Σχολή Οικονομικών Επιστημών και Διοίκησης

Μεταπτυχιακό Πρόγραμμα Σπουδών *Διοίκηση, Τεχνολογία και Ποιότητα*

Μεταπτυχιακή Διατριβή

Ζητήματα συμμόρφωσης δομών υγείας με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR – General Data Protection Regulation)

Φοιτητής: Παναγιώτης Ρεντζιάς

Επιβλέπων Καθηγητής: κ. Στέφανος Γκρίτζαλης

Μάϊος 2020

Σχολή Οικονομικών Επιστημών και Διοίκησης

Μεταπτυχιακό Πρόγραμμα Σπουδών *Διοίκηση, Τεχνολογία και Ποιότητα*

Μεταπτυχιακή Διατριβή

Ζητήματα συμμόρφωσης δομών υγείας με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR – General Data Protection Regulation)

Φοιτητής: Παναγιώτης Ρεντζιάς

Επιβλέπων Καθηγητής: κ. Στέφανος Γκρίτζαλης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών Διοίκηση, Τεχνολογία και Ποιότητα της Σχολή Οικονομικών και Διοίκησης του Ανοικτού Πανεπιστημίου Κύπρου.

Μάϊος 2020

Περίληψη

Το παρόν έργο, ρίχνει φως στο με ποιους τρόπους αλλάζει η καθημερινότητα, τα δικαιώματα και υποχρεώσεις των ασθενών, των εργαζομένων και κάθε ενδιαφερομένου εξαιτίας της νομοθέτησης του νέου, πανευρωπαϊκού Κανονισμού, έχοντας πρώτα εξηγήσει τους λόγους της εισαγωγής του και τις αρχές που τον χαρακτηρίζουν.

Διευκρινίζει τους τρόπους με τους οποίους ο Κανονισμός αναπροσαρμόστηκε στις συνθήκες της τρέχουσας πανδημίας, εκθέτει προβλήματα που θα έπρεπε να είχε επιλύσει μα συνεχίζουν να υφίστανται, όπως και πιθανούς μελλοντικούς τρόπους εξάλειψης των.

Εστιάζει ιδιαιτέρως στο κομμάτι της νομίμου και ασφαλούς επεξεργασίας των προσωπικών δεδομένων, εξηγώντας λεπτομερώς τις νομικώς προβλεπόμενες προϋποθέσεις απόκτησης και αξιοποίησης τους, τη διαδικασία οικοδόμησης της ανάλογης δομής και υποδομής, τον τρόπο αντίδρασης σε περιπτώσεις αποτυχίας και τις προβλέψεις επιβολής προστίμων.

Ο τομέας της υγείας είναι εκείνος στον οποίο κατά κόρων εφαρμόζεται επεξεργασία ευαίσθητων, προσωπικού χαρακτήρος δεδομένων και συνεπώς στην υγεία είναι που μοιραία θα ασκηθεί η εντονότερη πίεση για συμμόρφωση της ως προς τις επιταγές του νέου Κανονισμού.

Summary

The present project sheds light on the ways in which the daily life, the rights and obligations of patients, employees and any interested party changes due to the legislation of the new, pan-European Regulation, having initially explained the reasons for its introduction and the principles that characterize it.

It clarifies the ways in which the Regulation has been adapted to the conditions of the current pandemic, sets out problems that should have been resolved but continue to exist, as well as possible future ways of eliminating them.

It focuses on the legal and secure processing of personal data, explaining in detail the legally required conditions for their acquisition and utilization, the process of building the appropriate structure and infrastructure, how to react in cases of failure and penalty provisions.

The health sector is the one in which the processing of sensitive, personal data is highly applied, and therefore that's where the strongest pressure will be exerted for its compliance with the requirements of the new Regulation.

Ευχαριστίες

Ευχαριστώ τον ακαδημαϊκό υπεύθυνο του προγράμματος κύριο Robert Duval Hernandez, που πάντοτε και άμεσα ήταν διαθέσιμος να με καθοδηγήσει όσον αφορά στο οργανωτικό κομμάτι της εργασίας.

Ευχαριστώ τον επιβλέποντα καθηγητή μου, κύριο Στέφανο Γκρίτζαλη, αρχικά για το ενδιαφέρον και την ισχυρή ενθάρρυνση που μου έδωσε να προχωρήσω τη μελέτη μου ως φοιτητής της ενότητας ΔΤΠ522, σε κάποια συγκυρία όπου για σειρά λόγων είχα δυσκολία να ανταπεξέλθω.

Κατόπιν, ως επιβλέπων, ειδικά κατά το αρχικό στάδιο της εργασίας όπου διακατεχόμουν από άγνοια και ανησυχία, παρείχε σημαντική συμβολή στο να κάνω μια σωστή αρχή, της οποίας ακολούθησε μια ομαλή πορεία και ένα αίσιο τέλος.

Περισσότερο, οφείλω να ευχαριστήσω το Θεό, για το τεράστιο κουράγιο που μου έδωσε καθ' όλη αυτή την πολυετή μου πορεία ως φοιτητής του Ανοικτού Πανεπιστημίου Κύπρου, στο οποίο ολοκλήρωσα προπτυχιακές και μεταπτυχιακές σπουδές, όπου έπρεπε να συνδυάσω μεγάλου όγκου και δυσκολίας μελέτη, με μια νοσοκομειακή δουλεία χαρακτηριζόμενη από κυλιόμενα ωράρια, ανεπίτρεπτα υψηλό φόρτο εργασίας και πολλαπλές, χρονίζουσες δυσχέρειες πάσης φύσεως.

Φυσικά, ευγνώμων οφείλω να είμαι και θα είμαι για πάντοτε στο ίδιο το ΑΠΚΥ, το οποίο ανακάλυψα τυχαία, επάνω σε μια πολύ δύσκολη καμπή του νυν εργασιακού μου βίου και χάρη στην ύπαρξη του, μου έδωσε μια δεύτερη ευκαιρία, μια ευκαιρία ζωής να αποκτήσω ακαδημαϊκά εφόδια που ελπίζω να με βοηθήσουν στον απώτατο στόχο μου: την αλλαγή εργασιακού αντικειμένου.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΙΣΑΓΩΓΗ

Σύντομη περιγραφή του θέματος της έρευνας.

Το παρόν έργο, εξετάζει το με ποιους τρόπους πάροχοι και λοιπες δομές υπηρεσιών υγείας των Ευρωπαϊκών κρατών-μελών, οφείλουν να αναπροσαρμόσουν τις δομές και υποδομές τους, ώστε να ανταποκριθούν στις απαιτήσεις του νέου Κανονισμού για την Προστασία Δεδομένων Προσωπικού χαρακτήρος.

Στόχος και αντικειμενικοί σκοποί της έρευνας.

Η γενική κατεύθυνση της εργασίας, είναι αρχικά να εξετάσει το τι περιλαμβάνει ο νέος Κανονισμός, σε τι αποσκοπεί και με ποιους τρόπους επιδιώκει να το πετύχει. Εν συνεχεία, επιχειρεί να εξηγήσει το με ποιο τρόπο οφείλει να εφαρμόζεται στις δομές υγείας κάθε ευρωπαϊκής χωράς, τις δυσλειτουργίες που έχουν προκύψει κατά την εφαρμογή του, όπως και προτάσεις για το τι μέλει γενέσθαι.

Δομή της διπλωματικής έρευνας.

Η εργασια ξεκινά κάνοντας μια ιστορική αναδρομή στις αφορμές και τα γεγονότα που οδήγησαν έως την οικοδόμηση του ΓΚΠΔ. Ακολουθεί μια γενική επισκόπηση του τι περιλαμβάνεται στα 99 του άρθρα και η επεξήγηση ορισμένων θεμελιώδους σημασίας τεχνικών και νομικών ορισμών που εμπεριέχει και που θα μας ακολουθούν καθ’ όλη μας τη διαδρομή.

Εν συνεχεία, προσεγγίζεται το οργανωτικό κομμάτι του έργου, όπου με περιεκτική και κατανοητή γλώσσα γίνεται επεξήγηση του συνόλου των προβλεπομένων θεμελιωδών αρχών από τις οποίες υποχρεωτικώς και καθ’ ολοκληρίαν οφείλει να διέπεται κάθε επεξεργασία ατομικών δεδομένων που διεξάγεται στις δομές υγείας και συγκεκριμένων νομικών προϋποθέσεων και λοιπών υποχρεώσεων, στη βάση των οποίων δύνανται να εκτελούν επεξεργασίες. Εξετάζονται τα δικαιώματα που ο Κανονισμός επιτρέπει σε ασθενείς και λοιπούς ενδιαφερομένους, όπως και το ποια δικαιώματα τους αποστερεί και γιατί.

Ακολουθεί ένα κυρίως τεχνικής φύσεως μέρος, όπου αναλύονται συγκεκριμένες τεχνικές έννοιες που άπτονται της ασφάλειας των δεδομένων, κυρίως αυτών που επεξεργάζονται ηλεκτρονικά μέσω των Π.Σ. του οργανισμού και όλες οι προϋποθέσεις διασφάλισης του απορρήτου.

Κατόπιν, επικαιροποιείται περαιτέρω, διερευνώντας για τις επιπτώσεις και μεταβολές που η τρέχουσα πανδημία προκάλεσε στον τρόπο επεξεργασίας προσωπικής φύσεως δεδομένων στο χώρο της υγείας και μελετώντας την αποκαλυπτική νεοκδοθείσα, πολύμηνο πανευρωπαϊκή έρευνα της Κομισιόν, που εκθέτει περιφερειακές νομικές δυσλειτουργίες, που συνεχίζουν να υφίστανται σήμερα, τρία έτη μετά τη θέση του Κανονισμού σε ισχύ.
Κλείνει με ένα ειδικό, 'ανασκοπικό' κεφάλαιο, που απαντά σύντομα σε κοινές, εύλογες απορίες που οι διάφοροι ενδιαφερόμενοι μπορεί να εκφέρουν.

<u>Μεθοδολογία, Περιορισμοί και βασικά συμπεράσματα.</u>
Κατά κύριο λόγο, η ερεύνα μας είναι εμπειρικής-ποιοτικής φύσεως.
Το πρόσφατο του αντικειμένου και ο εν γένει χαρακτήρας της προσανατολίζει σε έρευνα κατά βάση διαδικτυακή, με αρκετές αναφορές από έντυπη βιβλιογραφία. Επίσημα έγγραφα του ελληνικού υπουργείου υγείας και της Κομισιόν, έπαιξαν καταλυτικό ρόλο στο να έλθει η παρούσα μελέτη εις πέρας.

Συνθήκες όπως το lockdown και η πάγια απροθυμία δημοσίων λειτουργών να αποκριθούν σε σχετικές έρευνες, δεν διευκολύνουν κατ' ιδίαν συνεντεύξεις.
Το γενικό συμπέρασμα είναι ότι ο Κανονισμός πέτυχε σε σημαντικό βαθμό το στόχο του να ενισχύσει την προστασία των προσωπικών δεδομένων και την ασφαλή τους ροή εντός της ΕΕ, εισάγοντας μια φιλοσοφία ''ανθρωποκεντρικής προσέγγισης της τεχνολογίας''.

Χαρακτηριστικός της επιτυχίας του GDPR είναι ο παγκόσμιος αντίκτυπος που είχε, αφού ενέπνευσε νέα ή αναβαθμισμένα πρότυπα προστασίας δεδομένων σε πολλές χώρες και χρησίμευσε ως παγκόσμιος 'καθοριστής' προτύπων για τη ρύθμιση της ψηφιακής οικονομίας. Υπάρχουν ωστόσο και αρκετά ακόμα βήματα να γίνουν.

Κεφάλαιο 1

Η ιστορική διαδρομή και η φυσιογνωμία του κανονισμού.

Τα πάντα ξεκινούν ήδη από το μακρινό 1945, οπότε και οι ηγέτες της διαλυμένης από τον Β' ΠΠ Ευρώπης, αντιλήφθησαν ότι ο καλύτερος τρόπος να εξασφαλίσει η συνεχής και σταθερή ειρήνη και ευημερία, ήταν η ενθάρρυνση της ευρύτερης δυνατής διεθνούς συνεργασίας. Προς ενίσχυση της προσπάθειας αυτής, το ίδιο έτος ιδρύθηκε ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ), με έδρα το Παρίσι.

Το 1980, ο ΟΟΣΑ εξέδωσε ένα σύνολο Κατευθυντηρίων Γραμμών, αποσκοπούντων στην προστασία της ιδιωτικής ζωής, γνωστό ως *«Κατευθυντήριες Γραμμές για την προστασία της ιδιωτικής ζωής και των διασυνοριακών ροών δεδομένων»,* που αποτέλεσε προπομπό του σημερινού Κανονισμού, διότι από αυτά τα Guidelines, πηγάζουν πολλές από τις σημαντικές Αρχές προστασίας δεδομένων αυτού.

Οι Κατευθυντήριες Γραμμές του ΟΟΣΑ, έγιναν αμέσως αποδεκτές σε παγκόσμιο επίπεδο ως πρότυπο για δίκαιες πρακτικές πληροφόρησης. Ωστόσο, πρόκειται για μη δεσμευτικό, εθελοντικού χαρακτήρα πλαίσιο. Συνεπώς, κάθε χώρα νομοθέτησε με τα δικά της μετρά και σταθμά, με αποτέλεσμα πολλούς και αντικρουόμενους μεταξύ τους νόμους προστασίας απόρρητου, οδηγώντας σε μεγάλη σύγχυση σε περιφερειακό επίπεδο. (Lewis Brisbois)

Το 1995, η ΕΕ ήρθε να συμμαζέψει το εν λόγω μωσαϊκό νομοθετημάτων, ενσωματώνοντας την οδηγία 95/46/ΕΚ, γνωστή ως *«Data Protection Directive»,* η οποία δέσμευε τα κράτη-μέλη στη θέσπιση νόμων ισοδυνάμων μεταξύ τους.
Επέβαλε επίσης την εξαγωγή δεδομένων μόνον προς ελάχιστες τρίτες χώρες, θεωρουμένων ως αξιόπιστους παραλήπτες στοιχείων ευρωπαίων πολιτών, δεδομένου ενός φερέγγυου σχετικού νομικού πλαισίου ή διεθνών συμφωνιών.

Επιπλέον, απαίτησε τη δημιουργία Ανεξαρτήτων Αρχών προστασίας δεδομένων σε κάθε χώρα-μέλος, ώστε να επιτηρούν την εφαρμογή της Οδηγίας και να λειτουργούν ρυθμιστικά, στις σχέσεις μεταξύ οργανισμών και πολιτών. (Lewis Brisbois)

Ωστόσο, πάρα το ότι η οδηγία του 1995 σκόπευε να γεφυρώσει τους διαφορετικούς εθνικούς νόμους, παρέμενε Οδηγία, αφήνοντας και πάλι σημαντικό χώρο για κατά το δοκούν νομοθετήματα. Το γεγονός αυτό, μαζί με την ξέφρενη αύξηση χρήσης δεδομένων που παρατηρείται πλέον, χάρη στην τεχνολογική πρόοδο, οδήγησαν την Κομίσουν στην ανάγκη υιοθέτησης αναβαθμισμένων ρυθμιστικών πρωτοβουλιών.

Η πρώτη ανακοίνωση από την Κομισιόν έγινε στις 25 Ιανουαρίου του 2012, για την πρόθεση της να εισαγάγει πανευρωπαϊκό νομοθέτημα περί προστασίας δεδομένων, ονομαζόμενο ως «*Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων»,* αποσκοπώντας στην:

- Εναρμόνιση όλων των κρατών-μελών.
- Βελτίωση των κανόνων μεταφοράς δεδομένων εκτός ΕΕ.
- Βελτίωση του ελέγχου του χρήστη, επί των στοιχείων ταυτότητας του.

Μετά από 4 έτη διαπραγματεύσεων, ψηφίστηκε ως νόμος της ΕΕ, την 27^{η} Απριλίου 2016 και κατέστη πλήρως εφαρμοστέος την 25^{η} Μαΐου του 2018, κατόπιν διετούς μεταβατικής περιόδου. Είναι δομημένος έτσι ώστε να καλύπτει τις απαιτήσεις προστασίας που απορρέουν από τη σημερινή τεχνολογία και με το Γενικό του χαρακτήρα του, δύναται να αναπροσαρμόζεται σε μελλοντικές απαιτήσεις, που θα επέρχονται χάρη στη συνεχή τεχνολογική καινοτομία, προστατεύοντας αποτελεσματικά τα θεμελιώδη δικαιώματα των ατόμων. (aithority.com)
Πλέον, οι οργανισμοί που επεξεργάζονται προσωπικά δεδομένα οφείλουν να λαβαίνουν μέτρα ώστε να διασφαλίζουν ότι τα δεδομένα προστατεύονται από προεπιλογή (by default), με τα απαραίτητα τεχνικά και οργανωτικά μέτρα και από το σχεδιασμό (by design), δηλαδή με προστασία ιδιωτικής ζωής και δεδομένων ενσωματωμένη στο σχεδιασμό και την αρχιτεκτονική των συστημάτων και τεχνολογιών.

Οργανισμοί εκτός της ΕΕ πρέπει επίσης να συμμορφώνονται και να ορίζουν έναν εκπρόσωπο εντός ΕΕ, προκειμένου να νομιμοποιούνται να συλλέγουν δεδομένα για τους πολίτες της. Σε περιπτώσεις παραβίασης, οι οργανισμοί υποχρεούνται να ενημερώνουν την οικεία αρχή προστασίας δεδομένων εντός 72 ωρών, εκτός εάν είναι απίθανο να αποτελέσει κίνδυνο για τα άτομα.

Η μεγαλύτερη αλλαγή που επέφερε, αφορά στο αυξημένο εδαφικό/γεωγραφικό πεδίο δικαιοδοσίας του GDPR, εκτεινόμενος σε ολόκληρη την ΕΕ, μα και πέραν των ορίων της, επηρεάζοντας κάθε εταιρεία ανά την υφήλιο που επιθυμεί να συνεργάζεται με έναν οργανισμό που εδρεύει στην ΕΕ.

Μια προφανής και κοινώς αντιληπτή αλλαγή που επήλθε, έγκειται στο ότι ο GDPR επιβάλει σε εταιρείες και οργανισμούς να ζητούν (ηλεκτρονική ή δια ζώσης) άδεια των δυνάμει καταναλωτών για το εάν και κατά πόσο θα επιτρέψουν τη συλλογή και επεξεργασία των ατομικών τους στοιχειών.

Αναγκάζει τους οργανισμούς παγκοσμίως να ‘κοιτάξουν στον καθρέφτη’ και να αξιολογήσουν τις πολιτικές και διαδικασίες τους, τις αρχές σχεδιασμού και τις στάσεις τους περί προστασίας προσωπικών δεδομένων.

Να σκεφτούν πιο προσεκτικά και σκόπιμα ποια δεδομένα να συλλέγουν και γιατί, το πώς και πότε να ενημερώνουν τα άτομα ή να λαμβάνουν συγκατάθεσή συλλογής ή κοινοποίησης των στοιχείων τους και να παρέχουν επαρκείς διασφαλίσεις για αυτά, καθιστάμενοι ως υπεύθυνοι διαχειριστές με κερδισμένη την εμπιστοσύνη του κοινού. (itgovernance.eu)

ΓΕΝΙΚΟ OVERVIEW ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ ΚΑΙ ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ ΠΟΥ ΕΙΣΑΓΑΓΕΙ.

Αποτελείται από συνολικά 99 Άρθρα.

Τα άρθρα 1 έως 11, περιλαμβάνουν γενικές διατάξεις όπως τους τρεις θεμελιώδεις στόχους του GDPR, όπως αναφέρθηκαν στην Εισαγωγή.

Το αρ.4 είναι ειδικής σημασίας καθότι εισαγάγει ορισμούς που θεσπίζονται για πρώτη φόρα. Συγκεκριμένα: τα ‘’γενετικά δεδομένα’’, τα ‘’βιομετρικά δεδομένα’’, και τα ‘’δεδομένα που αφορούν στην υγεία’’ (αναλύονται παρακάτω). Μεταφέρει επίσης αυτούσιους Όρους της οδηγίας 95/46/ΕΚ όπως: ‘’παραβίαση δεδομένων προσωπικού χαρακτήρα’’, ‘’Αρχή ελέγχου’’, ‘’εκπρόσωπος’’.

Εν συνεχεία, στο αρ.5 διατυπώνονται κάποιες θεμελιώδεις αρχές, προϋποθέσεις και κριτήρια από τις οποίες οφείλει να διέπεται κάθε επεξεργασία προσωπικών δεδομένων και ξεκαθαρίζεται το ποια προσωπικά δεδομένα τελούν υπο γενική απαγόρευση επεξεργασίας και τις όποιες επιμέρους εξαιρέσεις (επίσης αναλύονται παρακάτω).

Σημειώνεται ότι τα κράτη-μέλη, δικαιούνται να προσθέτουν και επιπλέον όρους/περιορισμούς όσον αφορά στην επεξεργασία των τριών νέων τύπων ευαίσθητων προσωπικών δεδομένων.

Στα άρθρα 12 έως 32, ο Κανονισμός προσδιορίζει τα δικαιώματα του υποκειμένου των δεδομένων και εν προκειμένω του ασθενούς (όπως αναλύονται διεξοδικά στο Κεφάλαιο 4). Στα άρθρα 24 έως 31 αναλύονται οι βασικές υποχρεώσεις των υπεύθυνων επεξεργασίας (νοσοκομείων), όπως και των εκτελούντων την επεξεργασία. (Ζωγραφόπουλος 2018: 9-11)

Τα άρθρα 32 έως 36 υποχρεώνουν τα έως άνω πρόσωπα να εφαρμόζουν τα δέοντα μέτρα εξασφάλισης της επεξεργασίας, ξεκαθαρίζουν τις υποχρεώσεις των προς την ΑΠΔΠΧ, όπως και κάθε ενέργεια που υποχρεούνται να εκπληρώνουν, προλαμβάνοντας ενδεχόμενα συμβάντα ασφαλείας αλλά και κατόπιν τέτοιων.

Κατόπιν, τα άρθρα 37 έως 43, εισαγάγουν το θεσμό του Υπευθύνου προστασίας Δεδομένων (DPO - Data Protection Officer), τον τρόπο διορισμού του και τα βασικά καθήκοντα του. Όπως και θέματα δεοντολογίας και χρήσης πιστοποιημένων μηχανισμών επεξεργασίας δεδομένων, δεσμευτικών για υπευθύνους και εκτελούντες επεξεργασίες.

Τα άρθρα 44 έως 50, αναφέρονται στις διαβιβάσεις προσωπικού χαρακτήρος δεδομένων των υποκειμένων προς τρίτες χώρες και διεθνείς οργανισμούς, τα κριτήρια που τις διέπουν, όπως και τις περιπτώσεις που αυτές απαγορεύονται. Εδώ, εμπλέκονται παράγοντες όπως το κράτος δικαίου της χώρας-παραλήπτη, το επίπεδο σεβασμού των ανθρωπίνων δικαιωμάτων, των θεμελιωδών ελευθεριών του ανθρώπου, το ποινικό δίκαιο και λοιπών άλλων. Συνεπώς, πρόκειται για περίπλοκο και κρίσιμης σημασίας τμήμα του Κανονισμού και αναλύεται ενδελεχώς στο Κεφάλαιο 8 της παρούσης.

Τα άρθρα 51 έως 59 υποχρεώνουν τα κράτη-μέλη να συστήσουν ανεξάρτητες εποπτικές Αρχές (στην Ελλάδα η ΑΠΔΠΧ), με στόχο την επίβλεψη της εφαρμογής το Κανονισμού και κατ επέκταση την προστασία των θεμελιωδών Ελευθεριών και δικαιωμάτων των φυσικών προσώπων, έναντι της επεξεργασίας, τις προϋποθέσεις ανεξαρτησίας των, τα προσόντα και υποχρεώσεις των στελεχών, την ενημέρωση του κοινού και τη διερεύνηση των καταγγελιών του.

