ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΙΑΤΡΙΚΗ ΣΧΟΛΗ
Β΄ ΨΥΧΙΑΤΡΙΚΗ ΚΛΙΝΙΚΗ
ΔΙΕΥΘΥΝΤΗΣ: ΚΑΘΗΓΗΤΗΣ Α. ΔΟΥΖΕΝΗΣ
ΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΑΤΤΙΚΟΝ

ΠΜΣ «ΨΥΧΙΑΤΡΟΔΙΚΑΣΤΙΚΗ»
ΔΙΕΥΘ. ΣΠΟΥΔΩΝ: ΚΑΘΗΓΗΤΗΣ Α. ΔΟΥΖΕΝΗΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ερμηνεία και συμμόρφωση των επαγγελματιών ψυχικής υγείας προς τον GDPR (Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων)

ΜΑΡΙΑ ΧΟΝΔΡΟΝΑΣΙΟΥ

Επιβλέπων Καθηγητής:
Αθανάσιος Δουζένης,
Καθηγητής Ψυχιατρικής
Β΄ Ψυχιατρική Κλινική ΕΚΠΑ

ΑΘΗΝΑ
Οκτώβριος 2019

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ερμηνεία και συμμόρφωση των επαγγελματιών ψυχικής υγείας προς τον GDPR (Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων)

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: Αθανάσιος Δουζένης,
Καθηγητής Ψυχιατρικής, Β΄ Ψυχιατρική Κλινική ΕΚΠΑ

Υπογραφή:

ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ:

1. **Ιωάννης Μιχόπουλος**,
Αναπληρωτής Καθηγητής Ψυχιατρικής, Β΄ Ψυχιατρική Κλινική ΕΚΠΑ

Υπογραφή:

2. **Χαρά Σπηλιοπούλου,**
Καθηγήτρια Ιατροδικαστικής και Τοξικολογίας Ιατρικής Σχολής ΕΚΠΑ

Υπογραφή:

Ημερομηνία εξέτασης:

Χαρακτηρισμός / Βαθμός:

Η συγγραφέας βεβαιώνει ότι το περιεχόμενο του παρόντος έργου είναι αποτέλεσμα προσωπικής εργασίας και ότι έχει γίνει η κατάλληλη αναφορά στην εργασία τρίτων, όπου κάτι τέτοιο ήταν απαραίτητο, σύμφωνα με τους κανόνες της ακαδημαϊκής δεοντολογίας.

Ευχαριστίες

Η ολοκλήρωση της παρούσας διπλωματικής εργασίας είναι αποτέλεσμα μιας προσπάθειας στην οποία συνέβαλαν καθοριστικά οι άνθρωποι που ήταν δίπλα μου και στους οποίους οφείλω ένα μεγάλο ευχαριστώ.

Αρχικά, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου και Διευθυντή του Προγράμματος Μεταπτυχιακών Σπουδών της «Ψυχιατροδικαστικής», Καθηγητή Ψυχιατρικής, κ. Αθανάσιο Δουζένη που μου έδωσε την ευκαιρία να διευρύνω τους ορίζοντές μου, γνωστικούς και εμπειρικούς, σε ένα νέο, συναρπαστικό επιστημονικό πεδίο.

Ευχαριστώ θερμά τον κ. Ιωάννη Μιχόπουλο, Αναπληρωτή Καθηγητή του Πανεπιστημίου, για τις πολύτιμες συμβουλές, την καθοδήγηση και την εμπιστοσύνη που μου έδειξε, καθώς και την κ. Χαρά Σπηλιοπούλου, Καθηγήτρια Ιατροδικαστικής και Τοξικολογίας, που δέχτηκε να συμμετέχει στην τριμελή επιτροπή εξέτασης της εργασίας μου.

Ευχαριστώ τον κ. Εμμανουήλ Λασκαρίδη και τον κ. Στέφανο Τοπάλη, διότι η επαγγελματική μας συνεργασία και η εμπειρία που μου έδωσαν ήταν το κίνητρο για την εκπόνηση της παρούσας μελέτης· τις συνοδοιπόρους μου σε αυτό το ταξίδι, Θεοδώρα Κανδρή, Ελπίδα Σπυρίδωνος και Ξανθή Ανυφαντή, που με αγάπη και ενθουσιώδες ενδιαφέρον στήριξαν την προσπάθειά μου μέχρι τέλους.

Το μεγαλύτερο ευχαριστώ το οφείλω στους γονείς μου, Νίκο και Χάιδω, και στην αδερφή μου, Άσπα, που ήταν και είναι δίπλα μου σε κάθε μου εγχείρημα, δίνοντάς μου φτερά για να πετάω όλο και ψηλότερα.

Πίνακας περιεχομένων

Περίληψη

Η παρούσα διπλωματική εργασία έχει ως στόχο τη μελέτη του βαθμού ενημέρωσης και του επιπέδου συμμόρφωσης με τον Γενικό Κανονισμό Προστασίας Προσωπικών δεδομένων (GDPR) των επαγγελματιών ψυχικής υγείας συγκριτικά με τους επαγγελματίες της νομικής επιστήμης. Επιχειρείται μια ενδεικτική αναφορά στις σημαντικότερες καινοτομίες του Κανονισμού με ιδιαίτερη έμφαση στην ασφάλεια της επεξεργασίας προσωπικών δεδομένων και η ανάδειξη των σημείων σύγκλισης και διαφοροποίησης της συμμόρφωσης μεταξύ ψυχιάτρων/ψυχολόγων και δικηγόρων. Συνολικά 136 άτομα ηλικίας 24-65 ετών (Μ.Ο = 36,80, Τ.Α= 9,46) από τον γενικό πληθυσμό της Ελλάδος και από τα οποία τα 53 άτομα ήταν επαγγελματίες ψυχικής υγείας και τα υπόλοιπα 83 άτομα ήταν δικηγόροι συμμετείχαν στην έρευνα με την μέθοδο της διαθεσιμότητας. Χρησιμοποιήθηκε το αυτοσυμπληρούμενο Ερωτηματολόγιο Συμμόρφωσης με τον Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR Compliance) το οποίο εξετάζει τον βαθμό συμμόρφωσης των συμμετεχόντων με τις επιταγές του κανονισμού σε ζητήματα προστασίας προσωπικών δεδομένων. Η ανάλυση έδειξε μια στατιστικά σημαντική θετική συσχέτιση μεταξύ της ενημέρωσης/γνώσης του κανονισμού προστασίας προσωπικών δεδομένων και της λήψη τεχνικών και οργανωτικών μέτρων ($p<0,001$). Επίσης, φάνηκε ότι οι επαγγελματίες ψυχικής υγείας λαμβάνουν περισσότερα τεχνικά και οργανωτικά μέτρα συγκριτικά με τους δικηγόρους ($p=0,003$) ενώ δεν παρατηρήθηκε στατιστικά σημαντική διαφορά ανάμεσα στις δύο ομάδες όσον αφορά την ενημέρωση/γνώση του κανονισμού προστασίας προσωπικών δεδομένων ($p=0,255$). Τα ευρήματα μας είναι σημαντικά καθώς αποτελούν τη βάση για την διεξαγωγή περαιτέρω έρευνας στην Ελλάδα με σκοπό την καλύτερη κατανόηση και συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Προσωπικών δεδομένων και άλλων επαγγελματικών πεδίων.

Λέξεις κλειδιά: Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, Δεδομένα υγείας, Δεδομένα ειδικής κατηγορίας, Επαγγελματίες ψυχικής υγείας, Δικηγόροι

Abstract

The purpose of this thesis is to study the level of information and the level of compliance with the General Data Protection Regulation (GDPR) of mental health professionals compared to legal professionals. An indicative reference is made to the most important innovations of the Regulation, with particular emphasis on the security of the processing of personal data and the emergence of points of convergence and differentiation of compliance between psychiatrists / psychologists and lawyers. A total number of 136 individuals with an age range between 24-65 years (mean age = 36.80, SD= 9.46) from the general population of Greece and from whom, 53 participants were mental health professionals and 83 participants were lawyers participated in the study through the method of availability sampling. The GDPR Compliance self-reported questionnaire was used which examines the degree of compliance of participants with the General Data Protection Regulation.The analysis reported a statistically significant positive relationship between the acknowledgment/information of the General Data Protection Regulation and the implementation of technical and organizational measures ($p<.001$). Moreover, Mann-Whitney U tests showed that mental health professionals were engaged in the implementation of technical and organizational measures to a greater extent when compared to lawyers ($p=.003$) whereas, a non significant difference between the two groups was observed regarding the acknowledgment/information of the General Data Protection Regulation ($p=.255$). Our findings are important since they constitute the basis for further research to be conducted into the cultural context of Greece in order to better understand and comply with the General Data Protection Regulation and other professional fields.

Keywords: General Data Protection Regulation (GDPR), Health Data, Special Category Data, Mental Health Professionals, Lawyers

1. Πρόλογος

Η παρούσα μελέτη επιδιώκει να διερευνήσει, αφενός το επίπεδο ενημέρωσης των επαγγελματιών των αντίστοιχων ειδικοτήτων αναφορικά με τις αρχές που διέπουν το δίκαιο προστασίας προσωπικών δεδομένων, ειδικότερα από την εφαρμογή του Ευρωπαϊκού Κανονισμού (ΕΕ) 679/2016 και έπειτα, και αφετέρου το βαθμό συμμόρφωσής τους στις απαιτήσεις του νέου νομοθετικού πλαισίου. Αρχικά, επιχειρείται μια σύντομη ιστορική αναδρομή στη νομοθεσία σχετικά με την προστασία των προσωπικών δεδομένων. Στη συνέχεια παρατίθεται το εννοιολογικό πλαίσιο των όρων «προσωπικά δεδομένα» και «προσωπικά δεδομένα υγείας».

Ακολούθως, εντοπίζονται οι συγκλίσεις και αποκλίσεις ανάμεσα στις δεσμεύσεις που πηγάζουν από την υποχρέωση τήρησης του επαγγελματικού απορρήτου και την υποχρέωση συμμόρφωσης με το δίκαιο προστασίας προσωπικών δεδομένων. Κατόπιν, αφού διευκρινίζονται ζητήματα σχετικά με τον χαρακτηρισμό ενός επαγγελματία ως υπεύθυνο επεξεργασίας καθώς και οι προϋποθέσεις νομιμότητας της επεξεργασίας προσωπικών δεδομένων, γίνεται αναφορά στις βασικές καινοτομίες που εισάγονται με το νέο νομοθετικό καθεστώς και ορίζεται ο σκοπός και η μεθοδολογία της παρούσας μελέτης. Ακολουθεί η περιγραφική ανάλυση και ο έλεγχος των ερευνητικών υποθέσεων που έχουμε θέσει. Κλείνοντας, παραθέτουμε επεξηγήσεις σχετικά με τα ευρήματα της έρευνάς μας, τους περιορισμούς που συναντήσαμε καθώς επίσης και μελλοντικές προτάσεις για περαιτέρω έρευνα.

1.1 Εισαγωγή

Οι σύγχρονες τεχνολογικές εξελίξεις έχουν δημιουργήσει μια τεράστια αύξηση της παραγωγής, της χρήσης και της πρόσβασης στην πληροφορία. Από την Οδηγία του 1995 (95/46/ΕΚ) μέχρι σήμερα έχουμε μεταβεί σε μια νέα τεχνολογική εποχή. Τότε, μόνο το 1% του παγκόσμιου πληθυσμού χρησιμοποιούσε το διαδίκτυο. Σήμερα, η υπολογιστική νέφους, τα κοινωνικά δίκτυα και οι «έξυπνες συσκευές» είναι στην καθημερινότητά μας, ενώ την ίδια στιγμή η συντριπτική πλειοψηφία των πληροφοριών παράγεται και επεξεργάζεται ηλεκτρονικά (Tankard, 2016).

Καθώς ο όγκος και η επεξεργασία της πληροφορίας αυξάνεται, το κόστος της επεξεργασίας της μειώνεται σε συνδυασμό με νέες πηγές άντλησης πληροφορίας (αισθητήρες, κάμερες, πληροφορίες γεωεντοπισμού) και νέες τεχνολογικές πλατφόρμες, όπως η διάχυτη υπολογιστική (ubiquitous computing), το Διαδίκτυο των Πραγμάτων (Internet of Things), το υπολογιστικό νέφος (cloud computing) κλπ. Ειδικότερα στον τομέα της υγείας, οι νέες τεχνολογίες e-health εφαρμόζονται στο μεγαλύτερο μέρος των λειτουργιών που αφορούν την υγειονομική περίθαλψη (ηλεκτρονική συνταγογράφηση, τηλεϊατρική, ηλεκτρονικός ιατρικός φάκελος). Σημειώνεται επίσης ραγδαία αύξηση των ιατρικών δεδομένων υπό την επίδραση των τεχνολογικών εξελίξεων και του αντίστοιχου αναπροσανατολισμού της παροχής υπηρεσιών υγείας και της έρευνας.

Η ταχύτατη επέκταση των νέων αυτών τεχνολογιών, η ανάπτυξη της οικονομικής δραστηριότητας, η διασυνοριακή διαβίβαση προσωπικών δεδομένων καθώς και η τάση για ενίσχυση της δημόσιας ασφαλείας, καθιστούν επιτακτική την ασφαλή επεξεργασία και προστασία των προσωπικών δεδομένων στην Ελλάδα (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, 2019).

Απέναντι σε αυτή την εξελισσόμενη κατάσταση, η Ευρωπαϊκή Ένωση (;ΕΕ) θέσπισε τον νέο Γενικό Κανονισμό για την προστασία των προσωπικών δεδομένων, του οποίου η εφαρμογή αναμένεται να συμβάλει μεταξύ άλλων στην προώθηση των εφαρμογών ηλεκτρονικής υγείας και στην άρση των εμποδίων για την ποιοτικότερη διασυνοριακή υγειονομική περίθαλψη.

Ο Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων

προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός Προστασίας Δεδομένων ;ΓΚΠΔ / General Data Protection Regulation ;GDPR) τέθηκε σε εφαρμογή το 2018. Από την εφαρμογή του, εγκαθιδρύεται ένα νέο νομοθετικό καθεστώς που καταργεί το προϊσχύσαν, ενώ παραμένουν σε ισχύ οι διατάξεις της Οδηγίας (2002/58/ΕΚ) σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.

Ειδικότερα για τα δεδομένα υγείας, ο Κώδικας Ιατρικής Δεοντολογίας (ΚΙΔ ; Ν. 3418/2005), και συγκεκριμένα οι διατάξεις του περί ιατρικού απορρήτου και τήρησης ιατρικού αρχείου (άρθρα 13 και 14) εφαρμόζεται συμπληρωματικά στο εκάστοτε ισχύον νομοθετικό πλαίσιο, καθώς προβλέπει ειδικότερες υποχρεώσεις για τους επαγγελματίες υγείας και τους βοηθούς τους. Αντίστοιχα, το ίδιο ισχύει και για τον Κώδικα Δεοντολογίας Δικηγορικού Λειτουργήματος.

Παρόλο που ο ΓΚΠΔ αναμένεται να ωφελήσει οργανισμούς και επιχειρήσεις, παρέχοντας ενιαία δομή και οργάνωση στις δραστηριότητες και στις υποχρεώσεις προστασίας των δεδομένων και επιτρέποντας πιο ολοκληρωμένες πολιτικές προστασίας δεδομένων σε επίπεδο ΕΕ, παράλληλα δημιουργεί νέες προκλήσεις. Η εφαρμογή των απαιτήσεων του ΓΚΠΔ απαιτεί σημαντικούς οικονομικούς και ανθρώπινους πόρους, καθώς και εκπαίδευση των εργαζομένων (Tikkinen - Piri, Rohunen & Markkula, 2018).

1.2 Σύντομη ιστορική αναδρομή

Η προστασία της ιδιωτικότητας αποτελεί ένα από τα θεμελιώδη ανθρώπινα δικαιώματα στο δυτικό κόσμο και πλαισιώνεται από νομοθετικά κείμενα τα οποία προσαρμόζονται και επικαιροποιούνται διαρκώς ώστε να ανταποκρίνονται στις ανάγκες προστασίας των υποκειμένων που γεννούν οι τεχνολογικές εξελίξεις. Ήδη από το 1953, η Ευρωπαϊκή Σύμβαση για την Προστασία των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών (ΕΣΔΑ) στο άρθρο 8 περιλαμβάνει το σεβασμό της ιδιωτικής και οικογενειακής ζωής ως ένα από τα θεμελιώδη δικαιώματα, χωρίς όμως να αναφέρεται ειδικότερα στην προστασία των προσωπικών δεδομένων, η οποία αποτελεί ειδικότερη έκφανση αυτού.

Η ελληνική νομοθεσία για την προστασία των προσωπικών δεδομένων διαμορφώθηκε κυρίως μέσα από την υποχρέωση προσαρμογής στην ευρωπαϊκή νομοθεσία. Ειδικότερα, ενώ χώρες όπως η Γερμανία, η Αυστρία, η Γαλλία και οι σκανδιναβικές χώρες είχαν ήδη από τη δεκαετία του ‘70 εισάγει σχετικές ρυθμίσεις στο εθνικό τους δίκαιο, η πρώτη φορά που διατυπώθηκε η αναγκαιότητα της δημιουργίας ενός σχετικού νομοθετικού πλαισίου στην Ελλάδα ήταν το 1983. Ομάδα εργασίας με επικεφαλής τον Αντιπρόεδρο του ΣτΕ Μ. Χαλαζωνίτη αναλαμβάνει τη σύνταξη προσχεδίου νόμου για την προστασία του απορρήτου της ιδιωτικής ζωής από τη χρήση ηλεκτρονικών υπολογιστών, το οποίο διέκρινε τα προσωπικά δεδομένα σε απλές προσωπικές, εμπιστευτικές και αυστηρώς εμπιστευτικές πληροφορίες. Για τις πληροφορίες της δεύτερης κατηγορίας η επεξεργασία επιτρεπόταν υπό αυστηρές προϋποθέσεις, ενώ για αυτές της τρίτης κατηγορίας απαγορευόταν οποιαδήποτε μορφή επεξεργασίας. Η αυστηρότητα με την οποία αντιμετωπίζονταν τα δεδομένα της τελευταίας κατηγορίας οφειλόταν στο γεγονός ότι μεταξύ άλλων αφορούσε πληροφορίες σχετικά με τις πολιτικές και φιλοσοφικές πεποιθήσεις του ατόμου σε μια χρονική περίοδο που οι μνήμες από τη δικτατορία ήταν ακόμη νωπές.

Από το 1989 έως το 1992 ακολούθησε σειρά σχεδίων νόμου, κανένα εκ των οποίων δε συζητήθηκε, καθιστώντας κάθε προσπάθεια θέσπισης νομοθετικού πλαισίου ατελέσφορη. Αξίζει να σημειωθεί ότι κοινό χαρακτηριστικό όλων αυτών των προσπαθειών ήταν το γεγονός ότι δεν ανταποκρίνονταν στις ανάγκες της εποχής, μιας εποχής ταχύτατων τεχνολογικών εξελίξεων. Παράλληλα, σε ευρωπαϊκό επίπεδο, ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) ήδη από το 1980

είχε θεσπίσει Κατευθυντήριες γραμμές για τη διασυνοριακή ροή των προσωπικών δεδομένων και την προστασία της ιδιωτικής ζωής. Το 1992 ενσωματώνεται στο ελληνικό δίκαιο (Ν. 2068/1992), το πρώτο διεθνές νομικά δεσμευτικό κείμενο σχετικά με την προστασία προσωπικών δεδομένων, η Σύμβαση του Συμβουλίου της Ευρώπης (108/1981) για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα.

Το 1997 ήρθε ο νόμος (Ν. 2472/1997) για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ο οποίος ενσωμάτωσε την Οδηγία (95/46/ΕΚ) που εισάγει ενιαίες απαιτήσεις από τα κράτη μέλη της Ευρωπαϊκής Ένωσης και ασκεί επίδραση στην κανονιστική εξέλιξη διεθνώς.

Ωστόσο, θεμελιώδους σημασίας για προστασία των ευαίσθητων προσωπικών δεδομένων ήταν η αναθεώρηση του Συντάγματος (2001) και ειδικότερα η εισαγωγή της διάταξης 9Α. Στη συγκεκριμένη διάταξη κατοχυρώνεται ρητά από το Σύνταγμα η προστασία των προσωπικών δεδομένων ως ατομικό δικαίωμα (δικαίωμα πληροφοριακού αυτοκαθορισμού) και ανατίθεται η διασφάλισή του σε ανεξάρτητη αρχή. Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) είχε ήδη συσταθεί με παλαιότερο νόμο (Ν. 2472/1997) και πλέον κατοχυρώθηκε και συνταγματικά. Το 2006 έρχεται ο νόμος (Ν. 3471/2006) για την προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.

Από το 2009 η Ευρωπαϊκή Επιτροπή είχε αρχίσει να εξετάζει εκ νέου το υπάρχον νομικό πλαίσιο για την προστασία των δεδομένων στην Ευρωπαϊκή Ένωση, ξεκινώντας μια σειρά διαβουλεύσεων. Έλαβε συνολικά 288 προτάσεις - διαβουλεύσεις από διάφορους δημόσιους και ιδιωτικούς φορείς, ακόμα και από ιδιώτες. Κοινός παρονομαστής όλων ήταν η ανάγκη ενημέρωσης και προσαρμογής της ισχύουσας νομοθεσίας για την προστασία των προσωπικών δεδομένων των κατοίκων της Ευρωπαϊκής Ένωσης, προκειμένου να ανταποκρίνεται στη σύγχρονη τεχνολογική ανάπτυξη και την παγκοσμιοποίηση. Ακολούθησαν σχετικές διαπραγματεύσεις μεταξύ των κρατών μελών και των αντίστοιχων φορέων της Ευρωπαϊκής Ένωσης για τέσσερα χρόνια, μέχρι την οριστικοποίηση του τελικού κειμένου του νέου Κανονισμού και την έγκρισή του από το Ευρωπαϊκό Κοινοβούλιο.

