Προστασία προσωπικών δεδομένων των ασθενών με καρκίνο

Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (ΕΕ 2016/679)

Μαρούσα Πρωτοπαπαδάκη –Ημερίδα ΕΛΛ.Ο.Κ Για τον αιματολογικό Καρκίνο- Θεσσαλονίκη 2.6.2018

Ποιος είναι ο στόχος του Κανονισμού;

- Ο Κανονισμός 2016/679 θεσπίζει :

- κανόνες που αφορούν **την προστασία των φυσικών προσώπων** έναντι της επεξεργασίας των δεδομένων προσωπικού και

- κανόνες που αφορούν την **ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα**

Τι καινούργιο εισάγεται με τον Κανονισμό ;

- Η προστασία των προσωπικών δεδομένων των φυσικών προσώπων δεν θεσπίζεται για πρώτη φορά . Με τον Κανονισμό 2016/679 δημιουργείται πλέον μια υποχρέωση **αυτορρύθμισης** όλων όσων επεξεργάζονται προσωπικά δεδομένα ώστε **να λαμβάνουν ,και να είναι σε θέση να αποδείξουν ότι λαμβάνουν, τεχνικά και οργανωτικά μέτρα** για τη συμμόρφωση τους προς τις υποχρεώσεις του Κανονισμού.
  - **Κυρίαρχη Αρχή η Λογοδοσία**

Ποια δεδομένα θεωρούνται προσωπικά ;

- Προσωπικά δεδομένα είναι κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο **φυσικό εν ζωή πρόσωπο** όπως το όνομα, ο αριθμός της ταυτότητας, το ΑΦΜ, το email, η οικογενειακή κατάσταση, μια IP(Internet Protocol) διεύθυνση, μια φωτογραφία , τα δεδομένα θέσης, και πολλά πολλά άλλα!

Υπάρχουν **ειδικές κατηγορίες** προσωπικών δεδομένων ;

- Ναι. Είναι τα δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα ,τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση , **καθώς και τα γενετικά δεδομένα ,τα βιομετρικά δεδομένα ,τα δεδομένα που αφορούν την υγεία** αλλά και όσα αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήριο προσανατολισμό

- **Ο Γενικός Κανονισμός δίνει μεγάλη βαρύτητα στα προσωπικά δεδομένα που αφορούν την υγεία !**

- **Προβλέπει τρεις ξεχωριστές κατηγορίες**
- **σχετικών δεδομένων !**

Ο Γενικός Κανονισμός δίνει σημασία στα θέματα υγείας !

- **Γενετικά δεδομένα:**

- τα δεδομένα προσωπικού χαρακτήρα που αφορούν τα γενετικά χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν, όπως προκύπτουν, ιδίως, από ανάλυση βιολογικού δείγματος του εν λόγω φυσικού προσώπου, ιδίως από χρωμοσωμική ανάλυση DNA ή RNA ή από την ανάλυση άλλου στοιχείου και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με την φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου

- **Βιομετρικά Δεδομένα :**

- δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα,

- **Αλλά και «δεδομένα που αφορούν την υγεία»:**

- Δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, περιλαμβανομένης της παροχής υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την παρελθούσα, τρέχουσα ή μελλοντική κατάσταση της υγείας του.Π.χ ένας αριθμός που αποδίδεται σε φυσικό πρόσωπο με σκοπό την πλήρη ταυτοποίηση του για σκοπούς υγείας

Κι άλλα «δεδομένα που αφορούν την υγεία»

- αλλά και πληροφορίες που προκύπτουν από εξετάσεις, ή αναλύσεις σε μέρος ή ουσία του σώματος, και κάθε πληροφορία σχετικά με ασθένεια, αναπηρία, κίνδυνο ασθένειας , ιατρικό ιστορικό, κλινική θεραπεία , ανεξαρτήτως πηγής , παραδείγματος χάριν από ιατρό ή άλλο επαγγελματία του τομέα της υγείας, νοσοκομείο ή ιατρική συσκευή

Ποιες ενέργειες θεωρούνται «επεξεργασία»

- Επεξεργασία είναι κάθε πράξη που πραγματοποιείται σε δεδομένα προσωπικού χαρακτήρα , με ή χωρίς χρήση αυτοματοποιημένων μέσων ,όπως η συλλογή ,η καταχώρηση, η οργάνωση ,η διάρθωση , η αποθήκευση, η προσαρμογή ,η μεταβολή , η ανάκτηση, η αναζήτηση πληροφοριών ,η χρήση , η κοινολόγηση , η διαβίβαση , η διάδοση ή κάθε άλλη μορφή διάθεσης , η συσχέτιση ,ο συνδυασμός, ο περιορισμός αλλά και η διαγραφή ή η καταστροφή

Ποιος θεωρείται «Υπεύθυνος Επεξεργασίας»;

- Υπεύθυνος Επεξεργασίας θεωρείται το φυσικό ή νομικό πρόσωπο ,η δημόσια Αρχή ,η υπηρεσία ή άλλος φορέας που ,μόνα τους ή από κοινού με άλλα, που καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα

Ποιος είναι ο «Εκτελών την Επεξεργασία»;

- Εκτελών την Επεξεργασία είναι το φυσικό ή νομικό πρόσωπο ,η δημόσια αρχή ,η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου επεξεργασίας.