Μεταξύ των άρθρων 60 έως 76, ορίζονται κάποιοι υποχρεωτικοί κανόνες συνεργασίας μεταξύ ΑΠΔΠΧ και λοιπών άλλων ενδιαφερομένων Αρχών εποπτείας, όπως και τις συνέπειες μη συμμορφώσεως. Θεσπίζει το λεγόμενο μηχανισμό Συνεκτικότητος, ώστε να προάγεται η διεθνής συνεργασία, υπο ενιαίο, συντονισμένο τρόπο λειτουργιάς. (Ζωγραφόπουλος 2018: 12-19)

Ως κορυφαίας σημασίας κρίνονται τα άρθρα 77 έως 84, όπου ξεκαθαρίζονται, συγκεκριμενοποιούνται και αναλύονται περαιτέρω τα δικαιώματα και οι υποχρεώσεις των ασθενών (ως υποκείμενα των δεδομένων), όπως η υποβολή καταγγελίας σε περίπτωση θεωρούμενης παραβίασης της ιδιωτικότητας, η δικαστική προσφυγή και η δικαστική υπεράσπιση του, οι αποζημιώσεις, τα πρόστιμα, τους υπαίτιους διαρροής και λοιπά, όπως αναλύονται στο Κεφάλαιο 7.

Στα 85 έως 91, θεσπίζονται συγκεκριμένες εξαιρέσεις/παρεκκλίσεις από τις ειδικές διατάξεις του Κανονισμού, επιτρέποντας σε κάποιες περιστάσεις το συγκερασμό μεταξύ προστασίας προσωπικών δεδομένων και δικαιώματος ελεύθερης έκφρασης (π.χ. ακαδημαϊκή, λογοτεχνική, καλλιτεχνική ή δημοσιογραφική ελευθερία του λόγου), τις προϋποθέσεις πρόσβασης του κοινού σε δημόσια αρχεία και τις ειδικές προϋποθέσεις επεξεργασίας ατομικών αριθμών (π.χ. ΑΜΚΑ), και άλλων στοιχειών ταυτότητας, όπως και το τι πρέπει να συμπεριλαβαίνει ένας φάκελος με δεδομένα προσωπικού χαρακτήρα, σχετικών με την υγεία.

Τα υπόλοιπα άρθρα, είναι τυπικού χαρακτήρα και περιλαμβάνουν κάποιες διατάξεις, μή σχετικές με την παρούσα έρευνα.

Όλες οι διατάξεις είναι ίσης ισχύος, οφείλουν να γίνονται σεβαστές και εφαρμοζόμενες ως ενιαίο σύνολο (διότι τέτοιο αποτελούν) και όχι επιλεκτικά.

Περά από τα 99 άρθρα, περιλαμβάνονται επίσης 173 αιτιολογικές σκέψεις, με πραγματιστικά παραδείγματα-σενάρια, που διαφωτίζουν αναφορικά με το πώς θα πρέπει να αντιμετωπίζονται διάφορα σχετιζόμενα με τον Κανονισμό ζητήματα. (Ζωγραφόπουλος 2018: 17-20)

ΒΑΣΙΚΟΙ ΟΡΙΣΜΟΙ

▪ Υποκείμενο *των δεδομένων*: δύναται να χαρακτηριστεί μόνον κάποιο εν ζωή φυσικό πρόσωπο, ακόμα και ένα έμβρυο, εφόσον γεννήθηκε ζωντανό. Συνεπώς, νομικά πρόσωπα και αποθνήσκοντες, δεν τυγχάνουν προστασίας των προσωπικών τους δεδομένων (αρ.4).

▪ Προσωπικά *δεδομένα:* (ή αλλιώς, τα δεδομένα προσωπικού χαρακτήρα): χωρίζονται σε δυο κατηγορίες. Τα απλά και τα ευαίσθητα.
Ως *'απλά'*, θεωρούνται: το ονοματεπώνυμο, η διεύθυνση κατοικίας, η διεύθυνση ηλεκτρονικού ταχυδρομείου, η διεύθυνση IP, δεδομένα τοποθεσίας, ο αριθμός τηλεφώνου, καταγραφές από κλειστά κυκλώματα τηλεόρασης (CCTV) και ηχογραφήσεις, αριθμοί ταυτοποίησης (π.χ. ΑΔΤ) και οικονομικά δεδομένα (αρ.9 παρ.1).

Ως *'ευαίσθητα'* (ή ειδική κατηγορία δεδομένων προσωπικού χαρακτήρα): η εθνικότητα, φυλετική καταγωγή, τα πολιτικά φρονήματα, οι θρησκευτικές και φιλοσοφικές πεποιθήσεις, η συμμετοχή σε συνδικαλιστική οργάνωση. Όπως και οι τρεις νέες έννοιες ευαίσθητων δεδομένων που για πρώτη φορά εισάγονται νομικά: τα *'γενετικά δεδομένα'*, τα *'βιομετρικά δεδομένα'* και αυτά που αφορούν στην παρελθούσα και παρούσα *'κατάσταση της υγείας'* του υποκειμένου, όπως και του σεξουαλικού προσανατολισμού.

Ως *'γενετικά δεδομένα'* κατά το άρθρο 4 παρ.13 του Κανονισμού, ορίζουμε τα: *δεδομένα προσωπικού χαρακτήρα, που αφορούν τα γενετικά χαρακτηριστικά φυσικού προσώπου, κληρονομηθέντα ή επίκτητα, όπως προκύπτουν από ανάλυση βιολογικού δείγματος* (αίμα, ούρα, σίελο, εγκεφαλονωτιαίο υγρό, κόπρανα) *του εν λόγω φυσικού προσώπου, παρέχοντα μοναδικές πληροφορίες αναφορικά με την φυσιολογία ή την υγεία του*». (Κανονισμός (ΕΕ) 2016/679)

Τα γενετικά δεδομένα άπτονται του σκληρού πυρήνα της Ιδιωτικότητος του υποκειμένου, καθότι η γενετική πληροφορία:

- Είναι μοναδική σε κάθε ανθρώπινο ον, μα συνάμα δύναται να αποκαλύψει στους έχοντες πρόσβαση, στοιχειά αναφορικά με βιολογικούς συγγενείς του ή φυλετικές και εθνοτικές του καταβολές και να καταστεί στοχοποιούμενος.
- Είναι πάγια, αδιαμφισβήτητη και υψηλού πληροφοριακού φορτίου.
- Συχνά είναι άγνωστη και για τον ίδιο το φορέα της και μη μεταβαλλόμενη εξ' ιδίας βουλήσεως.
- Είναι μεταβιβάσιμη από γενιά σε γενιά.
- Δύναται να υποκλαπεί καί καταχραστεί εν αγνοία του υποκειμένου.

Ως *'βιομετρικά δεδομένα'* κατά το άρθρο 4 παρ.13 του Κανονισμού, ορίζουμε τα: «*δεδομένα προσωπικού χαρακτήρα, που προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αναμφίβολη ταυτοποίηση του».*

Βάσει αυτού του ορισμού, τα βιομετρικά δεδομένα διαθέτουν τρία βασικά στοιχεία:

- Δημιουργούνται κατόπιν ειδικής τεχνικής επεξεργασίας, με ‘’βιομετρικές μεθόδους’’.
- Οι βιομετρικές αυτές μέθοδοι/τεχνικές, έχουν ως αντικείμενο επεξεργασίας τα βιολογικά, συμπεριφορικά και φυσικά χαρακτηριστικά του ατόμου.
- Αποσκοπούν στην αναντίρρητη ταυτοποίηση κάποιου συγκεκριμένου φυσικού προσώπου.

Τα βιομετρικά δεδομένα αποτελούν μοναδικά για κάθε άνθρωπο βιολογικά χαρακτηριστικά και αυτά είναι: τα δακτυλικά αποτυπώματα και το σχήμα των δάκτυλων, η ίριδα του οφθαλμού και ο αμφιβληστροειδής χιτώνας, η φωνή, το πρόσωπο, το σχήμα των χεριών, της οδοντοστοιχίας, των ώτων, η φλεβική διάταξη και οι πόροι του δέρματος. Όλα αυτά, καθίστανται αναγνωρίσιμα, μετρήσιμα, καταγράψιμα και αντιπαραβαλλόμενα με αντίστοιχα άλλων υποκειμένων, με μια εξελισσόμενη ποικιλία σύγχρονων τεχνικών μέσων. Παράδειγμα για την αποτελεσματικότητα και χρησιμότητα των βιομετρικών συστημάτων, αποτελεί η ευρύτατη πλέον χρήση του δακτυλικού αποτυπώματος και του σχήματος του προσώπου για το αυτόματο ξεκλείδωμα των σύγχρονων κινητών τηλεφώνων. Ομοίως, ένα ανθρώπινο ον, δύναται να αυθεντικοποιεί την ταυτότητα του, αποκτώντας πρόσβαση στο χώρο εργασίας του, φυλασσόμενες εγκαταστάσεις, ηλεκτρονική υγεία κ.ο.κ.

Να διευκρινιστεί ότι κάποια βιομετρικά στοιχεία ενίοτε αλλάζουν με την πάροδο του χρόνου (π.χ. σχήμα προσώπου), πάντοτε όμως παραμένουν μοναδικά και ανεπανάληπτα.

Ως *‘’δεδομένα σχετιζόμενα με την κατάσταση της υγείας’’* ορίζουμε το οτιδήποτε μπορεί να αναφέρεται εντός του ιατρικού φακέλου ενός φυσικού προσώπου: τρέχοντα και παρελθόντα προβλήματα υγείας, νοσηλείες και χειρουργικές επεμβάσεις, αλλεργίες, φαρμακευτικές αγωγές τρέχουσες και παρελθούσες, επισκέψεις σε ιατρούς, διαγνωστικές εξετάσεις.

Ωστόσο, θα πρέπει να αποσαφηνιστεί πως καταρχήν απλά δεδομένα, όπως ΑΜΚΑ και ονοματεπώνυμο, όταν αναφέρονται σε ασθενείς, διαβαθμίζονται και αυτά σε ευαίσθητα, διότι πλέον αφορούν στην κατάσταση της υγείας του υποκειμένου και αποτελούν μέρος του ιατρικού του φακέλου.

Ως πηγές προέλευσης απλών και ειδικών δεδομένων, δύνανται να χαρακτηριστούν: το ίδιο το υποκείμενο (ασθενής ή εργαζόμενος), αλλά και ετέρες πήγες όπως: ΕΚΑΒ, ΕΦΚΑ, ασφαλιστικές εταιρίες, άλλα νοσηλευτικά ιδρύματα. Στη δεύτερη περίπτωση, ο νυν υπεύθυνος επεξεργασίας, οφείλει να ενημερώσει το υποκείμενο ότι συλλέχτηκαν δεδομένα του από τη τάδε πηγή, το σκοπό της συλλογής, το τι ακριβώς συλλέχτηκε και το ποιοι πρόκειται να τα επεξεργαστούν, όπως επιβάλλεται από το άρθρα 14 του Κανονισμού. (Κανονισμός (ΕΕ) 2016/679)

▪ Υπεύθυνος *επεξεργασίας (PII Controller)*: Πρόκειται για νομικό πρόσωπο (σπανίως και φυσικό), δικαιούχο ιδιωτικότητας. Συγκεκριμένα, στο χώρο της υγείας, ο συνηθέστερος υπεύθυνος επεξεργασίας είναι τα νοσηλευτικά ιδρύματα (νοσοκομεία). Ορίζει τους σκοπούς της επεξεργασίας προσωπικού χαρακτήρος δεδομένων, όπως και τα μέσα με τα οποία θα εκτελείται – το 'γιατί' και το 'πώς'.
Πέραν τον νοσοκομείων, συνηθέστερα παραδείγματα υπευθύνων επεξεργασίας, αποτελούν: το Υπουργείο υγείας, το ΚΕΕΛΠΝΟ, οι Υγειονομικές περιφέρειες (ΥΠΕ), ο ΙΦΕΤ, το Ινστιτούτο Παστέρ, το ΕΚΑΒ. (ISO 29100:2011/2017)

▪ Ο *Εκτελών την επεξεργασία (PII Processor)*: μπορεί να είναι νομικό πρόσωπο, δημόσια Αρχή ή δημόσια υπηρεσία ή άλλος δημόσιος φορέας και υπο προϋποθέσεις και ιδιωτικός φορέας. Καθήκον του προσώπου αυτού είναι να επεξεργάζεται τα δεδομένα των υποκειμένων, για λογαριασμό και με την έγκριση του υπευθύνου επεξεργασίας. Σε κάθε περίπτωση, υπεύθυνος και εκτελών, είναι νομικώς ξεχωριστές οντότητες και θα πρέπει να μην συγχέονται. (ISO 29100:2011/2017)

▪ DPO *(Data Protection Officer) ή ΥΠΟ (Υπεύθυνος Προστασίας Δεδομένων)*: Κάθε υπεύθυνος επεξεργασίας, έχει κληθεί ήδη από το 2018 να ορίσει DPO (και αναπληρωτή του) κατόπιν πρόσκλησης εκδήλωσης ενδιαφέροντος και βάσει προσόντων όπως: η εμπειρογνωμοσύνη στον τομέα του Δικαίου προστασίας δεδομένων, προηγούμενη επαγγελματική πείρα και ικανότητα εκπλήρωσης καθηκόντων, όπως αυτά ορίζονται στο αρ.39. Ο DPO, συνιστά πάντοτε φυσικό πρόσωπο, εποπτεύει, συμβουλεύει, παρακολουθεί – δεν αποτελεί τον ''άνθρωπο για όλες τις δουλειές''. (Ζωγραφόπουλος)

▪ ΑΠΔΠΧ *(Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)*:

Πρόκειται για ανεξάρτητη διοικητική Αρχή, συνταγματικώς κατοχυρωμένη, ιδρυθείσα το Νοέμβριο του 1997, με τον νομο2472/1997, με σκοπό «*την προστασία του ατόμου, από την επεξεργασία δεδομένων προσωπικού χαρακτήρα».* Η όλο και αυξανόμενη σε παγκόσμιο επίπεδο, ηλεκτρονικώς και γραπτώς, καταχώρηση και χρήση προσωπικών δεδομένων από εταιρίες και κρατικούς φορείς, δημιουργεί όλο και περισσότερους κινδύνους για την ασφάλεια της ιδιωτικής ζωής των πολιτών.

Επί της βάσεως αυτής, κρίθηκε σκόπιμη η δημιουργία της συγκεκριμένης, ανεξάρτητης διοικητικής Αρχής. Σε περίπτωση μη ύπαρξης τέτοιας Αρχής σε χώρα της ΕΕ, πλέον επιβάλλεται η δημιουργία της από τον ΓΚΠΔ.

▪ *Αποδέκτης*: *«δημόσια αρχή, φυσικό ή νομικό πρόσωπο ή υπηρεσία ή άλλος φορέας που επεξεργάζεται προσωπικά δεδομένα, στον οποίο κοινολογούνται τα δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για 'Τρίτο', είτε όχι».* (ISO 29100:2011/2017)

▪ *Τρίτος*: Ο 'τρίτος', δεν δικαιούται να εκτελεί επεξεργασία. Ως τρίτος, ορίζεται *«κάθε φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή φορέας υγείας»,* με εξαίρεση: το υποκείμενο, τον υπεύθυνο και εκτελούντα και κάθε πρόσωπο εξουσιοδοτημένο από υπεύθυνο ή εκτελούντα, να εκτελεί επεξεργασίες. (ISO 29100:2011/2017)

Κεφάλαιο 2

Θεμελιώδεις Αρχές Ιδιωτικότητος που διέπουν την επεξεργασία απλών και ευαίσθητων προσωπικού χαρακτήρος δεδομένων.

Το άρθρο 5 του Κανονισμού, προβλέπει συγκεκριμένες Αρχές Ιδιωτικότητας που υποχρεωτικώς και συσσωρευτικώς διέπουν κάθε είδους επεξεργασία ατομικών δεδομένων, είτε έγγραφη, είτε ηλεκτρονική, είτε μεικτή.
Η μη τήρηση έστω μιας, καθιστά την επεξεργασία παράνομη. Όταν τα δεδομένα όλων γενικώς των υποκειμένων ενός φορέα-υπευθύνου επεξεργασίας, υφίστανται κατά πάγιο τρόπο επεξεργασία χωρίς την τήρηση όλων των ως κάτω, τότε λειτουργεί παρανόμως.

→ Η Αρχή της Νομιμότητας του σκοπού.

Τα δεδομένα, θα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο σύννομο θεμιτό και διαφανή ως προς το υποκείμενο των δεδομένων και μόνον ως προς το υποκείμενο των δεδομένων. Ουδείς τρίτος δικαιούται διαφάνειας.

Ούτος ώστε ο Υπεύθυνος επεξεργασίας να μπορεί να τεκμηριώσει τη νομιμότητα της επεξεργασίας, κατά το άρθρο 6 του Κανονισμού, θα πρέπει:

- Το υποκείμενο να έχει ενημερωθεί για κάθε σκοπούμενη επεξεργασία σε γλώσσα απλή, κατανοητή και αρμόζουσα στην έκαστοτε περίσταση, ειδικότερα όταν απαιτείται επεξεργασία ευαίσθητων δεδομένων και να έχει συναινέσει ενυπογράφως γι’ αυτή.

- Να υφίσταται εκ προοιμίου η εξασφάλιση πως οι σκοποί συμβαδίζουν με την τρέχουσα νομοθεσία. Ειδάλλως, να μην εκτελούνται οι επεξεργασίες.
- Η σκοπούμενη επεξεργασία να συμβαδίζει με το κύριο αντικείμενο του Υπευθύνου επεξεργασίας (π.χ. ένα νοσοκομείο-υπεύθυνος επεξεργασίας, έχει ως κύριο αντικείμενο του την παροχή υπηρεσιών υγείας και άρα, για σκοπούς άμεσα σχετιζόμενους με την υγεία των ασθενών-υποκειμένων των δεδομένων, δύναται να εκτελεί ανάλογες επεξεργασίες).
- Η επεξεργασία να είναι επιβεβλημένη, για σκοπούς διαφύλαξης κάποιου ζωτικού και εννόμου συμφέροντος του Υπευθύνου ή την εκτέλεση συμβάσεως ή άσκηση δημοσίας εξουσίας αναληφθείσας από τον Υπεύθυνο.

Ειδικά όταν ο Controller επεξεργάζεται ευαίσθητα δεδομένα, ενδέχεται να προϋποτίθεται να διαθέτει ειδική άδεια από την ΑΠΔΠΧ ή άλλη κυβερνητική αρχή.
(Ζωγραφόπουλος & ISO 29100:2011)

→ Η Αρχή του Περιορισμού του σκοπού.

Βάσει αυτής, οι οργανισμοί οφείλουν να συλλέγουν εκείνα τα στοιχεία PII που είναι απολύτως απαραίτητα για την εκάστοτε σκοπούμενη επεξεργασία και μόνον εκείνα. Για κάθε τύπο επεξεργασίας, ο εν λόγω Controller, οφείλει να έχει αποσαφηνίσει προσεκτικά, αιτιολογημένα και επίσημα το είδος και την ποσότητα των νομίμως και άκρως αναγκαίων προς συλλογή και επεξεργασία στοιχειών.

Σε περίπτωση που κάποιος Controller επιθυμεί να συλλέξει επιπλέον στοιχεία, για σκοπό άσχετο του αρχικού, δύναται μόνον κατόπιν ρητής, προαιρετικής συγκατάθεσης του υποκειμένου και αφού του παράσχει λεπτομερή πληροφόρηση.

Ωστόσο, να διευκρινιστεί ότι κατά το άρθρο 8 παρ.1 στοιχείο β΄, περαιτέρω επεξεργασία για λόγους αρχειοθέτησης (ως προς το δημόσιο συμφέρον), στατιστικούς, επιστημονικών και ιστορικών ερευνών, δεν θεωρείται ασύμβατη ως προς τους αρχικούς σκοπούς, αρκεί οι χρησιμοποιούμενες μέθοδοι να εξασφαλίζουν το ανέφικτο της ταυτοποίησης και να υφίστανται όλες οι κατάλληλες εγγυήσεις προστασίας των δεδομένων τους. (Ζωγραφόπουλος & ISO 29100:2011)

→ Η Αρχή της Ελαχιστοποίησης.

Βεβαίως βασίζεται στην αμέσως προηγούμενη, 'κτίζοντας' επάνω σε αυτή, επιβάλλοντας την αναδιάρθρωση διαδικασιών και πληροφοριακών συστημάτων κατά τρόπο που επιβάλλει περιορισμούς ως προς τον αριθμό των φυσικών προσώπων εχόντων πρόσβαση, αλλά και στο είδος και την ποσότητα των δεδομένων που το εκάστοτε πρόσωπο δικαιούται πρόσβαση, βάσει των νομίμων καθηκόντων του.

Επίσης, αξιώνει την οριστική διαγραφή δεδομένων όταν ο σκοπός της συλλογής τους έχει ολοκληρωθεί, εκτός εάν υφίστανται νομικές απαιτήσεις διατηρήσεως αυτών, όπως και το να αποφεύγεται η αναιτιολόγητη τήρηση περιττών αντιγράφων, εντύπων ή ηλεκτρονικών (στοιχείο γ').

Ακόμα παραπέρα, προωθεί (στο μέτρο του εφικτού):

- Τη διενέργεια επεξεργασιών δεδομένων χωρίς να απαιτείται η ταυτοποίηση των υποκειμένων τους.
- Τη μη παρακολούθηση από τον Controller της συμπεριφοράς τους.
- Τον περιορισμό της δυνατότητας να συνδεθούν τα συλλεγέντα δεδομένα με τα υποκείμενα τους.

→ Η Αρχή του Περιορισμού του χρόνου αποθήκευσης, διατήρησης και αποκάλυψης.

Η εν λόγω Αρχή, επιβάλει περιορισμούς στη χρήση, διατήρηση, αποκάλυψη και διαβίβαση δεδομένων, μόνο στα όσα είναι απαραίτητα προς εκπλήρωση εκάστου, σαφούς και νομίμου σκοπού και χρήση μόνον γι' αυτό εκτός αν η νομοθεσία προβλέπει κάτι διαφορετικό. Γενικά μιλώντας, τα ατομικά δεδομένα, θα πρέπει να διατηρούνται μόνον για το χρονικό διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας.

Ωστόσο, ειδικά για τους προαναφερθέντες σκοπούς αρχειοθέτησης, επιστημονικής και ιστορικής έρευνας και στατιστικούς, μπορούν να διατηρούνται για μεγαλύτερα χρονικά διαστήματα, αρκεί να εφαρμόζονται τα δέοντα τεχνικά και οργανωτικά μέτρα διασφάλισης τους. Συγκεκριμένα, σε ιδιωτικούς παρόχους υπηρεσιών υγείας, έως 10 έτη και σε δημοσίους, έως 20 έτη. Κατόπιν, καταστρέφονται κατά ασφαλή τρόπο και όχι με απλή, αβίαστη απόρριψη σε κάδους αχρήστων (στοιχείο ε΄). Στο αρ.89 παρ.1 προβλέπεται γενική ρήτρα επί της περιόδου τηρήσεως. (Ζωγραφόπουλος & ISO 29100:2011)

→ Η Αρχή της Ακρίβειας και της Ποιότητας των δεδομένων.

Δηλαδή, να συλλέγονται τα πραγματικά, τα ακριβή στοιχεία.

Συνεπώς θα πρέπει να:

- Επικαιροποιούνται όποτε είναι αναγκαίο, διαγράφοντας από τα συστήματα του ο υπεύθυνος επεξεργασίας τα πεπαλαιωμένα και ανακριβή, χωρίς καθυστερήσεις (εκτός αν η νομοθεσία επιτρέπει τη διατήρηση και outdated δεδομένων).
- Διασταυρώνεται η ορθότητα δεδομένων συλλεχθέτων από πρόσωπο διάφορο του υποκειμένου.
- Διασταυρώνεται η ορθότητα τυχόν νέων δεδομένων που εμφανίζει ένα υποκείμενο, επιδιώκοντας να τροποποιήσει ήδη υφιστάμενα (π.χ. με προσκόμιση σχετικής βεβαίωσης).
- Οι προϋποθέσεις αυτές αποκτούν ιδιαίτερη αξία όταν επίκειται λήψη απόφασης για την παραχώρηση ή την αποστέρηση κάποιου σημαντικού προνομίου ενός φυσικού προσώπου (στοιχείο δ').

