Τι είναι ο GDPR (General Data Protection Regulation);

Ο GDPR προσφέρει το ρυθμιστικό πλαίσιο που προσαρμόζεται στην πραγματικότητα του σημερινού ψηφιακού κόσμου, ενώ ταυτόχρονα θέτει τον ιδιώτη πολίτη της Ευρωπαϊκής Ένωσης (ΕΕ) στην κορυφή της διαχείρισης των προσωπικών του δεδομένων.

Ο κανονισμός GDPR ή Γενικός Κανονισμός για την Προστασία των Δεδομένων (ΓΚΠΔ) είναι ένα σύνολο κανόνων που αποσκοπούν στην καλύτερη προστασία των πολιτών της ΕΕ όσον αφορά τα προσωπικά τους δεδομένα και έρχεται να αντικαταστήσει την οδηγία 95/46 / ΕΚ. για την προστασία των δεδομένων που υπήρχε ήδη από το 1995. Η ειδοποιός διαφορά ανάμεσα τους είναι ότι η οδηγία για την προστασία των δεδομένων ήταν μια οδηγία, ενώ ο ΓΚΠΔ είναι ένας κανονισμός και σαν κανονισμός είναι δεσμευτικός για όλους αφήνοντας πολύ λίγα περιθώρια για εθνική ερμηνεία και μόνο σε τομείς όπου η ρύθμιση το επιτρέπει.

Στις αρχές του 2012, η Ευρωπαϊκή Επιτροπή δήλωσε ότι η ΕΕ έπρεπε να είναι περισσότερο σε αρμονία με την ψηφιακή εποχή, ενώ στις 15 Δεκεμβρίου 2015, το Ευρωπαϊκό Κοινοβούλιο, το Ευρωπαϊκό Συμβούλιο και η Ευρωπαϊκή Επιτροπή κατέληξαν σε συμφωνία σχετικά με τους νέους κανόνες προστασίας δεδομένων.

Ο GDPR έχει σχεδιαστεί για μια ενιαία ψηφιακή αγορά στην οποία οι οργανισμοί που επεξεργάζονται προσωπικά δεδομένα των πολιτών της ΕΕ γνωρίζουν τι μπορούν να κάνουν και τι δεν μπορούν να κάνουν με αυτά τα δεδομένα και τέθηκε σε ισχύ στις 25 Μαΐου 2018.

Οι σημαντικότερες αλλαγές του νέου Κανονισμού

Τα κύρια στοιχεία των νέων κανόνων για την προστασία των δεδομένων είναι τα παρακάτω:

- Ένα μοναδικό σύνολο κανόνων για ολόκληρη την ήπειρο: διασφαλίζοντας την ασφάλεια δικαίου για τις επιχειρήσεις και το ίδιο επίπεδο προστασίας των δεδομένων για όλους τους πολίτες της ΕΕ.

- Εξωεδαφικό πεδίο εφαρμογής: Οι ίδιοι κανόνες ισχύουν για όλες τις εταιρείες που προσφέρουν τις υπηρεσίες τους στην ΕΕ, ακόμη και όταν οι εταιρείες αυτές είναι εγκατεστημένες εκτός της ΕΕ.

- Ισχύ για όλες τις επιχειρήσεις: Η εφαρμογή του κανονισμού για την προστασία των δεδομένων δεν εξαρτάται από το μέγεθος της εταιρείας ή του οργανισμού σας αλλά από τη φύση των δραστηριοτήτων της. Ωστόσο, μερικές από τις

υποχρεώσεις του ΓΚΠΔ μπορεί να μην εφαρμόζονται σε όλες τις μικρομεσαίες επιχειρήσεις (ΜΜΕ) όπως για παράδειγμα η ανάγκη ορισμού ενός υπευθύνου προστασίας δεδομένων (GDPO, General Data Protection Officer).

