Εγχειρίδιο Εφαρμογής του Γενικού Κανονισμού για την Προστασία των Προσωπικών Δεδομένων (ΓΚΠΠΔ-GPDR)

Με το παρόν δίδεται η βασική ενημέρωση σχετικά με τη νέα Ευρωπαϊκή Νομοθεσία Προστασίας Προσωπικών Δεδομένων που τέθηκε σε πλήρη εφαρμογή στις 25 Μαΐου 2018, καθώς και κάποια συγκεκριμένα μέτρα που πρέπει άμεσα να λάβουν όλα τα οδοντιατρεία για τη συμμόρφωσή τους.

1. Εισαγωγή

Η συγκεκριμένη νομοθεσία αποτελείται από:

1/τον Κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της Οδηγίας 95/46 ΕΚ.

2/Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου.

3/Οδηγία (ΕΕ) 2016/681 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 σχετικά με τη χρήση των δεδομένων που περιέχονται στις καταστάσεις ονομάτων επιβατών (PNR) για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων

4/ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2018/1725 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 23ης Οκτωβρίου 2018 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ

Δεδομένα προσωπικού χαρακτήρα αποτελούν οι πληροφορίες που αναφέρονται σε συγκεκριμένο υποκείμενο, εφόσον μπορούν άμεσα ή έμμεσα (σε συνδυασμό με άλλα στοιχεία) να το ταυτοποιήσουν (ταυτότητες, ΑΦΜ, ΑΜΚΑ, αριθμοί πιστωτικών καρτών, εξετάσεις), είτε τα στοιχεία αυτά είναι έντυπα είτε είναι ηλεκτρονικά. Ευαίσθητα προσωπικά δεδομένα είναι αυτά που αναφέρονται στη φυλετική ή εθνική του προέλευση, στα πολιτικά του φρονήματα, στις θρησκευτικές ή φιλοσοφικές του πεποιθήσεις, στη συμμετοχή του σε συνδικαλιστική οργάνωση, **στην υγεία του, στην κοινωνική του πρόνοια**, στην ερωτική του ζωή, τις ποινικές διώξεις και καταδίκες του, καθώς και στη συμμετοχή του σε συναφείς με τα

ανωτέρω ενώσεις προσώπων. Τα ευαίσθητα δεδομένα προστατεύονται από το Νόμο με αυστηρότερες ρυθμίσεις (και επιφέρουν διπλάσια πρόστιμα) από ότι τα απλά προσωπικά δεδομένα, καθώς αποτελούν ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα που χρήζουν μεγαλύτερης προστασίας, πρέπει να υποβάλλονται σε επεξεργασία για σκοπούς σχετικούς με την υγεία, μόνο όταν τούτο απαιτείται για την επίτευξη αυτών των σκοπών προς όφελος φυσικών προσώπων και της κοινωνίας συνολικά, ιδίως στο πλαίσιο της διαχείρισης υπηρεσιών και συστημάτων υγείας και κοινωνικής πρόνοιας. Οπότε εξ επαγγέλματος οι οδοντίατροι διαχειρίζονται «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 κατάσταση της υγείας του.

Η επεξεργασία προσωπικών δεδομένων, η διαδικασία δηλαδή στην οποία αναφέρεται ο Κανονισμός, συμπεριλαμβάνει τη συλλογή, την καταχώρηση, την οργάνωση, τη διάρθρωση, την αποθήκευση κλπ. των δεδομένων αυτών. Σε περίπτωση διαρροής δεδομένων, η ευθύνη απέναντι στο νόμο είναι **αντικειμενική και νόθος**, βαραίνει πρωταρχικά τη διοίκηση και συνεπώς **η συμμόρφωση είναι υποχρεωτική για όλους**.

2. Αρχές και Δικαιώματα

Κάθε επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ιδίως δεδομένων υγείας, θα πρέπει πρωταρχικά να εξυπηρετεί τον άνθρωπο και να διέπεται από τις **Αρχές** τις νομοθεσίας:

1. Το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα δεν είναι απόλυτο δικαίωμα· πρέπει να εκτιμάται σε σχέση με τη λειτουργία του στην κοινωνία και να σταθμίζεται με άλλα θεμελιώδη δικαιώματα, σύμφωνα με την αρχή της επικουρικότητας και αναλογικότητας.
2. Η αρχή της διαφάνειας απαιτεί οποιαδήποτε ενημέρωση που απευθύνεται στο κοινό ή στο υποκείμενο των δεδομένων να είναι συνοπτική, εύκολα προσβάσιμη και εύκολα κατανοητή και να χρησιμοποιείται σαφής και απλή διατύπωση και, επιπλέον, κατά περίπτωση, απεικόνιση.
3. Η αρχή της προσβασιμότητας εξασφαλίζει το δικαίωμα του παρόχου των δεδομένων στην πρόσβαση και στην διόρθωση αυτών.
4. Η αρχή της λογοδοσίας υποχρεώνει τη διοίκηση να γνωστοποιήσει την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην αρμόδια εποπτική αρχή εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος, εκτός εάν ο υπεύθυνος επεξεργασίας μπορεί να αποδείξει, ότι η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να επιφέρει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.
5. Η Αρχή της ελαχιστοποίησης των δεδομένων υποχρεώνει την επιχείρηση να συλλέγει και να κατακρατά μόνο τα δεδομένα που είναι τελείως απαραίτητα για την εξυπηρέτηση των εννόμων συμφερόντων αυτής και να τα διαγράφει με το πέρας αυτής.