→ Η Αρχή της Γνωστοποίησης, της Διαφάνειας και της Ανοικτότητας.

Εκ των προτέρων Γνωστοποίηση του υποκειμένου:

- Ότι τα δεδομένα του υφίστανται επεξεργασία, τους σκοπούς της, την ταυτότητας του Υπευθύνου και του τρόπου επικοινωνίας μαζί του.
- Όταν πρόκειται να λάβουν χώρα μείζονες αλλαγές επί των διαδικασιών χειρισμού των PII στοιχειών τους.
- Κάθε πληροφορίας αναφορικά με τα δικαιώματα τους.

Με Διαφάνεια και Ανοικτότητα:

- Του εξηγούμε λεπτομερώς και κατανοητά τι και γιατί το συλλέγουμε και από ποιον θα είναι ορατό.
- Δημοσιεύουμε στο κοινό πληροφόρηση για τις πολιτικές και πρακτικές που διέπουν τον τρόπο επεξεργασίας.

Σε περίπτωση υποβολής σχετικού αιτήματος, η πληροφόρηση θα πρέπει να παρέχεται στο υποκείμενο εντός ενός μηνός το αργότερο. Σε άλλη περίπτωση, το υποκείμενο δύναται να καταγγείλει το γεγονός στην αρμόδια εποπτική αρχή και εν και πάλι δεν ευοδωθεί, να κινηθεί δικαστικά. (Ζωγραφόπουλος & ISO 29100:2011)

→ Η Αρχή της ατομικής Συμμετοχής και Πρόσβασης.

Επιτρέπει στο υποκείμενο την αυθεντικοποιημένη πρόσβαση, επανεξέταση, τροποποίηση και διαγραφή των δεδομένων του, με σύντομη διαδικασία, άνευ κόστους. Επιβάλει στον Υπεύθυνο να διασφαλίσει πως το υποκείμενο θα προσπελαύνει τα δικά του και μόνον στοιχεία, με μόνη εξαίρεση την περίπτωση που το υποκείμενο εξουσιοδοτήσει γραπτώς άλλο φυσικό πρόσωπο να δράσει για λογαριασμό του. Υπογραμμίζεται πως η εν λόγω Αρχή μόνο εν μέρει τυγχάνει εφαρμογής στο χώρο της υγείας.

→ Η Αρχή της Συγκατάθεσης και της Επιλογής.

Η Συγκατάθεση, αφόρα στο δικαίωμα του υποκειμένου για ελεύθερη επιλογή ή άρνηση παροχής των PII στοιχειών του, προς επεξεργασία, πάντοτε κατόπιν προηγούμενης αναλυτικής επεξηγήσεως των επιπτώσεων μιας ενδεχόμενης άρνησης ή αποδοχής.

Η Επιλογή, αφορά στο δικαίωμα τα υποκείμενα να αποφασίζουν για τον τρόπο χειρισμού των PII τους από τον Controller (συμφωνούνται κατά τη συγκατάθεση), όπως και για την εύκολη και χωρίς κόστος άρση της συγκαταθέσεως τους, με ταυτόχρονη-αυτόματη εξαίρεση των δεδομένων του από περαιτέρω επεξεργασία.

Σημειώνεται πως σε περίπτωση συγκατάθεσης από ανήλικο, αυτή θεωρείται αυτομάτως άκυρη σε περίπτωση απουσίας έγκρισης από κηδεμόνα.

Επίσης, οφείλει να υφίσταται η δυνατότητα περαιτέρω επεξεργασίας στοιχειών PII, για περιπτώσεις που κάτι τέτοιο απαιτηθεί νομικά, λογούς ζωτικού συμφέροντος του υποκειμένου ή εκτέλεσης συμβολαίου.

Υπογραμμίζεται πως η εν λόγω Αρχή δεν τυγχάνει εφαρμογής στο χώρο της υγείας. (Ζωγραφόπουλος & ISO 29100:2011)

→ Η Αρχή της Ακεραιότητας και Εμπιστευτικότητας των δεδομένων.

Δηλαδή, να διασφαλίζεται πως τα δεδομένα θα επεξεργάζονται κατά τρόπο ασφαλή, προστατευόμενα από ενδεχομένη ακούσια ή εκούσια υποκλοπή, αλλοίωση ή διαγραφή, πάλι με τη χρήση ενδεδειγμένων μέτρων διασφάλισης (στοιχείο στ').

Συνοπτικά:

- Η ψευδονωμοποίηση και η κρυπτογράφηση, θεωρούνται οι βέλτιστες πρακτικές.
- Η τήρηση αντιγράφων ασφάλειας και η κατάλληλη εκπαίδευση του προσωπικού.
- Η διαβαθμισμένη πρόσβαση, αποκλείοντας πιθανότητα επεξεργασίας από μή εξουσιοδοτημένα πρόσωπα.
- Εξασφαλίζεται ότι δεν θα βρίσκονται πλέον έγγραφα με προσωπικά δεδομένα ασθενών αφύλακτα και εκτεθειμένα, σε μη ασφαλείς χώρους.

  Ακόμα και στην περίπτωση απόρριψης στα άχρηστα, θα πρέπει προηγουμένως να έχουν καταστραφεί ελεγχόμενα - όχι να απορρίπτονται σε ακέραιη μορφή.
- Εν τελεί, αφού έχουμε λάβει όλα τα κατάλληλα μέτρα πρόληψης και αντιμετώπισης κίνδυνου, προβαίνουμε σε μελέτη αντικτύπου, όπως επιβάλει το άρθρο 35, η οποία και θα πρέπει να επαναλαμβάνεται εν ευθέτω χρόνω και οι πολιτικές ασφαλείας να επικαιροποιούνται περιοδικώς, διότι δεν νοείται πολιτική ασφαλείας που να εκτίνεται στο άπειρο - οφείλουμε πάντοτε να βρισκόμαστε ένα βήμα πιο μπροστά από τις ενδεχόμενες απειλές.
- Δυσμενείς επιπτώσεις σε επιπτώσεις μή τήρησης των ως άνω.

(Οι πολιτικές ασφαλείας αναλύονται στο Κεφάλαιο 6).

→ Η Αρχή της Λογοδοσίας.

Δηλαδή, ο υπεύθυνος επεξεργασίας αλλά και ο εκτελών την επεξεργασία, οφείλουν να λειτουργούν κατά την παρ.1 του εν λόγω άρθρου, τηρώντας το σύνολο των ως άνω Αρχών, έχοντας στήσει αναλόγως διαδικασίες, τεχνικά και οργανωτικά μέσα, μα και όντας ευρισκόμενοι σε θέση να αποδείξουν την ανά πάσα στιγμή ότι τις τηρούν, έχοντας αυτοτελή ευθύνη προς την ΑΠΔΠΧ και τα δικαστήρια.

Αναλυτικότερα, οφείλουν:

- Να έχουν καταγράψει, επικοινωνήσει και εκπαιδεύσει κάθε εσωτερικό εμπλεκόμενο.
- Σε περίπτωση διαβίβασης στοιχείων σε τρίτο φορέα, να έχουν βεβαιωθεί πως εκείνος διαθέτει τουλάχιστον ιδίου επιπέδου προστασία αυτών.
- Εγκαίρως και ανελλιπώς να ενημερώνουν τα υποκείμενα για κάθε πιθανή η επιβεβαιωμένη παραβίαση των δεδομένων τους και να έχουν ετοιμάσει μηχανισμό αποζημίωσης/αποκατάστασης θυμάτων παραβίασης.

- Να έχουν εγκαταστήσει αρμόζουσες εσωτερικές διαδικασίες υποβολής παραπόνων και καταγγελιών των υποκειμένων, προς υπεράσπιση νομίμων δικαιωμάτων τους.

Ειδικότερα, η δυνατότητα Επανόρθωσης, είναι κομβικής σημασίας, κατά την Αρχή της Λογοδοσίας, αφού παράσχει στα υποκείμενα την ευχέρεια να εγκαλέσουν τον Υπεύθυνο για αμέλεια ή κακοδιαχείριση των PII στοιχείων τους. Ομοίως και η διαδικασία Αποκατάστασης, που προσφέρει στους θιγομένους αντισταθμίσματα κατόπιν συμβαμάτων, όπως: κλοπή ταυτότητας, δυσφήμιση, κατάχρηση στοιχείων ή εσφαλμένες τροποποιήσεις τους. Φυσικά, η ουσιαστική αποκατάσταση θυμάτων data breach, είναι δύσκολη υπόθεση. Δεν εξισούται με συμβάν χρηματικής απώλειας, ούτε εξιλεώνεται με χρηματική αποζημίωση. Η ύπαρξη ενδεικνυομένων, συμβαδιζόντων με τη νομοθεσία σχετικών διαδικασιών, αυξάνει την εμπιστοσύνη στον οργανισμό. (Ζωγραφόπουλος & ISO 29100:2011)

Συμπερασματικά, οι υποχρεώσεις Υπευθύνου και Εκτελούντος, δε μπορούν να θεωρούνται 'προκαθορισμένες' και 'παγιοποιημένες', αλλά 'δυναμικές', αφού αναδιαμορφώνονται αναλόγως αναγκών, βάσει της καθημερινής τριβής και των αποτελεσμάτων κάθε Μελέτης Αντίκτυπου.

Προαιρετικά και ούτος ώστε η αποδειξιμότητα υπάρξεως των να καθίσταται ευκολότερη, συνίσταται η υιοθέτηση από τον οργανισμό σχετικών, επισήμων (εκδοθείσα από αρμοδία εποπτική αρχή) 'Κωδίκων Δεοντολογίας' αλλά και η τήρηση ενός 'μηχανισμού πιστοποίησης' υιοθετουμένου από κάποιο επίσημο φορέα (π.χ.TUV) με δυνατότητα να απονέμει τέτοιες πιστοποιήσεις σε ενδιαφερομένους οργανισμούς.

→ Η Αρχή της Ασφάλειας των πληροφοριών.

Επιτάσσει:

- Τη λήψη και τακτική επανεκτίμηση των μέτρων διασφάλισης της ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας των PII δεδομένων σε όλα τα επίπεδα του οργανισμού, έναντι κάθε πιθανής απειλής, βασιζομένων στη νομοθεσία, στην αποτίμηση κίνδυνου, στα πρωτόκολλα ISO, την εκτίμηση κόστους/οφέλους, την πιθανότητα εκδήλωσης συμβάντος και των δυνητικών επιπτώσεων του.
- Τα κατάλληλα και εκπαιδευμένα πρόσωπα να έχουν διαβαθμισμένη πρόσβαση στην απαραίτητη πληροφόρηση.

Κεφάλαιο 3

Βασικές ενέργειες που αποσκοπούν στη συμμόρφωση με τον κανονισμό.

→ Προβλέπονται 4 συγκεκριμένοι σκοποί για την επεξεργασία απλών δεδομένων προσωπικού χαρακτήρος, στη βάση των οποίων τέτοια επεξεργασία τεκμηριώνεται νομικά, κατά το άρθρο 9 παρ.2 του ΓΚΠΔ και αρκεί να συντρέχει έστω ένας εξ' αυτών:

1) Ο σκοπός της παροχής ιατρικών υπηρεσιών.
2) Ο σκοπός της εκπλήρωσης κάποιου δημοσίου συμφέροντος.
3) Ο σκοπός του να εξυπηρετηθούν τα δικαιώματα και οι υποχρεώσεις του υπευθύνου επεξεργασίας ή του υποκειμένου, για ζητήματα κοινωνικού δικαίου εργατικού δικαίου, κοινωνικής ασφάλισης και προστασίας.
4) Ο σκοπός να διενεργηθεί κάποια επιστημονική έρευνα (π.χ. πειράματα εμβολίων). (Ζωγραφόπουλος 2018: 23)

→ Προβλέπονται 5 συγκεκριμένοι σκοποί, οι οποίοι αποτελούν τις νομικές βάσεις που θεμελιώνουν τη δυνατότητα στον υπεύθυνο επεξεργασίας, να επεξεργαστεί ευαίσθητα δεδομένα προσωπικού χαρακτήρος, κατά το άρθρο 6 παρ.1 του ΓΚΠΔ και αρκεί να συντρέχει έστω ένας εξ' αυτών.

1) Η παροχή ιατρικών υπηρεσιών.
2) Η εκπλήρωση κάποιου δημόσιου συμφέροντος σχετικού με τη δημόσια υγεία.
3) Η ανάγκη εκτελέσεως συγκεκριμένων υποχρεώσεων και ασκήσεως συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας και του υποκειμένου των δεδομένων.
4) Ο σκοπός της θεμελίωσης, άσκησης ή υποστήριξης νομικών διεκδικήσεων.
5) Σκοποί αρχειοθέτησης, στατιστικής ή ιστορικής έρευνας. (Ζωγραφόπουλος 2018: 24)

→ Είναι θεμελιώδους σημασίας να ξεκαθαριστεί πως στον τομέα της υγείας, δεν επιτρέπεται η μη παροχή υπηρεσιών υγείας, απλώς επειδή το υποκείμενο αρνήθηκε να συγκαταθέσει για την επεξεργασία των προσωπικών του δεδομένων, γεγονός που τεκμηριώνεται από την υπ' αριθμόν 1 νομική βάση για το ελεύθερο της επεξεργασίας ευαίσθητων δεδομένων: την παροχή ιατρικών υπηρεσιών (αρ.9παρ.2)

→ Συγκατάθεση απαιτείται μόνον σε προκαθορισμένες περιπτώσεις, (όπως π.χ. συμμετοχή σε κάποια κλινική δοκιμή) και δίνεται μόνον εγγράφως. Σε κάθε περίπτωση, τα ευαίσθητα δεδομένα δύνανται να τύχουν επεξεργασίας μόνον από επαγγελματία επιφορτισμένο με την υποχρέωση τήρησης του ιατρικού απορρήτου (ιατροί, νοσηλευτές, αναλυτές δειγμάτων). Αποθηκεύονται για προκαθορισμένο χρόνο.

→ Πριν ένας φορέας ξεκινήσει την οποιαδήποτε επεξεργασία ατομικών δεδομένων, οφείλει να προβεί σε σειρά προπαρασκευαστικών ενεργειών, ως εξής:

- Διασφάλιση των διαδικασιών που προστατεύουν τα δικαιώματα του υποκειμένου κατά τα άρθρα 12 έως 22 του Κανονισμού.
- Προσδιορισμός και καθιέρωση οργανωτικών και τεχνικών μέτρων διασφάλισης του απορρήτου κάθε επεξεργασίας, είτε ηλεκτρονικής, είτε έγχαρτης.
- Ορισμός DPO.
- Καταγραφή και τυποποίηση κάθε είδους επεξεργασίας που σκοπεύει ο οργανισμός να εκτελεί, όπως και η διασφάλιση τήρησης αρχείου για την κάθε επεξεργασία που θα πραγματοποιείται.
- Διενέργεια μελέτης αντίκτυπου (αναλύεται στο Κεφάλαιο 6).

Κεφάλαιο 4

Περί δικαιωμάτων

των ασθενών.

Η ύπαρξη του εν λόγω κεφαλαίου, απαιτείται διότι στο χώρο της υγείας τα δικαιώματα του ασθενούς-υποκειμένου των δεδομένων, δεν εξισούνται με τα δικαιώματα του υποκειμένου κατά τη γενική έννοια, όπως είχε αναλυθεί στο προηγούμενο κεφάλαιο. Ισχύει σειρά εξαιρέσεων.

Μια από τις βασικές υποχρεώσεις ενός υπευθύνου επεξεργασίας στο χώρο της υγείας, αποτελεί η διαφανής ενημέρωση του υποκειμένου των δεδομένων (π.χ. ασθενών, εργαζομένων, αιμοδοτών, συμμετεχόντων σε κλινικές μελέτες).

Με χρήση σαφούς, κατανοητής διατυπώσεως, ο υπεύθυνος επεξεργασίας οφείλει να διασφαλίζει ότι το υποκείμενο έτυχε πλήρους ενημερώσεως για την επεξεργασία των προσωπικού χαρακτήρος δεδομένων του, τα αποτελέσματα της οποίας θα πρέπει να είναι εύκολα προσβάσιμα στο υποκείμενο, σε έγγραφη μορφή, με έντυπο ξεχωριστό για καθεμία εκ προαναφερθεισών κατηγοριών δεδομένων. Ακολούθως, του παράσχεται και προφορική ενημέρωση. (Ζωγραφόπουλος 2018: 33)

Πρέπει να τονιστεί ότι κατά την Αρχή της Λογοδοσίας, και δεδομένου του ότι στον τομέα της υγείας γίνεται κατά κόρων (και περισσότερο από οποιοδήποτε άλλο τομέα) επεξεργασία ευαίσθητων προσωπικών δεδομένων, η ενημέρωση οφείλει να γίνεται πάντοτε εγγράφως, ώστε ο υπεύθυνος επεξεργασίας να βρίσκεται στη θέση να αποδεικνύει τη νόμιμη εκπλήρωση των υποχρεώσεων του.

Οφείλει επίσης να ξεκαθαριστεί η διαφορά μεταξύ της ‘’έγγραφης ενημέρωσης’’ και ‘’της συγκατάθεσης’’ του ασθενούς. Όπως ήδη εξηγήθηκε, ο υπεύθυνος επεξεργασίας με κύριο ρόλο την παροχή υπηρεσιών υγείας, ουδεμία συγκατάθεση οφείλει να έχει από τον ασθενή (υποκείμενο) ώστε να επεξεργαστεί τα ευαίσθητα δεδομένα του. Συνεπώς, όταν ο ασθενής (ενυπογράφως) λαμβάνει τα (κατά την Αρχή της Λογοδοσίας) προαναφερθέντα έγγραφα, επί της ουσίας, με την υπογραφή του, απλώς αποδέχεται ότι έλαβε γνώση για την επεξεργασία – όχι ότι συγκατάθεσε γι’ αυτή. (Ζωγραφόπουλος 2018: 33)

Πρέπει επίσης να καταστεί σαφές πως στο χώρο της υγείας (και όπως αναλύεται παρακάτω), αρκετές από τις Θεμελιώδεις Αρχές που προβλέπει το άρθρο 5 του ΓΚΠΔ, δεν είναι εφαρμόσιμες, καθιστώντας τα δικαιώματα ασθενών και λοιπών υποκειμένων, περιορισμένα.

ΔΙΚΑΙΩΜΑΤΑ ΤΩΝ ΥΠΟΚΕΙΜΕΝΩΝ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΤΑ ΟΠΟΙΑ ΤΥΓΧΑΝΟΥΝ ΕΦΑΡΜΟΓΗΣ ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ ΥΓΕΙΑΣ.

√ Στις γνωστές, συγκεκριμένες εξαιρέσιμες περιπτώσεις όπου ρητά η νομοθεσία ζητεί συγκατάθεση υποκειμένου (πειράματα-κλινικές μελέτες), αυτή πρέπει πάντοτε να παράσχεται εγγράφως (αρ.4).

Να ξεκαθαριστεί ωστόσο πως δεν απαιτείται ενημέρωση του υποκειμένου για την περίπτωση που κάποια άλλη δημόσια υπηρεσία ή Αρχή απαιτήσει να της διαβιβαστούν προσωπικά δεδομένα του υποκειμένου ώστε να διεξαγάγει έρευνα στα πλαίσια της εκπλήρωσης της κύριας αποστολής της (πχ. δικαστήρια, εισαγγελία, στρατιωτικές αστυνομικές ή λιμενικές αρχές, ΑΑΔΕ, ΕΦΚΑ ή ΕΟΠΥΥ), αφού σε τέτοια περίπτωση δεν θεωρούνται ‘’αποδέκτες’’.

Διευκρινίζεται επίσης πως στους ως άνω, δεν συμπεριλαμβάνεται η ΕΛΣΤΑΤ, η όποια κατά τον Ν.3632/2010, έχει δικαίωμα πρόσβασης μόνον σε ανωνυμοποιημένες πληροφορίες (πρωτογενή στατιστικά στοιχεία), ώστε να εκπληρώσει την κύρια αποστολή της.

√ Το δικαίωμα Πρόσβασης του υποκειμένου στα δεδομένα του.

Το αρ.15 του Κανονισμού, δίδει τη δυνατότητα ανεμπόδιστης πρόσβασης και λήψης αντιγράφων των προσωπικού χαρακτήρος δεδομένων του, σε έντυπη και ηλεκτρονική μορφή, χωρίς την οποιαδήποτε αιτιολόγηση ή υποχρέωση επίκλησης ειδικού εννόμου συμφέροντος. Προβλέπεται και προστασία, για την περίπτωση που ένας τρίτος ζητεί πρόσβαση στα δεδομένα του υποκειμένου. Τέτοια πρόσβαση δύναται να εγκριθεί μόνον κατόπιν έγγραφης αδείας από το υποκείμενο ή με την ειδική εξαίρεση να συντρέχει κάποια εκ των σχετικών νομικών βάσεων των άρθρων 6 ή 9 του Κανονισμού (π.χ. υπεράσπιση δικαιωμάτων ενώπιων δικαστηρίου).

√ Το δικαίωμα του υποκειμένου στη διόρθωση των δεδομένων του.

Το αρ.16 του Κανονισμού και βάσει της Αρχής για την Ακρίβεια των δεδομένων, προβλέπει τη δυνατότητα διόρθωσης των στοιχείων, η οποία πρέπει να διεξάγεται από τον υπεύθυνο χωρίς καθυστερήσεις.

√ Το κατά το άρθρο 18 δικαίωμα στον Περιορισμό της επεξεργασίας των δεδομένων μόνον για τον αρχικό σκοπό για τον οποίο και είχαν συλλεχτεί (αφορά κυρίως σε ιδιώτες επεξεργαστές-παρόχους υπηρεσιών υγείας).

√ Το αρ.19 του Κανονισμού, επιβάλει στον υπεύθυνο την υποχρέωση γνωστοποίησης στο υποκείμενο τυχόν διορθώσεων ή διαγραφών προσωπικών του δεδομένων ή συμβάντων παραβίασης αυτών (data breaches). (Ζωγραφόπουλος 2018: 33-39)

ΔΙΚΑΙΩΜΑΤΑ ΥΠΟΚΕΙΜΕΝΩΝ ΤΩΝ ΔΕΔΟΜΕΝΩΝ, ΤΑ ΟΠΟΙΑ ΔΕΝ ΤΥΓΧΑΝΟΥΝ ΕΦΑΡΜΟΓΗΣ ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΥΓΕΙΑΣ.

× Το δικαίωμα του υποκειμένου στην εναντίωση επεξεργασίας δεδομένων του.

Το αρ.21 του Κανονισμού, προβλέπει τη δυνατότητα του υποκειμένου να αιτηθεί διακοπή επεξεργασίας των απλών προσωπικού χαρακτήρα δεδομένων του, για ιδίους λογούς (π.χ. εφόσον περιχύουν τα θεμελιώδη δικαιώματα και εξουσίες του υποκειμένου ή το ατομικό του συμφέρον, ιδίως όταν το υποκείμενο είναι ανήλικος).

Ωστόσο, όπως είναι εύλογο και κατά τη προαναφερθείσα βάση του αρ.9 παρ.2 του ΓΚΠΔ, το δικαίωμα της αντίταξης/αντίρρησης, δεν δύναται να εφαρμοστεί.

Υπο προϋποθέσεις, υπάρχει η δυνατότητα να μην στερηθούν το δικαίωμα αυτό οι εργαζόμενοι του υπευθύνου επεξεργασίας- φορέα παροχής υπηρεσιών υγείας.

× Το δικαίωμα του υποκειμένου για εναντίωση στην αποκλειστικά αυτοματοποιημένη λήψη αποφάσεων και κατάρτιση ατομικού προφίλ.