Το 2016 ψηφίστηκε ο ΓΚΠΔ, ο οποίος από το 2018 απέκτησε υποχρεωτική εφαρμογή για όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης χωρίς την ανάγκη της

ψήφισης σχετικής νομοθεσίας από το κάθε κράτος μέλος διότι ως Κανονισμός έχει άμεση εφαρμογή.

Το 2019 ψηφίστηκε ο εθνικός νόμος (Ν. 4624/2019), ο οποίος εισάγει μέτρα εφαρμογής του ΓΚΠΔ σε εθνικό επίπεδο. Σκοπός του νέου νομοθετικού πλαισίου είναι η προστασία όλων των πολιτών της ΕΕ από παραβιάσεις της ιδιωτικής τους ζωής και των προσωπικών τους δεδομένων.

2. Εννοιολογικό πλαίσιο

2.1 Τι είναι προσωπικά δεδομένα

Προσωπικά δεδομένα είναι κάθε πληροφορία σχετική με ένα φυσικό πρόσωπο, εφόσον αυτό το φυσικό πρόσωπο ταυτοποιείται ή μπορεί να ταυτοποιηθεί (δηλαδή ακόμη και εάν δεν προσδιορίζεται ποιο είναι το πρόσωπο που αφορά η πληροφορία, αλλά αυτό μπορεί να συναχθεί έμμεσα συνδυάζοντας άλλες πληροφορίες).

Σύμφωνα με τον ΓΚΠΔ «δεδομένα προσωπικού χαρακτήρα είναι κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου» (άρθρο 4 αριθ.1). Υποκείμενο των δεδομένων είναι το φυσικό πρόσωπο στο οποίο αναφέρονται οι πληροφορίες αυτές. Το ενωσιακό δίκαιο για την προστασία προσωπικών δεδομένων δεν περιλαμβάνει την προστασία των νομικών προσώπων όσον αφορά την επεξεργασία των δεδομένων που αναφέρονται σε αυτά.

Ο ορισμός που δίνεται στην παραπάνω διάταξη είναι ευρύτατος και ο λόγος είναι ότι ο ενωσιακός νομοθέτης επέλεξε αυτόν τον ορισμό, ώστε να περιλαμβάνεται στην έννοια των προσωπικών δεδομένων κάθε είδους πληροφορία που αφορά ένα φυσικό πρόσωπο (Working Party 29, 2007). Γίνεται δεκτό ότι πέρα από το ονοματεπώνυμο, το οποίο αποτελεί το πιο σύνηθες προσδιοριστικό της ταυτότητας

ενός υποκειμένου, ομοίως μπορούν να συμπεριληφθούν και ο αριθμός μητρώου κοινωνικής ασφάλισης (Α.Μ.ΚΑ.), ο αριθμός δελτίου αστυνομικής ταυτότητας, ο αριθμός φορολογικού μητρώου κ.α. (Αλεξανδροπούλου – Αιγυπτιάδου, 2016).

Επιπλέον, προσωπικό δεδομένο μπορεί να αποτελέσει και η σχέση ενός φυσικού προσώπου με άλλα πρόσωπα ή πράγματα, όπως ενδεικτικά η ψυχική του κατάσταση, οι απόψεις, οι επιθυμίες του, ο τρόπος συμπεριφοράς, η περιουσιακή και οικογενειακή του κατάσταση, η οικονομική και επαγγελματική του δραστηριότητα, η καταναλωτική του συμπεριφορά.

Στα προσωπικά δεδομένα εμπίπτουν πληροφορίες που άπτονται της ιδιωτικής και οικογενειακής ζωής των ατόμων υπό στενή έννοια, αλλά και πληροφορίες που αφορούν οποιαδήποτε δραστηριότητα του ατόμου, όπως οι εργασιακές σχέσεις ή η οικονομική και κοινωνική συμπεριφορά του ατόμου (Working Party 29, 2007). Μπορεί επίσης να αφορούν τις σχέσεις ενός φυσικού προσώπου με άλλα πρόσωπα ή πράγματα, όπως ενδεικτικά η ψυχική του κατάσταση, οι απόψεις, οι επιθυμίες του, ο τρόπος συμπεριφοράς, η περιουσιακή και οικογενειακή του κατάσταση, η οικονομική και επαγγελματική του δραστηριότητα, η καταναλωτική του συμπεριφορά (Μήτρου, 2014).

Αντίθετα, σύμφωνα με τον ΓΚΠΔ δεν αποτελούν προσωπικά δεδομένα όσα δεδομένα έχουν καταστεί ανώνυμα κατά τρόπο ώστε η ταυτότητα του υποκειμένου των δεδομένων να μην μπορεί ή να μην μπορεί πλέον να εξακριβωθεί, ούτε μεταξύ άλλων για στατιστικούς ή ερευνητικούς σκοπούς (Αιτιολογική Σκέψη 26).

Ειδικότερα, στην έννοια των προσωπικών δεδομένων εμπίπτουν τόσο αντικειμενικές πληροφορίες, όπως είναι για παράδειγμα η παρουσία μιας ουσίας στο αίμα, όσο και υποκειμενικές πληροφορίες, γνώμες ή αξιολογήσεις, π.χ. ο Α είναι φερέγγυος δανειστής (Ιγγλεζάκης, 2018). Το κατά πόσο μια πληροφορία είναι αληθής ή ακριβής δεν επηρεάζει την υπαγωγή της στο προστατευτικό πεδίο του δικαίου των προσωπικών δεδομένων (Working Party 29, 2007).

Η μορφή με την οποία αποθηκεύονται ή χρησιμοποιούνται τα προσωπικά δεδομένα δεν ασκεί επιρροή στην εφαρμογή της νομοθεσίας για την προστασία των δεδομένων. Ακόμη και κυτταρικά δείγματα ανθρώπινου ιστού μπορεί να αποτελούν προσωπικά δεδομένα, αφού φέρουν καταγεγραμμένο το DNA του προσώπου. Μια πληροφορία μπορεί να είναι αριθμητική, αλφαβητική, φωτογραφική ή ακουστική και μπορεί να περιλαμβάνεται είτε σε έγγραφο είτε στη μνήμη ενός ηλεκτρονικού

υπολογιστή. Κατά συνέπεια, τα δεδομένα ήχου και εικόνας αποτελούν επίσης προσωπικά δεδομένα (Ιγγλεζάκης, 2013).

Η ΑΠΔΠΧ έχει επιχειρήσει να διακρίνει τα προσωπικά δεδομένα από τις αξιολογικές κρίσεις διατυπώνοντας την άποψη ότι με την επιφύλαξη της αρχής της ακρίβειας, της αναλογικότητας, καθώς και του δικαιολογημένου ενδιαφέροντος του κοινού για ενημέρωση ως προς τα δεδομένα που κοινοποιούνται, προσβολές της προσωπικότητας από τυχόν παράνομους χαρακτηρισμούς και όχι επεξεργασία πληροφοριών για πραγματικά περιστατικά δεν εμπίπτουν στη δικαιοδοσία της (Παναγοπούλου - Κουτνατζή, 2016). Η αιτιολόγηση της θέσης αυτής είναι ότι ως δεδομένα νοούνται μόνο πληροφορίες, δηλαδή οντολογικές κρίσεις, σε αντίθεση με τις αξιολογικές κρίσεις που, ως έκφραση της προσωπικότητας του αξιολογούντος και του αξιολογούμενου, δεν εμπίπτουν στο πεδίο εφαρμογής του νόμου (Χριστοδούλου, 2013).

Η Ομάδα Εργασίας του άρθρου 29 ρητά δηλώνει ότι η έννοια των προσωπικών δεδομένων «περιλαμβάνει ‘υποκειμενικές’ πληροφορίες, γνώμες ή εκτιμήσεις», αναφερόμενη σε πληροφορίες που αποτελούν αντικείμενο επεξεργασίας σε τομείς, όπως ο τραπεζικός, ο ασφαλιστικός ή ο εργασιακός, στους οποίους είναι απαραίτητη, π.χ., η αξιολόγηση της φερεγγυότητας του δανειολήπτη ή της αποδοτικότητας του υπαλλήλου. (Working Party 29, 2001)

Η ως άνω προσέγγιση μπορεί κατά συνέπεια να τύχει εφαρμογής και σε περιπτώσεις αναγραφής αξιολογικών κρίσεων κατά τη λήψη ιστορικού ασθενούς από τον επαγγελματία ψυχικής υγείας. Άρα, στην έννοια των προσωπικών δεδομένων εμπίπτουν και οι προσωπικές σημειώσεις και αξιολογήσει του σχετικά με τον ασθενή.

2.2 Προσωπικά δεδομένα υγείας

Ανάλογα με το είδος της πληροφορίας, τα προσωπικά δεδομένα διαχωρίζονται σε απλά και ειδικής κατηγορίας ή αλλιώς ευαίσθητα. Υπό το παλαιότερο καθεστώς, τα δεδομένα που αφορούσαν την υγεία ορίζονταν ως «ευαίσθητα», ενώ με τον ΓΚΠΔ εισάγεται η έννοια των «δεδομένων ειδικής κατηγορίας» στην οποία περιλαμβάνονται τα γενετικά δεδομένα, τα βιομετρικά δεδομένα και τα δεδομένα υγείας. Ο διαχωρισμός αυτός υπάρχει και διατηρείται και στον ΓΚΠΔ λόγω της αυξημένης προστασίας που απαιτείται για την επεξεργασία τους, διότι σε περίπτωση αποκάλυψής τους μπορούν να επιφέρουν στο άτομο βαρύτατες συνέπειες όπως ο κοινωνικός αποκλεισμός, το στίγμα και οι διακρίσεις.

Ως δεδομένα ειδικής κατηγορίας σύμφωνα με ΓΚΠΔ ορίζονται οι πληροφορίες «που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό» (άρθρο 9 § 1).

Για τα δεδομένα υγείας, ειδικότερα, εισάγεται ένα ευρύ πλαίσιο το οποίο περιλαμβάνει «όλα τα δεδομένα που αφορούν την κατάσταση της υγείας του υποκειμένου των δεδομένων και τα οποία αποκαλύπτουν πληροφορίες για την παρελθούσα, τρέχουσα ή μελλοντική κατάσταση της σωματικής ή ψυχικής υγείας του υποκειμένου των δεδομένων. Ενδεικτικά μπορεί να είναι αριθμός, σύμβολο ή ένα χαρακτηριστικό ταυτότητας που αποδίδεται σε φυσικό πρόσωπο με σκοπό την πλήρη ταυτοποίησή του για σκοπούς υγείας, πληροφορίες που προκύπτουν από εξετάσεις ή αναλύσεις σε μέρος ή ουσία του σώματος, μεταξύ άλλων από γενετικά δεδομένα και βιολογικά δείγματα και κάθε πληροφορία σχετικά με ασθένεια, αναπηρία, κίνδυνο ασθένειας, ιατρικό ιστορικό, κλινική θεραπεία ή τη φυσιολογική ή βιοϊατρική κατάσταση του προσώπου.» (Αιτιολογική Σκέψη 35). Άλλωστε, σύμφωνα με τον ορισμό που έχει δώσει για την υγεία ο Παγκόσμιος Οργανισμός Υγείας (ΠΟΥ, 1946), «υγεία είναι η κατάσταση πλήρους σωματικής, νοητικής και κοινωνικής ευεξίας και

όχι απλώς η απουσία νόσου ή αναπηρίας». Συνεπώς, στα δεδομένα υγείας εντάσσεται κάθε πληροφορία που αφορά τόσο τη βιολογική υπόσταση όσο και την ψυχική υγεία ενός ανθρώπου, τις ανικανότητες ή τις αναπηρίες του καθώς και το ιατρικό ιστορικό ενός ασθενούς (Αρμαμέντος – Σωτηρόπουλος, 2005).

Οι αυξημένες εγγυήσεις του ΓΚΠΔ σχετικά με την επεξεργασία δεδομένων υγείας είναι εμφανείς και από ρυθμίσεις σύμφωνα με τις οποίες επιχειρήσεις ή οργανισμοί που επεξεργάζονται ειδικής κατηγορίας δεδομένα έχουν την υποχρέωση να τηρούν αρχείο δραστηριοτήτων (άρθρο 30 §5), ακόμη και αν η επιχείρηση ή ο οργανισμός απασχολεί λιγότερα από 250 άτομα (δηλαδή δεν επεξεργάζεται δεδομένα σε μεγάλη κλίμακα). Καθώς επίσης και από την υποχρέωση διενέργειας εκτίμησης αντικτύπου όταν η επεξεργασία περιλαμβάνει δεδομένα υγείας και γίνεται σε μεγάλη κλίμακα (άρθρο 35). Βάσει αυτής, η ΑΠΔΠΧ κατήρτισε ειδικό κατάλογο ο οποίος περιλαμβάνει τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου. Ενδεικτικά, καθίσταται υποχρεωτική στις περιπτώσεις συστημάτων ηλεκτρονικής συνταγογράφησης, ηλεκτρονικού φακέλου ή ηλεκτρονικής κάρτας υγείας (ΑΠΔΠΧ, 2018).

2.3 Σχέση προσωπικών δεδομένων και επαγγελματικού απορρήτου

2.3.1 Προσωπικά δεδομένα και ιατρικό απόρρητο

Το ιατρικό απόρρητο αποτελεί μια από τις θεμελιώδεις υποχρεώσεις του ιατρού απέναντι στον ασθενή και αναγνωρίζεται ως τέτοια από τον Όρκο του Ιπποκράτη (400 π.Χ.). Η προστασία του επαγγελματικού απορρήτου δεν υπάγεται στις ρυθμίσεις περί προσωπικών δεδομένων αλλά απαντάται τόσο σε διατάξεις του Ποινικού Κώδικα (άρθρο 371) (Παππάς, 2014), όσο και σε διατάξεις του Κώδικα Ιατρικής Δεοντολογίας (άρθρο 13). Η εξέχουσα σημασία της τήρησης του επαγγελματικού απορρήτου εμφανίζεται σε πολλούς δικαιϊκούς κλάδους, όπως το ποινικό δίκαιο, το πειθαρχικό δίκαιο, το δίκαιο των προσωπικών δεδομένων και το δίκαιο της αστικής ευθύνης (Λασκαρίδης, 2016).

Ειδικά στον τομέα της ψυχικής υγείας, η εχεμύθεια αποτελεί θεμελιώδη αρχή της θεραπευτικής σχέσης ιατρού – ασθενούς. Από τη λήψη ψυχιατρικού ιστορικού, πριν την έναρξη της θεραπευτικής διαδικασίας, η διαβεβαίωση περί τήρησης του απορρήτου είναι προϋπόθεση για την έναρξή της. Χωρίς αυτή, ο ασθενής δε θα ήταν πρόθυμος να μιλήσει ελεύθερα στον θεραπευτή του εκφράζοντας τις σκέψεις, τους φόβους και τις επιθυμίες του (Lubit, Ladds & Eth, 2009). Δεν ισχύει το ίδιο στην περίπτωση της ψυχιατρικής πραγματογνωμοσύνης, κατά την οποία ο ψυχίατρος – πραγματογνώμων έχει την υποχρέωση να ενημερώσει σαφώς εξ' αρχής τον εξεταζόμενο σχετικά με τους σκοπούς για τους οποίους διενεργείται και τα πρόσωπα τα οποία θα λάβουν γνώση του περιεχομένου της σχετικής έκθεσης (Ιακωβίδης, 2014).

Ενώ η υποχρέωση τήρησης του επαγγελματικού απορρήτου στον ΚΙΔ αφορά τη σχέση ιατρού και ασθενούς, η προστασία των δεδομένων προσωπικού χαρακτήρα έχει ευρύτερο πεδίο εφαρμογής από το ιατρικό απόρρητο (Παναγοπούλου – Κουτνατζή, 2015). Το απόρρητο, σύμφωνα με τον ΚΙΔ (άρθρο 13 §1) καλύπτει οποιοδήποτε στοιχείο αφορά τον ασθενή ή τους οικείους του το οποίο υποπίπτει στην αντίληψη του ιατρού ή το αποκαλύπτει ο ασθενής ή τρίτοι, στο πλαίσιο άσκησης των ιατρικών καθηκόντων του. Ενδεικτικά, ο επαγγελματίας ψυχικής υγείας στο πλαίσιο της άσκησης των καθηκόντων του λαμβάνει από τον ασθενή πληροφορίες σχετικά με

την οικογενειακή του ζωή, το παρελθόν του, πτυχές της προσωπικότητάς του κ.α. τις οποίες οφείλει να κρατήσει εμπιστευτικές (Κορσάνου, Δουζένης, Λύκουρας, 2010)

Κατά συνέπεια, το ιατρικό απόρρητο καλύπτει κάθε πληροφορία που συλλέγει και καταχωρεί ο ιατρός, ακόμη και αν πρόκειται για απλά δεδομένα, συμπεριλαμβανομένων βέβαια και των δεδομένων υγείας. Αντίθετα, τα δεδομένα υγείας από τη σκοπιά του ΓΚΠΔ, αποτελούν αντικείμενο προστασίας μόνο όταν εντάσσονται σε σύστημα πλήρως ή μερικώς αυτοματοποιημένης ή μη αυτοματοποιημένης επεξεργασίας και συμπεριλαμβάνονται ή πρόκειται να συμπεριληφθούν σε αρχείο ή σύστημα αρχειοθέτησης (άρθρο 2 §1).

Το ιατρικό απόρρητο δεν καλύπτει πληροφορίες που ταυτοποιούν μεν ένα φυσικό πρόσωπο, όμως είναι πλατιά διαδεδομένες, όπως είναι για παράδειγμα η ασθένεια ενός δημοσίου προσώπου, η οποία έχει διαδοθεί από τα ΜΜΕ. Αντίθετα, οι πληροφορίες που έχει ανακοινώσει ο ίδιος ο ασθενής σε στενό κύκλο προσώπων καλύπτονται από το ιατρικό απόρρητο, διότι δεν θεωρούνται ευρέως διαδεδομένες πληροφορίες (Λασκαρίδης, 2012). Τέτοια διάκριση απαντάται και στον ΓΚΠΔ, ο οποίος παρέχει νόμιμη βάση επεξεργασίας για τα δεδομένα υγείας τα οποία έχει προδήλως δημοσιοποιήσει το ίδιο το υποκείμενο των δεδομένων (άρθρο 9 §2 ε').

Σύμφωνα με τον ΚΙΔ, το ιατρικό απόρρητο καλύπτει όχι μόνο τον ασθενή αλλά και τους οικείους του (άρθρο 13 §1). Ο ιατρός δεν έχει καθήκον εχεμύθειας μόνο για πληροφορίες που λαμβάνει από τον ασθενή και αφορούν τρίτα πλην των οικείων πρόσωπα (Λασκαρίδης, 2012). Αντίστοιχος διαχωρισμός δεν υπάρχει στον ΓΚΠΔ, καθώς κάθε δεδομένο προσωπικού χαρακτήρα προστατεύεται στον ίδιο βαθμό ανεξάρτητα από το άτομο στο οποίο αφορά. Θα πρέπει όμως να σημειωθεί στο σημείο αυτό, ότι σε περίπτωση που ο ιατρός πληροφορηθεί κατά την εκτέλεση των καθηκόντων του προσωπικά δεδομένα που αφορούν τρίτα πρόσωπα από τον ασθενή (πχ. κατά τη διάρκεια μιας ψυχοθεραπευτικής σχέσης ή κατά τη διάρκεια λήψης ιατρικού ιστορικού) όχι μόνο δε γεννάται υποχρέωση ενημέρωσης των τρίτων αυτών από τον ιατρό «δυνάμει υποχρέωσης επαγγελματικού απορρήτου» (άρθρο 14 §5 δ'), αλλά σε περίπτωση που προέβαινε σε μια τέτοια ενέργεια θα παραβίαζε το απόρρητο έναντι του ασθενούς του (Working Party 29, 2018). Επίσης, ο ΓΚΠΔ προστατεύει μόνο τα προσωπικά δεδομένα φυσικών προσώπων εν ζωή. Αντίθετα, το ιατρικό απόρρητο ισχύει και μετά το θάνατο του ασθενούς. Μετά το θάνατο του ασθενούς

δικαίωμα να ζητήσουν την άρση του έχουν οι νόμιμοι κληρονόμοι του (Γνωμοδότηση Εισαγγελέα ΑΠ, 15/2007).

Ως προς την υποχρέωση τήρησης του ιατρικού αρχείου, ο ΚΙΔ ορίζει ότι «Ο ιατρός υποχρεούται να τηρεί ιατρικό αρχείο, σε ηλεκτρονική ή μη μορφή, το οποίο περιέχει δεδομένα που συνδέονται αρρήκτως ή αιτιωδώς με την ασθένεια ή την υγεία των ασθενών του. Για την τήρηση του αρχείου αυτού και την επεξεργασία των δεδομένων του εφαρμόζονται οι διατάξεις του ν. 2472/1997» (άρθρο 14 §1).

