Προστασία Προσωπικών Δεδομένων & Επεξεργασία Δεδομένων Υγείας

Αναστασία Παύλου

Attorney at Law (Athens Bar Association)

LL.M., CIPP-E

Στόχος Παρουσίασης

01

Προστασία Προσωπικών Δεδομένων και εισαγωγή στον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR).

02

Βασικές αρχές επεξεργασίας προσωπικών δεδομένων και νόμιμη βάση.

03

Συγκεκριμένα παραδείγματα επεξεργασίας προσωπικών δεδομένων υγείας.

04

Δικαιώματα υποκειμένων δεδομένων.

05

Υπεύθυνος Προστασίας Δεδομένων

06

Παραβιάσεις Προσωπικών Δεδομένων - Πρόστιμα

Νομικό Πλαίσιο

Νομικό Πλαίσιο

Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα 1948

- ΑΡΘΡΟ 12 Κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του, ούτε προσβολές της τιμής και της υπόληψης του. Καθένας έχει το δικαίωμα να τον προστατεύουν οι νόμοι από επεμβάσεις και προσβολές αυτού του είδους.

Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ) 1950

- Το άρθρο 8 της Σύμβασης της 4ης Νοεμβρίου 1950 για την προστασία των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών θεσπίζει το δικαίωμα σεβασμού της ιδιωτικής και της οικογενειακής ζωής όλων, της προσωπικής κατοικίας και της αλληλογραφίας.

Συμβούλιο της Ευρώπης Σύμβαση 108 1981

- Η Σύμβαση 108 περί προστασίας του ατόμου έναντι της αυτοματοποιημένης επεξεργασίας των δεδομένων προσωπικού χαρακτήρα είναι η πρώτη νομικά δεσμευτική διεθνής πράξη που θεσπίστηκε στον τομέα της προστασίας των δεδομένων. Σκοπός της είναι η διασφάλιση για κάθε φυσικό πρόσωπο του σεβασμού των δικαιωμάτων του και των θεμελιωδών ελευθεριών του, και ιδίως του δικαιώματός του στην ιδιωτική ζωή, έναντι της αυτοματοποιημένης επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.

Νομικό Πλαίσιο

Οδηγία 95/46/ΕΚ

- Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (1995).

Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (2000)

- Άρθρο 7 Σεβασμός της ιδιωτικής και οικογενειακής ζωής. Κάθε πρόσωπο έχει δικαίωμα στο σεβασμό της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και των επικοινωνιών του.
- Άρθρο 8 Προστασία των δεδομένων προσωπικού χαρακτήρα. 1. Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν. 2. Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο. Κάθε πρόσωπο δικαιούται να έχει πρόσβαση στα συλλεγέντα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους. 3. Ο σεβασμός των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητης αρχής.

Συνθήκη της Λισαβόνας (2009)

- Κάθε πρόσωπο έχει δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα που το αφορούν.2. Το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία, θεσπίζουν τους κανόνες σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης, καθώς και από τα κράτη μέλη κατά την άσκηση δραστηριοτήτων που εμπίπτουν στο πεδίο εφαρμογής του δικαίου της Ένωσης, και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών. Η τήρηση των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητων αρχών.

Νομικό Πλαίσιο

- Κανονισμός (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 (ΓΚΠΔ)
- Ο Κανονισμός κατατέθηκε το 2012 και τέθηκε σε ισχύ την 25/5/18.
- Ο Κανονισμός έχει άμεση ισχύ σε όλα τα Κράτη της Ε.Ε.
- Περιέχει 173 σκέψεις και 99 άρθρα (έκταση 5 φορές μεγαλύτερη από την οδηγία 95/46/ΕΚ).

- Ελλάδα: Νόμος 4624/2019
- Περιλαμβάνει μέτρα εφαρμογής του ΓΚΠΔ.

Πεδίο Εφαρμογής

- **Ουσιαστικό πεδίο εφαρμογής (άρθρο 2 ΓΚΠΔ):** Ο Κανονισμός εφαρμόζεται στην, εν όλω ή εν μέρει, αυτοματοποιημένη ή μη επεξεργασία δεδομένων προσωπικού χαρακτήρα φυσικών προσώπων.

- **Εδαφικό πεδίο εφαρμογής (άρθρο 3 ΓΚΠΔ):**

❖ Εφαρμογή σε Υπευθύνους Επεξεργασίας και Εκτελούντες την Επεξεργασία που λαμβάνει χώρα εντός ΕΕ.