Επιτρέπεται η επεξεργασία των ειδικών προσωπικών δεδομένων που αφορούν την υγεία ;

Κατ' αρχάς απαγορεύεται.

Εκτός αν συντρέχει μια από τις ρητά αναφερόμενες περιπτώσεις στον Κανονισμό οπότε είναι δυνατή η επεξεργασία.

Η ρητή συγκατάθεση του υποκειμένου αποτελεί τη βασική νομιμοποιητική βάση άρσης της απαγόρευσης.

Πώς πρέπει να παρέχεται η συγκατάθεση ;

- Η συγκατάθεση θα πρέπει να παρέχεται με **σαφή θετική ενέργεια η οποία να συνιστά ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει ένδειξη της συμφωνίας του υποκειμένου των δεδομένων** υπέρ της επεξεργασίας των δεδομένων που το αφορούν, για παράδειγμα με γραπτή δήλωση, μεταξύ άλλων με ηλεκτρονικά μέσα, ή με προφορική δήλωση. Επομένως, η σιωπή, τα προσυμπληρωμένα τετραγωνίδια ή η αδράνεια δεν θα πρέπει να εκλαμβάνονται ως συγκατάθεση.

Τι προβλέπει το σχέδιο του ελληνικού Νόμου ;

- Σύμφωνα με το ***σχέδιο*** του ελληνικού νόμου –αρ. 7 εφ' όσον η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν την υγεία θεμελιώνεται στη συγκατάθεση του υποκειμένου των δεομένων η συγκατάθεση αυτή πρέπει να είναι **ΡΗΤΗ και ΕΓΓΡΑΦΗ**

Τι καλύπτει η χορηγούμενη συγκατάθεση ;

- Η συγκατάθεση θα πρέπει να καλύπτει το σύνολο των δραστηριοτήτων επεξεργασίας που διενεργείται για τον ίδιο σκοπό ή για τους ίδιους σκοπούς**. Όταν η επεξεργασία έχει πολλαπλούς σκοπούς, θα πρέπει να δίνεται συγκατάθεση για όλους αυτούς τους σκοπούς**.

Πότε είναι νόμιμη η επεξεργασία των προσωπικών δεδομένων , ακόμα και αν δεν υπάρχει ρητή συγκατάθεση;

- **Όταν εξυπηρετείται κάποιος σκοπός που σχετίζεται είτε με το πρόσωπο, είτε με το δημόσιο συμφέρον είτε με το κοινωνικό σύνολο.**

- Όταν είναι απαραίτητη για την εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων **στον τομέα του εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας**, εφόσον παρέχονται κατάλληλες εγγυήσεις για τα θεμελιώδη δικαιώματα και τα συμφέροντα του υποκειμένου των δεδομένων

- -Όταν η επεξεργασία είναι απαραίτητη για την **διαφύλαξη ζωτικού συμφέροντος του υποκειμένου** των δεδομένων ή άλλου φυσικού προσώπου **αν το υποκείμενο είναι σωματικά ή νομικά ανίκανο** να συγκατατεθεί ή
- - όταν η επεξεργασία είναι απαραίτητη για την εκπλήρωση **καθήκοντος που εκτελείται προς το δημόσιο συμφέρον**
  - όταν η επεξεργασία είναι **απαραίτητη για σκοπούς προληπτικής ιατρικής ,εκτίμησης της ικανότητας προς εργασία του εργαζόμενου, ιατρικής διάγνωσης , παροχής υγειονομικής ή κοινωνικής περίθαλψης**

- όταν η επεξεργασία είναι απαραίτητη **για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, όπως η προστασία έναντι σοβαρών διασυνοριακών απειλών κατά της υγείας**
- Όταν η επεξεργασία γίνεται **για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον,για σκοπούς επιστημονικής, ιατρικής έρευνας ή για στατιστικούς σκοπούς** οι οποίοι είναι ανάλογοι του επιδιωκόμενου σκοπού, σέβονται την ουσία του δικαιώματος προστασίας και προβλέπουν κατάλληλα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και συμφερόντων των υποκειμένων.