Ο υποχρεωτικός χρόνος τήρησης του εν λόγω αρχείου σύμφωνα με τον ΚΙΔ είναι μια δεκαετία για τα ιδιωτικά ιατρεία και τις λοιπές μονάδες πρωτοβάθμιας φροντίδας υγείας και μια εικοσαετία σε κάθε άλλη περίπτωση από την τελευταία επίσκεψη του ασθενούς. Ο ΓΚΠΔ δεν ορίζει αντίστοιχο διάστημα τήρησης, καθώς αυτό επαφίεται στον εκάστοτε υπεύθυνο επεξεργασίας, ο οποίος όμως είναι υποχρεωμένος να το προσδιορίσει πριν την έναρξη της επεξεργασίας. Ο χρόνος αποθήκευσης των δεδομένων πρέπει να είναι συμβατός με την εκπλήρωση του σκοπού επεξεργασίας σύμφωνα με την αρχή του περιορισμού του χρόνου αποθήκευσης, όπως αποτυπώνεται στον ΓΚΠΔ (άρθρο 5 §1 ε'). Το γεγονός ότι ο ΚΙΔ θέτει αυτά τα χρονικά όρια, καθιστά αδρανές το δικαίωμα διαγραφής του υποκειμένου για όσο διάστημα υπάρχει η υποχρέωση τήρησης του ιατρικού αρχείου του (Ζωγραφόπουλος, 2018).

Στην υποχρέωση τήρησης απορρήτου καθώς και στην υποχρέωση συμμόρφωσης με τον ΓΚΠΔ υπόκεινται τόσο ο επαγγελματίας ψυχικής υγείας όσο και οι βοηθοί του. Η διαφορά έγκειται στο γεγονός ότι η παραβίαση του ιατρικού απορρήτου επισύρει κυρώσεις στον επαγγελματία που δεσμεύεται από αυτό, ενώ η παραβίαση προσωπικών δεδομένων επισύρει κυρώσεις στον εκάστοτε υπεύθυνο της επεξεργασίας, είτε πρόκειται για φυσικό είτε για νομικό πρόσωπο. Πλέον, με τον ΓΚΠΔ προβλέπονται τόσο διοικητικές όσο και αστικές κυρώσεις στον υπεύθυνο επεξεργασίας (Voigt & Von dem Bussche, 2017).

Τόσο από τον ΚΙΔ όσο και από τον Ποινικό Κώδικα, προβλέπεται σε εξαιρετικές περιπτώσεις η άρση του ιατρικού απορρήτου όταν η τήρησή του θα μπορούσε να βλάψει τον ασθενή ή τρίτο. Ειδικότερα, «αν ο υπαίτιος απέβλεπε στην εκπλήρωση καθήκοντός του ή στη διαφύλαξη έννομου ή για άλλο λόγο δικαιολογημένου ουσιώδους συμφέροντος δημόσιου ή του ίδιου ή κάποιου άλλου, το οποίο δεν μπορούσε να διαφυλαχθεί διαφορετικά» (άρθρο 371 §4 ΠΚ). Στην

καθημερινότητα των επαγγελματιών ψυχικής υγείας υπάρχουν ενίοτε και περιπτώσεις που είναι οριακές και όπου ενώ καλούνται αφενός να προστατεύσουν τα προσωπικά δεδομένα του ασθενούς τους, πρέπει αφετέρου να σταθμίσουν την πιθανότητα να τεθεί σε κίνδυνο η ζωή ή η σωματική ακεραιότητα ενός άλλου ανθρώπου (Κωνσταντινίδης, 2008).

Συμπερασματικά, το ρυθμιστικό πεδίου του ιατρικού απορρήτου είναι ευρύτερο από αυτό της προστασίας προσωπικών δεδομένων. Έτσι κάθε προσβολή των προσωπικών δεδομένων υγείας αποτελεί ταυτόχρονα και παραβίαση του ιατρικού απορρήτου. Αντίθετα, η παραβίαση του ιατρικού απορρήτου δεν αποτελεί και παραβίαση των διατάξεων περί προστασίας των προσωπικών δεδομένων υγείας του ασθενούς.

2.3.2 Προσωπικά δεδομένα και δικηγορικό απόρρητο

Ο ΓΚΠΔ ισχύει πέραν του δικηγορικού απορρήτου αλλά και παράλληλα με αυτό. Η υποχρέωση τήρησης της εμπιστευτικότητας και της ασφάλειας των προσωπικών δεδομένων που απορρέουν από τον ΓΚΠΔ συρρέουν με την υποχρέωση τήρησης εχεμύθειας και εμπιστευτικότητας όπως αποτυπώνεται στον Κώδικα Δεοντολογίας του Δικηγορικού Λειτουργήματος (άρθρα 32 και 36) και στον Κώδικα δικηγόρων (άρθρο 38). Ο δικηγόρος οφείλει να τηρεί αυστηρά εχεμύθεια για όσα του εμπιστεύεται ο εντολέας του κατά την ανάθεση και εκτέλεση της εντολής ή πληροφορείται κατά τη διάρκεια του χειρισμού της.

Το δικηγορικό απόρρητο αποτελεί μια από τις θεμελιώδεις εγγυήσεις της άσκησης του δικηγορικού λειτουργήματος. Πηγάζει τόσο από γενικούς συνταγματικούς κανόνες – ο σεβασμός στην προσωπική ζωή του ατόμου αναγνωρίζεται στο ελληνικό Σύνταγμα ως «δικαίωμα στην ιδιωτική και οικογενειακή ζωή» (άρθρο 9 §1 Συντάγματος) και ως «δικαίωμα προστασίας προσωπικών δεδομένων» (άρθρο 9^{A} Συντάγματος), όσο και από ειδικότερους νομικά δεσμευτικούς κανόνες όπως ο Κώδικας Δικηγόρων ή κανόνες με δεοντολογικό χαρακτήρα όπως ο Κώδικας δεοντολογίας Δικηγορικού Λειτουργήματος (Αλεξανδροπούλου – Αιγυπτιάδου, 2016).

Σύμφωνα με τον Κώδικα Δικηγόρων (Ν. 4194/2013) το καθήκον τήρησης εχεμύθειας αποτελεί μια από τις θεμελιώδεις αρχές και αξίες του δικηγορικού λειτουργήματος. Ο δικηγόρος είναι υποχρεωμένος να τηρεί απαραβίαστη την εχεμύθεια υπέρ του εντολέα του, για όσα ο τελευταίος του εμπιστεύθηκε ή έμαθε κατά την άσκηση του δικηγορικού λειτουργήματος. Σύμφωνα με τον Κώδικα Δικηγόρων, η παραβίαση του επαγγελματικού απορρήτου αποτελεί όχι μόνο ποινικό αλλά και πειθαρχικό παράπτωμα (άρθρο 140 §2 δ'). Επίσης, εάν ο δικηγόρος κληθεί να καταθέσει ως μάρτυρας για υπόθεση στην οποία έχει αναμειχθεί με την ιδιότητά του ως δικηγόρος, οφείλει να αρνηθεί να καταθέσει όσα του έχει εμπιστευθεί ο εντολέας του ανεξαρτήτως εάν η μεταξύ τους σχέση εντολής έχει λυθεί ή παραμένει σε ισχύ (άρθρο 39).

Οι υποχρεώσεις εμπιστευτικότητας ισχύουν τόσο κατά τη διάρκεια όσο και μετά την περαίωση της υπόθεσης ή την ανάκληση της εντολής, ακόμη και μετά το θάνατο του εντολέα. Αντίθετα, το δίκαιο προστασίας προσωπικών δεδομένων

προστατεύει τα προσωπικά δεδομένα φυσικών προσώπων που βρίσκονται στη ζωή και όχι των θανόντων (Μήτρου, 2004).

Όπως και οι επαγγελματίες ψυχικής υγείας έτσι και οι δικηγόροι και κάθε είδους νομικοί παραστάτες στους οποίους οι εντολείς τους εμπιστεύονται λόγω του επαγγέλματός τους ιδιωτικά απόρρητα, καθώς και οι βοηθοί τους, έχουν ποινική ευθύνη σε περίπτωση παραβίασης του καθήκοντος τήρησης απορρήτου. Ο άδικος χαρακτήρας της πράξης, όπως προαναφέρθηκε, αίρεται σε εξαιρετικές περιπτώσεις.

2.4 Ο επαγγελματίας ψυχικής υγείας και ο δικηγόρος ως υπεύθυνοι επεξεργασίας

Υπεύθυνος της επεξεργασίας, σύμφωνα με τον ΓΚΠΔ είναι το φυσικό ή νομικό πρόσωπο που καθορίζει τους σκοπούς και τον τρόπο επεξεργασίας των προσωπικών δεδομένων (άρθρο 4 περ. 7'), ενώ εκτελών την επεξεργασία είναι το φυσικό ή νομικό πρόσωπο που επεξεργάζεται προσωπικά δεδομένα για λογαριασμό του υπευθύνου επεξεργασίας (άρθρο 4 περ. 8'). Ο χαρακτηρισμός ενός επαγγελματία ως υπευθύνου ή εκτελούντος την επεξεργασία είναι ιδιαίτερα σημαντικός, λόγω των διαφορετικών υποχρεώσεων που πηγάζουν από τον ΓΚΠΔ και της συνακόλουθης ευθύνης από την έλλειψη συμμόρφωσης.

Ως υπεύθυνος επεξεργασίας, ο δικηγόρος διαχειρίζεται δεδομένα προσωπικού χαρακτήρα, συνήθως απλά, συχνά όμως και ειδικής κατηγορίας, είτε πρόκειται για μια υπόθεση μεταξύ φυσικών προσώπων, είτε μεταξύ νομικών προσώπων. Αυτό συμβαίνει διότι ακόμη και στην περίπτωση νομικών προσώπων ο φάκελος δικογραφίας περιλαμβάνει πάντα και τα στοιχεία των νόμιμων εκπροσώπων, των μελών του διοικητικού συμβουλίου, διαφόρων συνεργατών κ.α. Πέραν αυτών, ένας φάκελος δικογραφίας περιλαμβάνει επίσης, τα προσωπικά δεδομένα των ίδιων των εντολέων, στοιχεία των αντιδίκων, των μαρτύρων, των δικαστικών επιμελητών, των πραγματογνωμόνων, ακόμη και στοιχεία δικηγόρων των αντιδίκων, συνεργατών δικηγόρων, ασκούμενων δικηγόρων καθώς και όσων προσώπων εμπλέκονται με οποιοδήποτε τρόπο στην υπόθεση κλπ. (Μήτρου, Γιαννόπουλος, Παναγοπούλου, Βαρβέρης, 2018).

Ένας δικηγόρος ο οποίος εκπροσωπεί τον πελάτη του στο δικαστήριο προβαίνει όχι μόνο σε αποθήκευση (σε ηλεκτρονικά ή χειρόγραφα αρχεία), αλλά και σε χρήση, κοινοποίηση, διαβίβαση και άλλες μορφές επεξεργασίας των προσωπικών δεδομένων του εντολέα του. Νομική βάση για την επεξεργασία όλων των αναγκαίων για την διεκπεραίωση της υπόθεσης δεδομένων είναι η σύμβαση εντολής μεταξύ δικηγόρου και πελάτη. Σκοπός της εντολής που δίνεται στον δικηγόρο δεν είναι η ίδια η επεξεργασία των δεδομένων, αλλά η εκπροσώπηση του εντολέα στο ακροατήριο, δηλαδή η εκτέλεση της σύμβασης εντολής. Κατά συνέπεια, οι δικηγόροι είναι

υπεύθυνοι επεξεργασίας, όταν επεξεργάζονται δεδομένα στο πλαίσιο της νόμιμης εκπροσώπησης των εντολέων τους. (Working Party 29, 2010).

Η Επίτροπος της Κύπρου πηγαίνει ένα βήμα παραπέρα και εξειδικεύει τον ρόλο των δικηγόρων σε σχετική γνώμη που έχει εκδώσει με ορισμένα ενδεικτικά παραδείγματα. Εν συντομία, υπεύθυνος επεξεργασίας είναι ο δικηγόρος που εκπροσωπεί τον πελάτη του ενώπιον Δικαστηρίου, ο οποίος συλλέγει και επεξεργάζεται προσωπικά δεδομένα αποκλειστικά για τον σκοπό αυτό, ενώ αντίθετα ο δικηγόρος που παρέχει νομικές συμβουλές, καταρτίζει συμβόλαια και διευθετεί γενικά εξωδικαστηριακές διευθετήσεις θεωρείται εκτελών την επεξεργασία. Το ίδιο ισχύει και για τον δικηγόρο ο οποίος παρέχει υπηρεσίες εξωτερικού νομικού συμβούλου οργανισμών και /ή άλλων εταιρειών συμπεριλαμβανομένων δικαστηριακών ή εξωδικαστηριακών υπηρεσιών (Επίτροπος Προστασίας Προσωπικών Δεδομένων Κύπρου, 2018).

Ο παραπάνω διαχωρισμός ανάλογα με τη φύση της υπόθεσης και της συμβατικής σχέσης μεταξύ δικηγόρου και εντολέα δεν απέχει πολύ από τη γνώμη της Ομάδας Εργασίας του άρθρου 29 σύμφωνα με την οποία, βασικό κριτήριο για τον χαρακτηρισμό κάποιου ως υπευθύνου επεξεργασίας είναι η «εμπειρογνωμοσύνη των μερών: σε ορισμένες περιπτώσεις, ο παραδοσιακός ρόλος και η επαγγελματική εμπειρογνωμοσύνη του παρόχου της υπηρεσίας διαδραματίζουν κυρίαρχο ρόλο, ο οποίος μπορεί να συνεπάγεται τον χαρακτηρισμό του ως υπευθύνου της επεξεργασίας των δεδομένων» (Working Party 29, 2010).

Έχει διατυπωθεί βέβαια και η άποψη ότι στην περίπτωση που ο εντολέας, ο οποίος έχει καθορίσει τον σκοπό και τα μέσα της επεξεργασίας των δεδομένων, παραχωρώντας τα στον δικηγόρο για να τον εκπροσωπήσει ενώπιον Δικαστηρίου ή εξωδικαστικά, καθίσταται ο ίδιος (ο πελάτης) υπεύθυνος επεξεργασίας και ο δικηγόρος εκτελών την επεξεργασία για λογαριασμό του πελάτη (Σωτηρόπουλος, 2018).

Αναφορικά με τους επαγγελματίες ψυχικής υγείας, όταν είναι αυτό-απασχολούμενοι, είναι υπεύθυνοι της επεξεργασίας, καθορίζοντας τους σκοπούς και τα μέσα επεξεργασίας προσωπικών δεδομένων στο πλαίσιο λειτουργίας του ιατρείου ή του γραφείου τους. Όταν όμως πρόκειται για νομικά πρόσωπα, όπως για παράδειγμα νοσοκομεία ή κλινικές, υπεύθυνο για την επεξεργασία είναι το νομικό

πρόσωπο, το οποίο μέσω της διοίκησής του καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας.

Σύμφωνα με την ΑΠΔΠΧ (Απόφαση 31/2008), οι ψυχολόγοι λογίζονται ως υπεύθυνοι επεξεργασίας αρχείου με ευαίσθητα προσωπικά δεδομένα και έχουν αντίστοιχες υποχρεώσεις με εκείνες των ιατρών και όχι ως εκτελούντες την επεξεργασία, ανεξάρτητα από το καθεστώς κάτω από το οποίο απασχολούνται. Το γεγονός αυτό δημιουργεί και αντίστοιχες υποχρεώσεις, καθώς ο υπεύθυνος της επεξεργασίας ορίζει το σκοπό και τα μέσα της επεξεργασίας, ενώ ο εκτελών την επεξεργασία ενεργεί κατ' εντολή και σύμφωνα με τις οδηγίες του υπεύθυνου.

Σε περίπτωση διαβίβασης ιατρικών αρχείων σε άλλη τοποθεσία, ο αρχικός υπεύθυνος επεξεργασίας δεδομένων μπορεί να παραμείνει υπεύθυνος. Όμως, καθώς τα διάφορα στοιχεία των αρχείων διαβιβάζονται σε διαφορετικά τμήματα ενός νοσοκομείου ή σε διαφορετικές γεωγραφικές τοποθεσίες, μπορεί να μην είναι πάντα το ίδιο εύκολο να εξακριβωθεί ποιος είναι υπεύθυνος για την προστασία των εκάστοτε δεδομένων (Stanberry, 1998).

2.5 Η νομιμότητα της επεξεργασίας

Τα ιατρικά δεδομένα εμπίπτουν στην ομάδα των δεδομένων ειδικής κατηγορίας, η επεξεργασία των οποίων σύμφωνα με τον ΓΚΠΔ κατ' αρχήν απαγορεύεται, κατ' εξαίρεση επιτρέπεται υπό προϋποθέσεις (άρθρο 9). Οι εξαιρέσεις αυτές, οι οποίες αφορούν την επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων και δεδομένων υγείας αναφέρονται περιοριστικά και αποτελούν τις νομιμοποιητικές βάσεις της επεξεργασίας.

Ως επεξεργασία προσωπικών δεδομένων ορίζεται «κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.» (άρθρο 4 §2). Με λίγα λόγια, ως επεξεργασία νοείται κάθε διαδικασία, με ή χωρίς αυτοματοποιημένα μέσα, που περιλαμβάνει προσωπικά δεδομένα.

Η επεξεργασία για να είναι νόμιμη είναι απαραίτητο να στηρίζεται σε μια ή περισσότερες από τις νομιμοποιητικές βάσεις που προβλέπονται στον ΓΚΠΔ (άρθρα 6 και 9). Η επεξεργασία ειδικών κατηγοριών δεδομένων επιτρέπεται, όπως ήδη έχει ειπωθεί, υπό προϋποθέσεις. Περιπτώσεις στις οποίες επιτρέπεται η επεξεργασία των ειδικών κατηγοριών δεδομένων και οι οποίες τυγχάνουν εφαρμογής όταν διενεργείται επεξεργασία από επαγγελματίες ψυχικής υγείας, αποτελούν ενδεικτικά:

(α) η επεξεργασία που γίνεται με ρητή συγκατάθεση του υποκειμένου,

(β) η επεξεργασία που γίνεται για την προστασία των ζωτικών συμφερόντων του υποκειμένου ή άλλου φυσικού προσώπου, εάν το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να συγκατατεθεί,

Η έννοια του «ζωτικού συμφέροντος»: Αναφέρεται πρωτίστως στο έννομο αγαθό της ζωής του υποκειμένου. Επίσης, περιλαμβάνει το έννομο αγαθό της υγείας, όταν αυτό συνδέεται με την επιβίωση του υποκειμένου, δηλαδή όταν η υγεία του

απειλείται σε τέτοιο βαθμό που θέτει σε κίνδυνο τη ζωή του. Επιπλέον, ζωτικά συμφέροντα μπορούν να θεωρηθούν, lato sensu, και τα οικονομικά έννομα αγαθά του υποκειμένου (ιδιοκτησία και περιουσία) όταν η διαφύλαξή τους συνδέεται άμεσα με την επιβίωση του υποκειμένου (Αρμαμέντος & Σωτηρόπουλος, 2005). Αντίστοιχη ρύθμιση υπάρχει και στον ΚΙΔ (άρθρο 12 §3 εδ. α΄), σύμφωνα με την οποία «κατ' εξαίρεση δεν απαιτείται συναίνεση στις επείγουσες περιπτώσεις, κατά τις οποίες δεν μπορεί να ληφθεί κατάλληλη συναίνεση και συντρέχει άμεση, απόλυτη και κατεπείγουσα ανάγκη παροχής ιατρικής φροντίδας».

(γ) η επεξεργασία που είναι απαραίτητη για σκοπούς προληπτικής ή επαγγελματικής ιατρικής, εκτίμησης της ικανότητας προς εργασία του εργαζομένου, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών βάσει της εφαρμοστέας νομοθεσίας ή δυνάμει σύμβασης με επαγγελματία του τομέα της υγείας,

(δ) η επεξεργασία που είναι απαραίτητη για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, όπως η προστασία έναντι σοβαρών διασυνοριακών απειλών κατά της υγείας ή η διασφάλιση υψηλών προτύπων ποιότητας και ασφάλειας της υγειονομικής περίθαλψης και των φαρμάκων ή των ιατροτεχνολογικών προϊόντων,

(ε) η επεξεργασία είναι απαραίτητη για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς

Απαραίτητη η επεξεργασία για αποτροπή σοβαρού κινδύνου για τη δημόσια ασφάλεια: Εάν υφίσταται ένας ειδικός δημοσίου δικαίου κίνδυνος είτε για συλλογικά (δημόσια τάξη, συνταγματική νομιμότητα, προστασία του κράτους και των νομικών προσώπων του) είτε για ατομικά έννομα αγαθά (ζωή, υγεία, ελευθερία) πρέπει λόγω αναγκαιότητας να επιτρέπεται η επεξεργασία. Επιτρέπεται όταν το αντικείμενο προστασίας είναι το κοινό όφελος/κοινό συμφέρον. Η επεξεργασία ευαίσθητων δεδομένων επιτρέπεται μόνο κατ' εξαίρεση για αποφυγή σημαντικών κινδύνων για το κοινό καλό/γενικότερο συμφέρον της κοινωνίας και μόνο σε περίπτωση «επιτακτικής αναγκαιότητας», ενώ παράλληλα διευκρινίζεται ο απολύτως εξαιρετικός χαρακτήρας της ρύθμισης (π.χ. ανθρώπινα δικαιώματα, ειρήνη, ελευθερία, ασφάλεια) και η στάθμιση με τα δικαιώματα του υποκειμένου (Schulz, 2018).

