεν είναι σε θέση να χειριστούν. Αυτά τα μεγάλα σύνολα δεδομένων μπορούν να περιλαμβάνουν δομημένα και μη δομημένα δεδομένα, όπως κείμενο, εικόνες και βίντεο, και τυπικά χαρακτηρίζονται από τα τρία V: όγκο, ταχύτητα και ποικιλία. Η ικανότητα ανάλυσης και εξαγωγής πολύτιμων πληροφοριών από μεγάλα δεδομένα γίνεται ολοένα και πιο σημαντική για τις επιχειρήσεις και τους οργανισμούς, καθώς μπορεί να βοηθήσει στη λήψη γρήγορων αποφάσεων και να προωθήσει την καινοτομία.

Τα μεγάλα δεδομένα χρησιμοποιούνται στην υγειονομική περίθαλψη για τη βελτίωση των αποτελεσμάτων των ασθενών, τη μείωση του κόστους και την προώθηση της καινοτομίας.

Υπάρχουν πολλοί τρόποι με τους οποίους τα μεγάλα δεδομένα χρησιμοποιούνται στην υγειονομική περίθαλψη, όπως:

- Ηλεκτρονικά αρχεία υγείας (EHRs): Τα EHR παράγουν μεγάλο όγκο δεδομένων που μπορούν να χρησιμοποιηθούν για τη βελτίωση της φροντίδας των ασθενών και την ενημέρωση της έρευνας.
- Υποστήριξη κλινικών αποφάσεων: Τα μεγάλα δεδομένα μπορούν να χρησιμοποιηθούν για την ανάπτυξη προγνωστικών μοντέλων που βοηθούν τους γιατρούς να λαμβάνουν πιο ενημερωμένες αποφάσεις σχετικά με τη φροντίδα των ασθενών.
- Διαχείριση της υγείας του πληθυσμού: Τα μεγάλα δεδομένα μπορούν να χρησιμοποιηθούν για τον εντοπισμό προτύπων και τάσεων στην υγεία ενός πληθυσμού, τα οποία μπορούν να ενημερώσουν την πολιτική για τη δημόσια υγεία και να βελτιώσουν τα συνολικά αποτελέσματα για την υγεία.
- Εξατομικευμένη ιατρική: Τα μεγάλα δεδομένα μπορούν να χρησιμοποιηθούν για τη δημιουργία εξατομικευμένων σχεδίων θεραπείας για ασθενείς με βάση τα γενετικά και μοριακά τους προφίλ.
- Ιατρική έρευνα: Τα μεγάλα δεδομένα μπορούν να χρησιμοποιηθούν για τον εντοπισμό νέων στόχων φαρμάκων και για την επιτάχυνση της διαδικασίας ανάπτυξης φαρμάκων.

Η χρήση μεγάλων δεδομένων στην υγειονομική περίθαλψη βρίσκεται ακόμη στα αρχικά της στάδια, αλλά αναμένεται να συνεχίσει να αυξάνεται και να διαδραματίζει ολοένα και πιο σημαντικό ρόλο στον κλάδο της

υγειονομικής περίθαλψης. (<!>boyd, <!>danah, & Crawford, K. (2011). Six Provocations for Big Data. Social Science Research Network: A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society. https://doi.org/10.2139/ssrn.1926431)

(Viceconti, M., Hunter, P., & Hose, R. (2015). Big data, big knowledge: big data for personalized healthcare. IEEE Journal of Biomedical and Health Informatics, 19(4), 1209–1215. https://doi.org/10.1109/JBHI.2015.2406883)

(Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Ullah Khan, S. (2015). big data" on cloud computing: Review and open research issues. Information Systems, 47, 98–115. https://doi.org/10.1016/j.is.2014.07.006)

(https://en.wikipedia.org/wiki/Big_data)

2.3 Ιστορική Αναδρομή

Στα παλαιότερα χρόνια μέχρι και το 1960 δεν είχε δημιουργηθεί ένας ψηφιοποιημένος φάκελος υγείας και για αυτό το ιστορικό του κάθε ασθενή ατομικά αποθηκευόταν σε διάφορους φακέλους που ήταν δύσκολο στην διερεύνηση του ώστε να γνωρίσει το ιστορικό του πριν οποιασδήποτε διάγνωσης ή συνέχιση οποιασδήποτε θεραπείας. Οι πρώτες σκέψεις για την δημιουργία ενός ηλεκτρονικού φακέλου ήταν γύρω στο 1960 που το είχαν εφαρμόσει στην κλινική Mayo clinic στην Νέα Υόρκη. Ήταν οι πρώτοι που υιοθέτησαν το ηλεκτρονικό σύστημα υγείας αλλά λόγω της υψηλής επένδυσης που έπρεπε να γίνει σε ηλεκτρονικά συστήματα, μόνο τα μεγαλύτερα ιδρύματα μπορούσαν να το χρηματοδοτήσουν. Παρόλα ταύτα, αυτή η προσέγγιση ήταν η πρώτη που προσπαθούσε να καταγράψουν δεδομένα γύρω από το ιστορικό ενός ασθενή. Είχε σαν σκοπό να καταγράφει όχι μόνο διαγνώσεις και φάρμακα αλλά και το ιστορικό της υγείας, παράπονα, πρόοδος του ασθενή κλπ.

Βλέποντας την σημαντικότητα του ηλεκτρονικού φακέλου υγείας , μέσα στην μέση του 1960 η εταιρία Lockheed Martin Corporation ανάπτυξε διάφορα ηλεκτρονικά συστήματα τα οποία είναι γνωστά μέχρι και σήμερα τα λεγόμενα “πληροφοριακά κλινικά συστήματα”.(Electronic Health Records (EHR) - Introduction, Key Players, Uses. (2022). https://www.ignitedata.com/electronic-health-record-ehr-systems-a-brief-history-and-3-key-players/)

Η συντελούμενη επανάσταση στον χώρο της εξελισσόμενης τεχνολογίας των υπολογιστών και της δικτύωσής τους επιφέρει σημαντικές αλλαγές στον τρόπο με τον οποίο αντιλαμβανόμαστε την έννοια και το περιεχόμενο της φροντίδας της υγείας του πολίτη. Η εισαγωγή των σύγχρονων τεχνολογιών της επιστήμης της Πληροφορικής στο χώρο της υγείας συμβάλλει αποφασιστικά στη διαμόρφωση ανοιχτών κέντρων παροχής υγειονομικής φροντίδας. Η εφαρμογή αυτή της Πληροφορικής είναι σε θέση να καλύψει τις εξής τουλάχιστον δραστηριότητες:

1. Διοίκηση και διαχείριση των υγειονομικών υπηρεσιών.

2. Αποθήκευση, ανάκτηση και μετάδοση ιατρονοσηλευτικών πληροφοριών πάσης φύσεως.

3. Επεξεργασία, διαχείριση και μεταφορά ιατρικής εικόνας και άλλων σημάτων βιολογικής φύσεως.

4. Διαγνωστικά συστήματα.

2.4 Ο Περί Ηλεκτρονικής Υγείας Νόμος 59(Ι)/2019

Ο περί Ηλεκτρονικής Υγείας Νόμος του 2019 (59(Ι)/2019) καταδεικνύει ότι ο ηλεκτρονικός φάκελος υγείας μπορεί να είναι διαθέσιμος είτε από κοντά είτε από μακριά έτσι ώστε να καταστεί δυνατή η διάγνωση, η θεραπευτική αντιμετώπιση και η συνεχής φροντίδα της υγείας του πολίτη κατά τη διάρκεια της προγραμματισμένης ή χωρίς προγραμματισμό παροχής υπηρεσιών υγείας. (Κυπριακή Δημοκρατία. (2019). Επίσημη Εφημερίδα Της Κυπριακής Δημοκρατίας Παράρτημα Πρώτο Νομοθεσία-Μέρος Ι. https://www.mof.gov.cy/mof/gpo/gazette.nsf/C9CDC1A32095E496C225872C004069B5/$file/4699%2019%204%202019%20PARARTHMA%201o%20MEROS%20I.pdf).

2.5 Κυριότερες Διαφορές

Αξιοσημείωτη πληροφορία για το κοινό είναι αναφέρουμε τις διαφορές του ηλεκτρονικού φακέλου υγείας με τον Ηλεκτρονικό Ιατρικό Φάκελο (Electronic Medical Record) και παρακάτω χρονολογικά πιο ήρθε πρώτο**.**

Ο ηλεκτρονικός ιατρικός φάκελος περιέχει αρχεία του ασθενή όπως ιστορικό, διαγράμματα, όνομα, επώνυμο, λεπτομέρειες του ασθενή, τιμολόγια κοστολόγησης και πληροφορίες περί ασφάλειες. Επιπρόσθετα είναι σε ψηφιακή μορφή και διατηρείται/συντηρείται από μόνο ένα πάροχο/χρήστη. Τώρα αντίθετα με τον ηλεκτρονικό Ιατρικό Φάκελο, ο Ηλεκτρονικός Φάκελος Υγείας περιέχει τόσο τα προαναφερόμενα δεδομένα όσο και άλλα επιπρόσθετα, όπως π.χ.

- χρήσιμα εργαλεία που μπορεί να χρησιμοποιήσει κάποιος για να πάρει σημαντικές αποφάσεις για τον ασθενή,
- επιτρέπει τις πληροφορίες που είναι καταγραμμένες στο αρχείο να είναι προσβάσιμες από διάφορούς χώρους και τοποθεσίες από όλο τον κόσμο και όχι από μόνο μια τοποθεσία.
- μοιράζονται και ενημερώνονται οι πληροφορίες του ασθενή σε πραγματικό χρόνο χωρίς καμία καθυστέρηση.

Μέσω του EHR μπορείς να πάρεις μια ολική εικόνα της κλινικής κατάστασης του ασθενή ενώ μέσω του EMR αυτό δεν είναι εφικτό.

Καταληκτικά, τα EHR παρέχουν πολλά πιθανά οφέλη τόσο για τους ασθενείς όσο και για τους κλινικούς γιατρούς, συμπεριλαμβανομένων ποικίλων κλινικών, οργανωτικών και κοινωνικών αποτελεσμάτων. Ενώ τα EHR μπορεί να είναι εξαιρετικά εργαλεία για τους κλινικούς γιατρούς, δεν μπορούν να λειτουργήσουν καλά μεμονωμένα.