❖ Καταλαμβάνει και δραστηριότητες εγκαταστάσεως υπευθύνου ή εκτελούντος την επεξεργασία εκτός Ε.Ε. όταν η επεξεργασία αφορά σε υποκείμενα που βρίσκονται εντός Ε.Ε. κι οι δραστηριότητες σχετίζονται με

❖ α) την προσφορά αγαθών ή υπηρεσιών στα εν λόγω υποκείμενα των δεδομένων στην Ένωση, ανεξαρτήτως εάν απαιτείται πληρωμή από τα υποκείμενα των δεδομένων, ή β) την παρακολούθηση της συμπεριφοράς τους, στον βαθμό που η συμπεριφορά αυτή λαμβάνει χώρα εντός της Ένωσης.

Ορισμοί (αρ. 4 ΓΚΠΔ)

- **«Δεδομένα προσωπικού χαρακτήρα»:** κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο **(«υποκείμενο των δεδομένων»)** το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.

- **«Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα (ευαίσθητα δεδομένα)»**: κάθε πληροφορία που αφορά στη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν στην υγεία ή δεδομένων που αφορούν στη σεξουαλική ζωή φυσικού προσώπου ή στον γενετήσιο προσανατολισμό προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.

Ορισμοί (αρ. 4 ΓΚΠΔ)

- **«Δεδομένα που αφορούν στην 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.

- **«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 και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με την φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου».

- **«Βιομετρικά δεδομένα»**: τα 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».

- **«Επεξεργασία»:** κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.

Ορισμοί (αρ. 4 ΓΚΠΔ)

- **«Ανωνυμοποίηση»**: η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων.

- **«Ψευδωνυμοποίηση»:** η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο.

- **«Υπεύθυνος επεξεργασίας»:** το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους

- **«Από κοινού υπεύθυνοι επεξεργασίας»:** δύο ή περισσότεροι υπεύθυνοι επεξεργασίας, οι οποίοι καθορίζουν από κοινού τους σκοπούς και τα μέσα της επεξεργασίας.

- **«Εκτελών την επεξεργασία»:** το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας.

Δεδομένα υγείας και εμπιστευτικότητα

- **Γιατί τα δεδομένα που αφορούν στην υγεία εμπίπτουν στα ευαίσθητα προσωπικά δεδομένα (άρθρο 9 ΓΚΠΔ)?**

✓ Η τυχόν αποκάλυψη δεδομένων υγείας ενδέχεται να επιφέρει δυσμενείς συνέπειες για το άτομο κοινωνικά.

- **Ιατρικό απόρρητο (άρθρο 13 Κώδικα Ιατρικής Δεοντολογίας):**

➢ Ο ιατρός οφείλει να τηρεί αυστηρά απόλυτη εχεμύθεια για οποιοδήποτε στοιχείο υποπίπτει στην αντίληψή του ή του αποκαλύπτει ο ασθενής ή τρίτοι, στο πλαίσιο της άσκησης των καθηκόντων του, και το οποίο αφορά στον ασθενή ή τους οικείους του.

➢ Για την αυστηρή και αποτελεσματική τήρηση του ιατρικού απορρήτου, ο ιατρός οφείλει:

α) Να ασκεί την αναγκαία εποπτεία στους βοηθούς, στους συνεργάτες ή στα άλλα πρόσωπα που συμπράττουν ή συμμετέχουν ή τον στηρίζουν με οποιονδήποτε τρόπο κατά την άσκηση του λειτουργήματός του.

β) Να λαμβάνει κάθε μέτρο διαφύλαξης του απορρήτου και για το χρόνο μετά τη με οποιονδήποτε τρόπο παύση ή λήξη άσκησης του λειτουργήματός του.

➢ Η υποχρέωση τήρησης και διαφύλαξης του ιατρικού απορρήτου δεν παύει να ισχύει με το θάνατο του ασθενή.

- **Η έννοια του απορρήτου δεν ορίζεται**

➢ Ακόμα και η αποκάλυψη του ονόματος ενός ασθενή μπορεί να συνιστά απόρρητο καθώς το γεγονός της επίσκεψης σε κάποιον ιατρό συγκεκριμένης ειδικότητας είναι δυνατόν να συναχθεί η ασθένειά του.