Ο ΓΚΠΔ προβλέπει και άλλες περιπτώσεις στις οποίες επιτρέπεται η επεξεργασία ειδικών κατηγοριών δεδομένων, ωστόσο οι ανωτέρω είναι οι πιο συνήθεις νόμιμες βάσεις για την επεξεργασία δεδομένων ασθενών που διενεργείται από ιατρούς. Διευκρινίζεται ότι δεν χρειάζεται να συντρέχουν όλες οι παραπάνω βάσεις επεξεργασίας, αλλά μία. Η συνηθέστερη αλλά και ενδεικτική ως ειδικότερη όταν πρόκειται για δεδομένα ασθενών είναι αυτή της παροχής υπηρεσιών υγείας (Ζωγραφόπουλος, 2018).

Για τους δικηγόρους, οι συνήθεις βάσεις επεξεργασίας προσωπικών δεδομένων των εντολέων τους αφορούν απλά δεδομένα (άρθρο 6). Εξυπακούεται ότι σε περίπτωση που συλλέγουν δεδομένα υγείας ή άλλης ειδικής κατηγορίας, καθώς και δεδομένα που αφορούν ποινικές διώξεις, καταδίκες και αδικήματα θα πρέπει να αναζητηθεί η αντίστοιχη νομιμοποιητική βάση (άρθρο 9).

Ειδικότερα, οι ενδεικτικότερες νομιμοποιητικές βάσεις επεξεργασίας αυτής της επαγγελματικής ομάδας είναι:

(α) Η επεξεργασία γίνεται με σκοπό την εκτέλεση σύμβασης μεταξύ του δικηγόρου και του εντολέα του.

(β) Όταν η επεξεργασία αφορά σκοπούς οι οποίοι δεν εντάσσονται στη σύμβαση εντολής μεταξύ δικηγόρου και εντολέα, η λήψη συγκατάθεσης του υποκειμένου.

(γ) Η επεξεργασία είναι απαραίτητη για την εκπλήρωση έννομης υποχρέωσης

(δ) Η επεξεργασία είναι απαραίτητη για σκοπούς υπέρτερου εννόμου συμφέροντος του δικηγόρου ή τρίτου, εκτός εάν έναντι αυτών υπερτερεί το συμφέρον ή τα δικαιώματα του εντολέα.

2.6 Οι καινοτομίες του Κανονισμού (ΕΕ) 2016/679

2.6.1 Ο ρόλος του Υπεύθυνου Προστασίας Προσωπικών Δεδομένων

Σύμφωνα με την αρχή της λογοδοσίας η οποία εισάγεται με τον ΓΚΠΔ, οι υπεύθυνοι και εκτελούντες την επεξεργασία εντάσσονται σε ένα νέο καθεστώς «αυτό-συμμόρφωσης» στο πλαίσιο του οποίου είναι υποχρεωμένοι να προσαρμόσουν τα τεχνικά και οργανωτικά συστήματά τους με τρόπο ώστε να μπορούν να αποδεικνύουν, ανά πάσα στιγμή, ενώπιον των εποπτικών αρχών ότι έχουν επιτύχει πλήρη συμμόρφωση με τις απαιτήσεις του. Μια από τις ρυθμιστικές μεθόδους αυτής της αρχής που αποτελεί συνάμα και καινοτομία του Κανονισμού είναι ο θεσμός του Υπεύθυνου Προστασίας Προσωπικών Δεδομένων (ΥΠΔ). Ο θεσμός αυτός προβλεπόταν από την Οδηγία (95/46/ΕΚ), ως ένα από τα προαιρετικά μέτρα, χωρίς ωστόσο να αξιοποιηθεί από τον Έλληνα νομοθέτη (Ιγγλεζάκης, 2018).

Το άτομο που διορίζεται ως ΥΠΔ σε μια εταιρεία ή έναν οργανισμό, πρέπει να διαθέτει ειδικές γνώσεις στο δίκαιο και στις πρακτικές προστασίας προσωπικών δεδομένων (συγκεκριμένα χρησιμοποιείται ο όρος «εμπειρογνωσία») και να παρέχει συνδρομή στον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία κατά την παρακολούθηση της εσωτερικής συμμόρφωσης προς τον ΓΚΠΔ.

Ο ΥΠΔ μπορεί να είναι εσωτερικός (σε καθεστώς εξαρτημένης εργασίας) ή εξωτερικός (παρέχοντας υπηρεσίες με σύμβαση παροχής υπηρεσιών). Η τήρηση διαφάνειας σχετικά με την επεξεργασία προσωπικών δεδομένων επιβάλλει τη δημοσιότητα των στοιχείων του ΥΠΔ. Τα στοιχεία του δημοσιοποιούνται στην ΑΠΔΠΧ μέσω ειδικού εντύπου που υπάρχει αναρτημένο στην ιστοσελίδα της.

Είναι σημαντικό η θέση του ΥΠΔ να διέπεται από ανεξαρτησία, ακόμη και όταν πρόκειται για εσωτερικό ΥΠΔ, ώστε να αποφεύγονται περιπτώσεις σύγκρουσης συμφερόντων. Απαγορεύεται η κατοχή θέσης ή ρόλου που συνεπάγεται σύγκρουση συμφερόντων, ήτοι θέση από την οποία καθορίζεται ο σκοπός και τα μέσα επεξεργασίας ή ρόλου που αφορά την εκπροσώπηση της εταιρείας ή την υπεράσπιση των επιλογών της στην επεξεργασία προσωπικών δεδομένων (άρθρο 38 §6). Δε μπορεί με άλλα λόγια το ίδιο πρόσωπο να κατέχει ταυτόχρονα θέση «εσωτερικού ελεγκτή» και «ελεγχόμενου». Τέτοιες θέσεις αφορούν τον διευθύνοντα σύμβουλο,

διοικητικό γενικό διευθυντή, οικονομικό διευθυντή, αρχίατρο, προϊστάμενο ανθρωπίνων πόρων, προϊστάμενο τμήματος μάρκετινγκ ή τμήματος πληροφορικής κλπ. Επίσης, οι θέσεις νομικών συμβούλων, δικηγόρων, υπεύθυνων διασφάλισης απορρήτου ή ασφάλειας προσωπικών δεδομένων, μπορεί υπό προϋποθέσεις να δημιουργήσουν σύγκρουση συμφερόντων όταν παράλληλα ανατίθενται στα πρόσωπα αυτά τα καθήκοντα του ΥΠΔ (Working Party 29, 2017)

Αρμοδιότητα του ΥΠΔ είναι να διευκολύνει τη συμμόρφωση του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία με τις διατάξεις του ΓΚΠΔ καθώς και να αποτελεί σημείο επαφής και μεσολάβησης ανάμεσα σε υπεύθυνο επεξεργασίας, εποπτικές αρχές και υποκείμενα των δεδομένων. Ο ρόλος του είναι συμβουλευτικός και όχι αποφασιστικός καθώς δεν φέρει προσωπική ευθύνη για τη μη συμμόρφωση με τον Κανονισμό (Lambert, 2016).

Είναι σημαντικό να ειπωθεί ότι δεν συνιστα επεξεργασία μεγάλης κλίμακας και συνακόλουθα δε γεννάται υποχρέωση ορισμού Υπεύθυνου Προστασίας Προσωπικών Δεδομένων η επεξεργασία δεδομένων ασθενών από ιδιώτη ιατρό ή άλλον επαγγελματία υγείας (Αιτιολογική Σκέψη 91) και η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα από ιδιώτη δικηγόρο. Αντίθετα, νομικά πρόσωπα όπως τα νοσοκομεία και οι κλινικές που διενεργούν μεγάλης κλίμακας επεξεργασία δεδομένων υγείας οφείλουν να ορίσουν ΥΠΔ (Working Party 29, 2017).

2.6.2 Ιδιωτικότητα εξ' ορισμού και από τον σχεδιασμό (privacy by design and by default) – Ασφάλεια επεξεργασίας

Οι έννοιες της ιδιωτικότητας, της εμπιστευτικότητας και της ασφάλειας των πληροφοριών δεν είναι ταυτόσημες. Ο όρος *«ιδιωτικότητα» (privacy)* αναφέρεται στην προστασία της ιδιωτικής ζωής ενός ατόμου και είναι μια ευρύτερη έννοια από την περιορισμένη πρόσβαση σε πληροφορίες σχετικά με ένα άτομο. Η παραβίαση της ιδιωτικής ζωής συμβαίνει όταν αποκτάται μη εξουσιοδοτημένη πρόσβαση στην ιδιωτική ζωή ενός ατόμου (Schoeman, 1984).

Η εμπιστευτικότητα (confidentiality) αφορά την τήρηση μυστικών των πληροφοριών που διαβιβάζονται από ένα άτομο σε ένα άλλο. Η παραβίαση του απορρήτου λαμβάνει χώρα όταν ο παραλήπτης ή ο κάτοχος των πληροφοριών αυτών δεν προστατεύει ή αποκαλύπτει σκόπιμα αυτές τις πληροφορίες σε κάποιον τρίτο χωρίς τη συναίνεση του υποκειμένου (Beauchamp & Childress, 1994).

Η ασφάλεια της επεξεργασίας των προσωπικών δεδομένων είναι μια ευρύτερη έννοια από την εμπιστευτικότητα, η οποία καλύπτει την προστασία της ιδιωτικής ζωής. Γενικά, αναφέρεται στις διαδικασίες, τόσο τις τεχνικές όσο και τις οργανωτικές, που είναι απαραίτητες για την προστασία της συλλογής, αποθήκευσης και μετάδοσης των πληροφοριών. Τόσο η εμπιστευτικότητα όσο και η ασφάλεια της επεξεργασίας των προσωπικών δεδομένων δεν είναι μόνο ένα τεχνικό ζήτημα. Σχετίζονται κυρίως με την κουλτούρα και τις διαδικασίες που έχουν προβλεφθεί εσωτερικά σε ένα οργανισμό ή μια επιχείρηση (Roy McClell & Victoria Thomas, 2002).

Οι διατάξεις του ΓΚΠΔ σχετικά με την ασφάλεια της επεξεργασίας (άρθρο 25) είναι μεταξύ των πλέον καινοτόμων του πρόσφατα μεταρρυθμισμένου καθεστώτος προστασίας προσωπικών δεδομένων. Αποσκοπούν κυρίως στην ανάπτυξη συστημάτων πληροφοριών που έχουν εκ των προτέρων ενσωματώσει τις απαιτήσεις του Κανονισμού (Bygrave, 2017). Η ιδέα της ενσωμάτωσης της προστασίας δεδομένων στα συστήματα πληροφορικής δεν είναι εντελώς νέα. Η Οδηγία (95/46/ΕΚ) αναφέρεται για παράδειγμα στη λήψη κατάλληλων τεχνικών και οργανωτικών μέτρων τόσο κατά τον σχεδιασμό του συστήματος επεξεργασίας όσο και κατά τη διάρκεια της επεξεργασίας, με στόχο τη διατήρηση της

ασφάλειας. Ωστόσο, ο ΓΚΠΔ εισάγει την απαίτηση τα ηλεκτρονικά συστήματα να σχεδιάζονται και να κατασκευάζονται κατά τέτοιο τρόπο ώστε να ελαχιστοποιείται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα (Schaar, 2010).

Συγκεκριμένα ο ΓΚΠΔ προβλέπει ότι ο εκάστοτε υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασίας πρέπει να λαμβάνουν τα κατάλληλα τεχνικά και οργανωτικά μέτρα για τη μέγιστη δυνατή ασφάλεια των προσωπικών δεδομένων (άρθρο 32). Παραδοσιακά, ο όρος ασφάλεια προσωπικών δεδομένων, χρησιμοποιείται για να περιγράψει τις μεθόδους και τεχνικές που ακολουθούνται προκειμένου να επιτευχθεί η προστασία των τριών αρχών στις οποίες στηρίζεται το δίκαιο περί προστασίας προσωπικών δεδομένων:

Εμπιστευτικότητα (confidentiality): Τα δεδομένα δεν πρέπει να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα.

Ακεραιότητα (integrity): Τα δεδομένα πρέπει να είναι ακριβή, ακέραια και ορθά – όχι εσφαλμένα, αλλοιωμένα ή μη ενημερωμένα.

Διαθεσιμότητα (availability): Τα δεδομένα πρέπει να είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους. Η διαθεσιμότητα αξιόπιστων πληροφοριών έχει τεράστιο αντίκτυπο στις αποφάσεις σχετικά με τη φροντίδα των ασθενών (Neubauer & Heurix, 2011).

Σε περίπτωση που έχει παραβιαστεί έστω μια από τις τρεις αυτές αρχές γίνεται λόγος για περιστατικό ασφάλειας **(**National Institute of Standards and Technology ;NIST, 2017). Η δυνατότητα αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε περίπτωση συμβάντος αποτελεί ένα από τα ενδεδειγμένα μέτρα ασφαλείας σύμφωνα με τον ΓΚΠΔ (άρθρο 32).

Η μέθοδος της κρυπτογράφησης μαζί με την ψευδωνυμοποίηση προτείνονται από τον ΓΚΠΔ ως οι πλέον κατάλληλες για τη διασφάλιση της προστασίας των προσωπικών δεδομένων.

Κρυπτογράφηση (*encryption*) ονομάζεται η διαδικασία μετασχηματισμού ενός μηνύματος σε μία ακατανόητη μορφή με τη χρήση κάποιου κρυπτογραφικού αλγορίθμου ούτως ώστε να μην μπορεί να διαβαστεί από κανέναν εκτός του νόμιμου παραλήπτη. Η αντίστροφη διαδικασία όπου από το κρυπτογραφημένο κείμενο παράγεται το αρχικό μήνυμα ονομάζεται αποκρυπτογράφηση (*decryption*) (Menezes, 1996).

Ψευδωνυμοποίηση, σύμφωνα με τον ΓΚΠΔ είναι «η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο», (άρθρο 4 περ. 5).

Είναι χαρακτηριστικό ότι σε περίπτωση περιστατικού παραβίασης, εάν τα δεδομένα έχουν κρυπτογραφηθεί, ο υπεύθυνος επεξεργασίας δεν υποχρεούνται να ενημερώσει τα υποκείμενα δεδομένων (άρθρο 34 §3), καθώς τα δεδομένα θεωρείται ότι προστατεύονται επαρκώς, εφόσον η κρυπτογράφηση εφαρμόστηκε σωστά. Παρόλο που τα δεδομένα κρυπτογραφούνται, εξακολουθεί να είναι καλή πρακτική η ελαχιστοποίηση του όγκου των δεδομένων που συλλέγονται. Αυτό όχι μόνο συμβάλει στη μείωση της επιβάρυνσης της προστασίας των, αλλά σημαίνει επίσης ότι ο οργανισμός είναι λιγότερο πιθανό να παραβιάσει τις απαιτήσεις συμμόρφωσης διότι προκύπτει εύλογα ότι τα δεδομένα χρησιμοποιούνται μόνο για σκοπούς για τους οποίους συλλέχθηκαν και όχι για άλλους.

Η μέθοδος της ανωνυμοποίησης θα πρέπει να διακριθεί από αυτή της ψευδωνυμοποίησης. Συγκεκριμένα, ως ανωνυμοποίηση ορίζεται η διαδικασία διαγραφής των αναγνωριστικών προσωπικού χαρακτήρα σε εγγραφές δεδομένων, έτσι ώστε να μην είναι πλέον εφικτό τα ανωνυμοποιημένα δεδομένα να συσχετιστούν με το υποκείμενο των δεδομένων (Λαμπρινουδάκης, Γκρίτζαλης, Μήτρου, Κάτσικας, 2010).

Συνεπώς, η χρήση της ανωνυμοποίησης έχει ως αποτέλεσμα την αδυναμία προσδιορισμού του υποκειμένου των δεδομένων, σε αντίθεση με την ψευδωνυμοποίηση που αντικαθιστά την ταυτότητα του υποκειμένου των δεδομένων κατά τέτοιο τρόπο, ώστε να απαιτούνται συμπληρωματικές πληροφορίες για την ταυτοποίηση του υποκειμένου των δεδομένων. Τα δεδομένα τα οποία έχουν καταστεί ανώνυμα δεν εμπίπτουν το πεδίο εφαρμογής του ΓΚΠΔ, διότι δεν είναι δυνατό ή δεν είναι δυνατό πλέον να ταυτοποιήσουν ένα φυσικό πρόσωπο (Αιτιολογική Σκέψη 26). Για παράδειγμα, η δημοσίευση δικαστικής απόφασης από δικηγόρο χωρίς την αφαίρεση των ονομάτων των διαδίκων συνιστά παράνομη επεξεργασία. Οι δικαστικές

αποφάσεις θα πρέπει να δημοσιεύονται πάντα ανωνυμοποιημένες. (Απόφαση ΑΠΔΠΧ, 43/2009)

Τόσο η κρυπτογράφηση όσο και η ψευδωνυμοποίηση προτείνονται ως ενδεικτικές τεχνικές για την εξασφάλιση ενός επιπέδου προστασίας των προσωπικών δεδομένων, συμπεριλαμβανομένων και των προσωπικών δεδομένων ειδικών κατηγοριών (Λουκάς, 2017). Επίσης, ανεξάρτητα από το αν τα δεδομένα τα οποία τηρούνται είναι συναφή και πρόσφορα, απαιτείται και να είναι αναγκαία για την εξυπηρέτηση των συγκεκριμένων κάθε φορά σκοπών μιας επεξεργασίας (Αρμαμέντος & Σωτηρόπουλος, 2005). Ειδικά για τα δεδομένα υγείας, δεν είναι επιτρεπτή η διαβίβαση κι επαναχρησιμοποίηση των δεδομένων υγείας και – κατά μείζονα λόγο - των γενετικών δεδομένων εκτός του ιατρικού πλαισίου. Δεν θα πρέπει να έχει ως αποτέλεσμα την επεξεργασία δεδομένων προσωπικού χαρακτήρα για άλλους σκοπούς από τρίτους, όπως εργοδότες ή ασφαλιστικές εταιρείες και τράπεζες (Αιτιολογική σκέψη 54).

Σε γενικές γραμμές πάντως, οι έρευνες δείχνουν ότι όσο πιο ενημερωμένοι είναι οι επαγγελματίες σχετικά με τις απαιτήσεις του ΓΚΠΔ, τόσο περισσότερο φροντίζουν ώστε να λάβουν τα απαραίτητα μέτρα για την ασφάλεια της επεξεργασίας (ICAP, 2017). Ειδικά για τους δικηγόρους είναι χαρακτηριστικό, ότι όσο περισσότερο εμπλέκονται στη συμμόρφωση των οργανισμών ή των επιχειρήσεων ώς νομικοί σύμβουλοι ή ως υπεύθυνοι συμμόρφωσης, τόσο υψηλότερο είναι το επίπεδο ευαισθητοποίησης, γνώσης και κατανόησης καθώς και η αίσθηση του καθήκοντος συμμόρφωσης που δημιουργείται στον οργανισμό ή την επιχείρηση που τους απασχολεί (Parker, Rosen & Nielsen, 2009).

Η ΑΠΔΠΧ έχει αναρτήσει μια λίστα προτεινόμενων τεχνικών και οργανωτικών μέτρων, τα οποία χωρίζονται σε τρεις κατηγορίες, τα οργανωτικά μέτρα, τα τεχνικά μέτρα ασφάλειας και τα μέτρα φυσικής ασφάλειας. Ενδεικτικά, ως οργανωτικά μέτρα ασφαλείας προτείνονται η εκπαίδευση του προσωπικού, ο τακτικός έλεγχος και η καταστροφή δεδομένων και αποθηκευτικών μέσων. Ως τεχνικά μέτρα ασφαλείας, ο έλεγχος πρόσβασης, η τήρηση αντιγράφων ασφαλείας (back-up), η τήρηση αρχείων καταγραφής ενεργειών χρηστών και συμβάντων ασφαλείας. Τέλος, ως μέτρα φυσικής ασφαλείας προτείνονται ο έλεγχος φυσικής πρόσβασης και η προστασία φορητών μέσων αποθήκευσης. Πέρα από την εφαρμογή, απαιτείται η πρόβλεψη μιας διαδικασίας για την τακτική δοκιμή, εκτίμηση και

αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.

Ειδικότερα για τους επαγγελματίες ψυχικής υγείας, ενδεικτικά οργανωτικά μέτρα είναι η διαμόρφωση του χώρου όπου διενεργούνται οι συνεδρίες με ξεχωριστή είσοδο και έξοδο καθώς και η μη αναφώνηση του ονόματος του ασθενούς από τη γραμματεία (Joseph & Onek, 1991). Επίσης, δεν ενθαρρύνεται η αποστολή εμπιστευτικών πληροφοριών μέσω ηλεκτρονικού ταχυδρομείου, φαξ ή άλλων ηλεκτρονικών μέσων διότι είναι πιθανό να παραληφθεί από τρίτο, ειδικά στην περίπτωση του φαξ και του αυτόματου τηλεφωνητή που δεν υπάρχει προσωπικός κωδικός πρόσβασης (Αλεβίζος, 2008).

Πρότυπα ασφαλείας, όπως το ISO 27001 και το ISO 27002, βοηθούν τους οργανισμούς να διασφαλίσουν ότι διαθέτουν αποτελεσματικές μεθόδους ασφάλειας των δεδομένων. Το ISO 27001 δημιουργήθηκε αρχικά με σκοπό να συμβάλει στη διαχείριση της ασφάλειας των κυβερνητικών υπηρεσιών και των δεδομένων των πολιτών από τους παρόχους υπηρεσιών. Η χρήση του ISO 27001 συμβάλει στην εξασφάλιση της αρχής που περιέχεται στον ΓΚΠΔ, ότι υπάρχουν κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία των προσωπικών δεδομένων και συνάμα βοηθά τον υπεύθυνο επεξεργασίας να εντοπίσει τους ρόλους και τις αντίστοιχες ευθύνες, όπως για παράδειγμα ποιός μπορεί να επιτρέψει την πρόσβαση σε δεδομένα. Η χρήση τους δεν συνεπάγεται βέβαια την πλήρη συμμόρφωση με τις απαιτήσεις του Κανονισμού αλλά συμβάλλει σημαντικά στις διαδικασίες που πρέπει να θεσπίσει ο υπεύθυνος επεξεργασίας για να ανταποκριθεί σε αυτές (Tankard, 2016).