Κατά το αρ.22 του ΓΚΠΔ, προβλέπεται η δυνατότητα για το υποκείμενο να εναντιωθεί στη εν λόγω αυτοματοποιημένη επεξεργασία, αφού παράγει έννομα αποτελέσματα που αφορούν ή επηρεάζουν σημαντικά το υποκείμενο. Ωστόσο, η σχετική εναντίωση, δεν δύναται να τύχει εφαρμογής, όταν κύριος σκοπός του υπευθύνου επεξεργασίας είναι η παροχή υπηρεσιών υγείας.

× Το δικαίωμα στη Λήθη.

Το αρ.17 κατοχυρώνει το δικαίωμα στο υποκείμενο να αιτηθεί τα προσωπικά δεδομένα του να λησμονηθούν, δηλαδή να διαγραφεί κάθε πληροφορία που το αφορά και ευρίσκεται στην κατοχή ενός υπευθύνου επεξεργασίας, είτε σε ηλεκτρονική, είτε σε έντυπη μορφή.

Ωστόσο, η παρ.3 του ιδίου άρθρου, αποσαφηνίζει ότι το εν λόγω δικαίωμα αποκλείεται εφαρμογής στο χώρο της υγείας.

× Το δικαίωμα στη φορητότητα των δεδομένων.

Το αρ.20 του κανονισμού προβλέπει τη δυνατότητα, το υποκείμενο των δεδομένων να λαμβάνει τα προσωπικά του δεδομένα από τον υπεύθυνο επεξεργασίας σε κάποιο ευρέως χρησιμοποιούμενο μορφότυπο (π.χ. αρχείο pdf) και να τα διαβιβάζει ελεύθερα σε άλλο υπεύθυνο επεξεργασίας χωρίς την αντίρρηση του αρχικού ή και να τα διαβιβάζει απευθείας ο αρχικός υπεύθυνος σε άλλο υπεύθυνο, που θα του υποδείξει το υποκείμενο.

Ωστόσο, κατά την παρ.3 του άρθρου 20, η φορητότητα δεν δύναται να ασκηθεί σε περιπτώσεις επεξεργασιών σχετικών με την εκπλήρωση καθηκόντων που αποσκοπούν στο δημόσιο συμφέρον ή άσκησης δημόσιας εξουσίας. Δηλαδή, με απλά λόγια, φορείς υγείας του Δημόσιου (π.χ. ΕΚΑΒ, ΕΣΥ, ΕΦΚΑ), δεν δύνανται να επιτρέψουν στο υποκείμενο τη φορητότητα των δεδομένων τους.

Να διευκρινιστεί ότι δεν ισχύει το ίδιο όταν κάτοχος των δεδομένων του υποκειμένου είναι ιδιώτης πάροχος υπηρεσιών υγείας. Μέσω ενός τέτοιου, η φορητότητα ασκείται ελεύθερα. (Ζωγραφόπουλος 2018: 33-39)

Κεφάλαιο 5

Λοιπες υποχρεώσεις Υπευθύνων και Εκτελούντων επεξεργασίες.

Υπάρχουν περιπτώσεις όπου περισσότεροι του ενός υπευθύνου επεξεργασίας, καλούνται από κοινού να επεξεργαστούν προσωπικά δεδομένα του ιδίου υποκειμένου (ασθενούς).

Παράδειγμα αποτελεί η ηλεκτρονική πλατφόρμα του ΕΚΑΒ, όπου καταχωρούνται τα δεδομένα της τρέχουσας κατάστασης υγείας ασθενών που χρήζουν διακομιδής σε κάποιον πάροχο υγείας ή από έναν πάροχο σε κάποιον άλλο, πιο εξειδικευμένο (π.χ. μεταφορά εγκαυματία ή πολυτραυματία από γενικό, σε ειδικό νοσοκομείο). Ανάλογες από κοινού επεξεργασίες, γίνονται στο πλαίσιο του Εθνικού συστήματος αιμοδοσίας, όπου εμπλέκονται από κοινού: το Υπουργείο Υγείας, το Εθνικό Κέντρο Αιμοδοσίας (ΕΚΕΑ), τα νοσοκομεία και το εθνικό ηλεκτρονικό νεφοϋπολογιστικό σύστημα απεικονιστικών εξετάσεων (συμμετέχει πραγματική πληθώρα υπευθύνων επεξεργασίας).

→ Οι σχέσεις μεταξύ των υπευθύνων, ρυθμίζονται από μεταξύ τους συμφωνίες, είτε από το δίκαιο της ΕΕ, είτε το εθνικό δίκαιο της χώρας-μέλους, όπως αποσαφηνίζεται στο αρ.26 παρ.1 του ΓΚΠΔ.

→ Η συμφωνία μεταξύ παρόχων, τίθεται στη διάθεση κάθε ενδιαφερομένου υποκειμένου, το οποίο σε κάθε περίπτωση δύναται να ασκήσει τα νομικά του δικαιώματα έναντι καθενός από τους υπευθύνους επεξεργασίας, προς ίδιο έννομο συμφέρον.

→ Ο υπεύθυνος επεξεργασίας έχει την ευθύνη για τη σωστή επιλογή εκτελούντων την επεξεργασία. Δηλαδή, νομικών πρόσωπων που έχουν αντικειμενικώς κριθεί ως αξιόπιστα για την εφαρμογή των προβλεπομένων οργανωτικών και τεχνικών μέτρων πλήρους διασφάλισης των απαιτήσεων ασφαλείας κατά τον ΓΚΠΔ (αρ.28 παρ.1).

→ Απαγορεύεται σε εκτελούντα η ανάθεση επεξεργασιών σε τρίτο εκτελούντα, χωρίς προηγούμενη έγγραφη άδεια του υπευθύνου επεξεργασίας (αρ.28 παρ.2).

→ Κάθε επεξεργασία από τον εκτελούντα, θεμελιώνεται νομικώς βάσει του κοινοτικού ή εθνικού δικαίου, το οποίο και τον δεσμεύει σε σχέση με τον υπεύθυνο επεξεργασίας. Το κοινοτικό ή εθνικό δίκαιο, επίσης ξεκαθαρίζει τα δικαιώματα και υποχρεώσεις του υπευθύνου, τους επιτρεπτούς σκοπούς επεξεργασίας, τη χρονική διάρκεια φύλαξης και τις κατηγορίες υποκειμένων των οποίων τα δεδομένα μπορούν να τίθενται υπο επεξεργασία (αρ.28 παρ.3).

→ Εάν ο εκτελών δράσει κατά παράβαση των ως άνω, καθορίζοντας ο ίδιος τα μέσα και τους σκοπούς της επεξεργασίας, τότε θεωρείται οι ίδιος ως υπεύθυνος επεξεργασίας και όχι το νοσοκομείο ή ο εκάστοτε φορέας, τουλάχιστον για τις συγκεκριμένες επεξεργασίες που έγιναν κατά παράβαση (αρ.28 παρ.10).

→ Κάθε φορά που συντρέχει εκτέλεση επεξεργασίας προσωπικών δεδομένων, το υποκείμενο πρέπει να ενημερώνεται γι’ αυτή και τα αποτελέσματα της, όπως και για την ταυτότητα του εκτελούντος (αρ.4 στοιχ.9).

→ Εταιρίες (νομικά πρόσωπα) παροχής υπηρεσιών τεχνικής υποστήριξης (service ή αναβαθμίσεις) πληροφοριακών συστημάτων ή διαγνωστικού εξοπλισμού δημοσίων νοσοκομείων, δεν έχουν δικαίωμα πρόσβασης στα δεδομένα των ασθενών, εκτός κι αν αυτή κρίνεται αναγκαία και έχει προβλεφτεί ρητά στη μεταξύ τους σύμβαση. (Ζωγραφόπουλος 2018: 40-43)

Κεφάλαιο 6

Ζητήματα διασφάλισης απορρήτου και ασφαλούς επεξεργασίας (Data Protection).

Α) Τι ορίζουμε ως ''Ασφάλεια''.

Μια πληροφορία θεωρείται ασφαλής όταν χαρακτηρίζεται από:

- Εμπιστευτικότητα. Δηλαδή, καθίσταται μή προσβάσιμη από μή εξουσιοδοτημένους χρηστές-οντότητες-διαδικασίες.
- Ακεραιότητα. Δηλαδή, προστατεύεται η ορθότητα, η πληρότητα και η μη εξουσιοδοτημένη τροποποίηση της.
- Διαθεσιμότητα. Δηλαδή, είναι διαρκώς και αμέσως διαθέσιμη προς χρήση από κάθε εξουσιοδοτημένη οντότητα. (Sloot& Groot 2018: 9)

Η εξασφάλιση των πληροφοριών, προϋποθέτει την ύπαρξη ασφαλών Πληροφοριακών Συστημάτων. Ένα Π.Σ. θεωρείται ασφαλές όταν η λειτουργία του διέπεται από ένα οργανωμένο πλαίσιο εννοιών, αντιλήψεων, πολιτικών, αρχών, διαδικασιών, τεχνικών και μέτρων, απαραίτητων ώστε τα επιμέρους του στοιχεία και το Π.Σ. ως ολότητα να προστατεύονται από κάθε τυχαία ή σκόπιμη απειλή.

Ως Πληροφοριακό Σύστημα, ορίζουμε ένα οργανωμένο σύνολο πέντε στοιχείων (Ανθρώπων, Υλισμικού, Λογισμικού, Διαδικασιών και Δεδομένων), που αλληλεπιδρούν μεταξύ τους, όπως και με το περιβάλλον, σκοπεύοντας στην παραγωγή και διαχείριση πληροφοριών, προς εξυπηρέτηση προκαθορισμένων ανθρωπίνων αναγκών, εντός του πλαισίου ενός οργανισμού.

Απαιτείται φυσικά η ανάπτυξη μιας σαφούς εταιρικής πολίτικης ασφαλείας, κατανοητής και κοινώς αποδέκτης. Διακλαδώνεται σε Οργανωσιακό και Τεχνικό κομμάτι.

Το πρωτο, αναπτύσσεται σε ένα executive level έγγραφο που δεν τροποποιείται συχνά και αποσαφηνίζει τις κοινές και τις εξατομικευμένες ευθύνες κάθε ρόλου, εντός του οργανισμού. Ορίζει τη στρατηγική ασφαλείας και τον τρόπο υλοποίησης της.
Το δεύτερο παρέχει συχνά αναθεωρούμενες τεχνικές οδηγίες ορθής χρήσεως και προστασίας των τεχνολογικών πόρων. (ISO/IEC 29134:2017)

Υπενθυμίζεται πως κάθε πολιτική ασφαλείας θα πρέπει να καλύπτει <u>όλες</u> τις Αρχές Ιδιωτικότητος, όπως αναλυθήκαν στο Κεφάλαιο 2. Αλλιώς, είναι ανεπαρκής και <u>παράνομη</u>.

<u>Β) Βασικές επιταγές Ασφαλείας</u>.

Επιταγές προστασίας δεδομένων, ήδη από το σχεδιασμό των πληροφοριακών μας συστημάτων επεξεργασίας και εξ' ορισμού (data protection by design and by default). Το άρθρο 25 του ΓΚΠΔ, επιβάλει σε κάθε υπεύθυνο επεξεργασίας την υποχρέωση να διασφαλίζει το απόρρητο των υπο κατοχή τους απλών και ευαίσθητων δεδομένων, ήδη από το σχεδιασμό (by design) και εξορισμού (by default).

Ο υπεύθυνος, οφείλει διαρκώς να γνωρίζει και να λαμβάνει υπόψη τις τελευταίες εξελίξεις σε νομικό και τεχνολογικό επίπεδο, τη φύση και το κόστος εφαρμογής τυχόν νέων οργανωτικών και τεχνικών μέτρων, τους σκοπούς κάθε πιθανής επεξεργασίας και κυρίως των πιθανών επιπτώσεων σε περίπτωση που αυτή δεν γίνει με ασφάλεια (πχ. ζημιά σε θεμελιώδη δικαιώματα και ελευθερίες φυσικών πρόσωπων).
Τα θεμελιωδέστερα προτεινόμενα και υποχρεωτικά μέτρα, είναι η Ψευδονωμοποίηση και η Ελαχιστοποίηση των δεδομένων, όπως και η ενσωμάτωση συγκεκριμένων εγγυήσεων, όπως αυτές απαιτούνται από τον ΓΚΠΔ, ώστε να διασφαλίζονται στο μέγιστο τα δικαιώματα των υποκειμένων.

Ως ''Ψευδονωμοποίηση'', ορίζεται η επεξεργασία προσωπικού χαρακτήρος δεδομένων ώστε αυτά να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο, εκτός αν ο υπεύθυνος επεξεργασίας κάνει χρήση συμπληρωματικών πληροφοριών του υποκειμένου, οι οποίες νοείται ότι φυλάσσονται ξεχωριστά και επίσης υπόκεινται σε οργανωτικά και τεχνικά μέτρα. (Sharma & Menon 2020: 67)

Η ψευδονωμοποίηση δύναται να επιτευχτεί με ποικιλία τρόπων, όπως:

- Με κρυπτογράφηση: όπου τα αρχικά δεδομένα καθίστανται ακατάληπτα και αυτό δύναται να αντιστραφεί μόνο με τη χρήση 'κλειδιών'.
- Το Data Masking: τεχνική προστασίας με κάλυψη μέρους των δεδομένων με τυχαίους χαρακτήρες (π.χ. Αντωνακόπουλος Ιωάννης → AxxxxxxΣ Ixxxxς).
- Το Θόλωμα (blurring): Ενδείκνυται για εφαρμογή κυρίως σε εικονοσκοπήσεις (βίντεο) ή φωτογραφίες υποκειμένων, θολώνοντας το πρόσωπο τους σε βαθμό που η αναγνώριση του να καθίσταται μη εφικτή από μη εξουσιοδοτημένα πρόσωπα.
- Αναγραμματισμός στοιχείων PII (π.χ. Κυρίτσης → ηςρυστΚρ).

Ως ''Ελαχιστοποίηση'', ορίζεται η υποχρέωση του υπευθύνου επεξεργασίας να διασφαλίζει ότι θα τίθενται υπο επεξεργασία μόνον τα απαραίτητα για τον εκάστοτε σκοπό, προσωπικά δεδομένα. Βασίζεται προφανώς στην προαναφερθείσα Αρχή της Ελαχιστοποίησης. (Ζωγραφόπουλος 2018: 44-50)

Γ. Επιπλέον επιταγές Ασφαλείας.

Το αρ.32 του ΓΚΠΔ, καθορίζει επιπλέον πρόνοιες που οφείλουν να λαμβάνονται σε κάθε επεξεργασία και δεσμεύουν τον υπεύθυνο επεξεργασίας κάθε εκτελούντα και φυσικό πρόσωπο με αδειοδοτημένη πρόσβαση:

- Να δύνανται να διασφαλίζουν σε μόνιμη και αδιάλειπτη βάση την ακεραιότητα, τη διαθεσιμότητα, την αξιοπιστία, το απόρρητο της υπηρεσίας.
- Να δύνανται να αποκαταστήσουν τη διαθεσιμότητα και πρόσβαση των δεδομένων εν ευθέτω χρόνο σε περίπτωση τεχνικού ή φυσικού γεγονότος. Να διερευνήσουν τα αίτια πρόκλησης του ώστε να αποτρέψουν μελλοντική επανάληψη.
- Να διεξαγάγουν τακτικές, διαγνωστικού/προληπτικού χαρακτήρα δοκιμές των υφιστάμενων τεχνικών και οργανωτικών μέτρων, για έγκαιρο εντοπισμό τυχόν ευπαθειών, οι οποίες δυνάμει θα μπορούσαν να οδηγήσουν σε συμβάντα όπως: τυχαία ή εσκεμμένη καταστροφή, αλλοίωση ή απώλεια, προσπέλαση, κοινοποίηση ή πώληση προσωπικών δεδομένων ή οποιαδήποτε άλλη έκνομη επεξεργασία.

Το αρ.35 γίνεται πιο συγκεκριμένο και υποχρεώνει υπεύθυνο και εκτελούντες για τα κάτωθι, σε κάθε περίπτωση επεξεργασίας:

- Να λαμβάνουν μέτρα ώστε κάθε φυσικό και νομικό πρόσωπο επεξεργαζόμενο προσωπικού χαρακτήρος δεδομένων, να λειτούργει μόνον κατόπιν εντολής από τον υπεύθυνο επεξεργασίας.
- Σε περίπτωση παροχής δεδομένων για κλινική έρευνα και πειράματα, να έχουν διασφαλίσει την ανωνυμοποίηση των δεδομένων των υποκειμένων, την πρότερη ενημέρωση και λήψη γραπτής έγκρισης τους, όπως έχει προαναφερθεί.
- Να έχει προσδιοριστεί ονομαστικά το ποια φυσικά πρόσωπα (κατόπιν αξιολόγησης της φερεγγυότητας τους) θα έχουν πρόσβαση σε ποιες ακριβώς κατηγορίες προσωπικών δεδομένων και σε ποια συστήματα αρχειοθέτησης επεξεργασιών, κατόπιν διαμόρφωσης συγκεκριμένης πολιτικής ασφαλείας που θα επιτρέπει την πρόσβαση στα εν λόγω συστήματα.
- Η πρόσβαση να γίνεται μόνον με χρήση εξατομικευμένων κωδικών, οι οποίοι θα φυλάσσονται ασφαλώς, υπο την ευθύνη του κατόχου τους και τα τροποποιούνται σε τακτά διαστήματα.
- Να γίνονται τακτές αναβαθμίσεις λογισμικών, ιδίως αντιϊκής προστασίας.
- Να ελέγχεται και αποτρέπεται η αυθαίρετη απόσπαση σε εξωτερικά αποθηκευτικά μέσα προσωπικών δεδομένων ασθενών, μα και η εισαγωγή μέσω αυτών μη εγκεκριμένων λογισμικών στα πληροφοριακά συστήματα του υπευθύνου επεξεργασίας.
- Η τήρηση και συχνή ενημέρωση αντιγράφων ασφαλείας των δεδομένων και των επεξεργασιών τους σε κρυπτογραφημένη μορφή και νεφοϋπολογιστικό περιβάλλον.
- Η ασφαλής καταστροφή δεδομένων μετά το πέρας της υποχρεωτικής περιόδου τηρήσεως τους.
- Η τακτική επικαιροποίηση των πολιτικών ασφαλείας, λαμβάνοντας υπόψη τυχούσα πείρα από συμβάντα παραβίασης, είτε εντός, είτε σε αλλά νοσοκομεία και σχετικούς φορείς και με κύριο γνώμονα τη μη επανάπαυση, καθότι δε δύναται να υπάρξει πολιτική ασφαλείας που να μας καλύπτει απαράλλακτη εις το διηνεκές.

Τυχόν παραβιάσεις των ως άνω, δύνανται να οδηγήσουν σε βαριές κυρώσεις, πειθαρχικές, αστικές και ποινικές.

Πρέπει, ωστόσο, να διευκρινιστεί ότι τα ως άνω μέτρα, θεωρούνται επαρκή μόνον σε περιπτώσεις όπου δεν λαμβάνουν χώρα ευρείας κλίμακας επεξεργασίες προσωπικών δεδομένων, όπως σε γραφεία ιδιωτών ιατρών, φυσικοθεραπευτών, διατροφολόγων και ομοίων επαγγελματιών. Σε περίπτωση νοσοκομείου ή άλλου μεγάλου παρόχου υπηρεσιών υγείας, όπου επεξεργάζονται προσωπικά δεδομένα μεγάλου πλήθους υποκειμένων ετησίως, όλα τα ως άνω είναι βεβαίως υποχρεωτικά και πάλι όμως, δεν θεωρούνται επαρκή. Απαιτείται και διενέργεια Μελέτης Αντικτύπου. (Ζωγραφόπουλος 2018: 44-50)

Δ. DPIA (Data Protection Impact Assessment).

Το ‘’απόλυτο εργαλείο’’ αξιολόγησης του έκαστοτε τρέχοντος επιπέδου ασφάλειας, αποτελεί η Εκτίμηση Αντικτύπου Προστασίας Δεδομένων (ΕΑΠΔ) ή DPIA ή συντομότερα, ‘’Μελέτη Αντικτύπου’’ και επιβάλλεται από το άρθρο 35 του ΓΚΠΔ.

Κατά την 84η αιτιολογική σκέψη αυτού, σε περιπτώσεις όπου ένας υπεύθυνος επεξεργασίας διενεργεί πράξεις επεξεργασίας με υψηλή πιθανότητα έκθεσης σε κίνδυνο των δικαιωμάτων και των ελευθεριών των φυσικών προσώπων, ο υπεύθυνος υποχρεούται σε άσκηση μελέτης αντίκτυπου, όπου θα αξιολογηθεί το εάν υφίστανται κίνδυνοι, η φύση, η προέλευση, σοβαρότητα αυτών, τα μέτρα αντιμετώπισης και μελλοντικής τους αποτροπής, ώστε η επεξεργασία να είναι σε συμφωνία με τον Κανονισμό.

Ως ‘’Κίνδυνο’’, ορίζουμε τον κάθε ευλόγως αναγνωριζόμενο παράγοντα ή γεγονός με δυνητικά δυσμενείς επιπτώσεις στην ασφάλεια των δεδομένων του υποκειμένου, όπως: σωματική, ψυχική ή υλική βλάβη, δυσφήμιση ή διακρίσεις εναντίον του, υποκλοπή και κατάχρηση ταυτότητας, δημόσια έκθεση των θρησκευτικών, πολιτικών και φιλοσοφικών τους φρονημάτων, γενετικών τους δεδομένων ή στοιχεία για ενδεχόμενες ποινικές καταδίκες.

Η εκτίμηση αντικτύπου είναι ένα δυναμικό και επαναλαμβανόμενο σύνολο ενεργειών, πραγματοποιούμενο από τον εκάστοτε υπεύθυνο επεξεργασίας και αποτελεί ένα από τα εργαλεία συμμόρφωσης ως προς την Αρχή της Λογοδοσίας. Ο ΓΚΠΔ, συμπεριέλαβε το χαρακτηριστικό της λογοδοσίας (accountability) εντός των Θεμελιωδών Αρχών που διέπουν την επεξεργασία δεδομένων, ώστε ο υπεύθυνος να φέρει την ευθύνη και να βρίσκεται σε θέση να αποδείξει τη συμμόρφωση του με τις επιταγές του Κανονισμού.

Η DPIA, λαμβάνει χώρα κάθε φορά που έχουν προηγηθεί αλλαγές στα είδη των επεξεγαζομένων δεδομένων, στη φύση και στο πεδίο εφαρμογής τους, στο νομικό πλαίσιο που τη διέπει, στους σκοπούς που εξυπηρετούν και στα τεχνικά μέσα που χρησιμοποιούνται.

Ο Κανονισμός, επιτάσσει διεξαγωγή DPIA σε οργανισμούς που ασκούν σε μεγάλη κλίμακα έστω μια εκ των κάτωθι δραστηριοτήτων:

- Δημιουργία και επεξεργασία προφίλ φυσικών προσώπων για εκτεταμένες και συστηματικές επεξεργασίες με σκοπό τη λήψη αποφάσεων με άμεσες επιπτώσεις, σωματικές και νομικές, στα υποκείμενα.
- Επεξεργασία ευαίσθητων δεδομένων σε μεγάλη κλίμακα ή δεδομένων σχετικών με ποινικές καταδίκες.
- Κάθε συστηματική επιτήρηση ασφαλείας δημοσίων χώρων, με ηλεκτρονικά εποπτικά μέσα.
- Επεξεργασίες Big Data, δηλαδή ποσοτήτων προσωπικών δεδομένων σε εθνικό και διεθνές επίπεδο (εκατομμυρίων ανθρώπων) με δυνητικές επιπτώσεις στα δικαιώματα τους. (Sharma & Menon 2020: 74-75)

Είναι προφανές πως και οι τέσσερις αυτές δραστηριότητες συντρέχουν σε ένα σύστημα παροχής υπηρεσιών υγείας και μάλιστα κατά κόρων.

Μεθοδολογική προσέγγιση της DPIA.