Differences between EMR and EHR

EHR (electronic health record)	EMR (electronic medical records)
A digital record of health information	A digital version of a patient chart
Allows access to tools that providers can use for decision making	Is mainly used by providers for diagnosis and treatment
Allows a patient's medical information to be accessed from different places	Patient record cannot easily be sent outside the practice
Simplified sharing of updated, real-time information	Not designed to be shared outside the individual practice

Πίνακας 5 Οι κυριότερες διαφορές μεταξύ του Ηλεκτρονικού Φακέλου Υγείας και του Ηλεκτρονικού Ιατρικού Φακέλου

2.5.1 Πλεονεκτήματα του EHR έναντι του EMR

- Εύκολή πρόσβαση, ταχύτατη ενημέρωση των πληροφοριών του ασθενή έχοντας πλήρη και ακριβή εικόνα της κατάστασης του ασθενή δίνοντας έτσι σωστότερη ιατρική περίθαλψη.
- Μείωση χρόνου στην πρόσβαση και διαμοιρασμό πληροφορίων. Τα EHR διευκολύνουν επίσης την ασφαλή διατήρηση ιατρικών πληροφοριών και τη συλλογή και αξιολόγηση δεδομένων. Αυτό περιλαμβάνει την ταχύτερη παραγωγή αναφορών, τη διεξοδική διερεύνηση των τάσεων δεδομένων και τον αποτελεσματικότερο έλεγχο των αποθεμάτων.
- Υφίσταται καλύτερη επικοινωνία μεταξύ όλων των ιατρικών πάροχων στους οποίους έχει παραβρεθεί ο ασθενής με αποτελεσματική επικοινωνία μεταξύ τους για την καλύτερη ιατρική περίθαλψη του ασθενή.
- Λόγω της γρήγορης πρόσβασης στο σύστημα, μπορούν να αποφευχθούν και να μειωθούν λάθη κατά την διάρκεια σημαντικών αποφάσεων π.χ. εάν ένας ασθενής έχει οποιαδήποτε σημαντική διαταραχή σε αλλεργίες ή πιθανές παρενέργειες σε φαρμακευτική αγωγή που παίρνει ή και σημαντικές πληροφορίες που πρέπει να γνωρίζει κάποιος.
- Μια καλή χρήση των ΗΦΥ είναι να αποθηκεύει, να αναλύει και να παρακολουθά δεδομένα υγείας όλου του πληθυσμού δίνοντας στο προτέρημα έτσι στους παρόχους υγειονομικής περίθαλψης να εντοπίζουν και να ελέγχουν τυχών τάσεις που μπορούν να επιφέρουν οι ασθενής στο τυχών μέλλων.
- Δεν είναι μόνο οι παροχεις που έχουν πρόσβαση στα δεδομένα των ασθενών αλλά ακόμα και οι ίδιο οι ασθενείς, με την βοήθεια των εργαλείων που τους παρέχουν τα συστήματα κατανοούν την καλύτερη

την κατάστασης τους δίνοντας τους την ευκαιρία να διαχειριστούν και να πάρουν την υγειά στα χέρια τους, π.χ να έχουν καλύτερο έλεγχο πάνω στη ζωή τους.

- Έχουν την δυνατότητα να σχεδιαστούν με δυνατά συστήματα τα λεγόμενα 'robust security' που είναι συστήματα για δυνατή κρυπτογράφηση έτσι ώστε να μην μπορεί κάποιος να τα παραβιάσει ή να τα κλέψει.
- Μείωση κόστους στο τομέα της υγείας μέσω της αύξησης της αποδοτικότητας και της μείωσης των λαθών που γίνονται.
- Παρέχει βοήθεια στους παρόχους (π.χ. Ιατροί) έτσι ώστε να μπορούν να βρίσκουν και να ελέγχουν την εξέλιξη της υγείας του κάθε ασθενή, δίνοντας τους έτσι ευκαιρίες για θεραπευτικά σχέδια.
- Παρέχει συνολικές πληροφορίες οι οποίες μπορούν να χρησιμοποιηθούν για σκοπούς έρευνας έτσι ώστε να βρεθούν οι πηγές για διάφορες ασθένειες (καλύτερη καταπολέμηση κάθε αρρώστιας).

2.5.2 Μειονεκτήματα του EHR έναντι του EMR

Δεν πρέπει να βλέπουμε μόνο τα καλά οφέλη που μπορεί να μας επιφέρει η ψηφιοποίηση ενός ηλεκτρονικού φάκελου, αρκετές φορές μαζί με τα πλεονεκτήματα του υπάρχουν και κάποια μειονεκτήματα που μπορεί να προκύψουν μαζί του. Η Χρήση του ηλεκτρονικού φακέλου υγείας σε οργανισμούς μπορεί να επιφέρει και κάποια ρίσκα όπως

Θραύση και παράβαση νόμου της μυστικότητας : Άτομα που ξέρουν να διαχειρίζονται το διαδίκτυο γνωρίζουν πως τώρα με διαφορά προγράμματα τα ψηφιακά αρχεία υγείας είναι ευάλωτα στις σύγχρονες κυβερνοεπιθέσεις και παραβιάσεις δεδομένων, τα οποία μπορούν να θέσουν σε κίνδυνο το απόρρητο και την ασφάλεια των πληροφοριών των ασθενών μόνο με την χρήσει διάφορων μεθόδων όπως είναι τα bots ή και τα scams.

Περιορισμένη πρόσβαση: Ενώ φαίνεται η πρόσβαση στον ψηφιακό τομέα να είναι πάρα πολύ εύκολο, πολλοί πάροχοι έχουν περιορισμένη πρόσβαση στις ψηφιακές ιατρικές πύλες λόγω οικονομικού κόστους (υλικό και λογισμικό), έλλειψης γνώσης της τεχνολογίας κτλ.

Τεχνολογικές δυσλειτουργίες: Πότε δεν μπορούμε να γνωρίζουμε πόσο συχνά θα υπάρξουν οποιαδήποτε δυσλειτουργίες στο κομπιούτερ ή στα συστήματα του, εάν γίνονται συχνά αυτά τα σφάλματα θα κοστίσουν χρόνο, χρήμα.

Ανακριβείς Διαγνώσεις: Η τεχνολογία ολοένα και παίρνει τον έλεγχο με στόχο να στηριζόμαστε σταδιακά ολοένα και περισσότερο σ' αυτήν, αυτό οδηγεί στην μείωση των διάφορων ικανοτήτων στο τομέα υγείας αλλά ακόμη και στη αλληλεπίδραση μεταξύ ασθενών και ιατρού. Οι περισσότεροι ιατροί στηρίζονται πάνω στο τι δείχνουν τα ψηφιακά αποτελέσματα χωρίς να δίνουν σημασία στις δικές τους γνώσεις και σε φυσική εξέταση του ασθενή όπως θα έπρεπε να ήταν, έχοντας ως αποτέλεσμα να γίνονται ανακριβείς διαγνώσεις.

Τα μεγέθη επεξεργασίας των δεδομένων υγείας είναι αρκετά μεγάλη και δύσκολα στην επεξεργασίας , στην αναλυτικότητα τους με αποτέλεσμα στην καθυστερημένη επιλογή της φροντίδας του ασθενή.

Κόστος: Η εφαρμογή και η διατήρηση ενός συστήματος ΗΦΥ μπορεί να είναι δαπανηρή και τα μικρότερα ιατρεία ή κλινικές μπορεί να δυσκολεύονται να αντέξουν οικονομικά.

Διαλειτουργικότητα: Τα ηλεκτρονικά συστήματα υγείας ενδέχεται να μην είναι σε θέση να επικοινωνούν μεταξύ τους, καθιστώντας δύσκολη την κοινή χρήση δεδομένων ασθενών μεταξύ διαφορετικών παρόχων υγειονομικής περίθαλψης.

Ζητήματα απορρήτου και ασφάλειας: Περιέχουν ευαίσθητες προσωπικές και ιατρικές πληροφορίες και η ασφάλειά τους αποτελεί κρίσιμη ανησυχία. Εάν δεν είναι σωστά ασφαλισμένα, τα δεδομένα θα μπορούσαν να έχουν πρόσβαση ή να κλαπούν από μη εξουσιοδοτημένα άτομα.

Εκπαίδευση και προσαρμογή: Τα ηλεκτρονικά συστήματα απαιτούν την εκπαίδευση του προσωπικού για τη χρήση τους, κάτι που μπορεί να πάρει χρόνο και πόρους. Επιπλέον, κάποιο προσωπικό μπορεί να δυσκολεύεται να προσαρμοστεί στη νέα τεχνολογία.

Σφάλματα εισαγωγής δεδομένων: Τα ηλεκτρονικά συστήματα βασίζονται στην ακριβή εισαγωγή δεδομένων, αλλά μπορεί να προκύψουν σφάλματα λόγω ανθρώπινου λάθους, το οποίο μπορεί να οδηγήσει σε ανακριβή καταγραφή πληροφοριών ασθενούς.

Απώλεια προσωπικής επαφής: Με την αυξανόμενη χρήση των ΗΣΥ, υπάρχει ο κίνδυνος οι επαγγελματίες του ιατρικού τομέα να βασίζονται πολύ στην τεχνολογία και να χάσουν την προσωπική επαφή που είναι σημαντική για τη φροντίδα των ασθενών.

Χρόνος διακοπής λειτουργίας συστήματος: Τα ΗΣΥ εξαρτώνται από την τεχνολογία και ο χρόνος διακοπής λειτουργίας του συστήματος μπορεί να προκύψει λόγω προβλημάτων λογισμικού ή υλικού, τα οποία θα μπορούσαν να οδηγήσουν σε καθυστερήσεις στη φροντίδα των ασθενών.

Νομική και κανονιστική συμμόρφωση: Τα ΥΣΥ υπόκεινται σε διάφορες νομικές και ρυθμιστικές απαιτήσεις, όπως η HIPAA, και η μη συμμόρφωση μπορεί να οδηγήσει σε πρόστιμα και κυρώσεις.

2.5.3 Συμπέρασμα

Ο ΗΦΥ προσφέρει πάρα πολύ ωφελήματα τόσο στους παρόχους όσο και στους ασθενείς, όπως π.χ. βελτιωμένη ποιότητα φροντίδας, μεγαλύτερη ευκολία και αποδοτικότητα, πρόσβαση σε κυβερνητικά οικονομικά κίνητρα. Όμως από την άλλη, υπάρχουν και πάρα πολλά μειονεκτήματα όπως π.χ. κάποιες δυσκολίες και ανεπάρκειες, ανησυχίες για ενδεχόμενες ιδιωτικοποιήσεις και κυβερνο-ασφάλειες, αχρείαστες φοβίες προς τους ασθενείς, αυξημένες ανησυχίες για κακές πρακτικές εκ μέρους Ιατρών όπως επίσης θέματα κόστους τόσο σε χρόνο όσο και σε χρήμα.

Καταληκτικά, συγκρίνοντας τα υπέρ και τα κατά, οι ειδήμων και οι υπεύθυνοι για την εφαρμογή των εγκυκλίων συμφωνούν ότι εφόσον ο ΗΦΥ μπει σε πλήρη εφαρμογή, θα προσφέρει πολύ περισσότερα οφέλη στους ασθενείς, παρόχους και στην κοινωνία ολόκληρη.