2.6.3 Υποχρέωση γνωστοποίησης της παραβίασης

Μέχρι την εφαρμογή του ΓΚΠΔ δεν υπήρχε στα κράτη μέλη της ΕΕ ενιαία νομοθεσία σχετικά με την κοινοποίηση περιστατικού παραβίασης. Σε ορισμένα κράτη μέλη προβλεπόταν η υποχρέωση κοινοποίησης της παραβίασης, όμως στα περισσότερα όχι. Ο ΓΚΠΔ εισάγει την υποχρέωση κοινοποίησης της παραβίασης στη αρμόδια εποπτική αρχή εντός 72 ωρών από τη στιγμή που το περιστατικό έγινε αντιληπτό και την ενημέρωση των υποκειμένων των δεδομένων όταν πρόκειται για παραβίαση η οποία ενέχει υψηλό κίνδυνο για τα υποκείμενα. Η υποχρέωση αυτή δεν υφίσταται εάν η παραβίαση δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων (άρθρο 33 §1).

Ανεξάρτητα από το εάν η παραβίαση πρέπει να γνωστοποιηθεί στην εποπτική αρχή, ο υπεύθυνος επεξεργασίας πρέπει να τηρεί αρχεία για όλες τις παραβιάσεις, το οποίο περιλαμβάνει τα πραγματικά περιστατικά που αφορούν την παραβίαση δεδομένων προσωπικού χαρακτήρα, τις συνέπειες και τα ληφθέντα διορθωτικά μέτρα (άρθρο 33 §5).

Οι κυρώσεις έχουν γίνει αρκετά πιο αυστηρές σε σχέση με τον προηγούμενο καθεστώς. Είναι χαρακτηριστικό το γεγονός ότι το μεγαλύτερο πρόστιμο που έχει επιβληθεί από την ΑΠΔΠΧ με το παλαιότερο καθεστώς αφορά περιστατικό παραβίασης προσωπικών δεδομένων στη Γενική Γραμματεία Πληροφοριακών Συστημάτων. Η ΑΠΔΠΧ επέβαλε πρόστιμο ύψους 150.000 Ευρώ θεωρώντας ότι η Γενική Γραμματεία Πληροφοριακών Συστημάτων παραβίασε την υποχρέωσή της για λήψη κατάλληλων μέτρων ασφάλειας, γεγονός που οδήγησε σε ιδιαίτερα σοβαρό περιστατικό παραβίασης προσωπικών δεδομένων, δηλαδή σε διαρροή δεδομένων που αφορούν το σύνολο σχεδόν των φορολογουμένων στην Ελλάδα (Απόφαση ΑΠΔΠΧ 98/2013).

Με το νέο καθεστώς, για μια παραβίαση, οι οργανισμοί μπορεί να κληθούν να καταβάλουν πρόστιμο έως 10.000.000 EUR ή, σε περίπτωση επιχειρήσεων, έως το 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο. Για πιο σοβαρές παραβιάσεις, μπορεί να επιβληθεί διοικητικό πρόστιμο έως 20.000.000 EUR ή, σε περίπτωση επιχειρήσεων, έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου

εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο (Tankard, 2016).

2.6.4 Τα δικαιώματα των υποκειμένων

Ο ΓΚΠΔ εισάγει ορισμένα νέα δικαιώματα των υποκειμένων και ενισχύει κάποια από τα προϋπάρχοντα, ενδυναμώνοντας με αυτό τον τρόπο τη θέση των υποκειμένων.

Ενημέρωση: Υποχρεώνει τον υπεύθυνο επεξεργασίας να παρέχει στο υποκείμενο των δεδομένων κάθε πληροφορία σχετικά με την επεξεργασία των προσωπικών δεδομένων καθώς και τα στοιχεία επικοινωνίας του σε κατανοητή μορφή (Tikkinen-Piri, 2018). Οι πληροφορίες αυτές περιλαμβάνουν τα στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας και του ΥΠΔ, τους σκοπούς της επεξεργασίας και τη νομιμοποιητική της βάση, τους αποδέκτες των δεδομένων, το χρόνο τήρησης, τα δικαιώματα του υποκειμένου συμπεριλαμβανομένου του δικαιώματος καταγγελίας στην αρμόδια εποπτική αρχή κ.α. (άρθρο 13). Οι πληροφορίες αυτές θα πρέπει να παρέχονται στο υποκείμενο κατά τη συλλογή των προσωπικών του δεδομένων, ενώ εάν τα δεδομένα έχουν συλλεγεί από άλλη πηγή, εντός ενός μήνα από τη συλλογή τους (Working Party 29, 2018).

Από το δικαίωμα της ενημέρωσης υπάρχουν ορισμένες εξαιρέσεις οι οποίες πρέπει να ερμηνεύονται συσταλτικώς. Συγκεκριμένα, δεν υπάρχει υποχρέωση ενημέρωσης εφόσον το υποκείμενο διαθέτει ήδη τις πληροφορίες. Εάν τα δεδομένα συλλέγονται από άλλες πηγές δεν είναι υποχρεωτική η ενημέρωση εάν η παροχή των πληροφοριών είναι αδύνατη ή θα συνεπαγόταν δυσανάλογη προσπάθεια, ιδίως όταν πρόκειται για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς. Το ίδιο ισχύει και στην περίπτωση που η ενημέρωση «είναι πιθανόν να καταστήσει αδύνατη ή να βλάψει σε μεγάλο βαθμό την επίτευξη των σκοπών της εν λόγω επεξεργασίας». Κάθε επιχείρηση ή οργανισμός που διατηρεί έναν ιστότοπο θα πρέπει να δημοσιεύει στον ιστότοπο μια δήλωση σχετικά με την προστασία προσωπικών δεδομένων, τη συνήθως αποκαλούμενη «Πολιτική Ασφαλείας» ή «Πολιτική Προστασίας Προσωπικών Δεδομένων». Με τον τρόπο αυτό, το υποκείμενο αποκτά εύκολη πρόσβαση στην ενημέρωση που απαιτείται από τον ΓΚΠΔ (Working Party 29, 2018).

Πρόσβαση: Ο υπεύθυνος επεξεργασίας είναι υποχρεωμένος κατόπιν αιτήματος του υποκειμένου να επιβεβαιώσει το υποκείμενο σχετικά με την

επεξεργασία των δεδομένων του και να του παράσχει αντίγραφο αυτών των δεδομένων (άρθρα 12, 15). Θεμελιώδης έκφραση του δικαιώματος στην προστασία των προσωπικών δεδομένων, ως απόρροια της αρχής της διαφάνειας, είναι το δικαίωμα του υποκειμένου των δεδομένων να αποκτά πρόσβαση στα δεδομένα υγείας του, όπως τα αποτελέσματα των εξετάσεων, τις γνωματεύσεις των θεραπόντων ιατρών, τη θεραπεία ή επέμβαση (Λάτσιου, 2017).

Η ΑΠΔΠΧ έχει κρίνει ότι σε περιπτώσεις κατά τις οποίες ασκείται το δικαίωμα πρόσβασης από γονέα ανηλίκου, αυτό πρέπει να ικανοποιείται εφόσον ο γονέας έχει τη γονική μέριμνα του ανηλίκου. Ο γονέας ως ασκών από κοινού με το σύζυγο/εν διαστάσει σύζυγο του τη γονική μέριμνα των ανήλικων τέκνων τους, ταυτίζεται με τα υποκείμενα των επίμαχων δεδομένων προσωπικού χαρακτήρα (ΑΠΔΠΧ 18/2018 και 130/2013).

Για την κοινολόγηση δεδομένων υγείας, όπως το είδος των ιατρικών εξετάσεων ή τα περιεχόμενα του ιατρικού φακέλου ασθενούς σε τρίτο ακόμη κι αν πρόκειται για οικείο του ασθενούς (υποκειμένου), απαιτείται κατ' αρχήν η ενημέρωση του ασθενούς.

Διόρθωση: Το δικαίωμα διόρθωσης αφορά τη διόρθωση των εσφαλμένων στοιχείων ή τη συμπλήρωση των ελλιπών.

Διαγραφή: Το «δικαίωμα στη λήθη» είναι μια «αποκρυστάλλωση» της πιο θεμελιώδους επιθυμίας για «έλεγχο» των προσωπικών δεδομένων (Ausloos, 2012). Ο ΓΚΠΔ θετικοποιεί το προϋπάρχον δικαίωμα στη λήθη που αποτελεί μια εκδήλωση της ελεύθερης ανάπτυξης της προσωπικότητας του ατόμου (άρθρο 17). Συνίσταται στο δικαίωμα του ατόμου να διαγράψει από το διαδίκτυο δεδομένα που δεν επιθυμεί να παραμένουν δημοσιευμένα και δεν είναι χρήσιμα για την ενημέρωση του κοινού (Παναγοπούλου - Κουτνατζή, 2017). Επίσης, είναι το δικαίωμα των ατόμων να μην επεξεργάζονται πλέον τα δεδομένα τους και να διαγράφονται όταν δεν χρειάζονται πλέον για νόμιμους σκοπούς (European Commission, 2010). Το δικαίωμα διαγραφής συντρέχει με την υποχρέωση διαγραφής (ΑΠΔΠΧ, 2018).

Περιπτώσεις στις οποίες επιβάλλεται η διαγραφή είναι όταν η επεξεργασία ήταν παράνομη, τα δεδομένα δεν είναι πλέον αναγκαία σε σχέση με το σκοπό για τον οποίο συλλέχθηκαν, έχει γίνει ανάκληση της συγκατάθεσης και δεν υπάρχει άλλη νομιμοποιητική βάση επεξεργασίας, έχει προηγηθεί η άσκηση δικαιώματος εναντίωσης, τα δεδομένα συλλέχθηκαν κατά την παροχή υπηρεσίας της κοινωνίας της

πληροφορίας σε παιδί -ακόμη και όταν το δικαίωμα ασκείται από ενήλικα ή όταν πρόκειται για συμμόρφωση του υπεύθυνου επεξεργασίας με υποχρέωσή που πηγάζει εκ του νόμου (άρθρο 17).

Η διαγραφή των δεδομένων από συστήματα back-up δεν είναι απαραίτητη εφόσον τα δεδομένα δεν πρόκειται να χρησιμοποιηθούν για άλλο σκοπό και έχουν ληφθεί μέτρα για την αυτοματοποιημένη διαγραφή τους σε ορισμένο χρονικό διάστημα. Σε κάθε περίπτωση όμως, ο υπεύθυνος επεξεργασίας θα πρέπει να έχει προβλέψει διαδικασίες για την ασφαλή διαγραφή των δεδομένων του υποκειμένου που έχει ασκήσει νόμιμα το δικαίωμά του. Σύμφωνα με τον εφαρμοστικό νόμο (Ν. 4624/2019), «αν η διαγραφή σε περίπτωση μη αυτοματοποιημένης επεξεργασίας λόγω της ιδιαίτερης φύσης της αποθήκευσης δεν είναι δυνατή ή είναι δυνατή μόνο με δυσανάλογα μεγάλη προσπάθεια και το συμφέρον του υποκειμένου των δεδομένων για τη διαγραφή δεν θεωρείται σημαντικό, δεν υφίσταται το δικαίωμα του υποκειμένου και η υποχρέωση του υπεύθυνου επεξεργασίας να διαγράψει τα δεδομένα».

Περιορισμός της επεξεργασίας: Το δικαίωμα στον περιορισμό της επεξεργασίας ασκείται από το υποκείμενο όταν έχει ασκήσει ήδη αίτημα διόρθωσης π.χ. λόγω ανακρίβειας των δεδομένων του και ο υπεύθυνος επεξεργασίας εξετάζει το σχετικό αίτημα ή όταν η επεξεργασία είναι παράνομη ή όταν τα δεδομένα δεν είναι απαραίτητα πλέον για τον σκοπό της επεξεργασίας, αλλά το υποκείμενο ζητά την τήρησή τους για την άσκηση και υπεράσπιση νομικών του αξιώσεων. Επίσης, ασκείται όταν το υποκείμενο έχει ήδη ασκήσει δικαίωμα εναντίωσης.

Δεν πρόκειται για απόλυτο δικαίωμα καθώς ασκείται συνδυαστικά με τα δικαιώματα εναντίωσης ή διόρθωσης. Ο ΓΚΠΔ προτείνει πολλούς τρόπους περιορισμού της επεξεργασίας. Ενδεικτικά, τα δεδομένα μπορούν να μεταφερθούν προσωρινά σε άλλο σύστημα, να αποκλειστεί η πρόσβαση των χρηστών στα δεδομένα ή να μην είναι προσωρινά δημοσιευμένα στην ιστοσελίδα.

Φορητότητα: Το δικαίωμα στη φορητότητα είναι το δικαίωμα των υποκειμένων να λαμβάνουν τα δεδομένα προσωπικού χαρακτήρα που τα αφορούν, καθώς και το δικαίωμα να διαβιβάζουν τα εν λόγω δεδομένα σε άλλο υπεύθυνο επεξεργασίας. Πρόκειται για μια πλήρη καινοτομία του νέου νομοθετικού πλαισίου, δεδομένου ότι δεν υπάρχουν αντίστοιχες αναφορές σε παλαιότερη ευρωπαϊκή

νομοθεσία, πέραν αυτής των παρόχων τηλεπικοινωνιών. Η φορητότητα των αριθμών τηλεφώνου αποτελεί πρόδρομο του δικαιώματος που εισάγεται με τον ΓΚΠΔ.

Ο υπεύθυνος επεξεργασίας δεδομένων μπορεί να αποτρέψει την πλήρη άσκηση του δικαιώματος των χρηστών για φορητότητα των δεδομένων, εφόσον αποδείξει ότι το επίπεδο της τεχνολογικής ανάπτυξης του οργανισμού του καθιστά τεχνικά ανέφικτη την άμεση διαβίβαση των δεδομένων σε άλλο υπεύθυνο επεξεργασίας, για παράδειγμα, επειδή δεν υπάρχει διαλειτουργικότητα των συστημάτων, η οποία ενθαρρύνεται, αλλά δεν επιβάλλεται (De Hert et al, 2018). Με άλλα λόγια, το δικαίωμα μεταφοράς δεδομένων είναι σχεδιασμένο ως ένα μέσο για την ενίσχυση του ελέγχου των ατόμων σε προσωπικά δεδομένα.

Εναντίωση: Το υποκείμενο των δεδομένων δικαιούται να αντιτάσσεται οποτεδήποτε στην επεξεργασία των προσωπικών του δεδομένων, όταν η νομική βάση της επεξεργασίας είναι η εκπλήρωση σκοπού δημοσίου συμφέροντος ή η ικανοποίηση εννόμου συμφέροντος. Το δικαίωμα αυτό δεν μπορεί να ασκηθεί έναντι δημόσιου φορέα, όταν το δημόσιο συμφέρον υπερτερεί του δικαιώματος του υποκειμένου (Ν. 4624/2019).

2.7 Σκοπός της έρευνας και υποθέσεις

Η παρούσα μελέτη επιδιώκει να διερευνήσει, αφενός, το επίπεδο της ενημέρωσης, κατανόησης και συμμόρφωσης των επαγγελματιών ψυχικής υγείας και νομικής επιστήμης με τις αρχές που διέπουν το δίκαιο προστασίας προσωπικών δεδομένων, από την εφαρμογή του ΓΚΠΔ μέχρι σήμερα και αφετέρου να εντοπίσει τις διαφορές (εάν υπάρχουν) στη λήψη των κατάλληλων μέτρων μεταξύ των δυο επαγγελματικών κατηγοριών. Επομένως, διατυπώσαμε τις εξής υποθέσεις:

1) Η παράμετρος ενημέρωση/γνώση του ΓΚΠΔ θα συσχετίζεται θετικά με τη λήψη τεχνικών και οργανωτικών μέτρων.
2) Οι δικηγόροι θα είναι περισσότερο ενημερωμένοι για τα ζητήματα προστασίας προσωπικών δεδομένων συγκριτικά με τους επαγγελματίες ψυχικής υγείας.
3) Οι επαγγελματίες ψυχικής υγείας θα λαμβάνουν περισσότερα τεχνικά και οργανωτικά μέτρα συγκριτικά με τους δικηγόρους.

3. Ερευνητικό Μέρος / Μεθοδολογία

3.1 Δείγμα

Συνολικά 136 άτομα ηλικίας 24-65 ετών (Μ.Ο = 36,80, Τ.Α= 9,46) τα οποία προέρχονταν από τον γενικό πληθυσμό της Ελλάδος και τα οποία επιλέχθηκαν με την μέθοδο της διαθεσιμότητας συμμετείχαν στην παρούσα μελέτη. Για τις ανάγκες της έρευνας, εξετάστηκαν δυο ομάδες βασιζόμενες στην επαγγελματική ιδιότητα των συμμετεχόντων όπως αυτή των επαγγελματιών ψυχικής υγείας και αυτή των δικηγόρων.

Ομάδα Επαγγελματιών Ψυχικής Υγείας: Πενήντα τρεις επαγγελματίες ψυχικής υγείας, 11 άνδρες (20,8%) και 42 γυναίκες (79,2%) ηλικίας 24-65 ετών (Μ.Ο = 33,91, Τ.Α= 9,35) έλαβαν μέρος στην έρευνα. Πιο συγκεκριμένα, 46 άτομα (86,8%) ήταν ψυχολόγοι και 7 άτομα (13,2%) ψυχίατροι. Αναφορικά με το επίπεδο σπουδών τους, το 69,8% (n=37) δήλωσε ότι είναι κάτοχος μεταπτυχιακού, το 20,8% (n=11) δήλωσε ότι κατέχει το βασικό τίτλο σπουδών, το 5,7% (n=3) δήλωσε ότι έχει κάνει διδακτορικό ενώ το 3,8%(n=2) δήλωσε ότι έχει κάνει μεταδιδακτορικό. Επίσης, όσον αφορά το είδος απασχόλησης των ερωτηθέντων, 13 άτομα (24,5%) ανέφεραν ότι είναι απασχολούμενοι στο δημόσιο τομέα, 8 άτομα (15,1%) ότι εργάζονται στον ιδιωτικό τομέα και 32 άτομα (60,4%) ανέφεραν ότι εργάζονται ως αυτοαπασχολούμενοι.

Ομάδα Δικηγόρων: Ογδόντα τρεις δικηγόροι, 17 άνδρες (20,5%) και 66 γυναίκες (79,5%) ηλικίας 25-64 ετών (Μ.Ο = 38,65, Τ.Α= 9,11) συμμετείχαν στην έρευνα. Αναφορικά με το επίπεδο σπουδών τους, το 68,7% (n=57) δήλωσε ότι είναι κάτοχος μεταπτυχιακού, το 25,3% (n=21) δήλωσε ότι κατέχει το βασικό τίτλο

σπουδών και το 6,0% (n=5) δήλωσε ότι έχει κάνει διδακτορικό. Επίσης, όσον αφορά το είδος απασχόλησης των ερωτηθέντων, 5 άτομα (6,0%) ανέφεραν ότι είναι απασχολούμενοι στο δημόσιο τομέα, 17 άτομα (20,5%) ότι εργάζονται στον ιδιωτικό τομέα και 61 άτομα (73,5%) ανέφεραν ότι εργάζονται ως αυτοαπασχολούμενοι.

3.2 Μέσα συλλογής δεδομένων

Ερωτηματολόγιο Συμμόρφωσης με τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR Compliance): Αποτελείται συνολικά από 19 ερωτήσεις που εξετάζουν τον βαθμό συμμόρφωσης των συμμετεχόντων με τις επιταγές του κανονισμού σε ζητήματα προστασίας προσωπικών δεδομένων. Για τις ανάγκες της παρούσας έρευνας, εξάγει ένα συνολικό σκορ από το άθροισμα των 4 ερωτήσεων (1,3,5,18) που αξιολογούν την ενημέρωση/γνώση του ΓΚΠΔ, καθώς και ένα συνολικό σκορ από το άθροισμα των 6 ερωτήσεων (6,13,14,15,17,19) που αξιολογούν τον βαθμό λήψης τεχνικών/οργανωτικών μέτρων. Για παράδειγμα, μια ερώτηση που αφορά την ενημέρωση/γνώση του ΓΚΠΔ είναι «Έχετε λάβει κάποια εκπαίδευση σχετικά με την προστασία προσωπικών δεδομένων;». Παρομοίως, μια ερώτηση που αφορά την λήψη τεχνικών/οργανωτικών μέτρων είναι «Χρησιμοποιείτε μεθόδους ανωνυμοποίησης, ψευδωνυμοποίησης ή κρυπτογράφησης;». Η βαθμολόγηση των απαντήσεων γίνεται σε μία κλίμακα τύπου Likert κυμαινόμενη από το 1 έως το 4 (1= Καθόλου και 4 = Απολύτως) με την υψηλή βαθμολογία να αντιστοιχεί σε περισσότερη ενημέρωση/γνώση του ΓΚΠΔ και στη λήψη περισσότερων τεχνικών/οργανωτικών μέτρων αντίστοιχα. Στη συγκεκριμένη μελέτη, οι δείκτες αξιοπιστίας εσωτερικής συνέπειας για τις διαστάσεις της GDPR συμμόρφωσης βρέθηκαν να είναι οι εξής: ενημέρωση/γνώση του ΓΚΠΔ $\alpha = 0,82$ και λήψη τεχνικών/οργανωτικών μέτρων $\alpha = 0,83$.