Πλην αυτών, το υποκείμενο δεδομένων, δηλαδή ο ασθενής, έχει πλέον σαφή δικαιώματα που πρέπει σε κάθε περίπτωση να διαφυλάσσονται και να εξυπηρετούνται από τον Υπεύθυνο Επεξεργασίας, την επιχείρηση/οδοντίατρο: Δικαίωμα Πρόσβασης, Διόρθωσης, Εναντίωσης, Διαγραφής, Περιορισμού, Φορητότητας, Ανάκληση συγκατάθεσης, Εναντίωση στην Αυτοματοποιημένη λήψη αποφάσεων.

Συνεπώς ο ασθενής έχει δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα τα οποία συλλέχθηκαν και το αφορούν και να μπορεί να ασκεί το εν λόγω δικαίωμα ευχερώς και σε εύλογα τακτά διαστήματα, προκειμένου να έχει επίγνωση και να επαληθεύει τη νομιμότητα της επεξεργασίας. Αυτό περιλαμβάνει το δικαίωμα των υποκειμένων των δεδομένων να έχουν πρόσβαση στα δεδομένα που αφορούν την υγεία τους, για παράδειγμα τα δεδομένα των ιατρικών αρχείων τους τα οποία περιέχουν πληροφορίες όπως διαγνώσεις, αποτελέσματα εξετάσεων, αξιολογήσεις από θεράποντες ιατρούς και κάθε παρασχεθείσα θεραπεία ή επέμβαση. Επομένως, κάθε υποκείμενο δεδομένων θα πρέπει να έχει το δικαίωμα να γνωρίζει και να του ανακοινώνεται ιδίως για ποιους σκοπούς γίνεται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, εφόσον είναι δυνατόν για πόσο διάστημα γίνεται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ποιοι αποδέκτες λαμβάνουν τα δεδομένα προσωπικού χαρακτήρα, ποια λογική ακολουθείται στην τυχόν αυτόματη επεξεργασία δεδομένων προσωπικού χαρακτήρα και ποιες θα μπορούσαν να είναι οι συνέπειες της εν λόγω επεξεργασίας, τουλάχιστον όταν αυτή βασίζεται σε κατάρτιση προφίλ. Το δικαίωμα αυτό δεν θα πρέπει να επηρεάζει αρνητικά τα δικαιώματα ή τις ελευθερίες άλλων, όπως το επαγγελματικό απόρρητο ή το δικαίωμα διανοητικής ιδιοκτησίας και, ιδίως, το δικαίωμα δημιουργού που προστατεύει το λογισμικό. Ωστόσο, οι παράγοντες αυτοί δεν θα πρέπει να έχουν ως αποτέλεσμα την άρνηση παροχής κάθε πληροφορίας στο υποκείμενο των δεδομένων. Όταν ο υπεύθυνος επεξεργασίας επεξεργάζεται μεγάλες ποσότητες πληροφοριών σχετικά με το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας θα πρέπει να δύναται να ζητεί από το υποκείμενο, πριν δοθούν οι πληροφορίες, να προσδιορίζει τις πληροφορίες ή τις δραστηριότητες επεξεργασίας που σχετίζονται με το αίτημα.

Ο ασθενής έχει επίσης το δικαίωμα να ζητεί τη διόρθωση των δεδομένων προσωπικού χαρακτήρα που το αφορούν, καθώς και το «δικαίωμα στη λήθη», εάν η διατήρηση των εν λόγω δεδομένων παραβιάζει τον παρόντα κανονισμό ή το δίκαιο της Ένωσης στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας. Το υποκείμενο των δεδομένων θα πρέπει να έχει το δικαίωμα να ζητεί τη διαγραφή και την παύση της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που το αφορούν, εάν τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέγονται ή υποβάλλονται κατ' άλλο τρόπο σε επεξεργασία, εάν το υποκείμενο των δεδομένων αποσύρει τη συγκατάθεσή του για την επεξεργασία ή εάν αντιτάσσεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν ή εάν η επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν δεν είναι σύμφωνη προς τον παρόντα κανονισμό. Το δικαίωμα αυτό έχει ιδίως σημασία όταν το υποκείμενο των δεδομένων παρέσχε τη συγκατάθεσή του ως παιδί, όταν δεν είχε πλήρη επίγνωση των κινδύνων που ενέχει η επεξεργασία, και θέλει αργότερα να αφαιρέσει τα συγκεκριμένα δεδομένα προσωπικού χαρακτήρα, κυρίως από το διαδίκτυο. Το υποκείμενο των δεδομένων θα πρέπει να μπορεί να ασκήσει το εν λόγω δικαίωμα παρά το γεγονός ότι δεν είναι πλέον παιδί. Ωστόσο, η περαιτέρω διατήρηση των δεδομένων προσωπικού χαρακτήρα θα πρέπει να είναι σύννομη όταν είναι αναγκαία για την άσκηση του δικαιώματος