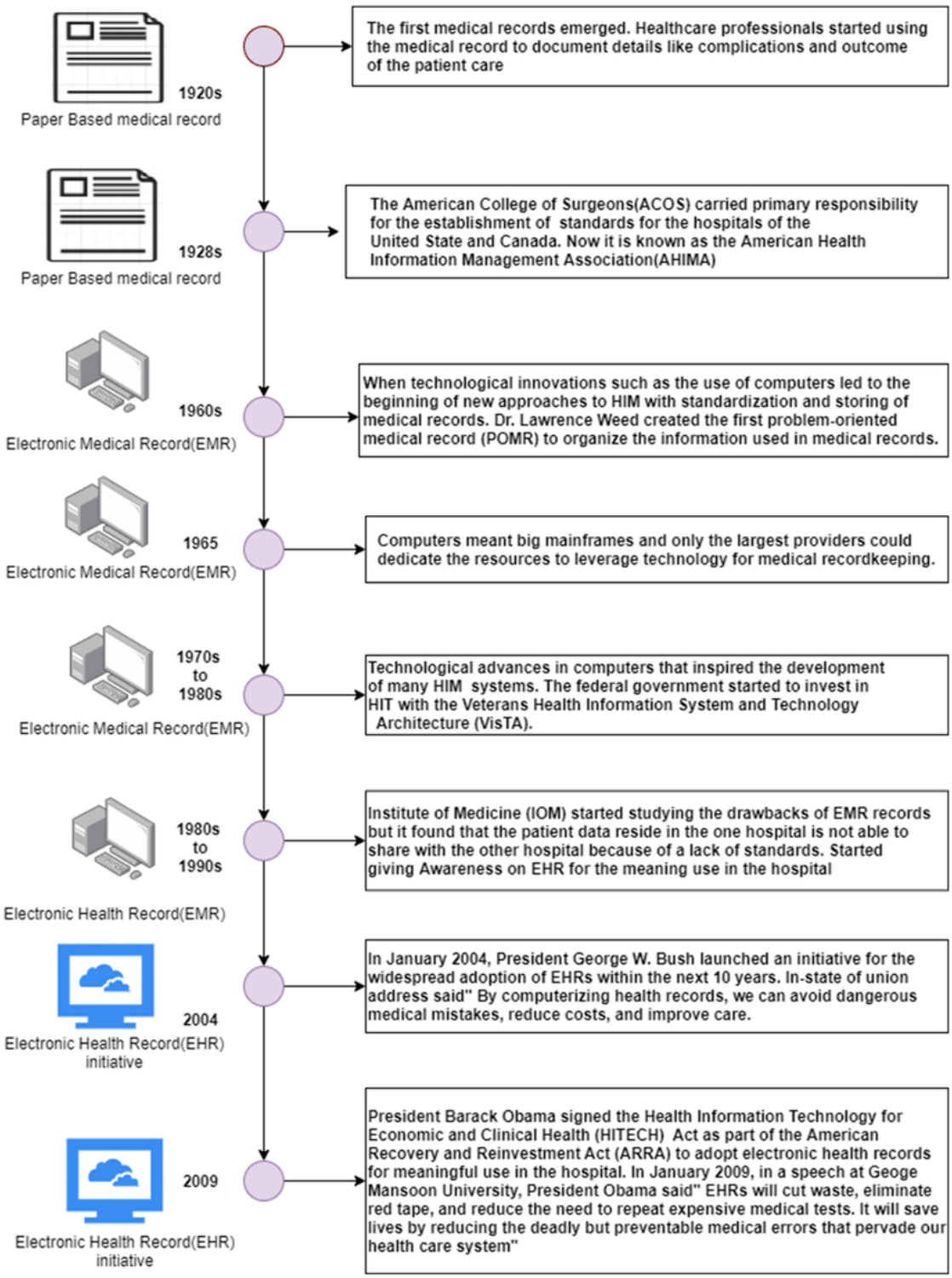
(Wheel | Advantages and Disadvantages of EHRs. (2020). https://www.wheel.com/companies-blog/advantages-and-disadvantages-of-ehrs)

(Parul Saini, W. T. (2021). EMR vs EHR - Difference between EMR and EHR. https://webmedy.com/blog/emr-and-ehr-difference/)

(Max Freedman. (2023). EMR vs. EHR: What's the Difference. https://www.businessnewsdaily.com/16204-emr-vs-ehr-explained.html)

(10 Advantages and Disadvantages of EHR [EHR vs EMR Differences] | PostDICOM. (n.d.). from https://www.postdicom.com/en/blog/advantages-and-disadvantages-of-ehr)

(Marlene Maheu. (2021). EMR & EHR: What Are the Important Differences that You Need to Know? https://telehealth.org/emr/)



Πίνακας 6 Η σταδιοδρομία του ιατρικού και του ηλεκτρονικού φάκελου υγείας μέχρι τώρα.(Health Services and Outcomes Research Methodology 2021, Manohara Pai M, Raghavendra Ganiga, Rajesh Kumar Sinha, https://www.researchgate.net/publication/348817075_Standard_electronic_health_record_EHR_framework_for_Indian_healthcare_system)

Πίνακας 6

2.6. Ο Ηλεκτρονικός Φάκελος Υγείας

Ο Ηλεκτρονικός Φάκελος Υγείας είναι μια συστηματοποιημένη συλλογή του ιστορικού και της κατάστασης υγείας του ασθενούς ο οποίος δημιουργείται, διατηρείται και συντηρείται από ένα γιατρό, Μονάδα υγείας ή άλλον επαγγελματία φροντίδα υγείας. Σύμφωνα με την Ευρωπαϊκή Επιτροπή Προτυποποίησης, Ιατρικός Φάκελος είναι «η αποθήκη όλων των πληροφορικών που αφορούν στο ιατρικό ιστορικό του ασθενούς, έτσι ώστε να αποτελεί τη βάση της διάγνωσης και της θεραπευτικής αντιμετώπισης του ασθενούς αλλά και τη βάση επιδημιολογικών ερευνών. Επιπλέον, παρέχει πληροφορίες διοικητικής, οικονομικής και στατιστικής φύσεως, καθώς και ποιοτικού ελέγχου».

Ο ηλεκτρονικός φάκελος αποτέλεσε τη μόνη αξιόπιστη εφαρμογή του ιατρικού, νοσηλευτικού και εργαστηριακού έργου, καθώς περιόρισε τα σφάλματα, βελτίωσε την παραγωγικότητα και τις ιατρικές αποφάσεις του προσωπικού, παρείχε ουσιαστική υποστήριξη στη χορήγηση της κατάλληλης φαρμακευτικής αγωγής και στον εντοπισμό μη φυσιολογικών τιμών στις εργαστηριακές εξετάσεις και βελτίωσε συνολικά την Ηλεκτρονικός Φάκελος Ασθενούς 2016 11 ποιότητα παροχής υπηρεσιών υγείας (Garg et al. (2005)). Απαραίτητη, όμως, προϋπόθεση για την ανάπτυξη ενός ηλεκτρονικού φακέλου υγείας είναι η ύπαρξη ενός Ολοκληρωμένου Πληροφοριακού Συστήματος.

Ο Ηλεκτρονικός Φάκελος Υγείας ήταν ένα πρωτόγνωρο ιατροτεχνολογικό φαινόμενο με ιδιαίτερα χαρακτηριστικά και πολύ διαφορετικό από τον παραδοσιακό χειρόγραφο ιατρικό φάκελο. Είναι σημαντικό να σημειωθεί ότι με την γέννηση του κάθε τέκνου, αυτόματα δημιουργείται και ένας ηλεκτρονικός φάκελος.

2.7 Ηλεκτρονικός Φάκελος στην Κύπρο

Ο Ιατρικός Ηλεκτρονικός Φάκελος έκανε την άφιξη του στην Κύπρο τον Σεπτέμβριο 2019. Αυτό σήμαινε πως κάθε Ιατρός έπρεπε να καταχωρεί και να αποθηκεύει τα προσωπικά αποτελέσματα της εξέτασης του κάθε ασθενή. Σε κάθε επίσκεψη ο ιατρός καταχωρούσε τα αποτελέσματα του ασθενή στην βάση δεδομένων έτσι ώστε τα νέα δεδομένα που καταχωρούνταν να έχουν συνοχή με τα παλιά. Εάν δεν υπήρχε υφιστάμενος ΗΦΥ, τότε έπρεπε να δημιουργηθεί ένας καινούργιος και παράλληλα ένα αντίγραφο ασφαλείας στην Ενιαία Τράπεζα Ηλεκτρονικών φακέλων Υγείας. Αυτό είχε σαν στόχο τη τήρηση και αποθήκευση των δεδομένων υγείας του κάθε ασθενή δημιουργώντας έτσι μία πλήρη εικόνα του ιατρικού ιστορικού του.

Η προβολή των ιατρικών στοιχείων του ασθενή θα είναι προσβάσιμα τόσο στους παρόχους στην Κύπρο όσο και σε όλες της Ευρωπαϊκές χώρες πράγμα που δίνει το δικαίωμα στον ασθενή να επισκέπτεται γιατρούς όχι μόνο στην Κύπρο αλλά και στο εξωτερικό και θα διευκολύνει μ' αυτόν τον τρόπο τη διάγνωση ή πρόσβαση στο ιστορικό υγείας του ασθενή. Ασθενείς με χρόνια προβλήματα θα βοηθηθούν πάρα πολύ. Επιπρόσθετα να αναφερθεί ότι η οποιαδήποτε εξαγωγή δεδομένων υγείας πρέπει να γίνεται μόνο με τη συγκατάθεση του κάθε πολίτη ξεχωριστά.

Όσο για τους παρόχους ο κάθε γιατρός που εξετάζει τον ασθενή θα παίρνει την αμοιβή του (ιατρική αποζημίωση) από την χώρα που ο ασθενής είναι εγγεγραμμένος χωρίς ο ασθενής να πληρώνει οποιοδήποτε ποσό.

Αυτό είναι το λεγόμενο ΓΕΣΥ που έχουμε τώρα στην Κύπρο.

(Periklis., Rompolas., Panicos., Masouras., Sotiris.,Avgousti.,Andreas., Charalambous., (2023). Ο Ηλεκτρονικός Φάκελος Υγείας στο Γενικό Σύστημα Υγείας της Κύπρου)

(Στέλιου Στυλιανού. (2019). Θα βλέπουμε τα ιατρικά μας δεδομένα με ένα κλικ - Τα δεδομένα | Offsite. https://www.offsite.com.cy/eidiseis/topika/tha-blepoyme-ta-iatrika-mas-dedomena-me-ena-klik-ta-dedomena)

Πάνω σε καθημερινή βάση, επισκεπτόμαστε διαδικτυακώς διάφορες ιστοσελίδες για αγορά φαρμάκων ή για ενημέρωση πάνω σε φάρμακα που μας ενδιαφέρουν. Μέσω όμως της πλατφόρμας που επισκεπτόμαστε, υπάρχουν διάφοροι αλγόριθμοί που αποθηκεύουν και συλλέγουν διάφορα δεδομένα για εμάς. Αναλόγως της ρύθμισης της διαδικτυακής πλατφόρμας που είμαστε, καταγράφονται κάποια στοιχεία τα οποία μπορούν να περιέχουν ή να μην περιέχουν προσωπικά δεδομένα. Η εταιρεία/πλατφόρμα που θα συλλέγει τα δεδομένα πρέπει να διαχειρίζεται με μεγάλη προσοχή και εχεμύθεια τα προσωπικά δεδομένα πάντα βάσει της νομοθεσία περί την προστασία των προσωπικών δεδομένων.

2.8 Δικαίωμα Πρόσβασης στον ΗΦΥ

Ο κάθε ηλεκτρονικός ιατρικός φάκελος είναι ατομικός και μοναδικός για κάθε πελάτη/ασθενή και μπορεί να είναι προσβάσιμος για:

- Τον ίδιο το πολίτη που είναι ο κάτοχος του συγκεκριμένου Ηλεκτρονικού φακέλου υγείας.
- Άτομο που παρέχει υπηρεσίες υγείας για τον ασθενή όπως ο προσωπικός σου Ιατρός, άτομα που έχουν πρόσβαση στο ίδιο το φάκελο λόγω χειρισμού ή/και γενικώς που έχουν την εξουσιοδότηση του πάντα όμως σύμφωνα με τις διατάξεις της παραγράφου του άρθρου 25.
- Ο καθορισμένος αντιπρόσωπος του κατόχου Ηλεκτρονικού Φακέλου Υγείας, στον οποίο ο πολίτης έχει παραχωρήσει εξουσιοδότηση (σύμφωνα με τις διατάξεις της παραγράφου (γ) του άρθρου 25 του εν λόγω Νόμου).