3.3 Διαδικασία

Εξαιτίας της έλλειψης ενός εργαλείου που να μετράει την γνώση και συμμόρφωση με τον ΓΚΠΔ σε γενικό επίπεδο, το παρόν ερωτηματολόγιο αποτελεί μια αρχική προσπάθεια της ερευνήτριας μέσα από την εμπειρία της και την ενδελεχή ανασκόπηση της βιβλιογραφίας επί του αντικειμένου της έρευνας, να αποτυπώσει σε ορισμένες ερωτήσεις ένα βασικό επίπεδο γνώσης και συμμόρφωσης με τον ΓΚΠΔ, προσαρμοσμένο στις ιδιαιτερότητες των υπό εξέταση ειδικοτήτων. Για παράδειγμα, για τους επαγγελματίες ψυχικής υγείας χρησιμοποιήθηκαν όροι όπως ασθενείς, θεραπευτικές συνεδρίες, κλπ. ενώ για τους δικηγόρους όροι όπως εντολείς. Το ερωτηματολόγιο αποτελείται από πέντε ερωτήσεις που αφορούν δημογραφικά στοιχεία, υπό τον τίτλο «Δημογραφικά Στοιχεία» και δεκαεννέα ερωτήσεις που αφορούν ζητήματα ενημέρωσης και εναρμόνισης με τις απαιτήσεις του ΓΚΠΔ, υπό τον τίτλο «GDPR COMPLIANCE». Πιο συγκεκριμένα, τέσσερις εξ' αυτών αφορούν την ενημέρωση γύρω από το νέο νομοθετικό πλαίσιο και έξι εξ' αυτών αφορούν τη συμμόρφωση με τις απαιτήσεις του ΓΚΠΔ, ενώ οι λοιπές είναι γενικές ερωτήσεις, όπως για παράδειγμα «Έχει ορίσει η Διοίκηση του φορέα στον οποίο εργάζεστε Υπεύθυνο Προστασίας Προσωπικών Δεδομένων;»

. Έχει ληφθεί η συγκατάθεση των συμμετεχόντων για τη συμμετοχή στην έρευνα πριν τη συμπλήρωση του ερωτηματολογίου. Τα δεδομένα που συλλέχθηκαν είναι ανώνυμα και δεν ταυτοποιούν τα φυσικά πρόσωπα που συμμετείχαν στην έρευνα.

Η συλλογή του δείγματος της έρευνας έγινε με ηλεκτρονικά μέσα από την κοινότητα. Το ερωτηματολόγιο δημιουργήθηκε μέσω της φόρμας Google Docs και διανεμήθηκε σε μεμονωμένους επαγγελματίες και ομάδες επαγγελματιών μέσα από κοινωνικά δίκτυα (LinkedIn, Facebook) από τον Αύγουστο 2019 έως τον Σεπτέμβριο 2019.

Η διαδικασία διαρκούσε κατά μέσο όρο από πέντε έως δέκα λεπτά, ανάλογα με την εξοικείωση των συμμετεχόντων με το αντικείμενο της έρευνας.

3.4 Στατιστική επεξεργασία

Ο έλεγχος κανονικότητας έδειξε ότι τα δεδομένα μας δεν σχηματίζουν κανονική κατανομή, με αποτέλεσμα η ανάλυση να πραγματοποιηθεί με την εφαρμογή μη παραμετρικών δοκιμασιών. Πιο συγκεκριμένα, για τη συσχέτιση ανάμεσα στην ενημέρωση/γνώση του ΓΚΠΔ και τη λήψη τεχνικών και οργανωτικών μέτρων, χρησιμοποιήθηκε ο συντελεστής συσχέτισης Spearman rho. Επίσης, όσον αφορά τις διαφορές στην ενημέρωση/γνώση του ΓΚΠΔ και τη λήψη τεχνικών και οργανωτικών μέτρων ανάμεσα στους δικηγόρους και στους επαγγελματίες ψυχικής υγείας εφαρμόστηκε η δοκιμασία των Mann-Whitney για ανεξάρτητα δείγματα.

3.5 Αποτελέσματα έρευνας

3.6.1 Περιγραφική Ανάλυση

Στον Πίνακα 1 παρουσιάζονται οι περιγραφικοί στατιστικοί δείκτες του δείγματος (διάμεσος τιμή και εύρος) για τις παραμέτρους της ενημέρωσης/γνώσης του ΓΚΠΔ και της λήψης τεχνικών/οργανωτικών μέτρων τόσο στους επαγγελματίες ψυχικής υγείας (n=53) όσο και στους δικηγόρους (n=83). Γενικά, οι επαγγελματίες ψυχικής υγείας φαίνεται να παρουσιάζουν υψηλότερη βαθμολογία μόνο στην παράμετρο της λήψης τεχνικών/οργανωτικών μέτρων συγκριτικά με τους δικηγόρους.

Πίνακας 1

Περιγραφικοί στατιστικοί δείκτες (διάμεσος και εύρος) για τις παραμέτρους της ενημέρωσης/γνώσης του ΓΚΠΔ και της λήψης τεχνικών/οργανωτικών μέτρων στους επαγγελματίες ψυχικής υγείας και στους δικηγόρους (N=136).

	Διάμεσος	Εύρος
Επαγγελματίες ψυχικής υγείας (n=53)		
Ενημέρωση/γνώση	8,00	12
Τεχνικά/Οργανωτικά μέτρα	16,00	15
Δικηγόροι (n=83)		
Ενημέρωση/γνώση	8,00	12
Τεχνικά/Οργανωτικά μέτρα	14,00	17

Παρακάτω και καθαρά για περιγραφικούς λόγους παρατίθεται ο πίνακας κατανομής συχνοτήτων (Πίνακας 2) ορισμένων ερωτήσεων που διερευνούν την συμμόρφωση τόσο των επαγγελματιών ψυχικής υγείας όσο και των δικηγόρων σε

ζητήματα προστασίας προσωπικών δεδομένων. Πιο συγκεκριμένα, στην ερώτηση που διερευνά αν η διοίκηση του φορέα που εργάζονται οι συμμετέχοντες έχει ορίσει ΥΠΔ, 22 επαγγελματίες ψυχικής υγείας (41,5%) και 40 δικηγόροι (48,2%) απάντησαν πώς δεν έχει οριστεί κάποιος ΥΠΔ από τον φορέα τον οποίο εργάζονται. Επιπλέον, στην ερώτηση που διερευνά την εφαρμογή κάποιας πιστοποίησης (ISO 27799) από τον φορέα απασχόλησης των ερωτηθέντων, το 45,3% των επαγγελματιών ψυχικής υγείας (n=24) και το 66,3% των δικηγόρων αντιστοίχως (n=55) απάντησε αρνητικά, ότι δηλαδή δεν χορηγείται κάποιο είδος πιστοποίησης από τον φορέα απασχόλησης των συμμετεχόντων. Επίσης, σχετικά με την ερώτηση που διερευνά την γραπτή ενημέρωση των υποκειμένων (ασθενείς, εντολείς) για τα δικαιώματα τους πριν την καταγραφή των προσωπικών δεδομένων τους, τόσο οι επαγγελματίες ψυχικής υγείας (56,6%) όσο και οι δικηγόροι (36,1%) απάντησαν ότι παρέχουν έγγραφη ενημέρωση στους ασθενείς/πελάτες σχετικά με τα δικαιώματα τους. Παρομοίως και αναφορικά με την δυνατότητα των υποκειμένων να ζητήσουν πρόσβαση στα προσωπικά τους δεδομένα μέσω κάποιας έντυπης φόρμας ή μέσω e-mail, το 75,5% των επαγγελματιών ψυχικής υγείας (n=40) και το 63,9% των δικηγόρων (n=53) απάντησαν θετικά, ότι δηλαδή παρέχουν πρόσβαση στα προσωπικά δεδομένα των ασθενών/εντολέων τους έπειτα από δική τους απαίτηση.

Πίνακας 2

Πίνακας κατανομής συχνοτήτων σε ερωτήσεις που διερευνούν την συμμόρφωση σε ζητήματα προστασίας προσωπικών δεδομένων στους επαγγελματίες ψυχικής υγείας και στους δικηγόρους (N=136).

	Συχνότητα	Έγκυρο %	Αθροιστικό %
Επαγγελματίες ψυχικής υγείας (n=53)			
Υπεύθυνος Προστασίας Προσωπικών Δεδομένων:			
Ναι	17	32,1	32,1

Όχι	22	41,5	73,6
Δεν γνωρίζω	14	26,4	100,0
Εφαρμογή Πιστοποίησης (ISO 27799):			
Ναι	14	26,4	26,4
Όχι	24	45,3	71,7
Δεν γνωρίζω	15	28,3	100,0
Έγγραφη Ενημέρωση των Δικαιωμάτων των Υποκειμένων:			
Ναι	30	56,6	56,6
Όχι	21	39,6	96,2
Δεν γνωρίζω	2	3,8	100,0
Πρόσβαση στα Προσωπικά δεδομένα των Υποκειμένων:			
Ναι	40	75,5	75,5
Όχι	4	7,5	83,0
Δεν γνωρίζω	9	17,0	100,0

Δικηγόροι (n=83)

Υπεύθυνος Προστασίας Προσωπικών Δεδομένων:			
Ναι	21	25,3	25,3
Όχι	40	48,2	73,5
Δεν γνωρίζω	22	26,5	100,0
Εφαρμογή Πιστοποίησης (ISO 27799):			
Ναι	6	7,2	7,2
Όχι	55	66,3	73,5
Δεν γνωρίζω	22	26,5	100,0
Έγγραφη Ενημέρωση των Δικαιωμάτων των Υποκειμένων:			
Ναι	30	36,1	36,1
Όχι	48	57,8	94,0
Δεν γνωρίζω	5	6,0	100,0

Πρόσβαση στα Προσωπικά δεδομένα των Υποκειμένων:			
Ναι	53	63,9	63,9
Όχι	21	25,3	89,2
Δεν γνωρίζω	9	10,8	100,0

Συνεχίζοντας στο ίδιο μήκος κύματος και σχετικά με την ερώτηση που αφορά την διαφοροποίηση των δικαιωμάτων πρόσβασης στα προσωπικά δεδομένα των υποκειμένων ανάλογα με την ειδικότητα του κάθε εργαζομένου, το 52,8% των επαγγελματιών ψυχικής υγείας (n=28) απάντησε πως διαφοροποιούνται τα δικαιώματα πρόσβασης στα προσωπικά δεδομένα των υποκειμένων ανάλογα με την ειδικότητα ενώ το 38,6% των δικηγόρων (n=32) ανέφερε ότι δεν υπάρχει κάποια διαφοροποίηση. Επίσης, αναφορικά με τις διαδικασίες που περιλαμβάνουν την διαγραφή ή την καταστροφή των δεδομένων έπειτα από την ολοκλήρωση της επεξεργασίας τους, το 41,5% των επαγγελματιών ψυχικής υγείας (n=22) ανέφερε ότι τηρούνται οι διαδικασίες διαγραφής ή καταστροφής των δεδομένων σε αντίθεση με το 51,8% των δικηγόρων (n=43) που απάντησαν ότι δεν τηρούνται οι διαδικασίες διαγραφής ή καταστροφής των δεδομένων. Εν συνεχεία και σχετικά με τα προσωπικά δεδομένα που αφορούν ανηλίκους, το 45,3% των επαγγελματιών ψυχικής υγείας (n=24) ανέφερε ότι τηρεί προσωπικά δεδομένα ανηλίκων ενώ το 51,8% των δικηγόρων (n=43) δήλωσε ότι δεν τηρεί καθόλου προσωπικά δεδομένα ανηλίκων. Τέλος, όσον αφορά την χρήση τηλεδιάσκεψης μέσω skype, το 56,6% των επαγγελματιών ψυχικής υγείας (n=30) ανέφερε ότι δεν διενεργεί θεραπευτικές συνεδρίες με τους ασθενείς του μέσω τηλεδιάσκεψης και το 79,5% των δικηγόρων (n=66) ότι δεν επικοινωνεί με τους εντολείς του μέσω τηλεδιάσκεψης αντιστοίχως (Πίνακας 3).

Πίνακας 3

Πίνακας κατανομής συχνοτήτων σε ερωτήσεις που διερευνούν την συμμόρφωση σε ζητήματα προστασίας προσωπικών δεδομένων στους επαγγελματίες ψυχικής υγείας και στους δικηγόρους (N=136).

	Συχνότητα	Έγκυρο %	Αθροιστικό %
Επαγγελματίες ψυχικής υγείας (n=53)			
Διαφοροποίηση στη Πρόσβαση Προσωπικών Δεδομένων :			
Ναι	28	52,8	52,8
Όχι	11	20,8	73,6
Δεν γνωρίζω	14	26,4	100,0
Διαδικασίες Διαγραφής/Καταστροφής Δεδομένων:			
Ναι	22	41,5	41,5
Όχι	20	37,7	79,2
Δεν γνωρίζω	11	28,8	100,0
Τήρηση Προσωπικών Δεδομένων Ανηλίκων:			
Καθόλου	10	18,9	18,9
Λίγο	9	17,0	35,8
Αρκετά	10	18,9	54,7
Απολύτως	24	45,3	100,0
Χρήση Τηλεδιάσκεψης (skype):			
Καθόλου	30	56,6	56,6
Λίγο	6	11,3	11,3
Αρκετά	9	17,0	84,9
Απολύτως	8	15,1	100,0
Δικηγόροι (n=83)			
Διαφοροποίηση στη Πρόσβαση Προσωπικών Δεδομένων :			
Ναι	17	20,5	20,5
Όχι	32	38,6	59,0

Δεν γνωρίζω	34	41,0	100,0
Διαδικασίες Διαγραφής/Καταστροφής Δεδομένων:			
Ναι	32	38,6	38,6
Όχι	43	51,8	90,4
Δεν γνωρίζω	8	9,6	100,0
Τήρηση Προσωπικών Δεδομένων Ανηλίκων:			
Καθόλου	43	51,8	51,8
Λίγο	20	24,1	75,9
Αρκετά	11	13,3	89,2
Απολύτως	9	10,8	100,0
Χρήση Τηλεδιάσκεψης (skype):			
Καθόλου	66	79,5	79,5
Λίγο	8	9,6	89,2
Αρκετά	7	8,4	97,6
Απολύτως	2	2,4	100,0

3.6.2 Έλεγχος Υποθέσεων και Ερευνητικών Ερωτημάτων

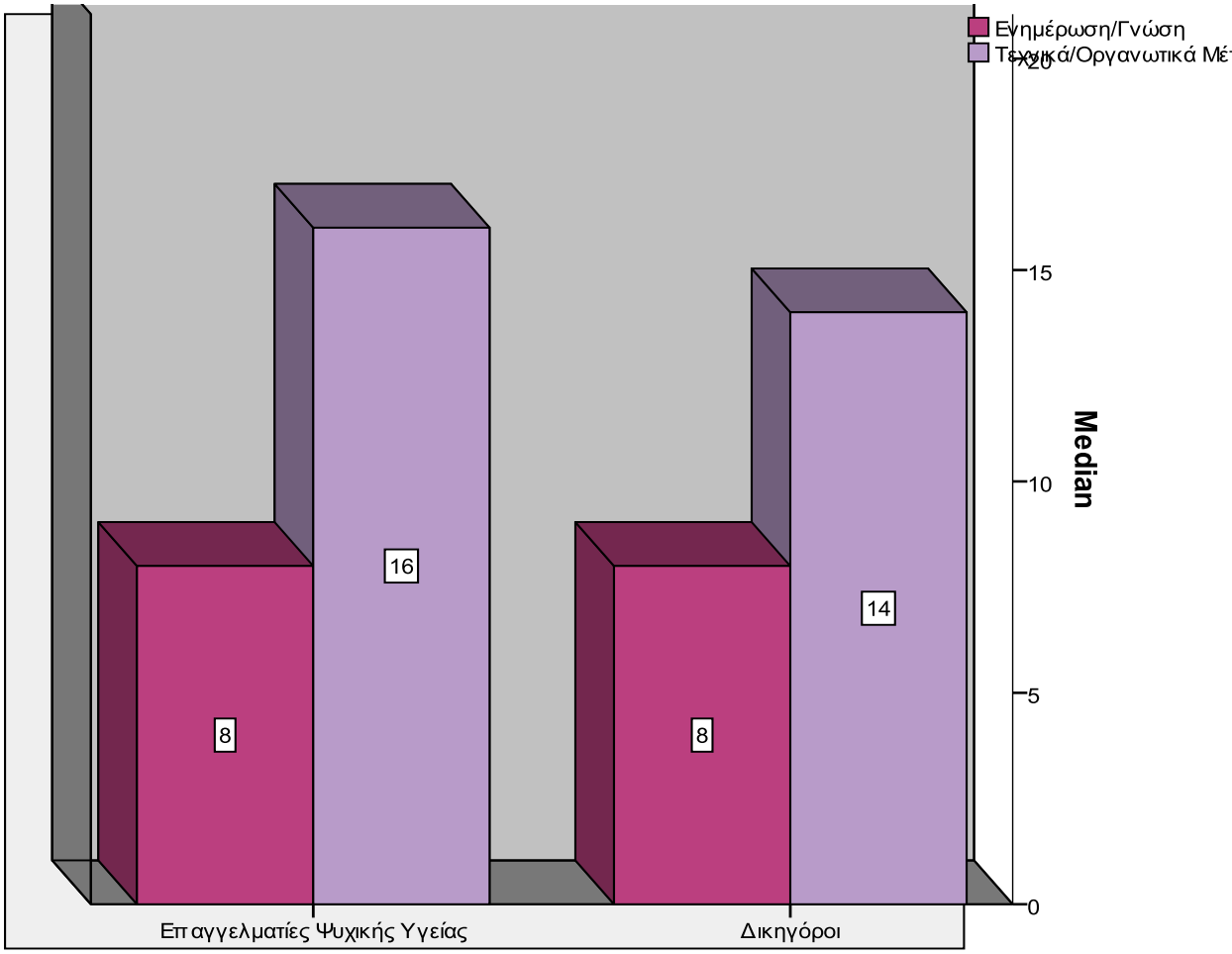
Ο έλεγχος κανονικότητας έδειξε ότι τα δεδομένα δεν σχηματίζουν κανονική κατανομή, με αποτέλεσμα η ανάλυση να πραγματοποιηθεί με την εφαρμογή μη παραμετρικών δοκιμασιών. Πιο συγκεκριμένα, οι τιμές συμμετρίας (skewness) και κύρτωσης (kurtosis) υπολογίστηκαν ως έξης: Για την παράμετρο της ενημέρωσης/γνώσης του ΓΚΠΔ, οι τιμές της συμμετρίας και κύρτωσης βρέθηκαν να είναι S= 0,48 και K=0,79 αντιστοίχως, με την τυπική τιμή της συμμετρίας να είναι στατιστικά σημαντική z = 2,34 (z <+/- 1,96) και την τυπική τιμή της κύρτωσης να μην είναι στατιστικά σημαντική z = -1,93 (z <+/- 1,96). Για την παράμετρο της λήψης τεχνικών/οργανωτικών μέτρων, οι τιμές της συμμετρίας και κύρτωσης βρέθηκαν να είναι S= -0,24 και K= -0,92 αντιστοίχως, με την τυπική τιμή της συμμετρίας να μην είναι στατιστικά σημαντική z = -1,16 (z <+/- 1,96) και την τυπική τιμή της κύρτωσης να είναι στατιστικά σημαντική z = - 2,23 (z <+/- 1,96). Επίσης, τα αποτελέσματα του Kolmogorov-Smirnov test έδειξαν ότι τα δεδομένα δεν σχηματίζουν κανονική κατανομή. Για την παράμετρο της ενημέρωσης/γνώσης του ΓΚΠΔ, τα αποτελέσματα από το Kolmogorov-Smirnov test έδειξαν ότι D (136)=0,15, p<0,001 ενώ για την παράμετρο της λήψης τεχνικών/οργανωτικών μέτρων τα αποτελέσματα από το Kolmogorov-Smirnov test έδειξαν ότι D (136)=0,09, p= 0,008.

Όσον αφορά τη διερεύνηση της πρώτης ερευνητικής μας υπόθεσης, ότι δηλαδή η παράμετρος ενημέρωση/γνώση του ΓΚΠΔ, θα συσχετίζεται θετικά με τη λήψη τεχνικών και οργανωτικών μέτρων, χρησιμοποιήθηκε ο συντελεστής συσχέτισης Spearman rho. Συγκεκριμένα, η ανάλυση έδειξε μια στατιστικά σημαντική θετική συσχέτιση μεταξύ της ενημέρωσης/γνώσης του ΓΚΠΔ και της λήψη τεχνικών και οργανωτικών μέτρων [rho(136) = 0,48, p<0,001].

Στη συνέχεια και αναφορικά με την δεύτερη ερευνητική μας υπόθεση ότι οι δικηγόροι θα είναι περισσότερο ενημερωμένοι για τα ζητήματα προστασίας προσωπικών δεδομένων συγκριτικά με τους επαγγελματίες ψυχικής υγείας, εφαρμόστηκε η δοκιμασία των Mann-Whitney για ανεξάρτητα δείγματα. Πιο συγκεκριμένα, η ανάλυση έδειξε ότι δεν υπάρχει στατιστικά σημαντική διαφορά ανάμεσα στους δικηγόρους (διάμεσος=8,00, εύρος=12) και στους επαγγελματίες

ψυχικής υγείας (διάμεσος=8,00, εύρος=12) στην ενημέρωση/γνώση του ΓΚΠΔ U(N1=53, N2=83) = 2052,50 p=0,255.