ελευθερίας της έκφρασης και ενημέρωσης, για τη συμμόρφωση με νομική υποχρέωση, για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς, ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

3. Οδηγίες Συμμόρφωσης

Επειδή το πλαίσιο συμμόρφωσης που προβλέπει ο Κανονισμός είναι αρκετά αόριστο, αλλά ιδιαίτερα αυστηρό, με πρόστιμα που ανέρχονται σε 200,000 Ευρώ και ελέγχους από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, σας προτείνουμε τις παρακάτω ενδεικτικές **ενέργειες συμμόρφωσης, που ισχύουν για όλους τους Τύπους Οδοντιατρείων**:

1. Αναλυτική Χαρτογράφηση των Προσωπικών Δεδομένων της Επιχείρησης, σε φυσική και ψηφιακή μορφή και Εξασφάλιση Νομικής Βάσηςγια την Επεξεργασία τους, π.χ. Συγκατάθεση.
2. Δημιουργία και διατήρηση του ψηφιακού Αρχείου Δραστηριοτήτων Επεξεργασίας Δεδομένων.
3. Ανάλυση Ασφάλειας Πληροφοριακών Συστημάτων (ασύρματα δίκτυα, λειτουργικά συστήματα, τοίχος προστασίας, αντίγραφα ασφαλείας, πιστοποιητικά ασφαλείας εξυπηρετητών).
4. Συμβάσεις Εμπιστευτικότητας με προσωπικό και εξωτερικούς συνεργάτες – λογιστές, οδοντοτεχνίτες κ.α.
5. Εκτίμηση Αντικτύπου για την Προστασία των Προσωπικών Δεδομένων – όπου χρειάζεται.
6. Να απαντά μέσα σε 30 ημέρες σε κάθε σχετικό αίτημα του ασθενούς το οποίο αφορά στα δεδομένα του, είτε ικανοποιώντας το δικαίωμα (π.χ. δίνοντας στον ασθενή αντίγραφο του ιατρικού φακέλου), είτε απορρίπτοντας αιτιολογημένα το αίτημα (π.χ. αρνούμενος αίτημα διαγραφής), είτε εξηγώντας τους λόγους καθυστέρησης. Σε περίπτωση καθυστέρησης οφείλει πάντως να απαντά θετικά ή αρνητικά εντός 3 μηνών από το αίτημα.
7. Να γνωστοποιεί στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα εντός 72 ωρών από τη στιγμή που ενημερώνεται για κάθε τυχόν παραβίαση του αρχείου του, αλλά και τους ασθενείς του εάν η παραβίαση ενδέχεται να τους προκαλέσει υψηλό κίνδυνο.

Σας επισημαίνουμε ότι τα παραπάνω βήματα συμμόρφωσης είναι απαραίτητα για όλους τους τύπους οδοντιατρείων και προς διευκόλυνση σας διανέμεται με το παρόν και ένα έγγραφο με Γενικές Συμβουλές Συμμόρφωσης**.** Επίσης και για δική σας διευκόλυνση, στην ιστοσελίδα του Συλλόγου θα αναρτηθούν τα εξής χρήσιμα έγγραφα (πρότυπα):

1. Πρότυπο έγγραφο συγκατάθεσης
2. Πρότυπη σύμβαση εχεμύθειας/εμπιστευτικότητας με Εξωτερικούς Συνεργάτες
3. Πρότυπο ΑΔΕΔ

Η χρήση των εγγράφων αυτών από μόνη της δεν εξασφαλίζει τη συμμόρφωση της επιχείρησης καθώς το περιεχόμενο των εγγράφων διαφέρει σημαντικά ανάλογα τη φύση του οδοντιατρείου, τα δεδομένα που συλλέγονται και τους σκοπούς όπου χρησιμοποιούνται,αλλά έχει ως στόχο την κατανόηση και την εξοικείωση των μελών με τα νέα πρότυπα που επιβάλει η νομοθεσία.

Με εκτίμηση και υπευθυνότητα, οι Υπεύθυνοι Συμμόρφωσης:

Γιάννης Γκαντάρας	Γιάννης Γιαγλάρας	Γιώργος Τσούμας
Επιστήμονας Πληροφορικής	Νομικός Υπ.	Ασφ. Συστημ.