Ύπαρξη νομικής και ηθικής δέσμευση τήρησης ιατρικού απορρήτου και διασφάλισης εμπιστευτικότητας.

Αρχές Επεξεργασίας Προσωπικών Δεδομένων (αρ. 5 ΓΚΠΔ)

(α) **Η αρχή της νομιμότητας, της αντικειμενικότητας και της διαφάνειας**: Τα προσωπικά δεδομένα πρέπει να υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων.

- Ο υπεύθυνος επεξεργασίας διασφαλίζει ότι έχει πάντοτε **νόμιμη βάση επεξεργασίας** και έχει **ενημερώσει τα υποκείμενα των δεδομένων** αναλυτικά για τους σκοπούς επεξεργασίας και για τα δικαιώματά τους.
- Η ενημέρωση πρέπει να βρίσκεται σε εμφανές και εύκολα προσβάσιμο σημείο (λ.χ. στην είσοδο του ιατρείου ή της κλινικής).
- Σε περίπτωση που απαιτείται συγκατάθεση για την επεξεργασία, η ενημέρωση θα πρέπει να συνοδεύει το κείμενο της συγκατάθεσης.

(β) **Η αρχή (περιορισμού) του σκοπού**: Τα προσωπικά δεδομένα συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς· η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς.

- **Ο Υπεύθυνος επεξεργασίας πρέπει να ενημερώνει το υποκείμενο των δεδομένων εάν χρησιμοποιήσει τα δεδομένα για οποιονδήποτε άλλο σκοπό και να διασφαλίζει την ύπαρξη νόμιμης βάσης επεξεργασίας** (π.χ. Ένας δερματολόγος δεν μπορεί να χρησιμοποιήσει τα email των ασθενών του για να διαφημίσει μια καινούρια θεραπεία. Εκτός εάν έχει ήδη ενημερώσει τους ασθενείς για τον σκοπό επεξεργασίας και έχει για παράδειγμα λάβει την προηγούμενη συγκατάθεσή τους).

Αρχές Επεξεργασίας Προσωπικών Δεδομένων (αρ. 5 ΓΚΠΔ)

(γ) **Η αρχή της ελαχιστοποίησης των δεδομένων (“data minimization”)**: Η αρχή αυτή προβλέπει ότι τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να είναι κατάλληλα, συναφή και να περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία.

- Ο Υπεύθυνος Επεξεργασίας πρέπει να συλλέγει **μόνο τα δεδομένα που είναι αναγκαία** για το συγκεκριμένο **σκοπό**. Σε μια φόρμα συλλογής δεδομένων το κάθε ζητούμενο στοιχείο πρέπει να μπορεί να αιτιολογηθεί.
- Μπορεί ο ιατρός να αποφασίσει ότι δεν θα συλλέγει το επάγγελμά του ασθενούς διότι δεν είναι αναγκαίο? Όχι! Σύμφωνα με το άρθρο 14 του Κώδικα Ιατρικής Δεοντολογίας τα ιατρικά αρχεία πρέπει να περιέχουν το ονοματεπώνυμο, το πατρώνυμο, το φύλο, την ηλικία, το επάγγελμα, τη διεύθυνση του ασθενή, τις ημερομηνίες της επίσκεψης, καθώς και κάθε άλλο ουσιώδες στοιχείο που συνδέεται με την παροχή φροντίδας στον ασθενή, όπως, ενδεικτικά και ανάλογα με την ειδικότητα, τα ενοχλήματα της υγείας του και το λόγο της επίσκεψης, την πρωτογενή και δευτερογενή διάγνωση ή την αγωγή που ακολουθήθηκε.
- Επιτρέπεται στον χώρο αναμονής ιατρείου / νοσηλευτικού ιδρύματος να είναι αναρτημένα σε οθόνη ορατά από όλους, τα ονοματεπώνυμα των εξεταζόμενων, την ώρα του ραντεβού τους και το ιατρείο, το οποίο επισκέπτονται; ΟΧΙ! Αυτό καθιστά σαφώς παραβίαση της αρχηγός της ελαχιστοποίησης των δεδομένων και της ακεραιότητας και εμπιστευτικότητας των δεδομένων).