Παρομοίως και σχετικά με την τρίτη ερευνητική μας υπόθεση ότι οι επαγγελματίες ψυχικής υγείας θα λαμβάνουν περισσότερα τεχνικά και οργανωτικά μέτρα συγκριτικά με τους δικηγόρους, εφαρμόστηκε η δοκιμασία των Mann-Whitney για ανεξάρτητα δείγματα. Πιο συγκεκριμένα, η ανάλυση έδειξε ότι υπάρχει στατιστικά σημαντική διαφορά ανάμεσα στις δυο ομάδες, με τους επαγγελματίες ψυχικής υγείας να λαμβάνουν περισσότερα τεχνικά και οργανωτικά μέτρα (διάμεσος=16,00, εύρος=15) συγκριτικά με τους δικηγόρους (διάμεσος=14,00, εύρος=17), U(N1=53, N2=83) = 1597,50 p=0,003 (βλ. Σχήμα 1).



Σχήμα 1. *Γράφημα που απεικονίζει τις διαφορές στις παραμέτρους της ενημέρωσης/γνώσης του ΓΚΠΔ και της λήψης τεχνικών/οργανωτικών μέτρων μεταξύ των επαγγελματιών ψυχικής υγείας και των δικηγόρων.*

4. Συζήτηση

4.1 Συμπεράσματα

Σύμφωνα με την πρώτη υπόθεσή μας, ότι δηλαδή η παράμετρος ενημέρωση/γνώση του ΓΚΠΔ θα συσχετίζεται θετικά με τη λήψη τεχνικών και οργανωτικών μέτρων, τα ευρήματά μας επιβεβαίωσαν παλαιότερες έρευνες, οι οποίες υποστήριξαν την ύπαρξη παρόμοιων θετικών συσχετισμών.

Πιο συγκεκριμένα, η πρωτογενής έρευνα της ICAP, που διενεργήθηκε τον Δεκέμβρη του 2017 στην Ελλάδα, λίγους μήνες πριν την εφαρμογή του ΓΚΠΔ, σε 210 επιχειρήσεις και οργανισμούς διαφορετικού τομέα και μεγέθους, έδειξε ότι το 80% των επιχειρήσεων δηλώνουν ότι δεν έχουν (επαρκή) γνώση του βαθμού συμμόρφωσης τους στο Νέο Γενικό Κανονισμό Προστασίας Δεδομένων. Παρά την συνειδητοποίηση ότι απαιτούνται πολλές ενέργειες για να επιτευχθεί πλήρης συμμόρφωση, η πλειοψηφία των συμμετεχόντων στην έρευνα παρουσιάζει σημαντικό ποσοστό αβεβαιότητας όσον αφορά την κατάσταση ετοιμότητας ή το πλάνο συμμόρφωσης.

Μια στις τέσσερις επιχειρήσεις δεν γνώριζε τον ΓΚΠΔ, ενώ το 22% δε γνώριζε ούτε τον ορισμό των προσωπικών δεδομένων. Παράλληλα, το 31% αξιολογεί ως μέτριο ή ανεπαρκές το επίπεδο ασφαλείας των συστημάτων του (και κατ' επέκταση των συστημάτων για την προστασία των προσωπικών δεδομένων). Ειδικά στις τουριστικές επιχειρήσεις το ποσοστό αυξάνεται σε 40% (ICAP, 2017).

Μια πρώτη εξήγηση του γεγονότος ότι η ενημέρωση είναι ανάλογη της λήψης μέτρων προστασίας, μπορεί να είναι ότι τόσο η ομάδα των ψυχιάτρων / ψυχολόγων, όσο και η ομάδα των δικηγόρων δεσμεύονται ήδη πολύ πριν από την εφαρμογή του ΓΚΠΔ από την υποχρέωση τήρησης απορρήτου. Η ενημέρωση και εξοικείωση με

έννοιες όπως η εχεμύθεια, η εμπιστευτικότητα και τα προσωπικά δεδομένα από το στάδιο των σπουδών τους, καθώς και το γεγονός ότι οι Κώδικες Δεοντολογίας τους επισύρουν πειθαρχικές κυρώσεις σε περίπτωση παραβίασης του καθήκοντος εχεμύθειας, σαφώς επηρεάζει θετικά τη λήψη μέτρων ασφαλείας κατά την επεξεργασία προσωπικών δεδομένων.

Επιπλέον, τα διδάγματα κοινής πείρας μας οδηγούν στο συμπέρασμα ότι η γνώση και η ενημέρωση (awareness), αποτελούν ενισχυτικό παράγοντα για τη λήψη μέτρων προς αποφυγή. Εν προκειμένω, οι κυρώσεις που καλούνται τόσο οι επαγγελματίες ψυχικής υγείας όσο και οι δικηγόροι να αντιμετωπίσουν μπορεί να είναι όχι μόνο πειθαρχικές, αλλά και ποινικές, αστικές και διοικητικές. Το γεγονός ότι ο ΓΚΠΔ προβλέπει πολύ υψηλότερο ύψος διοικητικού προστίμου σε περίπτωση μη συμμόρφωσης ή παραβίασης, σε συνδυασμό με το γεγονός ότι το νέο αυτό καθεστώς αυτό-συμμόρφωσης αναγκάζει τον εκάστοτε υπεύθυνο επεξεργασίας να προβαίνει σε λήψη όλων των απαραίτητων μέτρων προληπτικά, στο πλαίσιο της αρχής της λογοδοσίας, ενισχύει περαιτέρω την τάση για εφαρμογή μέτρων σε όσους είναι ενημερωμένοι σχετικά με το νέο νομοθετικό πλαίσιο.

Η δεύτερη ερευνητική μας υπόθεση, ότι οι δικηγόροι θα είναι περισσότερο ενημερωμένοι για τα ζητήματα προστασίας προσωπικών δεδομένων συγκριτικά με τους επαγγελματίες ψυχικής υγείας, δεν καταφέραμε να την επιβεβαιώσουμε.

Σύμφωνα με παλαιότερη έρευνα σχετικά με τη συμμόρφωση των οργανισμών και των επιχειρήσεων με κανονισμούς, φαίνεται ότι οι δικηγόροι, και ειδικότερα οι δικηγόροι που εντάσσονται στο προσωπικό του οργανισμού ή της επιχείρησης και στους οποίους έχει ανατεθεί η ευθύνη για τη συμμόρφωση είναι πιο ενεργοί και υπεύθυνοι σχετικά με την εφαρμογή των μέτρων συμμόρφωσης, την ενίσχυση της γνώσης και της κατανόησης του νομοθετικού πλαισίου καθώς και την παρακολούθηση της συμμόρφωσης εντός του οργανισμού από ό, τι άλλοι υπεύθυνοι συμμόρφωσης με διαφορετική επαγγελματική ιδιότητα (π.χ. οικονομικοί διευθυντές, στελέχη επιχειρήσεων ή άλλοι υπεύθυνοι συμμόρφωσης). Η ερμηνεία αυτής της διαφοράς που παρατηρείται έγκειται στη σπουδαιότητα που αποδίδουν οι δικηγόροι στη συμμόρφωση με το νόμο, καθώς για τους ίδιους αποτελεί προτεραιότητα στην ιεραρχία των στόχων ενός οργανισμού ή μιας επιχείρησης.

Τα δεδομένα της εν λόγω έρευνας επιβεβαιώνουν ότι όσο περισσότερο εμπλέκονται οι δικηγόροι στη συμμόρφωση των οργανισμών ή των επιχειρήσεων,

τόσο υψηλότερο είναι το επίπεδο ευαισθητοποίησης, γνώσης και κατανόησης καθώς και η αίσθηση του καθήκοντος συμμόρφωσης. (Parker, Rosen & Nielsen, 2009)

Το γεγονός ότι η έρευνά μας δεν επιβεβαίωσε προηγούμενα ερευνητικά ευρήματα είναι πιθανό να οφείλεται στην πολύ έντονη δραστηριοποίηση φορέων και από τους δυο επιστημονικούς κλάδους γύρω από την ενημέρωση σχετικά με το νέο νομοθετικό πλαίσιο και τις υποχρεώσεις συμμόρφωσης. Πιο συγκεκριμένα, ο Δικηγορικός Σύλλογος Αθηνών και ο Δικηγορικός Σύλλογος Θεσσαλονίκης, οι δυο μεγαλύτεροι της χώρας μας, διοργάνωσαν ημερίδες, σεμινάρια και ενημερωτικές εκδηλώσεις με σκοπό την έγκαιρη ενημέρωση των δικηγόρων σχετικά με το νέο νομοθετικό πλαίσιο. Ο Δικηγορικός Σύλλογος Αθηνών μάλιστα, εξέδωσε και σχετικό εγχειρίδιο συμμόρφωσης. Αντίστοιχες δράσεις διοργανώθηκαν και από τον Ιατρικό Σύλλογο Αθηνών καθώς και από το Υπουργείο Υγείας. Τον Ιούλιο του 2018 ο ΥΠΔ του Υπουργείου Υγείας δημοσίευσε έναν εξαιρετικά χρήσιμο πρακτικό οδηγό συμμόρφωσης των επαγγελματιών υγείας με τον ΓΚΠΔ.

Δε θα πρέπει επίσης να παραγνωρίσουμε το γεγονός ότι η υποχρέωση τήρησης επαγγελματικής εχεμύθειας και οι νομικές συνέπειες σε περίπτωση παραβίασής της, δεν εγκαινιάστηκαν το πρώτον με τον ΓΚΠΔ. Αντίθετα, τόσο το προηγούμενο νομοθετικό καθεστώς του δικαίου περί προστασίας προσωπικών δεδομένων (π.χ. αδειοδότηση από την ΑΠΔΠΧ για τήρηση αρχείου με ευαίσθητα δεδομένα), όσο κυρίως οι εγγενείς δεσμεύσεις των Κωδίκων Δεοντολογίας των ψυχιάτρων / ψυχολόγων και δικηγόρων είναι πιθανό να έχουν οδηγήσει σε ένα κοινό επίπεδο ενημέρωσης και ευαισθητοποίησης χωρίς ιδιαίτερες διαφοροποιήσεις.

Τέλος, η τρίτη ερευνητική μας υπόθεση ήταν ότι οι επαγγελματίες ψυχικής υγείας θα λαμβάνουν περισσότερα τεχνικά και οργανωτικά μέτρα συγκριτικά με τους δικηγόρους. Παρόλο που τα αποτελέσματα μας δεν μπορούν να επιβεβαιώσουν ή να απορρίψουν παλαιότερες έρευνες εξαιτίας της έλλειψης ερευνών στο συγκεκριμένο αντικείμενο, βρήκαμε ότι οι επαγγελματίες ψυχικής υγείας θα λαμβάνουν περισσότερα τεχνικά και οργανωτικά μέτρα συγκριτικά με τους δικηγόρους. Ένας λόγος για τον οποίο συμβαίνει αυτό μπορεί να είναι το γεγονός ότι σε αντίθεση με τους δικηγόρους, τα αρχεία των οποίων δεν περιλαμβάνουν πάντοτε δεδομένα ειδικής κατηγορίας, τα ιατρικά αρχεία πάντα περιέχουν δεδομένα υγείας. Αυτό σημαίνει ότι με το παλαιότερο καθεστώς (Ν.2472/1997) όλοι οι επαγγελματίες υγείας πριν τη

σύσταση αρχείου με δεδομένα υγείας ήταν απαραίτητο να λάβουν σχετική άδεια από την ΑΠΔΠΧ.

Επιπρόσθετα, οι επαγγελματίες ψυχικής υγείας είναι υποχρεωμένοι να τηρούν τα ιατρικά αρχεία για 10 έτη από την τελευταία επίσκεψη του ασθενούς, ενώ τα νοσηλευτικά ιδρύματα για 20 έτη από την τελευταία νοσηλεία. Αυτό σημαίνει ότι για να εξασφαλίσουν τη διαθεσιμότητα των δεδομένων οποτεδήποτε και αν ζητηθούν εντός του υποχρεωτικού χρόνου τήρησης, είναι απαραίτητο να λάβουν τα αντίστοιχα μέτρα ώστε να μη βρεθούν αντιμέτωποι με πειθαρχικές κυρώσεις.

Αντίθετα, οι δικηγόροι τηρούν τα δεδομένα του εντολέα μέχρι τη διεκπεραίωση της υπόθεσης, τη λήξη ή τη λύση της σύμβασης εντολής, χρονικές περίοδοι που συνήθως είναι αντίστοιχες και της βαρύτητας των υποθέσεων. Δεν προβλέπεται όμως υποχρεωτική περίοδος αποθήκευσης αφενός και αφετέρου, συχνά πρόκειται για δεδομένα τα οποία μπορούν να επανεκδοθούν, σε αντίθεση με τα περιεχόμενα ενός αρχείου όπως π.χ. μια ψυχιατρική εκτίμηση, μια ακτινογραφία, μια εξέταση αίματος, απεικονίζουν μια κατάσταση που δεν είναι δυνατό να αναπαραχθεί.

Τέλος, οι επαγγελματίες ψυχικής υγείας είναι περισσότερο εξοικειωμένοι με την ηλεκτρονική καταγραφή και αρχειοθέτηση δεδομένων. Το σύστημα ηλεκτρονικής συνταγογράφησης, ο ηλεκτρονικός ιατρικός φάκελος αποτελούν εργαλεία της καθημερινότητάς τους. Τις περισσότερες φορές τα ηλεκτρονικά συστήματα εξασφαλίζουν εξ' ορισμού και από το σχεδιασμό τους την προστασία των προσωπικών δεδομένων. Αντίθετα, οι δικηγόροι στην καθημερινότητά τους επεξεργάζονται προσωπικά δεδομένα ηλεκτρονικά, όμως κατά βάση στην πλειοψηφία τους τα τηρούν σε φυσικό αρχείο. Η κατάθεση των δικογράφων, η λήψη αντιγράφου αποφάσεων, η αποθήκευση εγγράφων δημοσίων φορέων, πιστοποιητικών κλπ. δημιουργεί ένα φυσικό αρχείο εγγράφων με μέτρα φυσικής ασφάλειας τα οποία είναι πιο δύσκολο να εφαρμοστούν σε αντίθεση με τα προκαθορισμένα μέτρα ασφάλειας στα ηλεκτρονικά αρχεία.

4.2 Περιορισμοί της έρευνας

Ένας από τους σημαντικότερους περιορισμούς που αντιμετωπίσαμε στην έρευνά μας είναι το γεγονός ότι λόγω της πρόσφατης αλλαγής της νομοθεσίας αναφορικά με τα προσωπικά δεδομένα, η σχετική βιβλιογραφία είναι εξαιρετικά φτωχή. Δεν υπάρχουν αρκετές έρευνες οι οποίες να παρέχουν απαντήσεις για το επίπεδο κατανόησης και συμμόρφωσης επαγγελματιών με τον ΓΚΠΔ, πόσο μάλλον των ειδικών κατηγοριών επαγγελματιών που μελετήσαμε στην παρούσα έρευνα.

Ένας ακόμη σημαντικός περιορισμός είναι το γεγονός ότι το παρόν ερωτηματολόγιο δε δύναται να καλύψει όλες τις περιπτώσεις του νέου νομοθετικού πλαισίου, παρά μόνο ορισμένες ενδεικτικές. Ο ΓΚΠΔ εισάγει ρυθμίσεις αναφορικά με διάφορα ζητήματα που είναι δύσκολο να καλυφθούν μέσα από ένα σύντομο ερωτηματολόγιο. Επειδή στην Ελλάδα δεν υπάρχει ερωτηματολόγιο, το οποίο μετράει το βαθμό ευαισθητοποίησης, ενημέρωσης, κατανόησης και συμμόρφωσης με τον ΓΚΠΔ και γι' αυτό το λόγο χρησιμοποιήθηκε τον παρόν, προτείνεται η δημιουργία ενός νέου ερωτηματολογίου, το οποίο θα μπορεί να φέρει ακριβή αποτελέσματα στον ελληνικό πληθυσμό αναφορικά με το επίπεδο συμμόρφωσης.

Επίσης, παρά το γεγονός ότι λάβαμε υπόψη δυο ομάδες επαγγελματιών, τα αποτελέσματα που εξήχθησαν δε γενικεύονται διότι θα πρέπει να συνυπολογίσουμε και το επίπεδο ευαισθητοποίησης άλλων επαγγελματικών κλάδων. Τότε, θα μπορούσαμε να πούμε πως θα έχουμε αποκτήσει μια γενικότερη και πληρέστερη εικόνα σχετικά με τα ζητήματα που προκύπτουν από την εφαρμογή του ΓΚΠΔ.

Τέλος, είναι σημαντικό σε μελλοντική έρευνα να συμπεριληφθούν και επαγγελματίες άλλων γεωγραφικών περιοχών, πέρα από την Αττική, ειδικότερα της επαρχίας όπου τόσο η πρόσβαση στην πληροφορία και στις εξελίξεις όσο και η εξειδίκευση καθώς και ο όγκος των δεδομένων παρουσιάζουν σημαντικές διαφορές.

4.3 Μελλοντικές προεκτάσεις

Σε βάθος χρόνου, είναι σημαντικό να διενεργηθούν περαιτέρω έρευνες, ώστε να παρακολουθήσουμε την εξέλιξη της παρούσας κατάστασης, καθώς είναι πολύ πιθανό να παρατηρηθούν ορισμένες αλλαγές από την επιβολή των πρώτων υψηλών προστίμων και έπειτα. Θα ήταν επίσης ωφέλιμη και η προσθήκη άλλων μεταβλητών που θα δώσει μια πιο ολοκληρωμένη και λεπτομερή εικόνα αναφορικά με τη συμμόρφωση.

Η καλύτερη αντιμετώπιση είναι πάντα η πρόληψη. Για το λόγο αυτό, είναι αναγκαία η περαιτέρω ενημέρωση των επαγγελματικών κλάδων που επεξεργάζονται μεγάλο όγκο προσωπικών δεδομένων (όπως ενδεικτικά ο τραπεζικός, ο ασφαλιστικός, ο τουριστικός και ο τηλεπικοινωνιακός τομέας). Η ανάγκη για ενημέρωση και ευαισθητοποίηση είναι το ίδιο επιτακτική τόσο σε επίπεδο δημοσίου όσο και σε επίπεδο ιδιωτικού τομέα. Ακολουθώντας το παράδειγμα των Συλλόγων των επαγγελματιών υγείας και των δικηγόρων θα πρέπει και άλλοι Σύλλογοι να εκδώσουν οδηγίες, κατευθυντήριες γραμμές και καλές πρακτικές για τους επαγγελματίες στους οποίους απευθύνονται.

Αντίστοιχα, θα πρέπει να υπάρξει ενημέρωση και ευαισθητοποίηση των υποκειμένων των δεδομένων. Η ενίσχυση των δικαιωμάτων τους καθώς και η εγκαθίδρυση του θεσμού του ΥΠΔ αποτελεί ένα σημαντικό βήμα που οδηγεί στην μεγαλύτερη προστασία τους και την ευκολότερη άσκηση των δικαιωμάτων τους. Η αρχή της διαφάνειας και η αρχή της λογοδοσίας έχουν θεμελιώδη σημασία στο νέο νομοθετικό καθεστώς. Η προάσπιση των δικαιωμάτων των υποκειμένων καθώς και τα μέσα προστασίας τους από την αθέμιτη επεξεργασία πρέπει μέσα από δράσεις, εκδηλώσεις και ενημερωτικό υλικό να διαδοθούν και να αξιοποιηθούν.

Τέλος, επειδή οι νέες γενιές μεγαλώνουν μέσα στην κοινωνία της πληροφορίας, σε ένα περιβάλλον κατά βάση ηλεκτρονικό, είναι απαραίτητο να διενεργούνται τακτικά εκπαιδευτικές δράσεις και σεμινάρια σε σχολεία. Τόσο τα παιδιά όσο και οι γονείς πρέπει να είναι ευαισθητοποιημένοι σε ζητήματα προσωπικών δεδομένων, να χρησιμοποιούν το διαδίκτυο με ασφάλεια και να ασκούν

επαρκώς τα δικαιώματα των παιδιών τους ως νόμιμοι αντιπρόσωποί τους σε περίπτωση παράνομης επεξεργασίας.

4.4 Επίλογος

Η προστασία των προσωπικών δεδομένων και ειδικότερα η αναγωγή των προσωπικών δεδομένων σε έννομο αγαθό που χρήζει προστασίας αποτελεί ιστορία των πρόσφατων δεκαετιών. Είναι λοιπόν αναμενόμενο, τόσο οι οργανισμοί και οι επιχειρήσεις όσο και τα υποκείμενα των δεδομένων, το κοινωνικό σύνολο εν γένει, να μην έχει ακόμα αντιληφθεί στον απόλυτο βαθμό τη σημασία της προστασίας των προσωπικών δεδομένων καθώς και τους κινδύνους που ελλοχεύουν από τη μη ασφαλή επεξεργασία τους.

Σε μια εποχή που οι «έξυπνες συσκευές», η διάχυτη υπολογιστική και το διαδίκτυο των πραγμάτων κυριαρχούν, η προστασία των προσωπικών δεδομένων θα πρέπει στη συνείδηση όλων να αποτελεί θεμελιώδες κεκτημένο. Όσο οι επόμενες γενιές θα μεγαλώνουν σε ένα καθεστώς όλο και μεγαλύτερης αυτοματοποίησης, η ανάγκη για ενημέρωση και ευαισθητοποίηση θα γίνεται ολοένα και πιο επιτακτική.