- Νέα και ισχυρότερα δικαιώματα για τους πολίτες: ενισχύονται το δικαίωμα ενημέρωσης, το δικαίωμα πρόσβασης και το δικαίωμα να λησμονούνται. - Ένα νέο δικαίωμα στη φορητότητα δεδομένων επιτρέπει στους πολίτες να μεταφέρουν τα δεδομένα τους από μια εταιρεία σε μια άλλη, δημιουργώντας νέες επιχειρηματικές ευκαιρίες.

- Υποχρέωση κοινοποίησης παραβίασης: Μια επιχείρηση που παραβιάζει δεδομένα, ή θέτει σε κίνδυνο το υποκείμενο των δεδομένων, υποχρεούται να ενημερώσει την αρχή προστασίας δεδομένων εντός 72 ωρών.

- Υψηλότερα πρόστιμα και σημαντικότερες οικονομικές κυρώσεις σε περίπτωση σοβαρής παραβίασης εκ μέρους ενός φορέα και σαφούς μη συμμόρφωσης.

Τι είναι τα δεδομένα προσωπικού χαρακτήρα;

Τα δεδομένα προσωπικού χαρακτήρα είναι πληροφορίες που αφορούν ένα **ταυτοποιημένο ή ταυτοποιήσιμο εν ζωή άτομο**. Διαφορετικές πληροφορίες οι οποίες, εάν συγκεντρωθούν όλες μαζί, μπορούν να οδηγήσουν στην ταυτοποίηση ενός συγκεκριμένου ατόμου, αποτελούν επίσης δεδομένα προσωπικού χαρακτήρα.

Τα δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα, έχουν κρυπτογραφηθεί ή για τα οποία **έχουν χρησιμοποιηθεί ψευδώνυμα** αλλά τα οποία μπορούν να χρησιμοποιηθούν για την επαναταυτοποίηση ενός ατόμου παραμένουν δεδομένα προσωπικού χαρακτήρα και εμπίπτουν στο πεδίο εφαρμογής του ΓΚΠΔ.

Τα δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί **ανώνυμα** με τέτοιον τρόπο ώστε το άτομο να μην είναι ή να μην είναι πια ταυτοποιήσιμο δεν θεωρούνται πλέον δεδομένα προσωπικού χαρακτήρα. Για να είναι πραγματικά ανώνυμα τα δεδομένα, η ανωνυμοποίηση πρέπει να είναι μη αντιστρέψιμη.

Ο ΓΚΠΔ προστατεύει τα δεδομένα προσωπικού χαρακτήρα **ανεξάρτητα από την τεχνολογία που χρησιμοποιείται για την επεξεργασία τους.** Είναι τεχνολογικά ουδέτερος και εφαρμόζεται τόσο στην αυτοματοποιημένη όσο και στη χειροκίνητη επεξεργασία, υπό την προϋπόθεση ότι τα δεδομένα οργανώνονται βάσει προκαθορισμένων κριτηρίων (π.χ. αλφαβητική σειρά). Επίσης, δεν έχει σημασία ο τρόπος που αποθηκεύονται τα δεδομένα – σε σύστημα τεχνολογίας πληροφοριών, μέσω βιντεοεπιτήρησης ή σε έντυπη μορφή. Σε όλες τις περιπτώσεις τα δεδομένα προσωπικού χαρακτήρα υπόκεινται στις απαιτήσεις προστασίας που προβλέπει ο ΓΚΠΔ.

Παραδείγματα δεδομένων προσωπικού χαρακτήρα:

- όνομα και επώνυμο
- διεύθυνση κατοικίας
- ηλεκτρονική διεύθυνση, π.χ. όνομα.επώνυμο@εταιρεία.com
- αναγνωριστικός αριθμός κάρτας
- δεδομένα τοποθεσίας (π.χ. η λειτουργία δεδομένων τοποθεσίας σε κινητό τηλέφωνο)[1]
- διεύθυνση διαδικτυακού πρωτοκόλλου (IP)
- αναγνωριστικό cookie[2]
- το αναγνωριστικό διαφήμισης του τηλεφώνου σας
- δεδομένα που φυλάσσονται από νοσοκομείο ή γιατρό, που θα μπορούσαν να είναι ένα σύμβολο που προσδιορίζει αποκλειστικά ένα άτομο.