Αρχές Επεξεργασίας Προσωπικών Δεδομένων (αρ. 5 ΓΚΠΔ)

(δ) **Η αρχή της ακρίβειας:** Τα δεδομένα προσωπικού χαρακτήρα θα πρέπει είναι ακριβή και, όταν είναι αναγκαίο να επικαιροποιούνται· πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας.

- Τα δεδομένα που συλλέγονται πρέπει να είναι ακριβή.
- Η υποχρέωση αυτή έχει βαρύνουσα σημασία όταν η ανακρίβειά των δεδομένων μπορεί να έχει επίδραση στο φυσικό πρόσωπο (π.χ εάν το email του ασθενούς δεν είναι ακριβές και σταλούν αποτελέσματα εξετάσεων σε άλλο φυσικό πρόσωπο αυτό συνιστά παραβίαση προσωπικών δεδομένων).
- Ο υπεύθυνος επεξεργασίας πρέπει σε τακτά χρονικά διαστήματα να φροντίζει για την επικαιροποίηση.

(ε) **Η αρχή του περιορισμού της περιόδου αποθήκευσης**: Η αρχή αυτή προβλέπει ότι τα δεδομένα προσωπικού χαρακτήρα, διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Τα δεδομένα αυτά, μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων.

- Μπορεί ο ιατρός η μια κλινική να αποφασίσει ότι δεν θα τηρεί αρχείο των ασθενών καθόλου? Όχι! Σύμφωνα με το άρθρο 14 του Κώδικα Ιατρικής Δεοντολογίας ο ιατρός υποχρεούται να τηρεί ιατρικό αρχείο, σε ηλεκτρονική ή μη μορφή. Η υποχρέωση διατήρησης των ιατρικών αρχείων ισχύει: α) Στα ιδιωτικά ιατρεία και τις λοιπές μονάδες πρωτοβάθμιας φροντίδας υγείας του ιδιωτικού τομέα, για 10 έτη από την τελευταία επίσκεψη του ασθενή. β) Σε κάθε άλλη περίπτωση, για 20 έτη από την τελευταία επίσκεψη του ασθενή.

Αρχές Επεξεργασίας Προσωπικών Δεδομένων (αρ. 5 ΓΚΠΔ)

(στ') **Αρχή της ακεραιότητας και της εμπιστευτικότητας**: τα δεδομένα προσωπικού χαρακτήρα, υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων.

- Η υποχρέωση αφορά τόσο στο ηλεκτρονικό όσο και στο φυσικό αρχείο και οι προεκτάσεις της παραβίασης της εμπιστευτικότητας είναι ιδιαιτέρως σημαντικές.
- Ο υπεύθυνος επεξεργασίας πρέπει να διασφαλίζει ότι έχει λάβει συγκεκριμένα μέτρα προστασίας
- Το φυσικό αρχείο πρέπει να τηρείται κλειδωμένο με διαβαθμισμένη πρόσβαση και να προστατεύεται από τυχόν απώλεια.
- Το ηλεκτρονικό αρχείο πρέπει να προστατεύεται με κατάλληλα μέτρα ασφαλείας από τυχόν διαρροή.

(ζ) **Αρχή της λογοδοσίας:** Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με όλες τις ανωτέρω αρχές.

Νομιμότητα Επεξεργασίας (αρ.6 ΓΚΠΔ)

Απλά Προσωπικά Δεδομένα – Νόμιμη Βάση Επεξεργασίας.

Η επεξεργασία είναι σύννομη μόνο εάν και εφόσον ισχύει τουλάχιστον μία από τις ακόλουθες προϋποθέσεις:

α) το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς,

β) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης,

γ) η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας,

δ) η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,

ε) η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας,

στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

Νομιμότητα Επεξεργασίας (αρ.9 ΓΚΠΔ)

Ευαίσθητα Προσωπικά Δεδομένα – Νόμιμη Βάση Επεξεργασίας.

Σύμφωνα με το άρθρο 9 του ΓΚΠΔ: Απαγορεύεται η επεξεργασία ευαίσθητων προσωπικών δεδομένων εκτός εάν συντρέχει μια από τις κατωτέρω περιπτώσεις:

α) το υποκείμενο των δεδομένων έχει παράσχει **ρητή συγκατάθεση** για την επεξεργασία αυτών των δεδομένων προσωπικού χαρακτήρα για έναν ή περισσότερους συγκεκριμένους σκοπούς, εκτός εάν το δίκαιο της Ένωσης ή κράτους μέλους προβλέπει ότι η απαγόρευση που αναφέρεται στην παράγραφο 1 δεν μπορεί να αρθεί από το υποκείμενο των δεδομένων.