- **Απαγορεύεται, ωστόσο, περαιτέρω επεξεργασία των δεδομένων υγείας για άλλους σκοπούς από τρίτους όπως εργοδότες ή ασφαλιστικές εταιρίες ή τράπεζες .**

- Σύμφωνα με τον Κανονισμό , **τα Κράτη Μέλη έχουν το δικαίωμα να διατηρούν ή να θεσπίζουν περαιτέρω όρους ή /και περιορισμούς** όσον αφορά την επεξεργασία των γενετικών δεδομένων, των βιομετρικών δεδομένων και των δεδομένων υγείας.

Ποιες Αρχές διέπουν την επεξεργασία των προσωπικών δεδομένων των ασθενών ;

- -Νομιμότητα, αντικειμενικότητα και διαφάνεια .
- -Περιορισμός του σκοπού.
- -Ελαχιστοποίηση των δεδομένων .
- -Ακρίβεια (διόρθωση ή διαγραφή) .
- -Περιορισμός της περιόδου αποθήκευσης.
- -Ακεραιότητα .
- -Εμπιστευτικότητα .
- Αρχή της Λογοδοσίας

Ποια δικαιώματα έχουν οι ασθενείς αναφορικά με τα προσωπικά δεδομένα τους;

Να λαμβάνουν πληροφορίες που αφορούν :

- -τα στοιχεία του Υπευθύνου Επεξεργασίας
- -τα στοιχεία του Υπευθύνου Προστασίας Δεδομένων
- -τους σκοπούς της επεξεργασίας και τη νομική βάση αυτής
- -τα έννομα συμφέροντα που επιδιώκονται
- -τους αποδέκτες αν υπάρχουν
- -την πρόθεση τυχόν περαιτέρω διαβίβασης
- -το χρονικό διάστημα αποθήκευσης

Ποια δικαιώματα έχουν οι ασθενείς αναφορικά με τα προσωπικά δεδομένα τους;

- την ύπαρξη δικαιώματος υποβολής αιτήματος για πρόσβαση και **διόρθωση** ή **διαγραφή δεδομένων** (δικαίωμα στη λήθη)
- τη **δυνατότητα ανάκλησης της συγκατάθεσης** ,όταν η επεξεργασία βασίζεται σε συγκατάθεση
- το **δικαίωμα υποβολής καταγγελίας** στην Εποπτική Αρχή

Άλλα δικαιώματα των ασθενών

- -Δικαίωμα **περιορισμού της επεξεργασίας**
- -Δικαίωμα στη **φορητότητα των δεδομένων** :Το υποκείμενο των δεδομένων θα πρέπει να έχει επίσης τη δυνατότητα να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν και που έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα διαλειτουργικό μορφότυπο, και να τα διαβιβάζει σε άλλον υπεύθυνο επεξεργασίας.

Δικαιώματα – Υποχρεώσεις

- **Τα δικαιώματα των ασθενών ως υποκειμένων των προσωπικών δικαιωμάτων αντιστοιχούν στις υποχρεώσεις** των Υπευθύνων Επεξεργασίας και των Εκτελούντων την Επεξεργασία αυτών οι οποίοι οφείλουν να λαμβάνουν, και να αποδεικνύουν ότι λαμβάνουν, εκείνα τα τεχνικά και οργανωτικά μέτρα που απαιτούνται για την ικανοποίηση των δικαιωμάτων των υποκειμένων.

Πότε και πώς παρέχονται οι πληροφορίες στους ασθενείς ;

- **Οι πληροφορίες παρέχονται δωρεάν προς τους ασθενείς εντός εύλογης προθεσμίας αλλά το αργότερο εντός μηνός δίδοντας εξηγήσεις για τους λόγους τυχόν καθυστέρησης.**

Υποχρεώσεις των συλλόγων ασθενών

- **Οι σύλλογοι ασθενών είναι Υπεύθυνοι Επεξεργασίας των δεδομένων των μελών τους .**
- **Ως Υπεύθυνοι Επεξεργασίας οφείλουν να λαμβάνουν οργανωτικά και τεχνικά μέτρα προστασίας των προσωπικών δεδομένων των μελών τους και να**
  - **Εκλαμβάνουν όλα τα δικαιώματα των μελών ως αντίστοιχες δικές τους υποχρεώσεις .**