- Διασφαλίζεται η εμπιστευτικότητα και το απόρρητο των δεδομένων των προσώπων που έχουν πρόσβαση ή είχαν πρόσβαση στα δεδομένα υγείας του Ηλεκτρονικού Φακέλου Υγείας σύμφωνα με τις διατάξεις του περί της Προστασίας των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και της Ελεύθερης Κυκλοφορίας των Δεδομένων αυτών Νόμου και του Κανονισμού (ΕΕ) 2016/679.
- Διαφορετικοί αναγνωριστικοί κωδικοί πρόσβασης δεδομένων στους κατόχους Ηλεκτρονικών Φακέλων Υγείας.

2.9 Περιεχόμενο Ηλεκτρονικού Φακέλου Υγείας

Περιέχει το βασικό σύνολο δεδομένων υγείας του πολίτη και τα δεδομένα υγείας που καταχωρεί ο ίδιο ο πολίτης ή άλλος αντιπρόσωπος του. Κάθε πάροχος (π.χ. ο προσωπικός γιατρός του κάθε πολίτη) υποχρεώνεται να καταχωρεί δεδομένα υγείας στο βασικό σύνολο δεδομένων υγείας. Η καταχώρηση δεδομένων εκ μέρους του πολίτη είναι προαιρετική. Τα δεδομένα υγείας περιέχουν αρχεία τα οποία συντάσσονται με έγγραφα ή ηλεκτρονικά ή με οποιοδήποτε άλλο τρόπο από τον πάροχο και δίνουν λεπτομερή στοιχεία ως προς την ταυτότητα του ασθενούς και του παρόχου, την ιατρική πληροφόρηση αναφορικά με τη θεραπεία που παίρνει ο ασθενής, το προηγούμενο ιατρικό ιστορικό του, τη διάγνωση της παρούσας ιατρικής κατάστασης του και της θεραπευτικής αγωγής που του παρέχεται. (Παγκυπρίως Δικηγορικός Συλλογος. Ο περί Ηλεκτρονικής Υγείας Νόμος του 2019 - 59(Ι)/2019 - 19 - Δημιουργία και

περιεχόμενο Ηλεκτρονικού Φακέλου Υγείας 2019. (https://www.cylaw.org/nomoi/enop/ind/2019_1_59/section-sccf5906ad-f094-4bdd-bf4b-d91d7caf4436.html)

2.10 Ο Ηλεκτρονικός Φάκελος Υγείας εξυπηρετεί κάποιους σκοπούς:

α) να υποστηριχτεί η φροντίδα υγείας του ατόμου εφ' όρου ζωής.

β) να προωθεί την έρευνα και την εκπαίδευση των επαγγελματιών υγείας.

γ) να βοηθά στην πρόσβαση και στο διαμοιρασμό πληροφοριών στους επαγγελματίες υγείας με φιλικό τρόπο καθώς ελέγχεται και η ασφάλεια των δεδομένων. Τα ηλεκτρονικά συστήματα αρχειοθέτησης προσφέρουν πρόσβαση σε έγγραφα από οποιαδήποτε τοποθεσία με σύνδεση στο διαδίκτυο, επιτρέποντας την απομακρυσμένη πρόσβαση και τη συνεργασία.

δ) Καλύτερη οργάνωση εγγράφων: Επειδή τα έγγραφα μπορούν να επισημανθούν με πληροφορίες και να αναζητηθούν χρησιμοποιώντας λέξεις-κλειδιά, τα ηλεκτρονικά συστήματα αρχείων διευκολύνουν την οργάνωση και την ανάκτησή τους.

ε) Βελτιωμένη απόδοση: Με την άρση της ανάγκης για μη αυτόματη αρχειοθέτηση, εύρεση και ανάκτηση εγγράφων σε χαρτί, η ηλεκτρονική αρχειοθέτηση μπορεί να εξοικονομήσει χρόνο και πόρους. Αυτό μπορεί επίσης να βοηθήσει στην εξάλειψη των λαθών και στην αύξηση της ακρίβειας.

Ζ) Αυξημένη ασφάλεια: Τα ηλεκτρονικά συστήματα αρχειοθέτησης μπορούν να προσφέρουν βελτιωμένα χαρακτηριστικά ασφαλείας, όπως προστασία με κωδικό πρόσβασης, κρυπτογράφηση και περιορισμούς πρόσβασης για την προστασία ευαίσθητων δεδομένων από ανεπιθύμητη πρόσβαση και απειλές στον κυβερνοχώρο.

Καταληχτικά, ο σκοπός της ηλεκτρονικής αρχειοθέτησης είναι να καταστήσει τη διαχείριση εγγράφων και πληροφοριών πιο αποτελεσματική και να αποδίδεται με πιο επαγγελματικό τρόπο.

Θα μπορούσαμε να μιλήσουμε για πολλά άλλα θέματα όπως π.χ. ποιοι έχουν δικαίωμα πρόσβασης στον Ηλεκτρονικό Φάκελο Υγείας, τις διαδικασίες πρόσβασης , ποια τα δικαιώματα/Υποχρεώσεις τόσων των κατόχων όσων και των Παρόχων Υπηρεσιών Υγείας, όμως επί του παρόντος δεν θα επεκταθούμε σ' αυτά.

2.11 Μέτρα Ασφαλείας που τηρούνται από την Τράπεζα Δεδομένων

Προς διασφάλιση και αντιμετώπιση κλοπής οποιωνδήποτε πληροφοριών (π.χ. να αλλοιωθούν τα στοιχεία ταυτοποίησης είτε του αποστολέα είτε του δέκτη, αλλοίωση πληροφοριών, διαγραφή/αλλαγή λογισμικού της Τράπεζας), πρέπει να γίνεται η πιστή τήρηση των πιο κάτω μέτρων ασφαλείας:-

- Να γίνεται η σωστή ταυτοποίηση των χρηστών μιας ανταλλαγής δεδομένων.
- Πρόσβαση μόνο σε εξουσιοδοτημένα άτομα.
- Η απαγόρευση διάρρευσης προσωπικών δεδομένων υγείας.
- Τα δεδομένα Υγείας να είναι μόνο διατεθειμένα σε εξουσιοδοτημένους χρήστες.

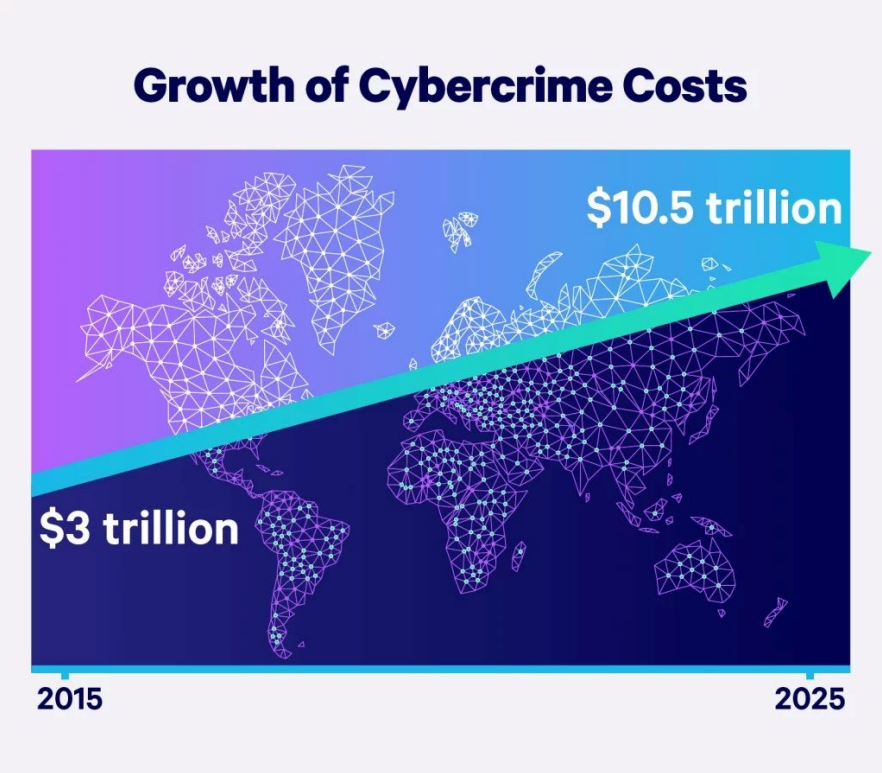
- Κωδικοποίηση όλων των πληροφοριών που είναι αποθηκευμένα στην Τράπεζα και στους χώρους όπου τηρούνται τα αντίγραφα ασφαλείας.
- Να διασφαλίζεται η ακεραιότητα των δεδομένων υγείας.
- Να είναι δυνατό η αναγνωσιμότητα πρόσβασης σε κάθε τροποποίηση ή επεξεργασία των δεδομένων.
- Να αποδίδεται ευθύνη για εισαγωγή, πρόσβαση ή τροποποίηση κάθε δεδομένου.
- Δια νόμου του άρθρου 30, θα πρέπει να υπάρχει η τήρηση αντιγράφων ασφαλείας.

Τέλος, σε κάθε πράξη που γίνεται στα προσωπικά δεδομένα υγείας του πελάτη να αναφέρεται ξεκάθαρα η ημερομηνία, η ώρα που έχει γίνει και το εξουσιοδοτημένο άτομο.

(Παγκυπρίως Δικηγορικός Συλλογος. Ο περί Ηλεκτρονικής Υγείας Νόμος του 2019 - 59(I)/2019 - 19 - Δημιουργία και περιεχόμενο Ηλεκτρονικού Φακέλου Υγείας 2019. https://www.cylaw.org/nomoi/enop/ind/2019_1_59/section-sccf5906ad-f094-4bdd-bf4b-d91d7caf4436.html)

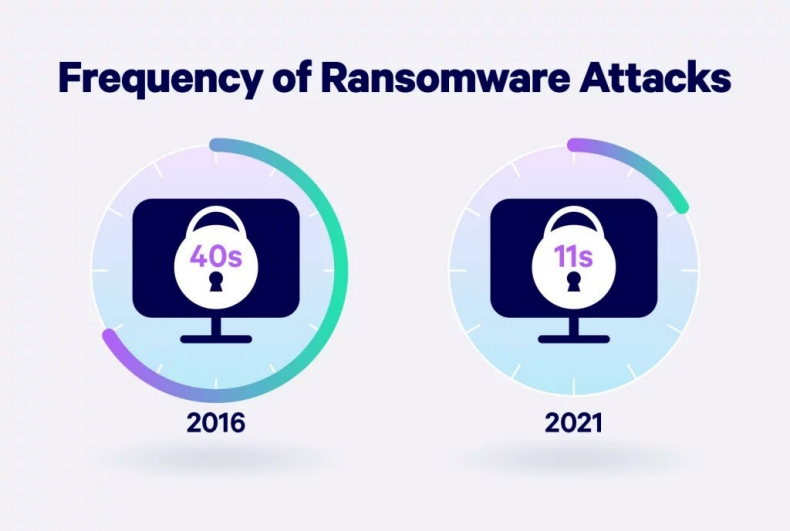
2.12 Κυβερνοεπιθέσεις (Cyber attacks)

Έχοντας προαναφέρει τα μειονεκτήματα που μπορεί να επιφέρει ο ηλεκτρονικός φάκελος υγείας, πρέπει να δώσουμε περισσότερη έμφαση στο κυριότερο πρόβλημα που είναι οι κυβερνοεπιθέσεις. Όπως βλέπουμε στο πιο κάτω πίνακα οι κυβερνοεπιθέσεις έχουν αυξηθεί σε ένα τερατώδες ποσοστό τα τελευταία χρόνια. Οι περισσότερες απάτες όπως π.χ. fishing, man in middle attack, χαμηλή προστασία στον ηλεκτρονικό υπολογιστή, είναι όλα παραδείγματα μέσα από τα οποία μπορεί ο καθένας/κάθε εταιρεία να θυματοποιηθεί διαδικτυακός. Οι τεχνικές των απατεώνων μπορεί να κυμαίνονται από μια απροσδόκητη επαφή μέσω email ή τηλεφώνου με σκοπό να κλέψουν πληροφορίες των ατόμων έτσι ώστε να τις χρησιμοποιήσουν εναντίον τους.