Σημαντικές πληροφορίες για τη συγκατάθεσή:

- Δικαίωμα ανάκλησης της συγκατάθεσης ανά πάσα στιγμή.

- Η ανάκληση της συγκατάθεσης δεν θίγει τη νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση προ της ανάκλησής της.

- Πριν την παροχή της συγκατάθεσης, το υποκείμενο των δεδομένων ενημερώνεται σχετικά

- **Η ανάκληση της συγκατάθεσης είναι εξίσου εύκολη με την παροχή της.**

- Εκτίμηση κατά πόσο η συγκατάθεση δίνεται ελεύθερα: Αν για την εκτέλεση σύμβασης, συμπεριλαμβανομένης της παροχής μιας υπηρεσίας, τίθεται ως **προϋπόθεση** η συγκατάθεση στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που δεν είναι αναγκαία για την εκτέλεση της εν λόγω σύμβασης.

- Η συγκατάθεση, δεν παρέχει νομική βάση για επεξεργασία προσωπικών δεδομένων, εάν υπάρχει σημαντική ανισορροπία μεταξύ της θέσης του προσώπου στο οποίο αναφέρονται τα δεδομένα και του υπευθύνου επεξεργασίας (και σκέψη 43).

Νομιμότητα Επεξεργασίας (αρ.9 ΓΚΠΔ)

Ευαίσθητα Προσωπικά Δεδομένα – Νόμιμη Βάση Επεξεργασίας.

Σύμφωνα με το άρθρο 9 του ΓΚΠΔ: Απαγορεύεται η επεξεργασία ευαίσθητων προσωπικών δεδομένων εκτός εάν συντρέχει μια από τις κατωτέρω περιπτώσεις:

β) η επεξεργασία 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 επιτρέπεται από το δίκαιο της Ένωσης ή κράτους μέλους ή από συλλογική συμφωνία σύμφωνα με το εθνικό δίκαιο παρέχοντας κατάλληλες εγγυήσεις για τα θεμελιώδη δικαιώματα και τα συμφέροντα του υποκειμένου των δεδομένων.

- Εφαρμόζεται κυρίως για τα ευαίσθητα δεδομένα που συλλέγει ο εργοδότης (π.χ άδεια ασθενείας).

γ) η επεξεργασία είναι απαραίτητη για την **προστασία των ζωτικών συμφερόντων** του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, εάν το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να συγκατατεθεί.

- Εφαρμόζεται σε περιπτώσεις που η ζωή του ανθρώπου βρίσκεται σε κίνδυνο άρα είναι ανίκανο να παρέχει τη συγκατάθεσή του.

δ) η επεξεργασία διενεργείται, με κατάλληλες εγγυήσεις, στο πλαίσιο των νόμιμων δραστηριοτήτων ιδρύματος, οργάνωσης ή άλλου μη κερδοσκοπικού φορέα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό στόχο και υπό την προϋπόθεση ότι η επεξεργασία αφορά αποκλειστικά τα μέλη ή τα πρώην μέλη του φορέα ή πρόσωπα τα οποία έχουν τακτική επικοινωνία μαζί του σε σχέση με τους σκοπούς του και ότι τα δεδομένα προσωπικού χαρακτήρα δεν κοινοποιούνται εκτός του συγκεκριμένου φορέα χωρίς τη συγκατάθεση των υποκειμένων των δεδομένων.

ε) η επεξεργασία αφορά δεδομένα προσωπικού χαρακτήρα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων.

Νομιμότητα Επεξεργασίας (αρ.9 ΓΚΠΔ)

Ευαίσθητα Προσωπικά Δεδομένα – Νόμιμη Βάση Επεξεργασίας.

Σύμφωνα με το άρθρο 9 του ΓΚΠΔ: Απαγορεύεται η επεξεργασία ευαίσθητων προσωπικών δεδομένων εκτός εάν συντρέχει μια από τις κατωτέρω περιπτώσεις (συνέχεια):

στ) η επεξεργασία είναι **απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων** ή όταν τα δικαστήρια ενεργούν υπό τη δικαιοδοτική τους ιδιότητα.