5. Βιβλιογραφία

5.1 Ξένη Βιβλιογραφία

Ausloos, J. (2012). The 'Right to be Forgotten'–Worth Remembering?. *Computer Law & Security Review*, *28* (2), 143-152.

Beauchamp, T. L., & Childress, J. F. (2001). *Principles of biomedical ethics*. Oxford University Press, USA.

Bygrave, L. A. (2017). Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements. *Oslo Law Review*, *4* (02), 105-120.

De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services. *Computer Law & Security Review*, *34* (2), 193-203.

Gola, P., Eichler, C., Franck, L., Klug, C., Lepperhoff, N., Nguyen, A., ... & Schulz, S. (2017). *Datenschutz-Grundverordnung: DS-GVO*.

Joseph, D. I., & Onek, J. N. (1991). Confidentiality in Psychiatry. 105-140

Katz, J., Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.

Lambert, P. (2016). The Data Protection Officer: Profession, Rules, and Role. *CRC Press*, 72.

Latsiou C. (2017). Health data protection-The experience of the Hellenic Data Protection Authority. *Bioethica*, *3* (2), 74-80.

Lubit, R. H., Ladds, B., & Eth, S. (2009). Ethics in Psychiatry. *Kaplan and Sadock's Comprehensive Text Book of Psychiatry. 9th ed*. Lippincott Williams & Wilkins.

McClelland, R., & Thomas, V. (2002). Confidentiality and Security of Clinical Information in Mental Health Practice. *Advances in Psychiatric Treatment, 8* (4), 291-296.

Neubauer, T., & Heurix, J. (2011). A Methodology for the Pseudonymization of Medical Data. *International Journal of Medical Informatics, 80* (3), 190-204.

NIST 800-12 rev1. (2017). An Introduction to Information Security, *NIST Special Publication 800-12 Revision 1*, s.l.

Parker, C. E., Rosen, R. E., & Nielsen, V. L. (2009). The Two Faces of Lawyers: Professional Ethics and Business Compliance with Regulation. *Geo. J. Legal Ethics*, *22*, 201.

Schaar, P. (2010). Privacy by design. *Identity in the Information Society*, 3 (2), 267-274.

Schoeman, F. D. (Ed.). (1984). *Philosophical Dimensions of Privacy: An Anthology*. Cambridge University Press.

Stanberry, B. (1998). The Legal and Ethical Aspects of Telemedicine. 2: Data Protection, Security and European Law. *Journal of Telemedicine and Telecare*, 4 (1), 18-24.

Tankard, C. (2016). What the GDPR Means for Businesses. *Network Security*, 6, 5-8.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies. *Computer Law & Security Review*, *34* (1), 134-153.

Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, 201.

5.2 Ελληνική Βιβλιογραφία

Αλεβίζος, Β. (2008). Εχεμύθεια και Ψυχιατρικό Απόρρητο – Νομικές και Δεοντολογικές Προεκτάσεις σε: Δουζένη, Α. - Λύκουρα, Λ. (επιμ. Έκδ.), *Ψυχιατροδικαστική*, 14 επ.

Αλεξανδροπούλου – Αιγυπτιάδου Ε. (2016). *Προσωπικά Δεδομένα*, Νομική Βιβλιοθήκη, σελ. 35 – 44.

Αρμαμέντος, Π. Δ., & Σωτηρόπουλος, Β. Α. (2005). *Προσωπικά Δεδομένα: Ερμηνεία Ν. 2472/1997: Με τις Τροποποιήσεις των Νόμων 2623/1998, 2703/1999, 2819/2000, 2915/2001, 3051/2002, 3090/2002 και 3156/2003*. Εκδόσεις Σάκκουλα, 37, 128 επ., 166 επ.

Ζωγραφόπουλος, Δ. (2018), *Προετοιμάστε τον Φορέα σας για τη Συμμόρφωση προς τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ/GDPR) Οδηγός προετοιμασίας – Βασικές κατευθύνσεις*, Υπουργείο Υγείας, 35.

Ιακωβίδης, Α. (2014), Εχεμύθεια σε: Δουζένη Α. – Λύκουρα Λ., *Ηθική και Δεοντολογία στην Ψυχική Υγεία*, ΒΗΤΑ Ιατρικές Εκδόσεις, 68.

Ιγγλεζάκης, Ι. (2018). *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679). Εισαγωγή στο νέο νομικό πλαίσιο προστασίας προσωπικών δεδομένων, 1η έκδοση,* Andy's Publishers, Θεσσαλονίκη.

Ιγγλεζάκης, Ι. (2013). Επεξεργασία Δεδομένων Εικόνας ή/και Ήχου μέσω Φωτογράφησης και Βιντεοσκόπησης από Δικαστικό Επιμελητή κατά τη Διαδικασία Αναγκαστικής Εκτέλεσης (γνωμ). Δίκαιο Μέσων Ενημέρωσης & Επικοινωνίας, 2/2013, 172 επ.

Κορσάνου, Α., Δουζένης, Α., Λύκουρας, Λ. (2010), Το Ιατρικό Απόρρητο στην Άσκηση της Ιατρικής με Έμφαση στην Άσκηση Ψυχιατρικής, *Αρχεία Ελληνικής Ιατρικής*, *27* (4):686-690.

Κωνσταντινίδης, Α. (2008). Ζητήματα της διατάραξης των πνευματικών λειτουργιών ή της συναίνεσης από τη σκοπιά της δικαστηριακής πρακτικής σε: Κουτσουράδη, Α., Μαλλιώρη, Μ., Σολδάτο, Κ., Καράκωστα, Ι., *Ψυχιατρική και Δίκαιο ΙΙΙ. Μειωμένη Νοητική Επάρκεια*, (έκδ.) Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή, 97-111.

Λαμπρινουδάκης, Κ., Γκρίτζαλης, Σ., Μήτρου, Λ., Κάτσικας, Σ. (2010). *Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών,* εκδ. Παπασωτηρίου.

Λασκαρίδης, Ε. (2016). Απόρρητο Επαγγελματιών και Βοηθών τους. *Έγκλημα, Κράτος και Ποινική Δικαιοσύνη: Σύγχρονα ζητήματα Ποινικού Δικαίου και Εγκληματολογίας*, 237-251.

Λασκαρίδης, Ε. (2012) σε: Λασκαρίδη Ε. (επιμ. έκδ.), *Ερμηνεία Κώδικα Ιατρικής Δεοντολογίας (Ν. 3418/2005),* άρ. 13 ΚΙΔ, αρ. 3-9, Νομική Βιβλιοθήκη, 160-163.

Λουκάς, Ν. (2017). Τεχνικά μέτρα του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR) Κρυπτογράφηση και Ψευδωνυμοποίηση (CDPO, PRINCE2/P), *Research Associate, Τμήμα Ψηφιακών Συστημάτων Πανεπιστημίου Πειραιά*, 123/2017, Συνήγορος.

Μήτρου, Λ. (2004). Προστασία Προσωπικών Δεδομένων. *Ασφάλεια Πληροφοριακών Συστημάτων*, Εκδόσεις Νέων Τεχνολογιών, 453.

Μήτρου, Λ., Γιαννόπουλος, Γ., Παναγοπούλου- Κουτνατζή, Φ., Βαρβέρης,Α. (2018). *Εγχειρίδιο (Manual) Εφαρμογής του Γενικού Κανονισμού Προσωπικών Δεδομένων (GDPR) για Δικηγόρους κατά την Ενάσκηση του Δικηγορικού Λειτουργήματος,* Εργαστήριο Νομικής Πληροφορικής της Νομικής Σχολής ΕΚΠΑ.

Παναγοπούλου – Κουτνατζή, Φ. (2015). Χορήγηση Δεδομένων Υγείας με Άδεια της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ΑΠΔΠΧ: μια Θεσμικη Αποτιμηση. *Εφημερίδα Διοικητικού Δικαίου,* 6, 758.

Παππάς, Σ. (2014) σε: Χαραλαμπάκη Α. (επιμ. Έκδ.), *Ποινικός Κώδικας, τόμ. α', Ερμηνεία κατ' άρθρο*, άρ. 161 ΠΚ, Νομική Βιβλιοθήκη.

Χριστοδούλου, Κ. *Δίκαιο Προσωπικών Δεδομένων*, εκδ. Νομική Βιβλιοθήκη, 15.

5.3 Νομικά Κείμενα

Κανονισμός (ΕΕ) 2016/679, *Προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)*.

ΟΟΣΑ (2013), *Κατευθυντήριες γραμμές σχετικά με την προστασία της ιδιωτικότητας και των διασυνοριακών ροών προσωπικών δεδομένων*

Οδηγία 2002/58/ΕΚ (2002), *Επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.*

Οδηγία 95/46/ΕΚ (1995), *Προστασία των φυσικών προσώπων έναντι της επεξεργασία δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.*

Σύμβαση 108/1981, *Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων, Συμβούλιο της Ευρώπης, CETS αριθ. 108, 1981*.

Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ)

Working Party 29. (2018). Guidelines on Transparency under Regulation 2016/679. *Brussels, Belgium: European Commission*, 40

Working Party 29. (2017) Guidelines on Data Protection Officers (‘DPOs’). *Brussels, Belgium: European Commission*, 8, 16

European Commission (2010). *A Comprehensive Approach on Personal Data Protection in the European Union*

Working Party 29. (2010). Opinion 1/2010 on the concepts of "controller" and "processor". *Brussels, Belgium: European Commission*, 34

Working Party 29. (2007). Opinion 4/2007 on the concept of personal data. *Brussels, Belgium: European Commission*, 4-7

Working Party 29. (2001). Recommendation 1/2001 on Employee Evaluation Data. *Brussels, Belgium: European Commission*

Working Party 29. (2001). Opinion 8/2001 on the processing of personal data in the employment context. *Brussels, Belgium: European Commission*

Σύνταγμα της Ελλάδας

Νόμος 2472/1997, *Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. (με ενσωματωμένες και τις τελευταίες τροποποιήσεις βάσει του Ν. 4139/2013).*

Νόμος 3471/2006, *Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν. 2472/97. (με ενσωματωμένες και τις τελευταίες τροποποιήσεις βάσει των Ν. 3783/2009, Ν. 3917/2011 και Ν. 4070/2012).*

Νόμος *4624/2019, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις.*

5.4 Ηλεκτρονικές Πηγές

Μήτρου Λ. (2014). *Προστασια Προσωπικων Δεδομενων – Νομος 2472/97* www.icsd.aegean.gr › website_files › proptyxiako (τελευταία ανάκτηση 26/9/2019)

Παναγοπούλου-Κουτνατζή Φ. (2017). *Η εξέλιξη του δικαιώματος στη λήθη (περί λήθης της λήθης;)* https://www.ethemis.gr/epistimoniki-arthrografia-fereniki-panagopoulou-koutnatzi (τελευταία ανάκτηση 26/9/2019)

Ο ρόλος των Λογιστών / Ελεγκτών και Δικηγόρων με βάση το ΓΚΠΔ http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/EDA70B647B2A7CBBC22583080041750C?OpenDocument (τελευταία ανάκτηση 5/10/2019)

Ασφάλεια Επεξεργασίας, ΑΠΔΠΧ https://www.dpa.gr/portal/page?_pageid=33,211421&_dad=portal&_schema=PORTAL (τελευταία ανάκτηση 5/10/2019)

Πολιτική Ασφαλείας, Σχέδιο Ασφαλείας και Σχέδιο Ανάκαμψης από Καταστροφές, ΑΠΔΠΧ https://www.dpa.gr/portal/page?_pageid=33,132337&_dad=portal&_schema=PORTAL (τελευταία ανάκτηση 16/92019)

Constitution Of The World Health Organization http://apps.who.int/gb/bd/PDF/bd47/EN/constitution-en.pdf?ua=1 (τελευταία ανάκτηση 29/9/2019)

Κατάλογος ΕΑΠΔ ΑΠΔΠΧ https://www.dpa.gr/portal/page?_pageid=33,223264&_dad=portal&_schema=PORTAL (τελευταία ανάκτηση 29/9/2019)

Έρευνα της ICAP Management Consultants για το GDPR https://dir.icap.gr/mailimages/GDPR_NEWSurvey.pdf (τελευταία ανάκτηση 26/9/2019)

Ετήσια Έκθεση ΑΠΔΠΧ 2014 https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ANNUALREPORTS/FILES%20ANNUAL%20REPORTS/ANNUAL%202014%20V2.0%20WEB%20VIEW.PDF (τελευταία ανάκτηση 21/9/2019)

Αποφάσεις ΑΠΔΠΧ 31/2008, 43/2009, 98/2013 130/2013 18/2018 https://www.dpa.gr/portal/page?_pageid=33%2C15453&_dad=portal&_schema=PORTAL&_piref33_15473_33_15453_15453.etos=2008&_piref33_15473_33_15453_15453.arithmosApofasis=31&_piref33_15473_33_15453_15453.thematikiEnotita=-1&_piref33_15473_33_15453_15453.ananeosi=%CE%91%CE%BD%CE%B1%CE%BD%CE%AD%CF%89%CF%83%CE%B7 (τελευταία ανάκτηση 26/9/2019)

Γνωμοδότηση Εισαγγελέα Αρείου Πάγου, 15/2007 https://www.eisap.gr/sites/default/files/consulations/4686-%CE%93%CE%9D%CE%A9%CE%9C.%2015-2007.pdf (τελευταία ανάκτηση 5/10/2019)

Παράρτημα

Ερμηνεία και συμμόρφωση των επαγγελματιών ψυχικής υγείας και νομικής επιστήμης με τον Γενικό Κανονισμό Προστασίας Προσωπικών δεδομένων (GDPR)

Το παρόν ερωτηματολόγιο αποτελεί μέρος της διπλωματικής εργασίας της Μαρίας Χονδρονάσιου, που διεξάγεται στο πλαίσιο του μεταπτυχιακού προγράμματος της Ψυχιατροδικαστικής του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών.

Το ερωτηματολόγιο αποσκοπεί στην καταγραφή του βαθμού της συμμόρφωσης των επαγγελματιών ψυχικής υγείας (ψυχιάτρων, ψυχολόγων) και των επαγγελματιών νομικής επιστήμης (δικηγόρων) με τις επιταγές του Κανονισμού σε ζητήματα προστασίας προσωπικών δεδομένων.

Η αποδοχή της συμμετοχή σας είναι εξαιρετικά σημαντική στην έρευνα καθώς θα συμβάλει στην παροχή πολύτιμων πληροφοριών γύρω από την κατανόηση του εν λόγω θέματος. Διασφαλίζουμε ότι οι απαντήσεις σας είναι απόλυτα εμπιστευτικές και πλήρως ανώνυμες. Παρακαλούμε να απαντήσετε σε όλες τις ερωτήσεις, επιλέγοντας κάθε φορά τον αριθμό της κλίμακας που σας εκφράζει περισσότερο, σύμφωνα με τις οδηγίες που δίνονται παρακάτω. Ο χρόνος που απαιτείται για τη συμπλήρωση του ερωτηματολογίου δεν αναμένεται να υπερβεί τα 10 λεπτά.

Ευχαριστούμε πολύ για τη συμμετοχή σας!

Ερευνήτρια : Μαρία Χονδρονάσιου (chondronasiou@gmail.com)

ΔΗΜΟΓΡΑΦΙΚΑ ΣΤΟΙΧΕΙΑ

Φύλο:

a) Άνδρας
b) Γυναίκα

Ηλικία:

Επίπεδο Σπουδών:

a) Προπτυχιακό
b) Μεταπτυχιακό
c) Διδακτορικό
d) Μεταδιδακτορικό

Ειδικότητα:

a) Ψυχίατρος
b) Ψυχολόγος
c) Δικηγόρος

Είδος Απασχόλησης:

a) Απασχολούμενος στο δημόσιο τομέα
b) Απασχολούμενος στον ιδιωτικό τομέα
c) Αυτοαπασχολούμενος

GDPR COMPLIANCE

Απαντήστε σε κάθε μια από τις παρακάτω ερωτήσεις σε μια κλίμακα από το 1 ως το 4 (1=ΚΑΘΟΛΟΥ, 2=ΛΙΓΟ, 3=ΑΡΚΕΤΑ, 4=ΑΠΟΛΥΤΩΣ)

1. Γνωρίζετε τον Ευρωπαϊκό Κανονισμό για την προστασία Προσωπικών Δεδομένων 679/2016;
   a) Καθόλου
   b) Λίγο
   c) Αρκετά
   d) Απολύτως

2. Έχει ορίσει η Διοίκηση του φορέα στον οποίο εργάζεστε Υπεύθυνο Προστασίας Προσωπικών Δεδομένων;
   a) Ναι
   b) Όχι
   c) Δε γνωρίζω

3. Έχετε λάβει κάποια εκπαίδευση σχετικά με την προστασία προσωπικών δεδομένων;
   a) Καθόλου
   b) Λίγο
   c) Αρκετά
   d) Απολύτως

4. Εφαρμόζετε στον φορέα στον οποίο εργάζεστε κάποια πιστοποίηση (π.χ. ISO 27799);
   a) Ναι
   b) Όχι
   c) Δε γνωρίζω

5. Έχετε ενημερωθεί από τον φορέα στον οποίο εργάζεστε σχετικά με την πολιτική ασφαλείας που ακολουθεί;
   a) Καθόλου
   b) Λίγο
   c) Αρκετά
   d) Απολύτως

6. Χρησιμοποιείτε μεθόδους ανωνυμοποίησης, ψευδωνυμοποίησης ή κρυπτογράφησης;
   a) Καθόλου
   b) Λίγο
   c) Αρκετά
   d) Απολύτως

7. Ενημερώνετε εγγράφως τα υποκείμενα (ασθενείς, εντολείς κλπ.) για τα δικαιώματά τους πριν καταγράψετε τα προσωπικά δεδομένα τους;
   a) Ναι
   b) Όχι
   c) Δε γνωρίζω

8. Έχουν τα υποκείμενα (ασθενείς, εντολείς κλπ.) τη δυνατότητα να ζητήσουν πρόσβαση στα προσωπικά τους δεδομένα (π.χ. μέσω έντυπης φόρμας, μέσω e-mail);
   a) Ναι
   b) Όχι
   c) Δε γνωρίζω

9. Διαφοροποιούνται τα δικαιωματα πρόσβασης στα προσωπικά δεδομένα των υποκειμένων (ασθενών, εντολέων κλπ.) ανάλογα με την ειδικότητα κάθε εργαζομένου (π.χ. περιορισμένη πρόσβαση σε νοσηλευτές ή διοικητικούς υπαλλήλους);

a) Ναι
b) Όχι
c) Δε γνωρίζω

10. Τηρείτε διαδικασίες για την διαγραφή ή την καταστροφή των δεδομένων όταν ολοκληρώνεται ο σκοπός της επεξεργασίας τους;
    a) Ναι
    b) Όχι
    c) Δε γνωρίζω

11. Τηρείτε προσωπικά δεδομένα ανηλίκων;
    a) Καθόλου
    b) Λίγο
    c) Αρκετά
    d) Απολύτως

12. Διενεργείτε θεραπευτικές συνεδρίες ή επικοινωνίες με πελάτες μέσω τηλεδιάσκεψης (π.χ. skype);
    a) Καθόλου
    b) Λίγο
    c) Αρκετά
    d) Απολύτως

13. Είναι επαρκή τα μέτρα που έχετε λάβει για την προστασία των προσωπικών δεδομένων από φυσικούς κινδύνους; (π.χ. πυρκαγιά, πλημμύρα, κλοπή χειρόγραφου αρχείου ή μέσων αποθήκευσης);
    a) Καθόλου
    b) Λίγο
    c) Αρκετά
    d) Απολύτως

14. Είναι επαρκή τα τεχνικά μέτρα που έχετε λάβει για την προστασία των προσωπικών δεδομένων από ηλεκτρονικούς/διαδικτυακούς κινδύνους (π.χ. κακόβουλο λογισμικό, μη εξουσιοδοτημένη πρόσβαση, επίθεση ιού);
    a) Καθόλου
    b) Λίγο
    c) Αρκετά
    d) Απολύτως

15. Είναι επαρκή τα μέτρα που έχετε λάβει ώστε να έχετε πρόσβαση στα προσωπικά δεδομένα φυσικών προσώπων μόνο εσείς ή/και οι εξουσιοδοτημένοι βοηθοί σας;
    a) Καθόλου
    b) Λίγο
    c) Αρκετά
    d) Απολύτως

16. Υπάρχουν περιορισμοί στην πρόσβαση του βοηθητικού προσωπικού στα αρχεία των υποκειμένων (ασθενών, εντολέων κλπ);
    a) Ναι
    b) Όχι
    c) Δε γνωρίζω

17. Είστε σε θέση να εντοπίσετε άμεσα ένα περιστατικό παραβίασης;
    a) Καθόλου
    b) Λίγο
    c) Αρκετά
    d) Απολύτως

18. Γνωρίζετε τις προϋποθέσεις και τη διαδικασία γνωστοποίησης των περιστατικών παραβίασης στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα;
    a) Καθόλου
    b) Λίγο
    c) Αρκετά
    d) Απολύτως

19. Είστε σε θέση να εξασφαλίσετε την άμεση ανάκτηση των αρχείων σας σε περίπτωση περιστατικού παραβίασης (π.χ. με τήρηση αντιγράφων ασφαλείας);
    a) Καθόλου
    b) Λίγο
    c) Αρκετά
    d) Απολύτως