Πίνακας 7 Αύξηση του Κόστους του Εγκλήματος στον Κυβερνοχώρο

Όπως βλέπουμε στον πιο κάτω πίνακα, το 2016 σε σύγκριση με το 2021, η συχνότητα να γίνει κυβερνοεπίθεση ήταν κάθε 40 δευτερόλεπτα Vs του 2021, όπου έχει μειωθεί σε 11 δευτερόλεπτα, δηλαδή η πιθανότητα κυβερνοεπίθεσης είναι πιο συχνή.



Πίνακας 8 Συχνότητα επιθέσεων

Στο πιο κάτω πίνακα, βλέπουμε πως οι εταιρείες έχουν σταδιακά επενδύσει εκατομμύρια χρήματα στην προστασία των προσωπικών δεδομένων. Πρέπει επίσης να λεχθεί ότι χωρίς τον GDPR τίποτα από αυτά δεν θα γίνονταν και όλα θα ήταν ανεξέλεγκτα.

Πίνακας 9 Δαπάνες για την Ασφάλεια των Πληροφοριών (βιβλιογραφία αναγράφετε στο τέλος της παραγράφου 2.12)

(2023 Must-Know Cyber Attack Statistics and Trends | Embroker .Mike McLean(2023), from https://www.embroker.com/blog/cyber-attack-statistics/)

2.13 Διαφορές Μεταξύ Χειρόγραφου Ιατρικού Φακέλου και του Ηλεκτρονικού.

Υπάρχουν αρκετές διαφορές μεταξύ των δύο αλλά κάτι που αξίζει να σημειωθεί είναι ότι η ψηφιακή μορφή προτιμάται από κάθε νεοεισερχόμενη ή/και υφιστάμενη εταιρεία.

Μερικές από τις διαφορές τους μπορούν να διατυπωθούν πιο κάτω:

Χειρόγραφος Ιατρικός Φάκελος	Ηλεκτρονικός Φάκελος Υγείας
• Έχει ελάχιστο κόστος.	• Ο Ηλεκτρονικός Φάκελος Υγείας μπορεί να χρησιμοποιηθεί από πολλούς χρήστες ταυτόχρονα έχοντας όλοι πρόσβαση στις πληροφορίες.

• Υπάρχει η ευχέρεια της ελεύθερης έκφρασης στο να γράψει κάποιος ιδιωτικός ιατρός τι θέλει. • Μια εταιρεία δεν χρειάζεται σπατάλη χρόνου ή χρήματος στην εκπαίδευση του ιατρικού προσωπικού εφόσον δεν απαιτείται κάποια ειδική εκπαίδευση. • Εύκολη μεταφορά του φακέλου εντός του νοσοκομείου χωρίς την χρήση ηλεκτρονικού υπολογιστή. • Εύκολη εισαγωγή δεδομένων. • Εύκολος στην χρήση του.	• Δεν χρειάζεται η μεταφορά του μεταξύ διάφορων τμημάτων εφόσον με τη χρήση ενός υπολογιστή μπορείς να έχεις οποιαδήποτε πληροφορία για τον ασθενή θέλεις χωρίς δε να υπάρχει η πιθανότητα να χαθεί οποιαδήποτε πληροφορία. • Εύκολη και γρήγορη είσοδος για την παροχή πληροφόρησης. • Διευκολύνεται η ιατρική απόφαση εφόσον όλα τα απαραίτητα στοιχεία που αφορούν τον ασθενή είναι συγκεντρωμένα σε μία βάση δεδομένων και μπορούν να παρέχουν μία συνολική εικόνα της κατάστασης υγείας του ασθενή ακόμη και όταν αφορά περίπλοκες περιπτώσεις και γρήγορη ανταλλαγή δεδομένων. • Τα δεδομένα προστίθενται στη βάση δεδομένων μέσω εξουσιοδοτημένων ατόμων και η οποιαδήποτε πρόσβαση στα εν λόγω δεδομένα καταγράφεται ονομαστικός. • Ελάχιστη χρήση αποθηκευτικού χώρου στο χώρο δουλείας χωρίς να υπάρχει ο φόβος να χαθούν σημαντικά δεδομένα. • Χρήση κωδίκων για την πρόσβαση σε εξουσιοδοτημένα πρόσωπα μόνο. • Μείωση γραφειοκρατίας της ιατρικής πράξης και παραχώρηση περισσότερου χρόνου στην εξέταση του ασθενή.

Πίνακας 10 Διαφορές του Ηλεκτρονικού Φακέλου Υγείας με του Χειρόγραφου

Μπότσης, Τ.-Χ. (2005). Ηλεκτρονικός ιατρικός φάκελος ασθενή. https://el.wikipedia.org/wiki/

(https://www.ehrinpractice.com/ehr-system-disadvantages.html)

2.14 HIPAA (Health Insurance Portability and Accountability Act- USA Health Care)

Αναφορικά για γενική γνώση, έξω από την ευρωπαϊκή ένωση υπαρχή η HIPAA. Όπως είχαμε προαναφέρει στην συγκεκριμένη διατριβή ο κανονισμός του GDPR συμπεριλαμβάνει όλους τους πολίτες που είναι ενεργή στην ευρωπαϊκή ένωση και ταξιδεύουν σε τρίτες χώρες(προστατευμένη και εκεί) . Σε αντιστοιχία με αυτό, στις τρίτες χώρες όπως για παράδειγμα την Αμερική έχουν μια ειδική ομοσπονδιακή νομοθεσία που λέγεται HIPPA.

Η HIPAA (Health insurance Portability and Accountability Act 1996) είναι μια ομοσπονδιακή νομοθεσία που έχει να κάνει με την προστασία των ευαίσθητων προσωπικών δεδομένων των ασθενών περί της υγείας

τους κατά την διάρκεια ορατότητας και λογοδοσίας τους. Η συγκεκριμένη νομοθεσία έχει μπει σε εφαρμογή από το 1996 και εφαρμόζεται μόνο για τους Αμερικανούς πολίτες στις Ηνωμένες Πολιτείες Αμερικής ή όπου σχετικά βρίσκονται οι Αμερικανοί πολίτες.

Η HIPAA θέσπισε απαιτήσεις για τη διατήρηση του απορρήτου των ιατρικών αρχείων των ανθρώπων, των διαγνώσεων υγειονομικής περίθαλψης, των πληροφοριών θεραπείας και άλλων ατομικά αναγνωρίσιμων πληροφοριών υγείας.

Το HIPAA περιλαμβάνει μέτρα που προσπαθούν να διευκολύνουν τους ανθρώπους να διατηρήσουν την ασφαλιστική τους κάλυψη υγείας όταν μετακινούν θέσεις εργασίας ή περνούν από ορισμένα γεγονότα ζωής.

Για να απλοποιήσει και να βελτιώσει την αποτελεσματικότητα, το HIPAA απαιτεί τη χρήση τυποποιημένων ηλεκτρονικών συναλλαγών και συνόλων κωδικών για διοικητικές δουλειές που σχετίζονται με την υγειονομική περίθαλψη, όπως η τιμολόγηση και η επεξεργασία αξιώσεων.

Το HIPAA ισχύει για καλυπτόμενες εταιρείες καθώς και για τις επιχειρηματικές τους συνδέσεις. Οι πάροχοι υγειονομικής περίθαλψης, τα σχέδια υγείας και τα κέντρα συμψηφισμού υγειονομικής περίθαλψης που μεταφέρουν πληροφορίες υγείας ηλεκτρονικά είναι παραδείγματα καλυπτόμενων οντοτήτων. Τα άτομα ή οι οργανισμοί που εκτελούν συγκεκριμένους ρόλους ή δραστηριότητες αναφέρονται ως επιχειρηματικοί συνεργάτες.

(Annas, G. J. (2003). HIPAA Regulations: A New Era of Medical-Record Privacy? HIPAA Regulations: A New Era of Medical-Record Privacy? Part of the Health Law and Policy Commons. https://scholarship.law.bu.edu/faculty_scholarship)

Κεφάλαιο 3

Συνδυασμός ΓΚΠΔ με Ηλεκτρονικό Φάκελο Υγείας.

Ο ΓΚΠΔ έχει μεγάλη επίδραση και επιρροή πάνω στον Ιατρικό Τομέα και την φροντίδα των ασθενών συμπεριλαμβανομένου τη συλλογή, την ανάλυση, τη διαχείριση και αποθήκευση των προσωπικών ευαίσθητων δεδομένων που αφορούν το ιατρικό ιστορικό των ασθενών. Όταν μιλάμε για «ιατρική πληροφορία» αναφερόμαστε σε οποιαδήποτε πληροφορία του ατόμου που έχει να κάνει με το ιστορικό υγείας του. Η οποιαδήποτε ιατρική πληροφορία θεωρείται ως «ευαίσθητα δεδομένα»(σύμφωνα με τον GDPR, τα δεδομένα υγείας θεωρούνται μια ειδική κατηγορία προσωπικών δεδομένων που απαιτεί πρόσθετη προστασία) τα οποία υπόκεινται σε αυστηρούς κανονισμούς. Οι Οργανισμοί Υγειονομικής Περίθαλψης (ΟΥΠ) πρέπει να λαμβάνουν ρητή συγκατάθεση από άτομα πριν συλλέξουν και επεξεργαστούν τα δεδομένα υγείας τους και πρέπει να διασφαλίσουν ότι αυτά τα δεδομένα υποβάλλονται σε επεξεργασία με ασφάλεια και εμπιστευτικότητα. Αυτό περιλαμβάνει τη λήψη κατάλληλων τεχνικών και οργανωτικών μέτρων για την προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση, τυχαία απώλεια ή ζημιά και άλλους κινδύνους. Τα μόνο άτομα που μπορεί να έχουν το δικαίωμα επεξεργασίας είναι οι επαγγελματίες υγείας οι οποίοι είναι δέσμιοι της υποχρέωσης τήρησης του ιατρικού απόρρητου. Αυτό μπορεί να έχει ως αποτέλεσμα την ακατάλληλη χρήση τέτοιων δεδομένων και τον ανάλογο αρνητικό αντίκτυπο πάνω στη ζωή ή/και τη φήμη του ασθενούς.