Ο Υπεύθυνος Επεξεργασίας φέρει την ευθύνη της προετοιμασίας και της διεξαγωγής της Μελέτης. Αρχικά, ζητεί από τον DPO και κατά δεύτερο λόγο και τους εκτελούντες επεξεργασίες, να συνδράμουν με συμβουλές γραπτώς τεκμηριωμένες (αρ.35 παρ.2 και αρ.28 παρ.3).

Επίσης, κατά το αρ.28 παρ.9, ο Υπεύθυνος οφείλει να επιζητήσει τις απόψεις των υποκειμένων των δεδομένων ή έστω των συνοδών τους και στην περίπτωση που το θεωρεί μή εφικτό, να τεκμηριώσει το λόγο. Τέτοιοι λόγοι μπορεί να αποτελούν: η διαφύλαξη διαβαθμισμένων επιχειρηματικών πλανών, η προστασία δημοσίων συμφερόντων ή η ανάγκη διαφύλαξης των μεθόδων επεξεργασίας.

Επιπλέον, κατά την ανάπτυξη νέων συστημάτων και κατά ορθή πρακτική, πρέπει να ζητούνται και οι απόψεις ειδικευμένων επιστημόνων όπως: νομικών, ειδικών ασφαλείας πληροφοριών και δικτύων, ειδικούς ανάλυσης και ανάπτυξης πληροφοριακών συστημάτων και σχετικού λογισμικού, κοινωνιολόγους, τη διοίκηση του φορέα και κάθε εμπλεκόμενο.
Το διεθνές πρότυπο ISO/IEC 29134:2017 μπορεί να αξιοποιηθεί ως μεθοδολογία εκπόνησης DPIA. Για τον προσδιορισμό των αναγκαίων οργανωτικών και τεχνικών μέτρων, μπορούν να αξιοποιηθούν τα πρότυπα ISO/IEC 27002 και 29151.

Καθ' όλη τη διάρκεια της προετοιμασίας και διεξαγωγής της Μελέτης, ο DPO θα πρέπει να έχει κεντρικό ρόλο, καθότι διαθέτει μοναδική εξειδίκευση στο αντικείμενο, όπως απαιτούν τα κριτήρια διορισμού του, συμβουλεύοντας σε ζητήματα όπως το κατά πόσο χρειάζεται εκτέλεση Μελέτης, τη μεθοδολογία που θα ακολουθηθεί, το κατά πόσο ο φορέας είναι ικανός να διεξαγάγει αξιόπιστη Μελέτη ή το αν θα πρέπει να ανατεθεί σε ιδιώτη εργολάβο μέσω outsourcing. Προτείνει νέα οργανωσιακά και τεχνικά μέτρα για αναβάθμιση της ασφαλείας και επιβλέπει συνολικά τη διαδικασία.

Με την εκτέλεση της DPIA, ο υπεύθυνος επεξεργασίας θα πρέπει να αξιολογήσει το κατά πόσο ο μηχανισμός επεξεργασιών που έχει στηθεί, επιτυγχάνει:

- Αποτροπή άσκησης ελέγχου στα ατομικά δεδομένα.
- Περιορισμό της πρόσβασης των χρηστών στις απολύτως απαραίτητες πληροφορίες.
- Την αποσόβηση διακρίσεων πάσης φύσεως.
- Την αποτροπή ενδεχόμενης υποκλοπής στοιχείων PII, οικονομικής ζημίας ή δυσφήμισης του υποκειμένου.
- Την αποτροπή οποιασδήποτε πρόσβασης σε στοιχεία που αφορούν στην: κατάσταση της υγείας, την προσωπικότητα, την εργασιακή απόδοση, την αξιοπιστία, τη συμπεριφορά του υποκειμένου, τη διεύθυνση κατοικίας του, τις ποινικές του καταδίκες και οτιδήποτε άλλο σημαντικό. (Sharma & Menon 2020: 76)

<u>Εκτέλεση της DPIA.</u>

Αρχικά, προσδιορίζεται η ομάδα εργασίας, με ορισμό τον DPO, υπευθύνου συντονισμού και υπευθύνου έγκρισης της τελικής Εκτίμησης, ρόλους που είθισται να αναλαμβάνει ο πρώτος. Καθορίζεται το πεδίο διερεύνησης και τα κριτήρια σοβαρότητας κάθε κινδύνου, βάσει συγκεκριμένων κλιμάκων αξιολόγησης των επιπτώσεων τους.

Προσδιορίζεται ο προϋπολογισμός, το χρονοδιάγραμμα και η εμπλοκή κάθε ενδιαφερομένου (από τις προαναφερθείσες ειδικότητες) και ξεκινά η διαβούλευση, όπου προσδιορίζονται οι υποβόσκοντες κίνδυνοι, αφού πέραν των προφανεστέρων (παράνομη τροποποίηση, απώλεια και κλοπή), μπορεί να εντοπιστούν και άλλοι, όπως: η μη τήρηση Άρχων όπως της Ελαχιστοποίησης και η μη ικανοποίηση των δικαιωμάτων των υποκειμένων για ενημέρωση, πρόσβαση και αντίρρηση, η παραβίαση λοιπών δικαιωμάτων και ελευθεριών τους, κενά ασφαλείας σε επίπεδο λογισμικού, μηχανολογικού εξοπλισμού και ελλιπής εκπαίδευση ή αναξιοπιστία εκτελούντων επεξεργασίες.

Κατόπιν, οι κίνδυνοι, αφού ιεραρχούνται, κρίνεται ο τρόπος αντιμετώπισης τους, από τρεις εναλλακτικές επιλογές: Τη ‘’μείωση’’, τη ‘’διατήρηση’’ και τη ‘’μεταβίβαση’’ τους.

- Στην πρώτη περίπτωση, επιδιώκουμε τη μεγίστη δυνατή απομείωση των ανιχνευθέντων κινδύνων με εφαρμογή καταλλήλων μέτρων.
- Στη δεύτερη, δεν προβαίνουμε σε κινήσεις διότι οι ανιχνευθέντες κίνδυνοι έχουν αξιολογηθεί ως μή σημαντικοί.
- Στην τρίτη, κάνουμε (έστω μερική) μεταβίβαση του κινδύνου μέσω ασφάλισης (σύμβασης με ασφαλιστική εταιρία). Αυτό, δύναται να ανακουφίσει οικονομικά τον υπεύθυνο επεξεργασίας σε περίπτωση επιβολής προστίμου από την αρμοδία εποπτική Αρχή, μα σίγουρα δεν θα αποτρέψει την αμαύρωση της δημοσίας εικόνας του φορέως.

Τα κατάλληλα μέτρα που αφορούν στην πρώτη περίπτωση μπορεί να είναι: ο περιορισμός των συνεπειών από επέλευση κινδύνου, η εξουδετέρωση πηγών κινδύνου, η μείωση αδυναμιών των πληροφοριακών συστημάτων, η αποτροπής επίτευξης συμβάντων παραβίασης μα και η ανάκαμψη από αυτά.

Πληθώρα τέτοιων μέτρων προβλέπονται στα ISO 27100 και 29000, ορισμένα εκ των οποίων είναι: ο φυσικός και ηλεκτρονικός έλεγχος πρόσβασης, χρήση up-to-date antivirus, εντοπισμός υπόπτων κινήσεων. (Κατευθυντήριες Γραμμές Ομάδας Άρθρου 29 2017: 17-25)

Η αποτελεσματικότητα κάθε μέτρου επαναξιολογείται μέχρι να εξαλειφθεί ή απομειώσει τον στοχευόμενο κίνδυνο σε αποδεκτά κατά ΓΚΠΔ επίπεδα.

Κατά το άρθρο 36, μετά το πέρας κάθε DPIA, κάθε φορέα υπηρεσιών υγείας, ηλεκτρονικό αντίγραφο της τελικής αναφοράς οφείλει να αποστέλλεται στον DPO του υπουργείου υγείας, μα και στην την αρμόδια Εποπτική Αρχή προς έλεγχο και έγκριση.

Συμπερασματικά, το κατά πόσο μια Μελέτη Αντικτύπου αποδειχτεί επιτυχής ή όχι, θα εξαρτηθεί από κριτήρια όπως:

- Το κατά πόσο ενθάρρυνε τη συμμετοχή κάθε εμπλεκομένου να εκφράσει απόψεις ή αντιρρήσεις.
- Την ικανότητα της ομάδος για εν τω βάθει ανάλυση, εντοπισμό, αξιολόγηση και αντιμετώπιση κινδύνων ασφαλείας δεδομένων.
- Το κατά πόσο φαίνεται να σέβεται τα δικαιώματα των υποκειμένων και επιτυγχάνει συμμόρφωση με κάθε Αρχή Ιδιωτικότητος και κώδικα δεοντολογίας.
- Η άσκηση των επεξεργασιών με χρήση καταλλήλου hardware, software, ανθρωπίνου δυναμικού και κανονιστικού πλαισίου επεξεργασίας.

Η Σύνταξη της τελικής αναφοράς της Μελέτης.

Ως εύλογο, με το πέρας της DPIA, συντάσσεται η τελική έκθεση με τα αποτελέσματα της, η οποία αποτελεί ένα μακροσκελές κείμενο με λεπτομερείς αναφορές σε θέματα εσωτερικής λειτουργιάς και θέματα τεχνικής φύσεως.

Στο τελικό αυτό κείμενο, ο Κανονισμός επιβάλει να περιέχονται τουλάχιστον τα εξής:

- Οι σκοποί της επεξεργασίας και τα νόμιμα συμφέροντα που επιδιώκονται.
- Μια διεξοδική περιγραφή του προβλεπομένου τρόπου επεξεργασίας.
- Την αξιολόγηση της Αναγκαιότητας και της Αναλογικότητας της επεξεργασίας ως προς τους επιδιωκόμενους σκοπούς.
- Την αξιολόγηση του κατά πόσο η σχεδιαζόμενη επεξεργασία είναι ασφαλής για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.
- Ποια μέτρα προβλέπονται για την αντιμετώπιση των κενών ασφαλείας και το κατά πόσο αυτά συμβαδίζουν (με αποδείξεις) με τις Αρχές του Κανονισμού.
- Έρευνα με τις απόψεις των υποκειμένων, εφόσον υφίσταται. (Κατευθυντήριες Γραμμές Ομάδας Άρθρου 29 2017: 17-25)

Η εμπλοκή της Εποπτικής Αρχής.

Σε κάθε περίπτωση, είτε πρόκειται για την πρώτη φορά που ο οργανισμός διεξάγει σχετική Μελέτη, είτε όχι, είναι υποχρεωτικό η αρμόδια Εποπτική Αρχή (στην Ελλάδα η ΑΠΔΠΧ), να έχει πρώτα αξιολογήσει και εγκρίνει την πραγματοποιηθείσα DPIA.
Ακόμα περισσότερο στην περίπτωση που παρά τη συνεχόμενη λήψη μέτρων, οι κίνδυνοι συνεχίζουν να παραμένουν υψηλοί, διακυβεύοντας δικαιώματα και ελευθερίες φυσικών προσώπων, ο Υπεύθυνος επεξεργασίας υποχρεούται να μην ξεκινήσει ή να διακόψει κάθε επεξεργασία και να έρθει σε επαφή με την ΑΠΔΠΧ, την οποία θα ενημερώσει με πάσα λεπτομέρεια, ώστε εν ευθετώ χρόνω αποσταλεί γραπτή απάντηση με συμβουλές προς τον Υπεύθυνο επεξεργασίας.

Πιο συγκεκριμένα, θα πρέπει να υποβληθεί στην εποπτική Αρχή φάκελος του φορέα, που θα περιλαμβάνει:

- Την ίδια την DPIA.
- Τα στοιχειά επικοινωνίας του DPO.
- Τις αντίστοιχες αρμοδιότητες Υπευθύνου και κάθε εκτελούντα επεξεργασίες.
- Τους σκοπούς και τα μέσα τις επιδιωκόμενης επεξεργασίας.
- Τα μέτρα που ελήφθησαν και ετέθησαν σε ισχύ για την προστασία των δικαιωμάτων και των ελευθερίων των υποκειμένων.
- Οποιαδήποτε άλλη λεπτομέρεια ζητηθεί από την Αρχή.

Η Εποπτική Αρχή, υποχρεούται να απαντήσει εντός 8 εβδομάδων, με την επιφύλαξη για επιπλέον 6, σε περίπτωση Μελέτης υψηλής πολυπλοκότητας.

Σε περίπτωση που η προβλεπόμενη διαδικασία επεξεργασιών όντως κριθεί ανεπαρκής για τις επιταγές του GDPR, η Αρχή δύναται να:

- Ενημερώσει τον Υπεύθυνο ότι ο μηχανισμός που έχει εγκαταστήσει, παραβιάζει τον Κανονισμό.
- Απορρίψει τη Μελέτη και να επιβάλει στους εμπλεκομένους να προβούν στις απαραίτητες βελτιώσεις εντός ευλόγου χρόνου.
- Παράσχει συμβουλευτική υποστήριξη για την επίτευξη των βελτιώσεων.
- Προβεί σε ενδελεχέστερη διερεύνηση σε περίπτωση που το πρόβλημα επιμείνει.

(Κοτσαλής & Μενουδάκος 2018: 224)

Κεφάλαιο 7

Data Breaches και υποχρεώσεις Υπευθύνου επεξεργασίας.

Στο αρ.4 παρ.12 του ΓΚΠΔ, ο ενωσιακός νομοθέτης, έχει ορίσει την ‘’παραβίαση δεδομένων’’ ως: «*παραβίαση ασφαλείας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ αδείας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρος, που διαβιβαστήκαν, αποθηκεύτηκαν ή υπεβλήθησαν καθ’ οποιονδήποτε τρόπο σε επεξεργασία*».

Αποτελεί συχνή διαπίστωση ότι οργανισμοί και επιχειρήσεις που πέφτουν θύματα τέτοιων επιθέσεων (παραβίασης δεδομένων που επεξεργάζονται-data breach), επιχειρούν συγκάλυψη του γεγονότος, καθώς ενδεχομένη κοινολόγηση του, πιθανότατα θα επιφέρει νομικές επιπτώσεις (π.χ. καταδίκες αποζημίωσης) και βεβαιότατα δυσφήμιση της εταιρίας με πιθανές μακροπρόθεσμες συνέπειες (έως και χρεοκοπία).

Οι οργανισμοί υπηρεσιών υγείας, δημόσιοι και ιδιωτικοί, κερδοσκοπικοί και μη, δεν παύουν να αποτελούν πιθανούς στόχους για έξωθεν ή και εκ των ένδον επιθέσεις ή και ακούσιες διαρροές.

<u>Η υποχρέωση ενημέρωσης της αρμοδίας Αρχής.</u>

Στο ίδιο άρθρο, ο Κανονισμός υποχρεώνει τον φορέα-υπεύθυνο επεξεργασίας σε αμελλητί γνωστοποίηση της παραβίασης στην αρμόδια Αρχή (ΑΠΔΠΧ), εντός 72 ωρών από τη στιγμή που απεκτήθη γνώση του γεγονότος και εφόσον ο υπεύθυνος διαθέτει έναν εύλογο βαθμό βεβαιότητος ότι πράγματι το συμβάν κατέληξε σε διαρροή δεδομένων.

Πιο συγκεκριμένα, είναι υποχρέωση του οποιουδήποτε φυσικού προσώπου με πρόσβαση στα Π.Σ. του νοσοκομείου μα και οποιουδήποτε εκτελούντος επεξεργασίες, εφόσον αντιληφτεί παραβίαση να ενημερώσει τον DPO του νοσοκομείου, ώστε να προβεί στα δέοντα.

Τι οφείλει να γνωστοποιηθεί στην ΑΠΔΠΧ.

α) Η φύση της παραβίασης, οι κατηγορίες και ο αριθμός των επηρεαζομένων υποκειμένων (έστω κατά προσέγγιση), όπως και ο αριθμός των αρχείων που επηρεαστήκαν.

β) Τα πλήρη στοιχεία επικοινωνίας του DPO, του φορέως-θύμα, όπως και οποιουδήποτε άλλου φυσικού ή νομικού προσώπου δύναται να παράσχει επιπλέον πληροφορίες.

γ) Τις εκτιμώμενες συνέπειες της παραβίασης.

δ) Περιγραφή των ληφθέντων και προτεινομένων μέτρων αντιμετώπισης της παραβίασης και μετριασμού των συνεπειών της.

Να σημειωθεί ότι δεν υπάρχει υποχρέωση γνωστοποίησης στην ΑΠΔΠΧ, εφόσον τα παραβιασθέντα δεδομένα είναι φύσεως τέτοιας που δεν ενδέχεται να προκληθούν κίνδυνοι για τα δικαιώματα και τις ελευθερίες των υποκειμένων.

Τέτοια, μπορεί να αποτελούν στοιχεία ήδη δημοσίως προσιτά ή στοιχεία που έχουν καταστεί μή προσπελάσιμα από μή εξουσιοδοτημένους, χάρη σε κατάλληλη κρυπτογράφηση.

Υποχρέωση ενημέρωσης των υποκειμένων των δεδομένων.

Κατά το αρ.34 παρ.1 του ΓΚΠΔ, υφίσταται υποχρέωση του υπευθύνου επεξεργασίας να ενημερώσει το υποκείμενα για την παραβίαση των δεδομένων τους, εφόσον υφίσταται ενδεχόμενο υψηλού ρίσκου για τα δικαιώματα και τις ελευθερίες των. Τους ανακοινώνονται ακριβώς οι ίδιες πληροφορίες όπως στην ΑΠΔΠΧ, πλην του στοιχείου (α). (Κοτσαλής & Μενουδάκος 2018: 225)

Η επικοινωνία με τα φυσικά αυτά πρόσωπα, θα πρέπει καταρχήν να είναι άμεση και ειδική. Ειδάλλως, θα πρέπει να επιλέγεται μέθοδος κοινοποίησης που μεγιστοποιεί τις πιθανότητες γνωστοποίησης στο σύνολο των θυμάτων (π.χ. δημόσια ανακοίνωση).

Η περίπτωση απόκρυψης γεγονότος παραβίασης.

Η παράληψη γνωστοποίησης μιας παραβίασης στην αρμόδια Αρχή ή/και στα υποκείμενα των δεδομένων, αποτελεί παράβαση του Κανονισμού και δύναται να επιφέρει διοικητικές κυρώσεις (κατά το αρ.84 παρ.4) και να επιβάλλει διορθωτικά μέτρα (αρ.58). Οι διοικητικές κυρώσεις αφορούν πρόστιμα έως 10 εκατομμύρια ευρώ ή σε περίπτωση ιδιωτικής εταιρίας, έως και το 2% του συνολικού παγκοσμίου ετησίου τζίρου (όποιο είναι το υψηλότερο). Επιπλέον, προβλέπεται διπλασιασμός των ως άνω σε περίπτωση υποτροπής.

Κατά το αρ.33 του Κανονισμού, κάθε περιστατικό παραβίασης θα πρέπει κοινοποιείται και στον DPO του Υπουργείου Υγείας, διότι αυτός έχει επιφορτιστεί με την εποπτεία όχι μόνον καθεαυτού του Υπουργείου, μα κάθε φορέως υπαγομένου σε αυτό, για το κατά πόσον τηρούν τις υποχρεώσεις που απορρέουν από τον Κανονισμό.

Εν κατακλείδι, εφόσον το περιστατικό έχει πλέον λάβει χώρα, ο εν λόγω φορέας/υπεύθυνος επεξεργασίας οφείλει τουλάχιστον να διδάσκεται από αυτό. Να διερευνήσει για τα αίτια που οδήγησαν στην αποτυχία, να τα διορθώσει και να πράττει στο εξής το καθετί προς αποφυγήν επαναλήψεως τέτοιου συμβάντος. Μια ενδεχόμενη αδιάφορη, παθητική στάση, θα ήταν ο,τι πιο απαράδεκτο, αφού πέρα από πλήρως παράνομο, προλειαίνει και το έδαφος για νέες παραβιάσεις.
(Κοτσαλής & Μενουδάκος 2018: 227)

Ενδελεχέστερη επισκόπηση σε ζητήματα Προστίμων λόγω Data Breach.
Ο Κανονισμός, δεν προβλέπει συγκεκριμένη λίστα με παραβιώσεις και αντίστοιχο για την κάθε μια πρόστιμο, άλλα την ξεχωριστή αξιολόγηση κάθε περίπτωσης.

Η εποπτική Αρχή, οφείλει να διερεύνα για όλα τα ειδικά χαρακτηριστικά κάθε υπόθεσης, με τρόπο συνεκτικό, λεπτομερή, αντικειμενικό και τεκμηριωμένο, επιβάλλοντας διορθωτικά μέτρα ή/και πρόστιμα (ή απλή έγγραφη επίπληξη) συμβαδίζοντα με τη φύση, τη σοβαρότητα και τις συνέπειες της παραβίασης.

Το ίδιο το ΕΣΠΔ, ενθαρρύνει τις εγχώριες εποπτικές Αρχές των κρατών-μελών να ακολουθούν μια κατά το δυνατόν ισορροπημένη και σταθμισμένη προσέγγιση όσον αφόρα στις αποφάσεις μεταξύ προστίμων και επιπλήξεων. Ενθαρρύνει επισήμως την ανταλλαγή εμπειρίας και τεχνογνωσίας μεταξύ των ενωσιακών εποπτικών Άρχων, ώστε να προάγεται η μέγιστη δυνατή συνεκτικότητα για αντίστοιχες αποφάσεις, σε όλη την ΕΕ.

Κατά το άρθρο 83 παρ.2 προβλέπεται μια εκτεταμένη σειρά κατευθυντηρίων γραμμών για την εκτίμηση του κατά πόσο κάποια παράβαση θα πρέπει να τιμωρηθεί με πρόστιμο και ποιο το αναλογούν ύψος αυτού.

Συνοπτικά, είναι οι εξής:

- Το είδος, η βαρύτητα και η διάρκεια της παράβασης.
- Το κατά πόσο η παράβαση προκλήθηκε από δόλο ή αμέλεια.
- Το κατά πόσο Υπεύθυνος και Εκτελών, προέβηκαν σε ενέργειες που μετριάζουν τη ζημιά επί των υποκειμένων.
- Το κατά πόσο Υπεύθυνος και Εκτελών, είχαν λάβει όλα τα δέοντα και αναμενόμενα οργανωτικά και τεχνικά μέτρα πρόληψης/αποτροπής.
- Τυχόν προηγούμενο ιστορικό ανάλογων παραλείψεων.
- Το κατά πόσο επέδειξε αγαστή συνεργασία με την Αρχή αναφορικά με την επανόρθωση της ζημιάς και την αποτροπή ενδεχόμενης νέας.
- Το ποιες κατηγορίες δεδομένων εκτέθηκαν και σε ποια έκταση.
- Το εάν η Αρχή ειδοποιήθηκε εγκαίρως (εντός 72 ωρών) για την παραβίαση ή το πληροφορήθηκε από τρίτους (π.χ. από ανώνυμες καταγγελίες ή φημολογίες στα media).