[1]Δεδομένα Τοποθεσίας: Αποτελούν υπηρεσίες που χρησιμοποιούν πληροφορίες όπως σήματα GPS, αισθητήρες συσκευής, σημεία πρόσβασης Wi-Fi και αναγνωριστικά πύργων κυψελών, που μπορούν να χρησιμοποιηθούν για τον υπολογισμό ή την εκτίμηση της ακριβούς τοποθεσίας

[2] Τα Cookies είναι μικρά αρχεία (text files), τα οποία αποστέλλονται και φυλάσσονται στον ηλεκτρονικό υπολογιστή του χρήστη, επιτρέποντας σε ιστοσελίδες, να λειτουργούν απρόσκοπτα και χωρίς τεχνικές ανωμαλίες, να συλλέγονται πολλαπλές επιλογές του χρήστη, να αναγνωρίζουν τους συχνούς χρήστες, να διευκολύνουν την πρόσβαση τους σε αυτή, και για τη συλλογή δεδομένων για τη βελτίωση του περιεχομένου της ιστοσελίδας. Τα Cookies δεν προκαλούν βλάβες στους ηλεκτρονικούς υπολογιστές των χρηστών αλλά και στα αρχεία που φυλάσσονται σε αυτούς.

Παραδείγματα δεδομένων που δεν θεωρούνται δεδομένα προσωπικού χαρακτήρα:

- αριθμός μητρώου εταιρείας
- ηλεκτρονική διεύθυνση του τύπου πληροφορίες@εταιρεία.com
- ανώνυμα δεδομένα

Τι ορίζει ο κανονισμός ως επεξεργασία δεδομένων;

Επεξεργασία δεδομένων θεωρείται κάθε πράξη που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων ηλεκτρονικών μέσων, σε προσωπικά και ευαίσθητα προσωπικά δεδομένα. Επομένως η συλλογή, η οργάνωση, η αποθήκευση, η προσαρμογή, η χρήση, η διάδοση και η διαγραφή δεδομένων σχετικών με ιατρικό ιστορικό ασθενών από επαγγελματίες υγείας (ιατρούς, φαρμακοποιούς, νοσηλευτές, διοικητικό προσωπικό ιατρείων, κλινικών και διαγνωστικών κέντρων) θεωρείται επεξεργασία δεδομένων.

Ποιες είναι οι βασικές αλλαγές που προκύπτουν από την εφαρμογή του GDPR

1. Ατομικές ελευθερίες & προσωπικό απόρρητο

Όλα τα φυσικά πρόσωπα, τα «υποκείμενα» στα οποία ανήκουν τα δεδομένα, έχουν ολοκληρωμένα δικαιώματα διαχείρισης στα προσωπικά τους δεδομένα, με πιο σημαντικά :

- να αποκτούν εύκολη πρόσβαση και να λαμβάνουν όλα τα δεδομένα **(δικαίωμα στην φορητότητα)**
- να ζητούν την διόρθωση σφάλματων
- να εναντιώνονται στην επεξεργασία τους
- να μπορούν να ζητούν την διαγραφή των προσωπικών τους δεδομένων **(δικαίωμα στην λήθη)**.