Αναφορικά με όλους τους ΟΥΠ (π.χ. πάροχοι, Επαγγελματίες Υγείας κλπ), πρέπει να συμμορφώνονται με τον GDPR όταν χειρίζονται προσωπικές πληροφορίες υγείας. Επιπλέον, Βάσει του άρθρου 37 του GDPR απαιτεί από αυτούς να ορίσουν έναν Υπεύθυνο Προστασίας Δεδομένων (DPO) για να επιβλέπει τη συμμόρφωση με τον κανονισμό. Τυχόν παραβιάσεις δεδομένων θα πρέπει να αναφερθούν στις αρμόδιες αρχές εντός 72 ωρών από τη στιγμή που θα λάβουν γνώση της οποιασδήποτε παραβίασης.

Σύμφωνα με τον GDPR, σε όλες τις περιπτώσεις οι πάροχοι υγειονομικής περίθαλψης οφείλουν να ζητούν τη συναίνεση των ασθενών. Η συγκατάθεση πρέπει να παρέχεται ελεύθερα, ρητά, ενήμερη και σαφής και να περιλαμβάνει μια ξεκάθαρη θετική πράξη. Οι ασθενείς πρέπει πάντα να ενημερώνονται για τον στόχο της συλλογής δεδομένων που αφορά την υγεία τους και πρέπει να τους επιτρέπεται να ανακαλούν με απλό τρόπο τη συγκατάθεση τους. Πρέπει επίσης να έχουν πρόσβαση στα δεδομένα τους, προκειμένου να τα τροποποιήσουν ή να τα ενημερώσουν ή/και να τα αποσύρουν ανά πάσα στιγμή.

Συνολικά, ο GDPR έχει σημαντικό αντίκτυπο στον κλάδο της Υγειονομικής Περίθαλψης και οι ΟΥΠ πρέπει να λάβουν μέτρα για να εξασφαλίσουν τη συμμόρφωση με τον κανονισμό για την προστασία του απορρήτου και της ασφάλειας των προσωπικών πληροφοριών υγείας. Επίσης ο GDPR άλλαξε δραστικά τον τρόπο με τον οποίο οι ΟΥΠ χρησιμοποιούν και διατηρούν όλες τις προσωπικές πληροφορίες π.χ. είχαν λάβει σοβαρά υπόψη το καθήκον τους να διατηρούν τις ευαίσθητες πληροφορίες σχετικά με το προσωπικό και τους

ασθενείς ασφαλής αλλά μέσω του GDPR έχει κάνει τη διαφορά στο ότι όλοι όσοι διατηρούν, χειρίζονται ή επεξεργάζονται προσωπικά δεδομένα, συμπεριλαμβανομένων των ιδρυμάτων υγειονομικής περίθαλψης, υποχρεούνται πλέον να συμμορφώνονται νομικά μαζί με τον GDPR. Λόγω της πολυπλοκότητας του GDPR και των υψηλών κυρώσεων που μπορεί να προκύψουν από την παραβίασή του, όλες οι επιχειρήσεις καλούνται να αναζητήσουν τη βοήθεια ειδικού για να διασφαλίσουν ότι επεξεργάζονται δεδομένα σύμφωνα με τον GDPR, αποφεύγοντας έτσι την πιθανότητα επιβολής προστίμων για παραβιάσεις του GDPR. (Briefings, How does the GDPR affect the medical industry? N. Pirilides & Associates LLC. (2020). https://www.pirilides.com/en/briefings/how-does-the-gdpr-affect-the-medical-industry/ppp-101/57/).

Αναφορικά με το άρθρο του Anton Hasselgren για τη συμμόρφωση του GDPR στο τομέα της Υγείας ανάφερε πως κάποιες σημαντικές νομικές αλλαγές που πρέπει τώρα κάθε ίδρυμα υγειονομικής περίθαλψης (ΙΥΠ) να ακολουθεί όπως :

- Κάθε πληροφορία και πράξει του ασθενή πρέπει να είναι μέχρι το σήμερα, χρησιμοποιώντας εκτίμηση επιπτώσεων προστασίας μέσα σε μια λίστα. Η λίστα πρέπει να περιλαμβάνει το λόγο επισκέψεις, τι δεδομένα πάρθηκαν και ποιος έχει πρόσβαση.
- Το ΙΥΠ μπορεί να δικαιολογήσει τον στόχο και την συλλογή των δεδομένων σύμφωνα με μία από τις έξι απαιτήσεις. (Συναίνεση, Εκτέλεση σύμβασης, Έννομο συμφέρον, Ζωτικό Συμφέρον, Νομική Απαίτηση, Δημόσιο Συμφέρον- GDPR)
- Είναι υποχρεούμενή να ενημερώσουν το ασθενή πώς τα δεδομένα του 1) αποθηκεύονται 2) γιατί αποθηκεύονται 3) πως τα επεξεργάζονται αυτά που αποθηκεύουν 4) ποιος έχει πρόσβαση σε αυτά 5) τι κάνουν για να κρατήσουν με ασφάλεια αυτά τα στοιχεία. Πάντα χρησιμοποιώντας απλή και κατανοητή διάλεκτο.
- Πρέπει να επιλέξουν κάποιον που θα είναι υπεύθυνος για τη συμμόρφωση των καταστάσεων με τον GDPR που επίσης εκείνος περιλαμβάνει την αξιολόγηση των πολιτικών προστασίας δεδομένων και την εφαρμογή τους.
- Εάν ζητηθεί από κάποιο ασθενή μέσω γραπτού αιτήματος να μάθει τι δεδομένα είναι αποθηκευμένα γι' αυτόν, τότε το συγκεκριμένο ιατρικό ινστιτούτο θα πρέπει να ανταποκριθεί εντός ενός μηνός από την ημερομηνία αίτησης, ενημερώνοντας τον μέσω γραπτής επιστολής.
- Εάν ζητηθεί από τον ασθενή να διαγραφούν τα δεδομένα του, τότε θα πρέπει εντός ενός μηνός να ακολουθήσουν τις οδηγίες του. Φυσικά υπάρχει το ενδεχόμενο να αρνηθούν να υλοποιήσουν το αίτημα του, εάν υπάρχουν λόγοι που νομικώς ευσταθούν να κρατηθούν ακόμη τα εν λόγω δεδομένα. Τόσο σ' αυτή την περίπτωση όσο και στην προηγούμενη που αναφέρθηκε, η ταυτότητα του ασθενή θα πρέπει να εξακριβωθεί.
- Εάν ζητηθεί από τον ασθενή να γίνει περιορισμός ή να σταματήσουν την διαδικασία επεξεργασίας των δεδομένων τους από το συγκεκριμένο ίδρυμα υγείας εάν το επιθυμούν. Βέβαια το ίδρυμα μπορεί εάν υπάρχουν λόγοι να συνεχίζει να τα αποθηκεύει αλλά η επεξεργασία τους θα πρέπει να είναι σίγουρα περιορισμένη.
- Τέλος, οι ασθενείς έχουν περισσότερη αυτονομία στα προσωπικά τους δεδομένα πάρα το ίδιο το ίδρυμα. Αυτό σημαίνει ότι οι άνθρωποι θα πρέπει να μπορούν να λαμβάνουν δεδομένα υγείας με ευανάγνωστο τρόπο και να τα μοιράζονται με άλλους παρόχους υγειονομικής περίθαλψης. Παραθέτοντας ένα παράδειγμα, εάν ένας ασθενής θέλει να πάρει ένα πλήρως ενημερωμένο ιστορικό της υγείας του, τότε το ιατρικό ίδρυμα θα πρέπει να του το προσκομίσει. (Hasselgren, A., Wan, P. K.,

Horn, M., Kralevska, K., Gligoroski, D., & Faxvaag, A. (2020). GDPR Compliance for Blockchain Applications in Healthcare. http://arxiv.org/abs/2009.12913)

Ο ΗΦΥ πρέπει να χρησιμοποιηθεί κατάλληλα έτσι ώστε να συνάδει με τους κανονισμούς του GDPR και η επίτευξη του γίνεται μέσω του κατάλληλου εξοπλισμού και αναβαθμισμένου λογισμικού. Υπάρχουν ιδιαίτεροι προβληματισμοί ως προς την χρησιμοποίηση του ΗΦΥ λόγω του ότι εγκυμονούν πολλοί κίνδυνοι όπως περιπτώσεις υποκλοπής ή κακόβουλης χρήσης των προσωπικών δεδομένων όπως επίσης οικονομικά και κρίσιμα ηθικά διλήμματα. Όμως είναι πολλά τα πλεονεκτήματα που εγείρονται εκ μέρους του ΗΦΥ γι' αυτό και προβάλλεται η ανάγκη για την καθιερωμένη εφαρμογή του.

Στο πιο κάτω πίνακα απεικονίζονται περισσότερες επιδράσεις στο τομέα της υγείας αλλά εμείς έχουμε αναφέρει τα βασικά.

Article in GDPR	Compliance	Impact in healthcare
Art. 30 (Records of processing activities), Art. 35 (Data protection impact assessment)	Able to conduct information audit to demonstrate GDPR compliance	HI is required to keep an up-to-date and detailed list of their processing activities using a data protection impact assessment. The list should include the purposes of the processing, what kind of data you process and who has access to it in the organization
Art. 6 (Lawfulness of processing), Art. 7 (Conditions for consent)	Legal justification for processing health data	HI can justify the purpose according to one of the six conditions. E.g Patients has given consent for the processing. Extra obligation such as the opportunity to revoke consent must be available to patients
Art. 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject)	Clear information about the data processing and legal justification in privacy policy	HI is obligated to inform patients that health data is collected. HI should explain why this is collected, how it is processed, who has the access and how it is secured using clear and plain language, particularly when addressing specifically to a child.
Art. 33 (Notification of a personal data breach to the supervisory authority), Art. 34 GDPR (Communication of a personal data breach to the data subject)	Have a process to notify the authorities in the event of a data breach	HI is required to notify the supervisor authority in their jurisdiction within 72 hours learning of the health data breached or exposed. Patients should be notified without undue delay in plain language, if the breach is likely to put them at risk.
Art. 32 (Security of processing)	Encrypt, pseudonymize or anonymize personal data whenever possible	HI is to encrypt, pseudonymize or anonymize PHI whenever feasible.
Art. 25 (Data protection by design and by default), Art. 5 (Principles relating to processing of personal data)	Data protection is considered at all times, including at the beginning of developing a product	HI should implement appropriate technical (encryption) and organizational measures(deleting patients data that is no longer needed) to protect data. HI which adheres to data protection principles when processing of personal data is involved.
Art. 25 (Data protection by design and by default)	Designated person for ensuring GDPR compliance across the organization	HI should designate someone that is accountable for GDPR compliance which includes evaluation of data protection policies and the implementation of policies. HI should be able to verify the patient's identity.
Art. 15 (Right of access by the data subject)	Able to verify the patients' identity	HI is obligated to furnish patients with complete information when they request it and should be able to comply within a month. HI should be able to verify the patient's identity.
Art. 17 (Right to erasure/ right to be forgotten)	Easy to delete personal data upon request	Patients should have the right to request to delete all health data and HI should honour their request within a month. HI may have grounds to deny the request such as compliance with a legal obligation. HI should be able to verify the patient's identity.
Art. 18 (Right to restriction of processing)	Easy to stop data processing upon request	Patients can request HI to restrict or stop processing their health data if certain grounds apply, such as dispute about the lawfulness of the processing. HI may be allowed to keep storing their data although the processing is restricted.
Art. 24 (Responsibility of the controller)	Establish the responsibility and liability of the controller	Any processing of personal data carried out by HI or on HIs behalf, responsibilities should be established which includes implementing appropriate technical and organisational measures. This is to ensure and to be able to demonstrate that processing is performed lawfully
Art. 20 (Right to data portability)	Easy to receive a copy of your personal data and share with another in a simple format	From a privacy standpoint, GDPR offers higher patients autonomy over their data, instead of HI. This means patients should be able to receive health data in a readable format or share with other HI.