Σημειώνεται ότι για την εκτίμηση του τύπου και βαρύτητας των κυρώσεων, παίζει ρόλο και το μέγεθος του Υπεύθυνου επεξεργασίας. Δηλαδή, όταν αυτός είναι φυσικό πρόσωπο (πχ. ιδιωτικό ιατρείο ή δικηγορικό γραφείο), δεν ενδείκνυται να του επιβληθεί το ίδιο πρόστιμο με μια μεγάλη διεθνή εταιρία, αφού η επιβάρυνση θα ήταν εξωπραγματικά δυσανάλογη. (Κατευθυντήριες Γραμμές Ομάδας Άρθρου 29 2017: 5-18)

Διευκρινίζεται ότι το άρθρο 84 του Κανονισμού, επιτρέπει στα κράτη-μέλη τη θέσπιση δικών τους, εθνικού επιπέδου κυρώσεων, για θέματα παραβίασης, αρκεί αυτά τουλάχιστον να είναι ισοδύναμης βαρύτητας με τις προβλεπόμενες εκ του Κανονισμού σχετικές διατάξεις. Δηλαδή, ένα κράτος-μέλος, θα μπορούσε να ψηφίσει νομοσχέδιο με σκληρότερες μόνον ποινές, όχι ελαφρύτερες. Πράγματι, το σχετικό ελληνικό νομοθέτημα, (Ν.4624/2019) δέχτηκε έντονες κριτικές από παράγοντες της αγοράς, καθότι εξάντλησε τη διακριτική του ευχέρεια στη βαρύτητα των ποινών. Συγκεκριμένα, προβλέπει ότι:

- *«Όποιος, χωρίς δικαίωμα: επεμβαίνει με οποιονδήποτε τρόπο σε σύστημα αρχειοθέτησης δεδομένων προσωπικού χαρακτήρα, και με την πράξη του αυτή λαμβάνει γνώση των δεδομένων αυτών τα αντιγράφει, αφαιρεί, αλλοιώνει, βλάπτει, συλλέγει, καταχωρεί, οργανώνει, διαρθρώνει, αποθηκεύει, προσαρμόζει, μεταβάλλει, ανακτά, αναζητεί πληροφορίες, συσχετίζει, συνδυάζει, περιορίζει, διαγράφει, καταστρέφει, τιμωρείται με φυλάκιση μέχρι ενός (1) έτους (εάν η πράξη δεν τιμωρείται βαρύτερα με άλλη διάταξη)».*

- *«Όποιος χρησιμοποιεί, μεταδίδει, διαδίδει, κοινολογεί με διαβίβαση, διαθέτει, ανακοινώνει ή καθιστά προσιτά σε μη δικαιούμενα πρόσωπα δεδομένα προσωπικού χαρακτήρα, τα οποία απέκτησε σύμφωνα με την περίπτωση της πρώτης παραγράφου ή επιτρέπει σε μη δικαιούμενα πρόσωπα να λάβουν γνώση των δεδομένων αυτών, τιμωρείται με φυλάκιση, (εάν η πράξη δεν τιμωρείται βαρύτερα με άλλη διάταξη)».*

- *«Εάν η ως άνω πράξη αφορά ειδικών κατηγοριών δεδομένα προσωπικού χαρακτήρα του άρθρου 9 παράγραφος 1 του ΓΚΠΔ ή δεδομένα που αφορούν ποινικές καταδίκες και αδικήματα ή τα σχετικά με αυτά μέτρα ασφαλείας του άρθρου 10 του ΓΚΠΔ, ο υπαίτιος τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή έως 100.000 ευρώ, (εάν η πράξη δεν τιμωρείται βαρύτερα με άλλη διάταξη)».*

- *«Εάν από τις πράξεις οποιασδήποτε εκ των άνωθι παραγράφων προκλήθηκε κίνδυνος για την ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή για την εθνική ασφάλεια, επιβάλλεται κάθειρξη και χρηματική ποινή έως 300.000 ευρώ».* (Opengov.gr)

Κεφάλαιο 8

Διαβιβάσεις προσωπικών δεδομένων ασθενών προς τρίτες χώρες.

Για την περίπτωση που απαιτηθεί μεταφορά ασθενούς από χώρα της Ε.Ε. ή του Ε.Ο.Χ. προς κάποια τρίτη, ο ΓΚΠΔ με τα άρθρα 44 έως 49, προβλέπει συγκεκριμένους μηχανισμούς που επιτρέπουν διαβιβάσεις προσωπικών δεδομένων έκτος Ε.Ε.

Επιγραμματικά:

- Η απόφαση επάρκειας της Ευρωπαϊκής Επιτροπής.
- Η ύπαρξη συγκεκριμένων Διασφαλίσεων για τα δεδομένα που θα διαβιβαστούν στο εξωτερικό (τρίτη χώρα).
- Ο Κατάλογος Παρεκκλίσεων εκ των άνωθι προϋποθέσεων, εφαρμοζόμενες σε ειδικές περιπτώσεις.

Αναλυτικότερα:

Α) <u>Διαβιβάσεις σύμφωνες με Αποφάσεις Επάρκειας</u>.

Η Ευρωπαϊκή Επιτροπή και οι εθνικές εποπτικές Αρχές (πχ. ΑΠΔΠΧ), παρακολουθούν συστηματικά τις εξελίξεις σε όλες τις τρίτες χώρες και αξιολογούν το κατά πόσο οι δημόσιες αρχές οι επιφορτισμένες με αρμοδιότητες σχετικές με την εθνική ασφάλεια, επεμβαίνουν στα Θεμελιώδη δικαιώματα των υποκειμένων σε βαθμό πέραν του απολύτως απαραιτήτου.

Συγκεκριμένα, αξιολογούνται κριτήρια όπως: το κράτος δίκαιου, ο σεβασμός στα ανθρώπινα δικαιώματα και θεμελιώδεις ελευθερίες, η ανεξαρτησία της δικαιοσύνης και των άρχων εποπτείας προσωπικών δεδομένων, τη δυνατότητα των υποκειμένων άσκησης αποτελεσματικών νομικών προσφυγών.

Κατόπιν σχετικών αξιολογήσεων που αναθεωρούνται περιοδικώς, έχει καταρτίσει τη λεγόμενη Λευκή Λίστα χωρών στις οποίες και επιτρέπεται εύκολα η διαβίβαση. Αυτές είναι: η Ανδόρα, η Αργεντινή, ο Καναδάς, τα Νησιά Φερόε, το Guernsey, το Ισραήλ, η Νήσος του Man, η Ιαπωνία, το Jersey, η Νέα Ζηλανδία, η Ελβετία και η Ουρουγουάη. Οι νομοθεσίες των χωρών αυτών αναφορικά με την προστασία των προσωπικών δεδομένων, αξιολογούνται ως ισοδύναμες με το δίκαιο της ΕΕ.

Επιπλέον, στη Λευκή Λίστα δεν συμμετέχουν μόνον χώρες, μα δύνανται να συμμετάσχουν και συγκεκριμένες δικαιοδοσίες, που μπορούν να χαρακτηριστούν επαρκείς προς διαβίβαση δεδομένων. Παράδειγμα: ο τομέας της υγείας ή ο χρηματοπιστωτικός τομέας μιας χώρας δύναται να ενταχθεί στη λίστα, ενώ η ίδια η χώρα να μην περιλαμβάνεται.

Ως επαρκείς, θεωρούνται και οι εταιρίες των ΗΠΑ που πληρούν τις νομικές προϋποθέσεις του μηχανισμού 'Privacy Shield', που υιοθετήθηκε τον Ιούλιο του 2016, δεδομένης της προηγηθείσης ψηφίσεως του GDPR. (Κοτσαλής & Μενουδάκος 2018: 269)

Β) <u>Διαβιβάσεις μέσω καταλλήλων Διασφαλίσεων</u>.

Ο ενωσιακός υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία, εφόσον διαπιστώσει ότι υφίστανται αποτελεσματικά ένδικα μέσα και ότι είναι εκτελεστά (στην τρίτη χώρα) τα θεμελιώδη δικαιώματα των υποκειμένων, μέσω Κωδίκων Δεοντολογίας και Μηχανισμών Πιστοποίησης, δύνανται να προχωρήσουν σε διαβίβαση (αρ.46).

Τέτοιες εγγυήσεις μπορεί να αποτελούν η ύπαρξη:

- Συγκεκριμένου δεσμευτικού μηχανισμού (συμφώνου με το αρ.42 του Κανονισμού) που εγγυάται πως ο υπεύθυνος ή ο εκτελών στην τρίτη χώρα, θα εφαρμόσει κάθε κατάλληλο προς διασφάλιση των δεδομένων, μεσο.
- Στην τρίτη χώρα, εγκεκριμένου Κώδικα Δεοντολογίας (συμφώνου με το αρ.40 του Κανονισμού) που εγγυάται τη διασφάλιση.
- Δεσμευτικού και εκτελεστού νομικού οχήματος, συμφωνημένου μεταξύ δημοσίων αρχών ή φορέων.
- Δεσμευτικών εταιρικών κανόνων, αρκεί να συμβαδίζουν με τις απαιτήσεις του ΓΚΠΔ (αρ.46-47,28-29,77,79). (Κοτσαλής&Μενουδάκος 2018: 271)

Γ) Παρεκκλίσεις εκ του Κανονισμού, για ειδικούς λογούς.

Όταν τα Α) και Β) δεν υφίστανται, σύμφωνα με το αρ.49 του Κανονισμού, δύνανται να εφαρμοστούν κάποιες ιδιαίτερες εξαιρέσεις για μεμονωμένα υποκείμενα δεδομένων (όχι για μαζικές επεξεργασίες), όπως:

- Το υποκείμενο, πλήρως ενημερωμένο για τους κινδύνους και με ανάληψη της πλήρους ευθύνης, συναινεί εγγράφως.
- Η διαβίβαση είναι αναγκαία για λόγους θεμελίωσης υπεράσπισης ή άσκησης ποινικών αξιώσεων.
- Όταν πρέπει να προστατευτούν τα ζωτικά συμφέροντα του υποκειμένου ή όταν αυτό είναι φυσικά ή νομικά μή ικανό να δώσει συγκατάθεση.
- Η διαβίβαση είναι απαραίτητη για σπουδαίους λόγους δημοσίου συμφέροντος, αρκεί να πρόκειται για λόγους αναγνωρισμένους από τη νομοθεσία της Ε.Ε. ή της χώρας μέλους όπου υπόκειται ο υπεύθυνος επεξεργασίας. (Κοτσαλής&Μενουδάκος 2018: 278)

Κεφάλαιο 9

Οι επιπτώσεις που επήλθαν στην επεξεργασία προσωπικών δεδομένων στο χώρο της υγείας, εξαιτίας της πανδημίας του ίου SARS-CoV-2.

Το Μάρτιο του 2020, με αφορμή το ξέσπασμα της πανδημίας του ιού SARS-CoV-2 (κορονοϊός) και της ασθένειας που αυτός προκαλεί, της COVID-19, η ΑΠΔΠΧ αναγνωρίζοντας το ιδιαίτερο και κρίσιμο της περιστάσεως, εξέδωσε ανακοίνωση με κατευθυντήριες γραμμές ως προς την επεξεργασία προσωπικών δεδομένων νοσούντων από τον συγκεκριμένο ιό, όπως και των συγγενών τους αλλά και των Υπευθύνων επεξεργασίας.

Οι κατευθυντήριες αυτές γραμμές, έχουν ως εξής:

Α) Κάθε πληροφορία αναφορικά με την κατάσταση της υγείας υποκειμένου το οποίο έχει ήδη διαγνωστεί θετικό τον ιό SARS-CoV-2, παραμένει διαβαθμισμένη ως ειδικής κατηγορίας δεδομένο, είτε ο ασθενής νοσηλεύεται από πάροχο υπηρεσιών υγείας, είτε νοσεί στην οικία του.

Β) Κάθε πληροφορία σχετική με την κλινική εικόνα ενός φυσικού προσώπου (πχ. συμπτώματα πυρετού, βήχα, καταρροής, δύσπνοιας, απώλεσης αισθήσεως της γεύσεως ή της οσφρήσεως), θεωρείται ευαίσθητο προσωπικό δεδομένο, αρκεί να έχει γίνει επεξεργασία του συγκεκριμένου δεδομένου, είτε αυτοματοποιημένη, είτε έγγραφη.

Συνεπώς, μια απλή ενημέρωση του υποκειμένου ότι ευρέθη θετικό στον ιό ή ότι η θερμοκρασία του ανιχνεύτηκε υψηλότερη του φυσιολογικού, δεν θεωρείται ευαίσθητο δεδομένο μα απλό, έως ότου επεξεργαστεί.

Διευκρινίζεται πως (κατά την Αρχή), πληροφορίες όπως: το ότι κάποιος συνεργάτης του υποκειμένου έχει βρεθεί θετικός στον ιό ή ότι ο συνεργάτης ή το ίδιο το υποκείμενο έχει ταξιδέψει πρόσφατα σε χώρα με έξαρση κρουσμάτων του ιού, δεν συνιστούν ευαίσθητες προσωπικές πληροφορίες, μα δύνανται υπο προϋποθέσεις να συνιστούν απλά δεδομένα προσωπικού χαρακτήρα.

Γ) Αναφορικά με τον ιδιωτικό τομέα, κατά την ΑΠΔΠΧ, κάθε εργοδότης οφείλει: «*να εξασφαλίζει την ασφάλεια και την υγεία του προσωπικού του, λαμβάνοντας κάθε αναγκαίο, συναφές προστατευτικό μέτρο προς αποφυγή κάθε σοβαρού, αμέσου και αναποφεύκτου κίνδυνου, εγγυώμενος το ασφαλές και υγιές του περιβάλλοντος εργασίας*».

Αφετέρου και οι εργαζόμενοι οφείλουν*:* «*να εφαρμόζουν κάθε κανόνα για την ασφάλεια των ιδίων και όποιων άλλων επηρεάζονται από τις πράξεις ή τις παραλείψεις τους (π.χ. ασθενείς), υποχρεούμενοι να αναφέρουν άμεσα στον εργοδότη ή στον εφημερεύοντα ιατρό, κάθε κατάσταση που πιθανώς συνιστά σοβαρό κίνδυνο για τη διασπορά του ιού».*

Οι εργοδότες, συνεχίζουν την επεξεργασία προσωπικών δεδομένων κατά τις γνωστές νομικές βάσεις των άρθρων 5,6 και 9, λαμβάνοντας υπόψη πλέον και τις ως άνω παραγράφους Α) και Β).

Δ) Επιπλέον, βάσει των νέων κατευθυντηρίων γραμμών, κάθε εργοδότης και για όσο διαρκεί η πανδημία, νομιμοποιείται να εγκαθιστά και χρησιμοποιεί στις εγκαταστάσεις του συσκευές θερμομέτρησης ανθρωπίνου σώματος ή/και υποχρεωτική συμπλήρωση φόρμας αναφορικά με ενδεχόμενη ή επιβεβαιωμένη νόσηση του ιδίου ή οικείου του προσώπου, πρόσφατη επίσκεψη σε κόκκινη περιοχή ή οτιδήποτε άμεσα σχετιζόμενο.

Νοουμένου και πάλι ότι θα πληρούνται οι παράγραφοι Α) και Β), πάντοτε προφανώς εντός του πλαισίου της Λογοδοσίας, της Ελαχιστοποίησης και κάθε ενδεδειγμένου τεχνικού και οργανωτικού μέτρου, όπως έχουν αναλυθεί.

Ξεκαθαρίζεται πως η ως άνω δυνατότητα έχει προσωρινό χαρακτήρα (όσο και η διάρκεια του καθεστώτος της πανδημίας) καθότι σε φυσιολογικές συνθήκες, τέτοιου είδους επεξεργασίες έχουν επαχθή χαρακτήρα και αποτελούν περιορισμό ανθρωπίνων δικαιωμάτων και άρα, δεν επιτρέπεται να αποκτήσουν χαρακτήρα γενικευμένο, παγιοποιημένο και συστηματικό.

Ε) Όπως προαναφέρθηκε, οι θανόντες, δεν τυγχάνουν των προστατευτικών προνομίων του Κανονισμού. Ωστόσο, κατά τις κατευθυντήριες γραμμές της Αρχής, ειδικά για τους θανόντες από κορονοϊό, προβλέπεται πλήρης προστασία των προσωπικών τους δεδομένων, όπως ακριβώς προβλέπεται και για τους εν ζωή ασθενείς. Η συγκεκριμένη πρόνοια, αποσκοπεί στην προστασία από ενδεχόμενη ταυτοποίηση, κοινωνικό στιγματισμό και στοχοποίηση εν ζωή συγγενών του θανόντος.

ΣΤ) Σε περίπτωση που κάποιος ασθενής-υποκείμενο των δεδομένων αποκαλύψει οικιοθελώς ότι νοσεί από κορονοϊό, ο πάροχος υπηρεσιών υγείας συνεχίζει να αντιμετωπίζει κανονικά τον ασθενή κατά τις επιταγές του Κανονισμού για την προστασία των ευαίσθητων προσωπικών δεδομένων.

Ζ) Η παροχή από τον φορέα πληροφοριών σε τρίτους, αναφορικά με την κατάσταση ασθενούς με κορονοϊό, ακόμα κι αν τηρεί πλήρως κάθε νόμιμη προϋπόθεση, δεν επιτρέπεται εάν υφίστανται βάσιμες υποψίες στιγματισμού και δημιουργίας προκαταλήψεως έναντι του υποκειμένου.

Η) Με ιδιαίτερη περίσκεψη θα πρέπει να γίνεται η αποκάλυψη προσωπικού χαρακτήρος στοιχείων ασθενών με κορονοϊό για δημοσιογραφικούς σκοπούς. Θα πρέπει να ‘ζυγίζεται’ προσεκτικά η αναγκαιότητα της αποκάλυψης και η έκταση των στοιχείων που θα αποκαλυφτούν. (Κατευθυντήριες Γραμμές ΑΠΔΠΧ 2020)

Περάν των ως άνω προστίθεται ότι με σχετική Κοινή Υπουργική Απόφαση (ΚΥΑ), επιβλήθηκε υποχρεωτική τηλεργασία, οπουδήποτε στον δημόσιο και ιδιωτικό τομέα είναι εφικτό, σε ποσοστό έως και 60% του συνόλου των εργαζόμενων και για όσους δεν είναι εφικτή τηλεργασία, επιβλήθηκε η προσέλευση και αποχώρηση τους κατά κύματα. Επίσης επέβαλε: την υποχρεωτική χρήση μάσκας την τήρηση απόστασης τουλάχιστον 1,5 μέτρου μεταξύ τους, την υποχρεωτική άδεια μετά αποδοχών σε καθένα με σοβαρό κείμενο νόσημα και τη διενέργεια συνεδριάσεων συλλογικών οργάνων μόνον μέσω τηλεδιάσκεψης, την εξυπηρέτηση του πολίτη με ηλεκτρονικό τρόπο όπου είναι εφικτό και σε άλλη περίπτωση μόνο κατόπιν ραντεβού, προς αποφυγή συνωστισμού. Σημειώνεται πως η ΑΠΔΠΧ, επίσης δημοσίευσε πακέτο Κατευθυντηρίων Γραμμών, αναφορικά με την ασφαλή εκτέλεση της τηλεργασίας.

Επιπλέον, το Υπουργείο Υγείας, με εγκύκλιο του προς τα νοσοκομεία με οδηγίες σχετικές με το επισκεπτήριο, τους συνοδούς ασθενών και την παραμονή ιατρικών επισκεπτών, προέβλεψε:

- Την αναστολή των επισκεπτηρίων, με εξαίρεση της δυνατότητας ενός και μόνο συνοδού όπου κρίνεται αναπόφευκτο και κατόπιν άδειας από τη διοικητική υπηρεσία. Ωστόσο, κάθε συνοδός με το παραμικρό σύμπτωμα λοιμώξεως το ανωτέρου αναπνευστικού (βήχας, πυρετός, ρινική καταρροή, δεκατική πυρετική κίνηση, φαρυγγαλγία) αποκλείεται εισόδου σε νοσοκομείο. Πρέπει επίσης να φέρει μάσκα, να είναι ενήμερος και να τηρεί κάθε λοιπό μετρό υγιεινής.
- Απαγόρευση εισόδου σε ιατρικούς επισκέπτες πλην εγκεκριμένων εξαιρέσεων, κατόπιν αιτήματος του Δ/ντου της Ιατρικής Υπηρεσίας.
- Τη διαχείριση των ως άνω με συνεργασία Διοικήσεως και οικείας Επιτροπής Λοιμώξεων και την ηλεκτρονική καταχώρηση κάθε διαπιστωμένα θετικού κρούσματος, αλλιώς συνίσταται πειθαρχικό παράπτωμα.

Να προστεθεί επίσης ότι λόγω του ξεσπάσματος του SARS-CoV-2, αρκετά νοσοκομεία, με αιτήματα τους προς το Υπουργείο υγείας και την ΑΠΔΠΧ, ζήτησαν άδεια για εγκατάσταση καμερών επιτήρησης σε χώρους πέραν των προβλεπόμενων, με σκοπό την ιχνηλάτηση των επαφών, σε διαδρόμους, προαύλιο ή κυλικείο, ασθενών θετικών στο ιό, που ίσως προκάλεσαν διασπορά του ιού. Ωστόσο, εισέπραξαν αρνητικές απαντήσεις στη βάση των σχετικών νομικών διατάξεων, όπως αναλύονται στο 11ο Κεφάλαιο. (Ζωγραφόπουλος)

Κεφάλαιο 10

Η αξιολόγηση της συμμόρφωσης των κρατών-μελών με τις επιταγές του κανονισμού.

<u>Εισαγωγικά</u>:

Στα μέσα του 2020 και επ' αφορμή της συμπληρώσεως 2 ετών από την θέση του Κανονισμού σε εφαρμογή, η Γενική Διεύθυνση Υγείας και Ασφάλειας των τροφίμων της ΕΕ, ξεκίνησε μια ευρεία πανευρωπαϊκή έρευνα με τίτλο *''Αξιολόγηση των κρατών-μελών της ΕΕ επάνω στα δεδομένα της υγείας, υπο το φως του GDPR''*. Υπήρξε σημαντική συμμετοχή εμπειρογνωμόνων από κάθε χώρα (ιατρών, νομικών, τεχνικών ασφαλείας και λοιπών εμπλεκόμενων στον κλάδο), οι οποίοι κατόπιν μηνών θεωρητικών διαβουλεύσεων και εργαστηριακών ερευνών, κατέληξαν σε συμπεράσματα που προκαλούν προβληματισμό μα και σε σειρά εμπεριστατωμένων σχετικών προτάσεων για τη διευθέτηση τους.

Η μελέτη, δημοσιεύτηκε επισήμως μόλις την 12^{η} Φεβρουαρίου του 2021 και συγκεκριμένα, εξέτασε για πιθανές διαφορές μεταξύ κρατών και για στοιχεία που ενδεχομένως επηρεάσουν δυσμενώς την εντός της ΕΕ διασυνοριακή ανταλλαγή δεδομένων υγείας, αποσκοπούσα σε παροχή υπηρεσιών υγειονομικής περίθαλψης, πρόληψης, έρευνας, χάραξη πολίτικων και εν γένει στο σεβασμό και τη άσκηση από τους ασθενείς, των δικαιωμάτων τους.

Δυστυχώς, η εν λόγω μελέτη που παραγγέλθηκε από την Ευρωπαϊκή Επιτροπή, κατέληξε στο συμπέρασμα ότι ενώ ο κανονισμός θεσπίζει οριζόντιους και άμεσα εφαρμοστέους κανόνες για όλα τα κράτη-μέλη, στην πράξη, υφίσταται ευρύς νομικός κατακερματισμός ανά τα κράτη αναφορικά με την επεξεργασία δεδομένων υγείας, που επιφέρει τα ως άνω προβλήματα.

Η πολυνομία αυτή οφείλεται στο ότι πολλές χώρες συνεχίζουν να εφαρμόζουν σε εκτεταμένο βαθμό την προϋπάρχουσα εθνική νομοθεσία και στην ύπαρξη διαφορετικών ερμηνειών των υποχρεώσεων που απορρέουν από τον ΓΚΠΔ και συνεπώς διαφορετικών τρόπων απόκρισης σε αυτές.

Συνεπώς, ούτος ώστε να διασφαλιστεί ότι τα εθνικά συστήματα υγειονομικής περίθαλψης θα κάνουν την καλύτερη δυνατή χρήση δεδομένων και θα υποστηρίξουν την ανάπτυξη ενός ευρωπαϊκού χώρου δεδομένων υγείας, πρέπει να αντιμετωπιστούν ορισμένα επιχειρησιακά και νομικά ζητήματα, μέσω πολύπλευρης προσεγγίσεως. Η μελέτη κατέληξε σε σειρά πιθανών μελλοντικών δράσεων σε επίπεδο ΕΕ, όπως προώθηση Κωδίκων Δεοντολογίας και κυρίως, νέα στοχευόμενη τομεακή νομοθέτηση.