2. Διαφάνεια, γνωστοποιήσεις & συμμόρφωση

Όλοι οι οργανισμοί, οι εταιρείες και οι ελεύθεροι επαγγελματίες θα πρέπει να εφαρμόζουν πολιτικές & διαδικασίες με τις οποίες:

- θα λαμβάνουν **την συγκατάθεση** για τη συλλογή και την επεξεργασία προσωπικών δεδομένων.
- θα παρέχουν σαφή γνωστοποίηση για τη συλλογή και την επεξεργασία δεδομένων φυσικών προσώπων.
- θα περιγράφουν τους λόγους και τις περιπτώσεις επεξεργασίας των προσωπικών δεδομένων.
- θα τηρούν αρχεία που θα παρέχουν αναλυτικές πληροφορίες για τις διαδικασίες επεξεργασίας των δεδομένων.
- θα προστατεύουν τα προσωπικά δεδομένα λαμβάνοντας κατάλληλα **μέτρα ασφαλείας** στο εσωτερικό τους και στις επικοινωνίες τους με τρίτους.
- θα ορίζουν τις πολιτικές αποθήκευσης, διατήρησης, ασφαλούς φύλαξης και διαγραφής δεδομένων τα οποία έχουν στην κατοχή τους, σε έντυπη και σε ηλεκτρονική μορφή.
- θα γνωστοποιούν **εντός 72 ωρών** στις αρχές και στους ενδιαφερόμενους, τις παραβιάσεις προσωπικών δεδομένων.

Η εφαρμογή του GDPR στους τομείς της Υγείας & των Κοινωνικών Υπηρεσιών

Ο Κανονισμός θα επηρεάσει δραστικά τον τρόπο με τον οποίο οι οργανισμοί, εταιρείες και επαγγελματίες συλλέγουν, διαχειρίζονται, επεξεργάζονται και αποθηκεύουν πληροφορίες που περιέχουν **«προσωπικά δεδομένα»** και ιδιαίτερα **«ευαίσθητα δεδομένα».**

Οι οργανισμοί και οι εταιρείες που παρέχουν **υπηρεσίες υγείας και κοινωνικής υποστήριξης** καθώς και όλοι οι επαγγελματίες του τομέα της Υγείας, έχουν αυξημένες υποχρεώσεις από την εφαρμογή του Κανονισμού.

Ασφαλιστικοί οργανισμοί δημόσιοι & ιδιωτικοί, κοινωνικές υπηρεσίες & δομές που ανήκουν σε δήμους ή στο δημόσιο τομέα, μη κερδοσκοπικά ιδρύματα, ενώσεις και επιστημονικοί φορείς υποστήριξης ασθενών, νοσοκομεία, πολυκλινικές, κλινικές, κέντρα αποκατάστασης, ειδικά θεραπευτήρια, διαγνωστικά κέντρα & οι επαγγελματίες υγείας θα πρέπει να αναλύσουν με **ιδιαίτερη προσοχή** τις απαιτήσεις του Κανονισμού και να αναλάβουν τις κατάλληλες ενέργειες τόσο για την κανονιστική τους συμμόρφωση, όσο και για την ενίσχυση της ασφάλειας των πληροφοριακών τους συστημάτων.

Αυξημένες υποχρεώσεις έχουν και οι εταιρείες που **προμηθεύουν** ιατροτεχνολογικό εξοπλισμό, πληροφοριακά συστήματα για την υγεία, υπηρεσίες προς τους ανωτέρω (όπως οι εταιρείες γραμματειακής υποστήριξης, φύλαξης & καθαρισμού), οι εταιρείες εκπόνησης «Κλινικών Μελετών» καθώς και οι φαρμακευτικές εταιρείες.

Ιδιαίτερη μέριμνα πρέπει να δοθεί στα θέματα ολοκληρωμένης ενημέρωσης και εκπαίδευσης **του προσωπικού** που συλλέγει και επεξεργάζεται τα «ευαίσθητα προσωπικά δεδομένα» των ασθενών και των ατόμων που λαμβάνουν υπηρεσίες κοινωνικής φροντίδας.

Οι ενέργειες που απαιτούνται για τη συμμόρφωση με τον GDPR είναι σημαντικές, απαιτούν συστηματική προετοιμασία και την επιλογή των κατάλληλων διαδικασιών & εργαλείων.

Πηγή: https://www.eugdpr.gr/health/