Πίνακας 11 Συνάφεια του GDPR στο Τομέα της Υγείας (GDPR Compliance for Blockchain Applications in Healthcare, Anton Hasslgren sep 2020)

3.2 GDPR & Προσωπικά Ηλεκτρονικά Αρχεία Υγείας.

Ο GDPR και τα Προσωπικά Ηλεκτρονικά Αρχεία Υγείας μοιράζονται ορισμένες ανησυχίες σχετικά με το απόρρητο και την ασφάλεια των δεδομένων.

Ο GDPR είναι μια νομοθεσία που επιχειρεί να προστατεύσει το απόρρητο και τα προσωπικά δεδομένα των πολιτών της Ευρωπαϊκής Ένωσης. Ισχύει για κάθε νομική οντότητα/φυσικό πρόσωπο που επεξεργάζεται προσωπικά δεδομένα ατόμων της ΕΕ, ανεξάρτητα από την τοποθεσία του. Επίσης καθορίζει πώς πρέπει τα προσωπικά δεδομένα να συλλέγονται, να υποβάλλονται σε επεξεργασία, να αποθηκεύονται και να προστατεύονται.

Τα Προσωπικά Ηλεκτρονικά Αρχεία Υγείας είναι ηλεκτρονικά αρχεία που περιέχουν το ιατρικό ιστορικό ενός ασθενούς (π.χ. ιατρικές συνταγές, γενικά αποτελέσματα διάφορων ιατρικών εξετάσεων mri, x-ray, αιματολογικές εξετάσεις και άλλα δεδομένα που σχετίζονται με την υγεία. Ο συνδυασμός αυτών των δύο στοχεύει στη βελτίωση της ποιότητας και της συνέχειας των υπηρεσιών, στην αύξηση της συμμετοχής των ασθενών και στην ενδυνάμωση των ανθρώπων να ελέγχουν τα δεδομένα που αφορούν την υγεία τους.

Όσον αφορά τις ομοιότητες, ο GDPR απαιτεί από τις επιχειρήσεις να λαμβάνουν τη ρητή συναίνεση των ατόμων πριν συλλέξουν, επεξεργαστούν ή αποκαλύψουν τα προσωπικά τους δεδομένα. Τα Προσωπικά Ηλεκτρονικά Αρχεία Υγείας, εν τω μεταξύ, περιλαμβάνουν ευαίσθητες πληροφορίες για την υγεία τους που θα πρέπει να διατηρούνται ασφαλείς και προσβάσιμες μόνο από εξουσιοδοτημένο προσωπικό και από τον ίδιο τον ασθενή.

Επιπλέον, ο GDPR και τα Προσωπικά Ηλεκτρονικά Αρχεία Υγείας προσπαθούν να εγγυηθούν ότι τα προσωπικά δεδομένα είναι ακριβή, ενημερωμένα και διατηρούνται με ασφάλεια. Παρέχουν επίσης στους ανθρώπους το δικαίωμα να βλέπουν, να τροποποιούν και να αφαιρούν ανακρίβειες αναφορικά με τα υφιστάμενα δεδομένα τους.

(Φερενίκη Παναγοπούλου – Κουτνατζή, «Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016/ΕΕ – Εισαγωγή και Προστασία Δικαιωμάτων», Αθήνα-Θεσσαλονίκη, Εκδόσεις Σάκκουλα, 2017)

(Μίνα Ζούλοβιτς, Εισήγηση στο 9 ο Πανελλήνιο Συνεδρίο της Ένωσης Ελλήνων Νομικών ΕΤΗΕΜΙS στα Ιωάννινα με θέμα «Προσωπικά Δεδομένα και Δικηγορία: Μία νέα πραγματικότητα – Ένα νέο κεφάλαιο στο νομικό κόσμο».)

Αναφορικά με άρθρο του 2019 το οποίο αναφέρει πόσο σημαντικό είναι η επίδραση του GDPR στον Ιατρικό Τομέα. Λόγω της μεγάλης και ταχύτατης εξέλιξης της ψηφιακής τεχνολογίας, ο GDPR φάνηκε αποτελεσματικός στο να αποτρέψει μία καταστροφική εξέλιξη σ΄ αυτήν τη ψηφιοποίηση. Ο Ιατρικός Τομέας αναγκάστηκε να κάνει σημαντικές δαπανηρές προσαρμογές για να συμμορφωθούν με αυτόν τον νέο κανονισμό που απαιτεί πολύ πιο αυστηρή προστασία για τα προσωπικά δεδομένα υγείας των ασθενών. Με αυτό αποδεικνύεται ότι οι προηγούμενες διασφαλίσεις για τα προσωπικά δεδομένα υγείας των ατόμων ήταν αρκετά ανεπαρκείς. (Yuan, B., & Li, J. (2019). The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation. International Journal of Environmental Research and Public Health, 16(6). https://doi.org/10.3390/IJERPH16061070)

Με βάση το άρθρο του Privacy Perfect τον Μάιο 2020, καταλήγει στο ότι όλοι όσοι εργάζονται στο τομέα της υγείας αναγκάζονται να συμμορφωθούν μαζί με τον κανονισμό GDPR και επιτέλους να επενδύσουν χρόνο,

χρήμα και να δώσουν προτεραιότητα στην ασφάλεια των προσωπικών δεδομένων των πελατών τους παραμένοντας έτσι προς το κοινό συμφέρον και των δύο μελών. Εάν πραγματικά οι επιχειρήσεις συμμορφωθούν μαζί με την νομοθεσία του, όχι μόνο θα μειωθούν οι ψηφιακές παραβιάσεις των προσωπικών δεδομένων των πελατών τους αλλά θα αυξηθεί και η εμπιστοσύνη τους προς τον οργανισμό, δημιουργώντας έτσι καλή φήμη, καλύτερη ομαλή μεταχείριση πελατών και παράλληλα αποφυγή μεγάλων προστιμάτων. (Healthcare institutions and GDPR compliance in a digital world. (2020). https://blog.privacyperfect.com/the-privacyperfect-blog/healthcare-institutions_gdpr-compliance-in-a-digital-world)

Επιπρόσθετα όλα τα ιδρύματα υγειονομικής περίθαλψης που δεν έδιναν την κατάλληλη προσοχή στο πώς αποθηκεύουν και διατηρούν τα προσωπικά δεδομένα των ασθενών τους, τώρα μέσω του GDPR θα πρέπει εστιάσουν την προσοχή τους και να δώσουν προτεραιότητα σε αυτά εφόσον είναι υποχρεωμένοι να συμμορφωθούν με αυτόν. Όπως προαναφέραμε προηγουμένως λόγω της πολυπλοκότητας του GDPR, θα ήταν καλό όλες οι επιχειρήσεις να ζητήσουν τη βοήθεια ειδικού για να διασφαλιστεί η σωστότερη επεξεργασία των προσωπικών δεδομένων σύμφωνα με τον GDPR, αποφεύγοντας επομένως την πιθανότητα επιβολής προστίμων για παραβιάσεις του GDPR ειδικά σε ειδικά συγκεκριμένες κατηγορίες όπως είναι τα δεδομένα υγείας ενός ασθενή. (Briefings, How does the GDPR affect the medical industry?, N. Pirilides & Associates LLC. (2020). https://www.pirilides.com/en/briefings/how-does-the-gdpr-affect-the-medical-industry/ppp-101/57/)

ΕΠΙΛΟΓΟΣ

Καταληκτικά, μπορούμε να πούμε πως σιγά σιγά θα συνεχίσει η ψηφιοποίηση των δεδομένων να εφαρμόζεται στον τομέα της Υγείας για την καλύτερη αντιμετώπιση διάφορων προβλημάτων που έχουμε τώρα αλλά και για καλύτερη οργάνωση και διευκόλυνση ολονών μας. Αυτό δεν θα παραμείνει μόνο στον τομέα της Ιατρικής αλλά σταδιακά εφαρμόζεται και σε άλλους τομείς όπως είναι σε τραπεζικά ιδρύματα, νομικές οντότητες, επιχειρήσεις, φυσικά πρόσωπα χωρίς να παίζει σημασία εάν είσαι μικρός ή μεγάλος, σημαντικός ή ασήμαντος, εκείνο που έχει σημασία είναι ότι εάν διαχειρίζεται κάποιος προσωπικά δεδομένα τότε θα πρέπει να αναλογίζεται τον κίνδυνο και τις συνέπειες που φέρουν μαζί αυτή η διαχείριση.

Το καλύτερο πράγμα που μπορούμε εμείς σαν πολίτες αλλά και σαν άτομα είναι να προσπαθήσουμε να προσαρμοστούμε το συντομότερο δυνατό στις καινούργιες αλλαγές, να αξιοποιήσουμε την διευκόλυνση και την πολυτέλεια της τεχνολογίας στο έπακρο αλλά ταυτόχρονα να είμαστε σε ετοιμότητα και προσεκτικοί στις συναλλαγές και που δίνουμε το δικαίωμα και σε ποιον να διαχειρίζεται τα δικά μας προσωπικά στοιχεία. Γνωρίζουμε καλά ότι η τεχνολογία εάν χρησιμοποιείται σωστά, φέρει μόνο καλά αλλά εάν χρησιμοποιείται με ανορθόδοξο τρόπο, τότε μπορεί να φέρει την καταστροφή. (Effie. (2020). Ιατρικός ηλεκτρονικός φάκελος υγείας και προστασία των προσωπικών δεδομένων Νομική και κοινωνιολογική προσέγγιση. www.mednet.gr/archives)

ΒΙΒΛΙΟΓΡΑΦΙΑ

Effie. (2020). Ιατρικός ηλεκτρονικός φάκελος υγείας και προστασία των προσωπικών δεδομένων Νομική και κοινωνιολογική προσέγγιση. www.mednet.gr/archives

Briefings, How does the GDPR affect the medical industry?, N. Pirilides & Associates LLC. (2020). https://www.pirilides.com/en/briefings/how-does-the-gdpr-affect-the-medical-industry/ppp-101/57/

Gonçalves-Ferreira, D., Sousa, M., Bacelar-Silva, G. M., Frade, S., Antunes, L. F., Beale, T., & Cruz-Correia, R. (2019). OpenEHR and General Data Protection Regulation: Evaluation of Principles and Requirements. JMIR Medical Informatics, 7(1), e9845. https://doi.org/10.2196/medinform.9845

Annas, G. J. (2003). HIPAA Regulations: A New Era of Medical-Record Privacy? HIPAA Regulations: A New Era of Medical-Record Privacy? Part of the Health Law and Policy Commons. https://scholarship.law.bu.edu/faculty_scholarship

Rennie Stuart. (2019). ARMA-Magazine-2019-02-ARMA-QA_-GDPR-Regulations-and-Electronic-Records (1).