Πιο συγκεκριμένα:

Η μελέτη διακρίνει 3 ευρείες Λειτουργίες σχετικές με την επεξεργασία δεδομένων στον τομέα της Υγείας:

1η Λειτουργία: Επεξεργασία δεδομένων για τους σκοπούς παροχής υγειονομικής και κοινωνικής πρόνοιας από τους παρόχους υγείας και περίθαλψης στον ενδιαφερόμενο ασθενή. Αυτό περιλαμβάνει τόσο την συμβατική δια ζώσης όσο και την τηλεφροντίδα χρησιμοποιώντας εργαλεία eHealth ή moblileHealth.

2η Λειτουργία: Επεξεργασία δεδομένων για ευρύτερους σκοπούς δημόσιας υγείας, συμπεριλαμβανομένου του σχεδιασμού, της διαχείρισης και βελτίωσης συστημάτων υγείας και πρόνοιας, την πρόληψη ή έλεγχο μεταδοτικών ασθενειών, την προστασία από σοβαρές απειλές για την υγεία και διασφάλιση υψηλών προδιαγραφών ποιότητας και ασφάλειας της υγειονομικής περίθαλψης και των ιατρικών προϊόντων και συσκευών.

3η Λειτουργία: Επεξεργασία δεδομένων για επιστημονική ή ιστορική έρευνα τόσο από δημόσιους όσο και από ιδιωτικούς οργανισμούς (τρίτα μέρη, που δεν είναι ο αρχικός υπεύθυνος δεδομένων), συμπεριλαμβανομένων των βιομηχανιών φαρμακευτικής και ιατρικής τεχνολογίας και των ασφαλιστικών φορέων.

Η 1η Λειτουργία, αφορά δεδομένα υγείας που συλλέγονται απευθείας από έναν ασθενή στο πλαίσιο παροχής υγειονομικής και κοινωνικής περίθαλψης με σκοπό την παροχή υπηρεσιών υγείας ή φροντίδας σε αυτόν τον ασθενή. Αυτό αναφέρεται γενικά ως *''πρωταρχική χρήση''*. Αυτά ενδέχεται να χρειαστεί να κοινοποιηθούν πέραν των εθνικών συνόρων σε περίπτωση ασθενούς που λαμβάνει περίθαλψη σε κράτος μέλος διαφορετικό από το οικείο κράτος-μέλος διαμονής του, για προγραμματισμένη, είτε απρογραμμάτιστη φροντίδα τουριστών, ή περίθαλψη ασθενών με σπάνιες παθήσεις, όπως προβλέπεται στην οδηγία 2011/24 / ΕΕ σχετικά με το δικαίωμα των ασθενών σε συνοριακή υγειονομική περίθαλψη και το συντονισμό των συστημάτων κοινωνικής ασφάλισης.

Τέτοιες υπηρεσίες μπορούν να παρέχονται από δημόσιους ή ιδιωτικούς παρόχους υγειονομικής περίθαλψης και να χρηματοδοτούνται από δημόσιους, ιδιωτικούς ή υβριδικούς φορείς ανάλογα με το σύστημα περίθαλψης του κράτους-μέλους.

Η 2η και η 3η αφορούν την επαναχρησιμοποίηση δεδομένων υγείας που συλλέχθηκαν αρχικά στο πλαίσιο παροχής φροντίδας, αλλά τα οποία αργότερα μπορούν να επαναχρησιμοποιηθούν για διαφόρους σκοπούς. Αυτό αναφέρεται ως *''δευτερεύουσα χρήση''*. Αυτή η χρήση μπορεί να ασκείται από δημόσιους φορείς όπως εθνικά συστήματα υγείας που είναι νόμιμοι πληρωτές (π.χ. ασφαλιστικό ταμείο), δημόσιοι ερευνητικοί φορείς (πχ. πανεπιστήμια ή εργαστήρια δημόσιας υγείας), από φορείς ελέγχου και πιστοποίησης φαρμάκων καθώς και από τη βιομηχανία (π.χ. εταιρείες φαρμακευτικής και ιατρικής τεχνολογίας, ασφαλιστικών και χρηματοοικονομικών υπηρεσιών, κοινωνικής δικτύωσης και ηλεκτρονικών ειδών ευρείας κατανάλωσης, καθώς και τεχνητής νοημοσύνης).
Αυτές οι Λειτουργιές, δύνανται να χρησιμοποιούν δεδομένα που παραμένουν εντός αποθετηρίων πρωτευούσης χρήσεως, όπως συστήματα ηλεκτρονικών αρχείων καταγραφής υγείας, αλλά μπορούν επιπλέον να μετακινηθούν σε άλλα (π.χ. μητρώα ασθενειών όπου συλλέγονται δεδομένα καταγραφής της συχνότητας εμφάνισης κρουσμάτων μιας ασθένειας και του επιπολασμού της σε εθνικό ή περιφερειακό επίπεδο).

Προφανώς, οι τρεις αυτές λειτουργίες μπορούν να πραγματοποιηθούν όταν η επεξεργασία εμπίπτει σε μία από τις εξαιρέσεις του άρθρου 9 παράγραφος 2 του GDPR.

Εντοπισθέντα προβλήματα και πιθανές δράσεις σε επίπεδο Ε.Ε.

Στην 1η Λειτουργία:

- Εκπρόσωποι από 18 κράτη-μέλη ανέφεραν ότι η ισχύουσα νομοθεσία στο οικείο τους κράτος-μέλος, δεν επαρκούσε για να διευκολύνει την ελεύθερη ροή δεδομένων που σχετίζονται με την υγεία μεταξύ των κρατών μελών και πρότειναν νομοθέτηση ενιαίου κατάλληλου εργαλείου διακυβέρνησης για υποδομή ανταλλαγής δεδομένων σε επίπεδο Ε.Ε.
- Εντοπίζεται ποικιλία νομικών βάσεων. Κάθε εθνικό σύστημα περίθαλψης λειτούργει υπο ένα σύνθετο ρυθμιστικό πλαίσιο με πολλούς νόμους και οδηγίες που υπαγορεύουν τον τρόπο παροχής των υπηρεσιών και διαχείρισης των προς επεξεργασία δεδομένων που εντάσσονται σε αυτό, άρα προκύπτει έλλειμμα νομικής συμβατότητας με συστήματα άλλων χωρών.
- Σε κάποιες χώρες διατηρούνται περισσότερα του ενός αρχεία με ιατρικής φύσεως δεδομένα ασθενών, που οδηγεί σε έλλειψη διαλειτουργικότητας μεταξύ συστημάτων εγγραφής, καθώς και σε ανικανότητα ταυτοποίησης ασθενούς και των θεραπόντων επαγγελματιών υγείας του. Συνεπώς, μπορεί να εμποδιστεί σημαντικά τη δυνατότητα των ασθενών να ασκήσουν το δικαίωμα τους για διασυνοριακή περίθαλψη ειδικότερα όσων αναγκάζονται σε επείγουσες διασυνοριακές διακομιδές ως πάσχοντες από σπανίζοντα νοσήματα.
- Φάνηκε επίσης ότι ενώ τα κράτη-μέλη σέβονται όλες τις απαιτήσεις του Κανονισμού αναφορικώς με το σύνολο των δικαιωμάτων των υποκειμένων των δεδομένων, ο βαθμός στον οποίο αυτά τα δικαιώματα πραγματικά ασκούνται από τους ασθενείς, παραμένει χαμηλός.

Παρόλο που απαιτούνται ορισμένοι περιορισμοί και εμπόδια σε ένα περιβάλλον υγειονομικής περίθαλψης, όπως η απαίτηση τήρησης πλήρους ιστορικού, περιλαμβάνουσα κάθε παρέμβαση υγειονομικής περίθαλψης έτσι ώστε οι μελλοντικές αποφάσεις περίθαλψης να αξιολογούνται στη βάση πλήρους σχετικής πληροφόρησης, η άσκηση των δικαιωμάτων των υποκειμένων στον τομέα της υγειονομικής περίθαλψης, παραμένει περιορισμένη. Αυτό προκύπτει κυρίως λόγω της μή έμφασης των ποικίλων Υπευθύνων επεξεργασίας στην πληροφόρηση ασθενών και πολιτών αναφορικά για την ύπαρξη των δικαιωμάτων αυτών.

- Σε περιπτώσεις παροχής υπηρεσιών υγείας εξ αποστάσεως (εφαρμογές τηλεϊατρικής σε smartphones και ηλεκτρονικούς υπολογιστές), σε όλη την ΕΕ και κατά παράβαση της παρ.2 του άρθρου 9 ζητείται συγκατάθεση του ασθενούς ώστε να γίνει επεξεργασία των δεδομένων του.

- Το πλέον χαρακτηριστικό εύρημα όλων είναι πως για την παροχή δια ζώσης υπηρεσιών υγείας, σε όλες τις χώρες της ΕΕ (πλην της Κύπρου), δεν επαρκεί να πληρούται έστω μια εκ των προϋποθέσεων του άρθρου 9 μα απαιτούνται και άλλες, επιπλέον, ποικίλες, εθνικές νομικές βάσεις (!).

Αντιμετώπιση:

Ο ίδιος ο GDPR, καθώς και η τομεακή νομοθεσία για τη διασυνοριακή περίθαλψη (σε κάποια κράτη-μέλη), όπως η ίδια η Συνθήκη της ΕΕ παρέχουν ευκαιρίες για να ξεπερνώνται τέτοια ζητήματα κατακερματισμού.

Όπως σημειώνεται στο άρθρο 9 παρ. 2 στοιχεία: ζ) και (ι) του ΓΚΠΔ, προβλέπεται η δυνατότητα η νομοθεσία της Ένωσης ή των μελών της να εξετάζει περαιτέρω την επεξεργασία δεδομένων σχετικών με την υγεία σε ορισμένες περιπτώσεις.

Επιπλέον, ο ΓΚΠΔ προβλέπει τη δυνατότητα δημιουργίας Κωδίκων Συμπεριφοράς από τους σχετικούς ενδιαφερόμενους φορείς για την αντιμετώπιση συγκεκριμένων αναγκών επεξεργασίας δεδομένων, στους οποίους (Κώδικες) δύναται να παραχωρηθεί πανευρωπαϊκού επιπέδου ισχύς, μέσω εκτελεστικής νομοθεσίας και συγκεκριμένα του άρθρου 40 παρ.9 του Κανονισμού.

Στην 2η Λειτουργία:

Αρχικά, σχεδόν σε όλα τα κράτη-μέλη υπάρχει εθνική νομοθεσία για την επεξεργασία δεδομένων της Λειτουργιάς 2 σύμφωνα με τα άρθρα 6 ή 9 του ΓΚΠΔ. Ωστόσο, φαίνεται πως υπάρχουν τεράστιες διαφορές μεταξύ τους σχετικά με τον τρόπο οργάνωσης της εποπτείας της αγοράς, αναφορικά με τα κυκλοφορούντα φαρμακευτικά σκευάσματα και ιατρικές συσκευές, κυρίως δηλαδή στην πρόσβαση των Εθνικών Οργανισμών Φάρμακων σε μητρώα ασθενειών για την εκτίμηση των (εκουσίων ή ακουσίων) επιπτώσεων σκευασμάτων και συσκευών, στην δημόσια υγεία.

Η πρόσβαση (εάν υφίσταται) σε προσωπικά σχετικά δεδομένα είναι συνήθως κατακερματισμένη από μια ποικιλία διατάξεων που έχουν θεσπιστεί με την πάροδο του χρόνου και συνεπάγονται διαφορετική καθοδήγηση από τις Αρχές Προστασίας Δεδομένων. Αν και στο σύνολό της, μια τέτοια νομοθεσία θα έπρεπε να είναι συνεκτική, ουδέν κράτος-μέλος βρέθηκε διαθέτει κεντρικό φορέα ο οποίος μπορεί να παρέχει πρόσβαση σε δεδομένα σε όλες τις διάφορες βάσεις δεδομένων πηγών (π.χ. σύστημα ηλεκτρονικής συνταγογράφησης, βιομηχανικά, ασφαλιστών υγείας κ.λ.π.) για λόγους δημόσιας υγείας. Συνεπώς, η πρόσβαση κρίνεται όχι μόνο κατακερματισμένη, αλλά και ανεπαρκής.
Ουδείς εκ των συμμετεχόντων απάντησε ότι φορείς της Ε.Ε. όπως ο Ευρωπαϊκός Οργανισμός Φαρμάκων ή το Ευρωπαϊκό Κέντρο Πρόληψης και Ελέγχου Νόσων έχουν άμεση πρόσβαση σε δεδομένα σχετικά με την αποστολή τους (!). Μάλιστα, ορισμένοι συμμετέχοντες τονίζουν επίσης την απογοήτευση τους με τις δυνατότητες επεξεργασίας δεδομένων υγείας για σκοπούς δημόσιας υγείας ακόμα και σε επίπεδο κρατών-μελών.

Αντιμετώπιση:

Συνεπώς (και) από τη συζήτηση αναφορικά με την αντιμετώπιση της τρέχουσας Πανδημίας, προκύπτει ότι απαιτείται περισσότερη έμφαση σε επίπεδο Ε.Ε. στη νομοθέτηση για τη διασφάλιση της ανταλλαγής δεδομένων ώστε να διευκολύνεται ο έγκαιρος εντοπισμός των νέων απειλητικών τάσεων για τη δημόσια υγεία. Όπως σημειώνεται στο κεφάλαιο 3, ο ΓΚΠΔ προβλέπει δυνατότητα για περαιτέρω νομοθεσία σε επίπεδο Ε.Ε. καθώς και σε εθνικό επίπεδο για την αντιμετώπιση αυτών των ζητημάτων.

Η αυξανόμενη ζήτηση για συστήματα υγειονομικής περίθαλψης, που οφείλονται στη γήρανση του πληθυσμού, καθώς και σε νέες απειλές για την υγεία, όπως ο κορονοϊός, θα μπορούσε να προσφέρει το απαιτούμενο ενδιαφέρον μεταξύ των κρατών μελών για να διερευνήσουν περαιτέρω νομοθετικές επιλογές. Επιπλέον, η άνοδος των νέων τεχνολογιών, όπως η τεχνητή νοημοσύνη, που θα εκτελεί υπερταχεία επεξεργασία μεγάλων ποσοτήτων δεδομένων (Big Data), θα επιφέρει σημαντική ώθηση σε επίπεδο Ε.Ε. διευκολύνοντας της καλύτερη χρήση των δεδομένων και διασφαλίζοντας ότι τα συστήματα υγειονομικής περίθαλψης της Ευρώπης θα είναι ανθεκτικότερα, όπως και ότι η Ε.Ε. μπορεί θα καθιερωθεί ως παγκόσμιος παίκτης στην ανάπτυξη νέων τεχνολογιών υγείας.

Στην 3η Λειτουργία:

Τα ζητήματα που προβλημάτισαν αναφορικά με την εν λόγω λειτουργία, εστιάζουν στον τρόπο με τον οποίο οι νομικές διαφορές μεταξύ των κρατών-μελών δυσχεράνουν τους ερευνητές στην προσβασιμότητα σε δεδομένα απαραίτητα για ερευνητικούς σκοπούς.

Εντοπίζεται ποικιλία διαφορετικών νόμων και κανονισμών που διέπουν την πρόσβαση σε δεδομένα υγείας εντός όσο και μεταξύ κρατών-μελών, επηρεάζοντας τους ερευνητές εσωτερικά και διασυνοριακά, καθιστώντας τους δύσκολο να εντοπίσουν το νομικό μείγμα που διέπει την εκτέλεση εκάστης έρευνας.
Αυτό το ζήτημα είναι εμφανές σε κάθε ερευνητική περιοχή, μα ακόμα περισσότερο σε ό,τι αφορά επεξεργασία γενετικών δεδομένων. Αυτές οι διαφορές επηρεάζουν πέρα από την προσβασιμότητα και άλλους παράγοντες όπως τη διαθεσιμότητα δεδομένων και το σεβασμό των δικαιωμάτων των υποκειμένων τους.

Όπως αναφέρθηκε από τους μελετητές, είναι σημαντικό τα ατομικά δικαιώματα που ισχύουν για τους ασθενείς (νοσηλευομένους νοσοκομείου), να παρέχονται και στους πολίτες, τους εκουσίως συμμετέχοντες σε έρευνες, φιλικά, με αποτελεσματική πληροφόρηση του και υπο διαφανείς διαδικασίες.

Αντιμετώπιση:

Η άποψη των ειδικών για την αντιμέτρηση των ως άνω, εστιάζει στην ανάγκη για περαιτέρω δράση σε επίπεδο ΕΕ, για δημιουργία ενός πιο οριζοντίου και πάνω από όλα πιο κατανοητού νομικού πλαισίου για την έρευνα που χρησιμοποιεί δεδομένα σχετιζόμενα με την υγεία.

Επιπλέον, το 85% των ερωτηθέντων που συμμετείχαν, υποστήριξαν την ανάγκη δράσης πανευρωπαϊκού επιπέδου, για την προαγωγή της αξίας που έχει η συνειδητή και κατόπιν εμπεριστατωμένης πληροφόρησης συγκατάθεση του συμμετέχοντος σε έρευνα υποκειμένου και την προώθηση πιο κοινών προσεγγίσεων στις νομικές βάσεις επαναχρησιμοποιήσεως δεδομένων προς επιπλέον διερεύνηση.

Κοινώς εντοπισθέντα Διαλειτουργικά ζητήματα.

Στη μελέτη επισημάνθηκε επίσης ότι τα ποικίλα εθνικά μοντέλα διακυβέρνησης, οι στρατηγικές και τα πλαίσια διακυβέρνησης για την πρόσβαση σε δεδομένα υγείας για δευτερεύοντες (κυρίως) σκοπούς, μπορεί να διαφέρουν σημαντικά μεταξύ των κρατών-μελών, εν μέρει και λόγω των διαφορετικού τύπου και προδιαγραφών πηγών δεδομένων που χρησιμοποιούνται (ηλεκτρονικά αρχεία υγείας, έγγραφα μητρώα, υποδομές και βάσεις δεδομένων).

Σε ορισμένα κράτη-μέλη υπάρχει μόνο ένας ή περιορισμένος αριθμός εθνικών οργανισμών (ή φορέων) εξουσιοδοτημένοι να χορηγούν άδειες για περαιτέρω χρήση δεδομένων που έχουν ήδη συλλεχθεί. Ταυτόχρονα, σε άλλα κράτη-μέλη το τοπίο είναι μακράν πιο αποκεντρωμένο, με ευρύ φάσμα φορέων να ρυθμίζουν την πρόσβαση σε δεδομένα υγείας για σκοπούς έρευνας και δημόσιας πολιτικής.

Η ποικιλομορφία τόσο εντός όσο και μεταξύ των κρατών-μελών δείχνει ότι η ανάπτυξη δυνητικών συνεργιών για τη μετάβαση σε ενιαία υποδομή διακυβέρνησης δεδομένων υγείας σε επίπεδο ΕΕ, θα είναι πολύπλοκο έργο.

Αντιμετώπιση:

Η Ευρωπαϊκή Επιτροπή έχει δεσμευτεί ότι θα κινηθεί προς αυτή την κατεύθυνση και έχει ήδη ανακοινώσει τη δημιουργία του Ευρωπαϊκού Χώρου Δεδομένων Υγείας, με τις λεπτομέρειες της υποδομής αυτής να βρίσκονται στο στάδιο της ανάπτυξης τους.

Ήδη ο κανονισμός Digital Gateway Regulation (2018/1724) της ΕΕ, προωθεί την Αρχή της καταγραφής δεδομένων ‘’μόνο μία φορά’’ (only once data-recording Principle) και την θεσμοθέτηση της επαναχρησιμοποίησης δεδομένων, όπου είναι εφικτό.

Επίκεντρο του είναι να καταστεί η κυβερνητική χρήση δεδομένων πιο αποτελεσματική και απλή, μειώνοντας το γραφειοκρατικό φόρτο για ασθενείς, πολίτες και οργανισμούς, χρησιμοποιώντας ξανά τα ήδη διαθέσιμα στα (κυβερνητικά συστήματα) δεδομένα.

Η καινοτόμος αυτή Αρχή απαιτεί από τις δημόσιες διοικήσεις να διασφαλίσουν ότι πολίτες και οργανισμοί θα παρέχουν κάποια πληροφορία μία και μοναδική φορά και πως οι δημόσιες υπηρεσίες θα αναλάβουν κάθε δράση, ώστε να επαναχρησιμοποιούν εσωτερικά αυτά τα δεδομένα (τηρώντας κάθε κανόνα προστασίας των), ώστε αποφεύγονται περιττές χρονοτριβές για πολίτες και οργανισμούς.
Η μελέτη πρότεινε δράσεις σε επίπεδο ΕΕ για τη στήριξη του Ευρωπαϊκού Χώρου Δεδομένων Υγείας και τη διασφάλιση της καλύτερης δυνατής χρήσης τους.

Αυτά περιλαμβάνουν:

▪ Κώδικες Δεοντολογίας με βάση τα ενδιαφερόμενα μέρη.

Το άρθρο 4 του GDPR προβλέπει την πιθανή ανάπτυξη διαφόρων εργαλείων ‘’ήπιας νομοθεσίας’’ που θα μπορούσαν να υποστηρίξουν την εφαρμογή κανόνων προστασίας δεδομένων, όπως οι Κώδικες Δεοντολογίας. Πρόκειται για ένα εθελοντικό εργαλείο υπευθυνότητας που βοηθά στην αποσαφήνιση συγκεκριμένων κανόνων προστασίας δεδομένων, απευθυνόμενων σε Υπευθύνους και Εκτελόντες επεξεργασίες, χρησιμεύοντας ως οδηγός, παρέχοντας λειτουργικό νόημα στις αρχές της προστασίας δεδομένων όπως ορίζονται εκ του GDPR.

Στον τομέα της υγείας, ούτος ώστε να καταστεί επιτυχημένος ένας τέτοιος Κώδικας, ενδείκνυται η σύσταση του κατόπιν διαβουλεύσεων τύπου bottom-up, δηλαδή από τη βάση προς τα πάνω, δίδοντας έμφαση στους κύριους ενδιαφερόμενους: ασθενείς, ιατρούς, ερευνητές και εμπειρογνώμονες της ιδιωτικής ζωής

Ωστόσο, κατά το άρθρο 40, ώστε να αναγνωριστεί επισήμως ως ‘’Κώδικας Συμπεριφοράς’’, ένας τέτοιος Κώδικας πρέπει να επικυρωθεί από την Αρχή Προστασίας Δεδομένων του κράτους-μέλους στο οποία πρόκειται να εφαρμοστεί.

Όταν προορίζεται για δραστηριότητες επεξεργασίας σε πολλά κράτη-μέλη, πρέπει να υποβληθεί από την αρμόδια Αρχή Προστασίας στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, το οποίο θα εκδώσει γνώμη. Εάν το Συμβούλιο επιβεβαιώσει ότι το σχέδιο συμμορφώνεται με τον ΓΚΠΔ, το υποβάλλει στην Ευρωπαϊκή Επιτροπή, η οποία, μέσω εκτελεστικής πράξης, δίδει γενική ισχύ στον Κώδικα, σε επίπεδο ΕΕ.

▪ <u>Νέα τομεακή νομοθεσία σε επίπεδο ΕΕ</u>.

Εφόσον κριθεί σκόπιμο, ένας Κώδικας Δεοντολογίας θα μπορούσε να αναβαθμιστεί, αποκτώντας νομικό καθεστώς σε επίπεδο ΕΕ, μέσω εκτελεστικής πράξης η οποία είναι νομικά δεσμευτική, επιβάλλοντας οριζόντιους όρους που διασφαλίζουν την ομοιόμορφη εφαρμογή της νομοθεσίας της ΕΕ.