Απλές οδηγίες συμμόρφωσης για τους συλλόγους ασθενών

- -Να περιλάβουν **ρήτρες εμπιστευτικότητας** στις συμβάσεις με τους εργαζόμενους και τους εξωτερικούς συνεργάτες .
- -Να υπάρχει **δυνατότητα πρόσβασης στα αρχεία των Η/Υ ανάλογα με την ιεραρχία(κάθετη πρόσβαση) αλλά και τα καθήκοντα(οριζόντια πρόσβαση)** ώστε να διασφαλιστεί ότι κάθε ένας έχει πρόσβαση σε εκείνα τα δεδομένα που απαιτεί και δικαιολογεί η θέση του (η γραμματέας για παράδειγμα δεν επιτρέπεται να έχει πρόσβαση σε ηλεκτρονικά αρχεία συνεδριών που συντάσσει ο ψυχολόγος του συλλόγου)

- –Να λαμβάνονται συστηματικά αντίγραφα ασφαλείας (back up)των ηλεκτρονικών αρχείων που να τηρούνται σε ασφαλές περιβάλλον-
- - Να χρησιμοποιούνται αυθεντικά προγράμματα και αντιικά συστήματα (antivirus) προστασίας των ηλεκτρονικών υπολογιστών.
- -Να υπάρχουν σύνθετοι ασφαλείς κωδικοί πρόσβασης στους Η/Υ (όχι το όνομα του χρήστη ή η ημερομηνία γέννησης ή το όνομα των παιδιών ή το 1234 και πολλά άλλα όμοια) .

- -Να μην καταγράφονται οι κωδικοί και να μην παραμένουν εμφανώς σε σημειώματα σε σημεία προσβάσιμα σε όλους .
- –Να μη κατεβάζουν οι εργαζόμενοι ανεξέλεγκτα δωρεάν προγράμματα από το διαδίκτυο, ούτε να χρησιμοποιούνται προγράμματα που δεν υποστηρίζονται πλέον όπως τα Windows XP
- -Να μην παρέχεται το wi-fi του συλλόγου στα μέλη του συλλόγου
- –Να ελέγχεται η προσβασιμότητα στο διαδίκτυο στους χρήστες των ηλεκτρονικών υπολογιστών στο σύλλογο.

- -Μεγάλη προσοχή στις φορητές συσκευές USB (στικάκια) για μεταφορά ιών .
- -Μέτρα όπως η κρυπτογράφηση(που δεν έχουν υψηλό κόστος) και η ψευδωνυμοποίηση αποτελούν εξαιρετικά μέσα για την ασφάλεια της επεξεργασίας
- -Αλλά και μέτρα για την ασφάλεια του χώρου : Να κλειδώνονται τα γραφεία, τα ντουλάπια με τα χειρόγραφα αρχεία, να μην παραμένουν ανοικτοί οι Η/Υ μετά το πέρας του ωραρίου των χρηστών .
- -Γνωστοποίηση παραβιάσεων στην ΑΠΡΠΔ εντός 72 ωρών

- Όσοι σύλλογοι διαθέτουν ιστοσελίδες οφείλουν να αναρτήσουν την πολιτική προστασίας των προσωπικών δεδομένων που εφαρμόζουν και να ενημερώνουν τα μέλη τους για ποιο σκοπό συλλέγουν και επεξεργάζονται τα δεδομένα τους , σε τι είδους επεξεργασία προβαίνουν, για πόσο διάστημα θα τα τηρούν στα αρχεία τους .Περαιτέρω να ενημερώνουν τα μέλη τους για τα δικαιώματα που τους παρέχει ο Κανονισμός : το δικαίωμα να ελέγχουν τα στοιχεία τους και αν χρειαστεί να τα διορθώνουν, το δικαίωμα να ανακαλούν οποτεδήποτε τη συγκατάθεση επεξεργασίας τους , το δικαίωμα να διαγραφούν τα δεδομένα τους, το δικαίωμα τους να μεταφέρουν τα δεδομένα τους . Για τη μαζική αποστολή email και newsletters να λαμβάνονται συναινέσεις .

- **Τήρηση Αρχείου Επεξεργασίας Δραστηριοτήτων**

(Η επεξεργασία περιλαμβάνει ειδικές κατηγορίες δεδομένων)

Περιλαμβάνει : Στοιχεία Υπευθύνου

Σκοπούς Επεξεργασίας

Κατηγορίες δεδομένων και υποκειμένων

Κατηγορίες αποδεκτών

Διασυνοριακές διαβιβάσεις

Προθεσμίες διαγραφή

Τεχνικά και Οργανωτικά Μέτρα

- **Ορισμός Υπευθύνου Επεξεργασίας ;(** είναι περίπτωση συστηματικής και τακτικής παρακολούθησης σε μεγάλη κλίμακα ή συνιστούν οι βασικές δραστηριότητες ενός συλλόγου ασθενών μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων;)

- **Διενέργεια Εκτίμησης Αντικτύπου** (επεξεργασία ευαίσθητων δεδομένων σε μεγάλη κλίμακα;)

- Σας ευχαριστώ πολύ !