Kumar, M., Raj, H., Chaurasia, N., & Gill, S. S. (2023). Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0. Internet of Things and Cyber-Physical Systems, 3, 309–322. https://doi.org/10.1016/j.iotcps.2023.05.006

Marlene Maheu. (2021). EMR & EHR: What Are the Important Differences that You Need to Know? https://telehealth.org/emr/

Parul Saini, W. T. (2021). EMR vs EHR - Difference between EMR and EHR. https://webmedy.com/blog/emr-and-ehr-difference/

10 Advantages and Disadvantages of EHR [EHR vs EMR Differences] | PostDICOM. (n.d.). Retrieved November 11, 2023, from https://www.postdicom.com/en/blog/advantages-and-disadvantages-of-ehr

Max Freedman. (2023). EMR vs. EHR: What's the Difference. https://www.businessnewsdaily.com/16204-emr-vs-ehr-explained.html

Apkon, M., & Singhaviranon, P. (2001). Impact of an electronic information system on physician workflow and data collection in the intensive care unit. Intensive Care Medicine, 27(1), 122–130. https://doi.org/10.1007/s001340000777

Kumar, M., Raj, H., Chaurasia, N., & Gill, S. S. (2023). Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0. Internet of Things and Cyber-Physical Systems, 3, 309–322. https://doi.org/10.1016/J.IOTCPS.2023.05.006

Franklin. (2018). GDPR subject access request (SAR) - 6 steps to deal with it. https://cybersmart.co.uk/blog/6-steps-to-deal-with-a-gdpr-subject-access-request-sar/

International Network Of Privacy Law Professionals. (2018). A brief history of data protection: How did it all start? | International Network of Privacy Law Professionals. https://inplp.com/latest-news/article/a-brief-history-of-data-protection-how-did-it-all-start/

The History of the General Data Protection Regulation | European Data Protection Supervisor. (n.d.). Retrieved November 8, 2023, from https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Chapter 1 – General provisions - General Data Protection Regulation (GDPR). (n.d.). Retrieved November 8, 2023, from https://gdpr-info.eu/chapter-1/

Wheel | Advantages and Disadvantages of EHRs. (2020). https://www.wheel.com/companies-blog/advantages-and-disadvantages-of-ehrs

General Data Protection Regulation (GDPR) – Official Legal Text. (n.d.). Retrieved November 1, 2023, from https://gdpr-info.eu/

ΠΑΓΚΥΠΡΙΟΣ ΔΙΚΗΓΟΡΙΚΟΣ ΣΥΛΛΟΓΟΣ. (n.d.). Ο περί Ηλεκτρονικής Υγείας Νόμος του 2019 - 59(I)/2019 - 19 - Δημιουργία και περιεχόμενο Ηλεκτρονικού Φακέλου Υγείας. 2019. Retrieved November 1, 2023, from https://www.cylaw.org/nomoi/enop/ind/2019_1_59/section-sccf5906ad-f094-4bdd-bf4b-d91d7caf4436.html

Στέλιου Στυλιανού. (2019). Θα βλέπουμε τα ιατρικά μας δεδομένα με ένα κλικ - Τα δεδομένα | Offsite. https://www.offsite.com.cy/eidiseis/topika/tha-blepoyme-ta-iatrika-mas-dedomena-me-ena-klik-ta-dedomena

Lab Ground. (2021). GDPR DPO, Controller, Processor and Other Roles | Ground Labs. https://www.groundlabs.com/blog/gdpr-responsibility/

Burgess Matt. (2020). What is GDPR? The summary guide to GDPR compliance in the UK | WIRED UK. https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

Κυπριακή, & Δημοκρατία. (2019). ΕΠΙΣΗΜΗ ΕΦΗΜΕΡΙΔΑ ΤΗΣ ΚΥΠΡΙΑΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ ΠΑΡΑΡΤΗΜΑ ΠΡΩΤΟ ΝΟΜΟΘΕΣΙΑ-ΜΕΡΟΣ Ι. https://www.mof.gov.cy/mof/gpo/gazette.nsf/C9CDC1A32095E496C225872C004069B5/$file/4699%2019%204%202019%20PARARTHMA%201o%20MEROS%20I.pdf

Raghupathi, W., & Raghupathi, V. (2014). Big data analytics in healthcare: promise and potential. Health Information Science and Systems, 2(1), 3. https://doi.org/10.1186/2047-2501-2-3

Viceconti, M., Hunter, P., & Hose, R. (2015). Big data, big knowledge: big data for personalized healthcare. IEEE Journal of Biomedical and Health Informatics, 19(4), 1209–1215. https://doi.org/10.1109/JBHI.2015.2406883

Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Ullah Khan, S. (2015). big data" on cloud computing: Review and open research issues. Information Systems, 47, 98–115. https://doi.org/10.1016/j.is.2014.07.006

Cappa, F., Oriani, R., Peruffo, E., & McCarthy, I. (2021). Big Data for Creating and Capturing Value in the Digitalized Environment: Unpacking the Effects of Volume, Variety, and Veracity on Firm Performance*. Journal of Product Innovation Management, 38(1), 49–67. https://doi.org/10.1111/jpim.12545

Kumar, M., Raj, H., Chaurasia, N., & Gill, S. S. (2023). Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0. Internet of Things and Cyber-Physical Systems, 3, 309–322. https://doi.org/10.1016/J.IOTCPS.2023.05.006

Μπότσης, Τ.-Χ. (2005). Ηλεκτρονικός ιατρικός φάκελος ασθενή. https://el.wikipedia.org/wiki/%CE%97%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CF%8C%CF%82_%CE%B9%CE%B1%CF%84%CF%81%CE%B9%CE%BA%CF%8C%CF%82_%CF%86%CE%AC%CE%BA%CE%B5%CE%BB%CE%BF%CF%82_%CE%B1%CF%83%CE%B8%CE%B5%CE%BD%CE%AE

Burgess, M. (n.d.). Help, my lightbulbs are dead! How GDPR became bigger than Beyonce. Wired.Co.Uk. from https://www.wired.co.uk/article/happy-gdpr-day-gdpr-hall-of-shame

Stallman, R. (2018). A radical proposal to keep your personal data safe. The Guardian. https://www.theguardian.com/commentisfree/2018/apr/03/facebook-abusing-data-law-privacy-big-tech-surveillance

Kalyanpur, N., & Newman, A. (2018). Today, a new E.U. law transforms privacy rights for everyone. Without Edward Snowden, it might never have happened. The Washington Post. https://www.washingtonpost.com/news/monkey-cage/wp/2018/05/25/today-a-new-eu-law-transforms-privacy-rights-for-everyone-without-edward-snowden-it-might-never-have-happened/?

Tiku, N. (2018). Europe's new privacy law will change the web, and more. Wired. https://www.wired.com/story/europes-new-privacy-law-will-change-the-web-and-more/

Jaffe, J., & Hautala, L. (2018). What the GDPR means for Facebook, the EU and you. CNET. https://www.cnet.com/how-to/what-gdpr-means-for-facebook-google-the-eu-us-and-you/

Butterworth, T. (2018). Europe's tough new digital privacy law should be a model for US policymakers. Vox. https://www.vox.com/the-big-idea/2018/3/26/17164022/gdpr-europe-privacy-rules-facebook-data-protection-eu-cambridge

Sample, I. (2017). AI watchdog needed to regulate automated decision-making, say experts. The Guardian. https://www.theguardian.com/technology/2017/jan/27/ai-artificial-intelligence-watchdog-needed-to-prevent-discriminatory-automated-decisions

Edwards, E. (2018). New rules on data protection pose compliance issues for firms. The Irish Times. https://www.irishtimes.com/business/technology/new-rules-on-data-protection-pose-compliance-issues-for-firms-1.3397742

Jeong, S. (2018). No one's ready for GDPR. The Verge. https://www.theverge.com/2018/5/22/17378688/gdpr-general-data-protection-regulation-eu

Solon, O. (2018). How Europe's "breakthrough" privacy law takes on Facebook and Google. The Guardian. https://www.theguardian.com/technology/2018/apr/19/gdpr-facebook-google-amazon-data-privacy-regulation

Hasselgren, A., Wan, P. K., Horn, M., Kralevska, K., Gligoroski, D., & Faxvaag, A. (2020). GDPR Compliance for Blockchain Applications in Healthcare. http://arxiv.org/abs/2009.12913

Your Europe. (2022). GDPR | Προσωπικά δεδομένα & ΓΚΠΔ - Your Europe. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm

Kamleitner, B., & Mitchell, V. (2019). Your Data Is My Data: A Framework for Addressing Interdependent Privacy Infringements. Journal of Public Policy & Marketing, 38(4), 433–450. https://doi.org/10.1177/0743915619858924

Summary of the GDPR's 10 key requirements - IT Governance Blog En. (n.d.) from https://www.itgovernance.eu/blog/en/summary-of-the-gdprs-10-key-requirements

The History of the General Data Protection Regulation | European Data Protection Supervisor. (n.d.). from https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Summary of the GDPR's 10 key requirements - IT Governance Blog En. (n.d.), from https://www.itgovernance.eu/blog/en/summary-of-the-gdprs-10-key-requirements

Legislation | European Data Protection Supervisor. (n.d.). from https://edps.europa.eu/data-protection/data-protection/legislation_en

Veale, M., Binns, R., & Ausloos, J. (2018). When data protection by design and data subject rights clash. International Data Privacy Law, 8(2), 105–123. https://doi.org/10.1093/idpl/ipy002

Zuiderveen Borgesius, F. J. (2016). Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation. Computer Law & Security Review, 32(2), 256–271. https://doi.org/10.1016/j.clsr.2015.12.013

Alizadeh, F., Jakobi, T., Boldt, J., & Stevens, G. (2019). Proceedings of Mensch und Computer 2019. In ACM International Conference Proceeding Series. ACM Press. https://doi.org/10.1145/3340764.3344913

Breaches up 54% this year - Millgate Ltd. (n.d.). Retrieved October 26, 2023, from https://millgate.co.uk/learn/breaches-up-50-this-year/

GDPR DPO, Controller, Processor and Other Roles | Ground Labs. (n.d.). from https://www.groundlabs.com/blog/gdpr-responsibility/

GDPR Greece - Τι είναι το GDPR και πως επηρεάζει τις επιχειρήσεις; (n.d.). from https://www.gdprgreece.com/article/5/gdpr

What are 8 Data Subject rights according to the GDPR – Data Privacy Manager. (2022). https://dataprivacymanager.net/what-are-data-subject-rights-according-to-the-gdpr/

Yuan, B., & Li, J. (2019). The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation. International Journal of Environmental Research and Public Health, 16(6). https://doi.org/10.3390/IJERPH16061070
Briefings, How does the GDPR affect the medical industry?, N. Pirilides & Associates LLC. (2020). https://www.pirilides.com/en/briefings/how-does-the-gdpr-affect-the-medical-industry/ppp-101/57/

Healthcare institutions and GDPR compliance in a digital world. (2020). https://blog.privacyperfect.com/the-privacyperfect-blog/healthcare-institutions_gdpr-compliance-in-a-digital-world