Μπορούν φυσικά επίσης να προβλεφθούν και άλλες νομικές πράξεις σε επίπεδο ΕΕ με στόχο την επίτευξη εναρμονισμένης προσέγγισης στην επεξεργασία δεδομένων για υγείας, η οποία θα καλύπτει τις αρχές διακυβέρνησης των δεδομένων, την υπεύθυνη χρήση των δεδομένων υγείας και την προσβασιμότητα στα δεδομένα υγείας, μέτρα ενθάρρυνσης για την προστασία της ανθρώπινης υγείας και ιδίως της καταπολέμησης μεγάλων διασυνοριακών υγειονομικών απειλών, τη δημιουργία συστημάτων ενιαίου σημείου επαφής, που διευκολύνουν τη δευτερογενή χρήση δεδομένων υγείας σε υπερεθνικό επίπεδο, διευκολύνοντας την έρευνα αλλά και μηχανισμού την άμεσης ανταλλαγής δεδομένων μεταξύ επαγγελματιών υγείας και για υποστήριξη των ασθενών στην άσκηση της φορητότητας των δεδομένων υγείας τους όταν χρειαστούν περίθαλψη σε άλλο κράτος-μέλος.

▪ Μη νομοθετικά μέτρα, συμπεριλαμβανομένων κατευθύνσεων και δράσεων πολιτικής για την υποστήριξη ενός ευρωπαϊκού χώρου δεδομένων για την υγεία.

Μπορούν να χρησιμευόσουν ως συμπληρωματικά των νομοθετικών μέτρων και των Κωδίκων Δεοντολογίας, ώστε να προάγουν τη συνεργασία πέραν των εθνικών ορίων. Συνοδευόμενα από χρηματοδοτικά εργαλεία, όπως το πρόγραμμα ‘’Ψηφιακή Ευρώπη’’ ή το μελλοντικό ‘’EU4Health’’, μπορούν να προωθήσουν την αποτελεσματικότερη συνεργασία στην κατασκευή κατάλληλων υποδομών, τη βελτίωση της ποιότητας των δεδομένων υγείας και την ανάπτυξη ψηφιακών ικανοτήτων στα κράτη-μέλη.

Εν κατακλείδι.

Η διεξαχθείσα μελέτη, καθιστά σαφές ότι υφίσταται σειρά περίπλοκων νομικών και επιχειρησιακών ζητημάτων που πρέπει να αντιμετωπιστούν ώστε να διασφαλιστεί ότι τα συστήματα υγειονομικής περίθαλψης ανά την ΕΕ, μπορούν να κάνουν την καλύτερη δυνατή χρήση δεδομένων για τις τρεις αλληλοσχετιζόμενες Λειτουργίες, καταλήγοντας στο ότι απαιτείται ένα υγιές επίπεδο νομικής και επιχειρησιακής διακυβέρνησης και μια σαφέστερη, κοινή κατανόηση των εννοιών του ΓΚΠΔ.

Επιπλέον, έδειξε ότι η συνεργασία μεταξύ των κρατών-μελών της ΕΕ είναι ζωτικής σημασίας. Μια τέτοια θα πρέπει να βασιστεί στην πείρα των εθνικών αρχών προστασίας δεδομένων καθώς και στους πολυάριθμους εθνικούς και κοινοτικούς φορείς που εκπροσωπούν ασθενείς, επαγγελματίες υγείας, ερευνητές και φαρμακοβιομηχανία. Η πανδημία έχει ενισχύσει την προθυμία συνεργασίας και παρέχει πολλές νέες μεθόδους για γρήγορη και αποτελεσματική δράση, με επίκεντρο την καλύτερη δυνατή προαγωγή των δικαιωμάτων στου ασθενούς.

Κεφάλαιο 11

Συχνές ερωτήσεις και απαντήσεις καθημερινής πρακτικής εφαρμογής του κανονισμού.

→ *Επιτρέπεται ένας πάροχος υπηρεσιών υγείας να αρνηθεί την παροχή υπηρεσιών υγείας σε κάποιο ασθενή, με το επιχείρημα ότι το υποκείμενο των δεδομένων (ασθενής) αρνήθηκε να συγκατάθεση για την επεξεργασία των προσωπικού χαρακτήρα δεδομένων του ?*

ΟΧΙ. Όπως εξηγήθηκε διεξοδικά, στον τομέα παροχής υπηρεσιών υγείας, τέτοιου είδους συγκατάθεση δεν απαιτείται, ούτε καν προβλέπεται [αρ.9 παρ.2 στοιχ. (θ') και (ή)]. Απαιτείται έγγραφη συγκατάθεση μονό σε περιπτώσεις συμμέτοχης σε επιστημονικές έρευνες, στα πλαίσια κλινικών δόκιμων (αιτιολογική σκέψη 161).

Η μόνη νομική βάση υπο την οποία ένας πάροχος δύναται να διακόψει την παροχή των υπηρεσιών του σε ασθενή, είναι σε περίπτωση δικής του, ελεύθερης, συνειδητής, ρητής συναίνεσης, με τη συμπλήρωση του ειδικού εγγράφου ''Δήλωσης Άρνησης Θεραπείας''. (Ζωγραφόπουλος 2018: 52)

→ *Απαιτείται προηγούμενη έγγραφη συγκατάθεση εργαζομένου σε φορέα παροχής υπηρεσιών υγείας για επεξεργασία ευαίσθητων προσωπικών δεδομένων του από τον πάροχο-εργοδότη ?*

ΟΧΙ. Βάσει των στοιχείων (β') και (η') της παρ.2 του αρ.9 του ΓΚΠΔ, ο πάροχος υπηρεσιών υγείας-υπεύθυνος επεξεργασίας έχει πλήρη ευχέρεια επεξεργασίας ευαίσθητων δεδομένων των εργαζομένων του για σκοπούς όπως: εκτίμηση εργασιακής ικανότητας, διενέργεια διαγνωστικών εξετάσεων, παροχή θεραπείας, λόγους ουσιαστικού δημοσίου συμφέροντος (π.χ. άσκηση δίωξης).

Ωστόσο, στο στοιχείο (α'), προβλέπεται η ανάγκη συγκατάθεσης μόνο σε περίπτωση που δεν είναι εφικτή η θεμελίωση επεξεργασίας ευαίσθητων δεδομένων σε οποιαδήποτε άλλη βάσει της παρ.2 του αρ.9.

→ *Δικαιούται ο ασθενής να λάβει αντίγραφο του ιατρικού του φακέλου από τον πάροχο-υπεύθυνο επεξεργασίας ?*

ΝΑΙ. Πρόκειται για σαφή άσκηση του δικαιώματος του υποκειμένου στην Πρόσβαση (αρ. 15 του Κανονισμού). Στη βάση αυτού, το υποκείμενο δικαιούται ανά πάσα στιγμή να λαμβάνει γνώση του περιεχομένου του φακέλου του και ο πάροχος, ως υπεύθυνος επεξεργασίας, υποχρεούται να του το παρέχει.

→ *Δικαιούται ο ασθενής να αιτηθεί διαγραφή περιεχομένου του ιατρικού του φακέλου ?*

ΟΧΙ. Έχει ήδη ξεκαθαριστεί πως το Δικαίωμα στη Λήθη δεν εφαρμόζεται στον τομέα παροχής υπηρεσιών υγείας. Επιπλέον, κατά τον κώδικα Ιατρικής Δεοντολογίας του Ν.34418/2005, αρ.14 παρ.4 ξεκαθαρίζεται ότι:

- Ιδιωτικά ιατρεία και λοιπες μονάδες Πρωτοβάθμιας Φροντίδας Υγείας, υποχρεούνται σε διατήρηση των ιατρικών αρχείων για 10 έτη από την τελευταία επίσκεψη του ασθενούς.
- Σε κάθε άλλη περίπτωση, προβλέπεται διατήρηση για 20 έτη. (Ζωγραφόπουλος 2018: 54)

→ *Δικαιούται το νοσηλευτικό ίδρυμα να αναγράφει σε οθόνη, σε χώρο αναμονής ορατά σε όλους, ονόματα εξεταζομένων, ώρα ραντεβού, ιατρείο που επισκέπτονται ή έστω τον ΑΜΚΑ τους ή τα αρχικά του ονοματεπωνύμου τους ?*

ΟΧΙ. Απαγορεύεται πλήρως κάθε τέτοια επεξεργασία, διότι παραβιάζει κατάφορα τις Θεμελιώδεις Αρχές της Ελαχιστοποίησης, της Ακεραιότητας και της Εμπιστευτικότητας των δεδομένων, όπως και τις πολυαναφερθείσες διατάξεις του αρ.9.

Το νόμιμο και σωστό, είναι να ενημερώνεται για τη σειρά του βάσει ανωνυμοποιημένου κωδικού μιας χρήσεως, ο οποίος του απονέμεται κατά τη στιγμή που κλείνει το ραντεβού και ακυρώνεται οριστικά με το πέρας αυτού.

→ *<u>Δικαιούται πάροχος-υπεύθυνος επεξεργασίας να χορηγήσει σε συγγενείς ή τρίτους ιατρικό φάκελο αποβιώσαντα ασθενούς</u> ?*

Κατά το αρ.4 του ΓΚΠΔ, μόνο ένα εν ζωή φυσικό πρόσωπο δύναται να απολαύει των προστατευτικών ρυθμίσεων του Κανονισμού, συνεπώς οι θανόντες εξαιρούνται αυτών. Ωστόσο, απαιτείται η υποβολή σχετικού αιτήματος στον φορέα από τον ενδιαφερόμενο, με επίκληση και απόδειξη συγκεκριμένου εννόμου συμφέροντος. Κατόπιν, ο φορέας αξιολογεί το αίτημα στη βάσει του αρ.13 και 14 του Κώδικα Ιατρικής Δεοντολογίας (ΚΙΔ), του ν.3418/2005 – εξαιρούνται οι αποθανόντες λόγω κορωνοϊού, όπως εξηγήθηκε. Φυσικά, ουδεμία επίκληση και απόδειξη προϋποτίθεται εάν ο αιτών είναι δημόσια ή δικαστική Αρχή ή εφόσον ο τρίτος ήδη διαθέτει στα χέρια του σχετική δικαστική απόφαση να του παραδοθεί ο φάκελος.

→ *<u>Δικαιούται τρίτος να ζητήσει αντίγραφα ιατρικού φακέλου ζώντος ασθενούς</u> ?*

Ναι, εφόσον υφίσταται:

- Κάποιος σαφής, προκαθορισμένος, νόμιμος σκοπός επεξεργασίας.
- Και έστω μια εκ των νομικών βάσεων του αρ.9 παρ.2 αναφορικά με τα ευαίσθητα προσωπικά δεδομένα.
- Και η διασφάλιση όλων των Θεμελιωδών Αρχών που διέπουν κάθε επεξεργασία προσωπικών δεδομένων.

Ωστόσο, ο πάροχος-υπεύθυνος επεξεργασίας, υποχρεούται προηγουμένως να ενημερώσει το υποκείμενο των δεδομένων για την επικείμενη διαβίβαση, δίδοντας του μια εύλογη προθεσμία για έκφραση πιθανών αντιρρήσεων.

→ *<u>Δικαιούται συγγενής να παραλάβει αποτελέσματα εξετάσεων, εφόσον ο ίδιος ο ασθενής δεν είναι σε θέση</u> ?*

Ναι, εφόσον ο ίδιος ο ασθενής-υποκείμενο των δεδομένων έχει εξουσιοδοτήσει γραπτώς συγκεκριμένο συγγενικό πρόσωπο να παραλάβει τα στοιχεία για λογαριασμό του. Σε μια τέτοια περίπτωση (κατά το αρ.15 του Κανονισμού), ο συγγενής ταυτίζεται με το υποκείμενο και αποκτά νόμιμο δικαίωμα πρόσβασης.

→ *<u>Δικαιούται ένας πάροχος υπηρεσιών υγείας να δίδει τηλεφωνικά πληροφορίες σχετικές με αποτελέσματα εξετάσεων και την εν γένει κατάσταση του υποκειμένου των δεδομένων</u> ?*

Κατά βάσην, δεν ενδείκνυται, λόγω κινδύνων που μπορεί να επέλθουν για τον ασθενή, όσο και τον πάροχο, καθότι πρόκειται για κρίσιμα, ευαίσθητα δεδομένα προσωπικού χαρακτήρα. Ο οποιοσδήποτε θα μπορούσε να ισχυριστεί τηλεφωνικώς ότι ‘’είναι ο ασθενής’’ ή ‘’συγγενής του’’…

Κατά το αρ.12 του ΓΚΠΔ, ο κανόνας είναι η εις χείρας επίδοση των στοιχείων. Επιτρέπει επίσης την ηλεκτρονική αποστολή, αρκεί το αρχείο να είναι κρυπτογραφημένο και να έχει προηγηθεί έγγραφη συγκατάθεση του υποκειμένου για ηλεκτρονική αποστολή. Το κλειδί αποκρυπτογράφησης, πρέπει να το λαμβάνει ξεχωριστά. (Ζωγραφόπουλος 2018: 58)

Κατά την παρ.1 του αρ.12, είναι εφικτή η τηλεφωνική ενημέρωση, αρκεί:

- Να υπάρχει έγγραφη αίτηση του υποκειμένου.
- Και η δυνατότητα του φορέα να ταυτοποιεί το υποκείμενο κάθε φόρα που τηλεφωνεί.
- Και η δυνατότητα του φορέα να αποδεικνύει κάθε φόρα ότι παρείχε πλήρη και προσήκουσα ενημέρωση στο υποκείμενο.

Οι ως άνω προϋποθέσεις είναι προφανώς δύσκολο να εκπληρούνται, συνεπώς, τέτοιου είδους επεξεργασία οφείλει να αποφεύγεται.

→ *<u>Δικαιούται ένας πάροχος υπηρεσιών υγείας να διαβιβάζει στοιχεία του φακέλου του ασθενούς σε ασφαλιστικές εταιρίες</u> ?*

Υφίστανται τρία ενδεχόμενα:

1) Ο ίδιος ο ασθενής ασκώντας το δικαίωμα της Πρόσβασης, ζητά και λαμβάνει από τον υπεύθυνο επεξεργασίας τα ευαίσθητα δεδομένα και κατόπιν τα μεταβιβάζει ο ίδιος στην ασφαλιστική, για οποιοδήποτε λόγο που αφορά στη μεταξύ τους σύμβαση.

2) Ναι, υπο τις ίδιες προϋποθέσεις που ισχύουν και στη διαβίβαση στοιχείων σε τρίτους και με προηγούμενη ενημέρωση και έγκριση του ασθενούς.

3) Ναι, κατόπιν εκούσιας, ελεύθερης, εν πλήρη επίγνωση έγγραφης εξουσιοδότησης. (Ζωγραφόπουλος 2018: 60)

→ *<u>Δύναται ένα νοσηλευτικό ίδρυμα να αποστείλει στοιχεία του ασθενούς σε άλλο νοσηλευτικό ίδρυμα, ώστε να λάβει μια 'δεύτερη άποψη'</u> ?*

Βεβαίως, αρκεί μόνον να θεμελιώνεται τέτοια κίνηση από την παρ.2 του αρ.9 το οποίο φυσικότατα και επιτρέπει τέτοια διαβίβαση, εφόσον αφορά σκοπούς παροχής υπηρεσιών υγείας. Ενδείκνυται ο ηλεκτρονικός τρόπος διαβίβασης, αρκεί το αρχείο να έχει ψευδωνυμοποιηθεί και κρυπτογραφηθεί. Εάν πρέπει να γίνει μέσω εταιρίας ταχυμεταφορών, είναι εφικτό, αρκεί να διασφαλίζεται η μή πρόσβαση αυτής στο περιεχόμενο, η ακεραιότητα και εμπιστευτικότητα των δεδομένων. (Ζωγραφόπουλος 2018: 62)

→ *<u>Ποιοι φορείς παροχής υπηρεσιών υγείας οφείλουν να διαθέτουν δικό τους DPO</u> ?*

Πρόκειται για υπάλληλο υπεύθυνο για μεγάλης κλίμακας δραστηριότητες επεξεργασίας ειδικών, κρισίμων κατηγοριών προσωπικών δεδομένων, αφού εργάζεται σε φορέα-πάροχο υπηρεσιών υγείας και άρα εκ φύσεως είναι υπόχρεος σε τακτική και συστηματική, μεγάλης κλίμακας παρακολούθηση των υποκειμένων των δεδομένων. Συνεπώς, κάθε νοσοκομειακή μονάδα, ανεξαρτήτως μεγέθους, υποχρεούται, όπως και οι Υγειονομικές Περιφέρειες και όλοι οι εποπτευόμενοι εξ' αυτών φορείς, οφείλουν να έχουν ορίσει DPO (με ειδική, εσωτερική διαδικασία που είχε τρέξει το 2018).

Εξαίρεση αποτελούν μικρές, αποκεντρωμένες, υποπτευόμενες από νοσοκομειακές μονάδες υπηρεσίες (π.χ. εξωτερικά ιατρεία και κέντρα υγείας) τα οποία καλύπτονται από τον DPO του αρμοδίου νοσοκομείου ή της ΥΠΕ.

→ *Είναι επιτρεπτή η χρήση βιντεοκαμερών σε εσωτερικούς και εξωτερικούς χώρους ενός νοσοκομείου, όπως και η καταγραφή του υλικού τους και για ποιο χρονικό διάστημα ?*

Κατά την οδηγία 1/2011, αρ.20 της ΑΠΔΠΧ, Ναι, υπο την προϋπόθεση να αποσκοπούν στη φύλαξη προσώπων και αγαθών, ωστόσο, μόνον σε χώρους όπου δεν δύναται να έχει πρόσβαση ασθενής ή επισκέπτης.

Ο GDPR, με την θέση του σε εφαρμογή δεν προϋποθέτει πλέον τη λήψη άδειας για εγκατάσταση καμερών, ωστόσο, ήδη από την DPIA, για νόμιμο λειτουργιά, επιβάλλεται σειρά άλλων προϋποθέσεων. Συγκεκριμένα, μπορούν να εγκατασταθούν κάμερες σε χώρους όπως: ταμεία, αποθήκες, σημεία εισόδου-εξόδου, ηλεκτρομηχανολογικές εγκαταστάσεις. Όχι όμως σε: κοινόχρηστους διαδρόμους, θαλάμους ασθενών, χώρους εξέτασης ή επεμβάσεων, τουαλέτες, γραφεία ιατρών και λοιπούς χώρους εργασίας.

Ως εξαίρεση, εγκατάσταση με σκοπό την παροχή υπηρεσιών υγείας (και όχι τη φύλαξη), επιτρέπεται σε ειδικούς χώρους, όπως: οι Μονάδες Εντατικής Θεραπείας, ψυχιατρικά ιδρύματα και ιδρύματα νοσηλείας βαρέως πασχόντων, καθότι οι συγκεκριμένοι ασθενείς δύνανται να προκαλέσουν σοβαρή βλάβη στην υγεία τους ή στην υγεία τρίτων.

Ούτος ώστε να επιτραπεί η εγκατάσταση συστημάτων βιντεοσκόπησης στους εν λόγω ειδικούς χώρους, απαιτείται η άδεια της ΑΠΔΠΧ, κατόπιν εκπλήρωσης συγκεκριμένων προϋποθέσεων, όπως περιγράφονται στην ως άνω οδηγία της εποπτικής Αρχής. (Ζωγραφόπουλος 2018: 64)

ΕΠΙΛΟΓΟΣ

Όπως φάνηκε στην εισαγωγή, ο Κανονισμός έρχεται από πολύ μακριά και όπως φάνηκε στην πορεία της έρευνας μας, θα πάει ακόμα πιο μακριά. Πολλές αλλαγές ακόμα έχουν να γίνουν, είτε σε εθνικό, είτε σε πανευρωπαϊκό επίπεδο, ώστε το συνολικό του αποτέλεσμα να κριθεί ως ιδανικό.

Αναμφίβολα, ο ΓΚΠΔ, οικοδομήθηκε επάνω στις καλύτερες των προθέσεων, μα αυτό φάνηκε πως δεν αρκεί. Χρειάζεται ουσιαστική αλλαγή νοοτροπίας του ανθρωπίνου παράγοντα και ισχυρότερη εθνική νομοθέτηση που όντως θα εφαρμόζεται, όπως επίσης δομές και υποδομές σε πολλές χώρες συνεχίζουν να χρήζουν αναμόρφωσης.

Ενδεικτικά, ακόμα κι σήμερα, στους χώρους αναμονής νοσοκομείων καλούν τους ασθενείς φωνάζοντας το όνομα τους, ενώ αυτοί ήδη διαθέτουν μιας χρήσεως ατομικό κωδικό ραντεβού και συχνά ουδείς αντιδρά διότι ούτε το κοινό ούτε οι λειτουργοί υγείας έχουν επίγνωση των δικαιωμάτων/υποχρεώσεων τους. Έχει επίσης παρατηρηθεί ότι πολλοί πολίτες έχουν μόνον ακουστά το δικαίωμα στη Λήθη, θεωρώντας το απολυτό και εκ των ων ουκ άνευ. Αρκετές επιχειρήσεις διεθνώς, υποχρεωθήκαν σε σημαντικό αριθμό προσλήψεων, ώστε να διευθετούν τις επιπλέον γραφειοκρατικές υποχρεώσεις που απορρέουν, επιβαρυνόμενες με σημαντικά κόστη.

Από την άλλη, έχει κατακόρυφα αυξηθεί το επίπεδο ασφαλείας των δεδομένων, αφού οι οργανισμοί υποχρεωθήκαν σε υιοθέτηση τεχνικών data security υψηλού επιπέδου αποτελεσματικότητας, το οποίο και αναγκάζονται διαρκώς να αναβαθμίζουν, αυξάνοντας έτσι την εμπιστοσύνη του κοινού προς τις ίδιες και επιταχύνοντας τον ψηφιακό μετασχηματισμό οικονομίας και κοινωνίας εν γένει.

Το καθεστώς της πανδημίας έδειξε ότι όταν υφίσταται η συναίσθηση μιας απειλής που αφόρα από κοινού όλους τους ευρωπαϊκούς λαούς, τότε ανακύπτει και η κοινή αντίληψη της ανάγκης για ευρείες συνεννοήσεις και συνεργασίες, που εν τέλει αποδίδουν και σε σύντομο διάστημα.

Ακριβώς αυτό το συνεργατικό πνεύμα είναι που θα πρέπει να μην εκλείψει κατά τα προσεχή έτη, ώστε ο παγκοσμίως σεβαστός και πρωτοπόρος αυτός Κανονισμός να συνεχίσει να εξελίσσεται και να επεκτείνεται καθώς έχει πολλούς ακόμη γλυκούς καρπούς να μας αποδώσει.

Βιβλιογραφία

ΒΙΒΛΙΑ ΚΑΙ ΑΡΘΡΑ

Ζωγραφόπουλος, Δ., (2018), Οδηγός Προετοιμασίας GDPR- Βασικές Κατευθύνσεις, Υπουργείο Υγείας, Αθήνα.

Κοτσαλής, Λ., Μενουδάκος Κ., (2018), Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR), Νομική Βιβλιοθήκη ΑΕΒΕ, Αθήνα.

Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων. (2017α), Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ), Ευρωπαϊκή Επιτροπή, Βρυξέλλες.

Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων. (2017β), Κατευθυντήριες γραμμές για την εφαρμογή και τον καθορισμό διοικητικών προστίμων για τους σκοπούς του κανονισμού 2016/679, Ευρωπαϊκή Επιτροπή, Βρυξέλλες.

Sharma, S., Menon, P. (2020), Data Privacy and GDPR Handbook, John Wiley & Sons, New Jersey.

Sloot, B., Groot, A. (2018), The Handbook of Privacy Studies, Amsterdam University Press.

ΙΣΤΟΣΕΛΙΔΕΣ

https://lewisbrisbois.com/assets/uploads/files/GDPR,_Part_I-_History_of_European_Data_Protection_Law.pdf [Πρόσβαση: 20 Απριλίου 2021]

https://aithority.com/technology/analytics/how-did-we-get-here-a-brief-history-of-the-gdpr/ [Πρόσβαση: 20 Απριλίου 2021]

https://www.itgovernance.eu/sv-se/eu-gdpr-key-changes-se [Πρόσβαση: 20 Απριλίου 2021]

https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EN [Πρόσβαση: 3 Ιανουαρίου 2021]

http://www.opengov.gr/ministryofjustice/?p=10609 [Πρόσβαση: 25 Απριλίου 2021]

https://www.iso.org/standard/45123.html [Πρόσβαση: 18 Ιανουαρίου 2021]