ζ) η επεξεργασία είναι απαραίτητη για λόγους ουσιαστικού δημόσιου συμφέροντος, βάσει του δικαίου της Ένωσης ή κράτους μέλους, το οποίο είναι ανάλογο προς τον επιδιωκόμενο στόχο, σέβεται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπει κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων

η) η επεξεργασία είναι απαραίτητη για **σκοπούς προληπτικής ή επαγγελματικής ιατρικής**, εκτίμησης της ικανότητας προς εργασία του εργαζομένου, **ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας** ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους ή δυνάμει σύμβασης με επαγγελματία του τομέα της υγείας.

- Αυτή είναι η κύρια βάση επεξεργασίας για την παροχή υπηρεσιών υγείας.

θ) η επεξεργασία είναι απαραίτητη για λόγους δημόσιου συμφέροντος στον τομέα της **δημόσιας υγείας**, όπως η προστασία έναντι σοβαρών διασυνοριακών απειλών κατά της υγείας ή η διασφάλιση υψηλών προτύπων ποιότητας και ασφάλειας της υγειονομικής περίθαλψης και των φαρμάκων ή των ιατροτεχνολογικών προϊόντων, βάσει του δικαίου της Ένωσης ή του δικαίου κράτους μέλους, το οποίο προβλέπει κατάλληλα και συγκεκριμένα μέτρα για την προστασία των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων, ειδικότερα δε του επαγγελματικού απορρήτου

Νομιμότητα Επεξεργασίας (αρ.9 ΓΚΠΔ)

Ευαίσθητα Προσωπικά Δεδομένα – Νόμιμη Βάση Επεξεργασίας.

Σύμφωνα με το άρθρο 9 του ΓΚΠΔ: Απαγορεύεται η επεξεργασία ευαίσθητων προσωπικών δεδομένων εκτός εάν συντρέχει μια από τις κατωτέρω περιπτώσεις (συνέχεια):

ι) η επεξεργασία είναι απαραίτητη για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς **επιστημονικής ή ιστορικής έρευνας** ή για στατιστικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1 βάσει του δικαίου της Ένωσης ή κράτους μέλους, οι οποίοι είναι ανάλογοι προς τον επιδιωκόμενο στόχο, σέβονται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπουν κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων.

- (σκέψη 159 ΓΚΠΔ): Όταν δεδομένα προσωπικού χαρακτήρα υφίστανται επεξεργασία για σκοπούς επιστημονικής έρευνας, ο κανονισμός θα πρέπει να ισχύει και για την επεξεργασία αυτή. Για τους σκοπούς του κανονισμού, η επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς επιστημονικής έρευνας θα πρέπει να ερμηνεύεται διασταλτικά, δηλαδή να περιλαμβάνει παραδείγματος χάριν τεχνολογική ανάπτυξη και επίδειξη, βασική έρευνα, εφαρμοσμένη έρευνα και ιδιωτικά χρηματοδοτούμενη έρευνα. Επιπλέον, θα πρέπει να λαμβάνει υπόψη τον στόχο της Ένωσης δυνάμει του άρθρου 179 παράγραφος 1 ΣΛΕΕ για την επίτευξη ενός ευρωπαϊκού χώρου έρευνας.

- Στους σκοπούς επιστημονικής έρευνας θα πρέπει να περιλαμβάνονται και μελέτες που πραγματοποιούνται για το δημόσιο συμφέρον στον τομέα της δημόσιας υγείας. Για να ληφθούν υπόψη οι ιδιαιτερότητες της επεξεργασίας δεδομένων προσωπικού χαρακτήρα για σκοπούς επιστημονικής έρευνας, θα πρέπει να ισχύουν ειδικοί όροι ιδίως όσον αφορά τη δημοσίευση ή με άλλο τρόπο δημοσιοποίηση δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των σκοπών επιστημονικής έρευνας. Εάν το αποτέλεσμα της επιστημονικής έρευνας ειδικότερα στον τομέα της υγείας αιτιολογεί τη λήψη περαιτέρω μέτρων προς το συμφέρον του υποκειμένου των δεδομένων, ισχύουν οι γενικοί κανόνες του παρόντος κανονισμού όσον αφορά τα μέτρα .

Παραδείγματα Νόμιμης Βάσης Επεξεργασίας για Δεδομένα Υγείας

European Health Data Space

Προκειμένου να αξιοποιηθεί πλήρως το δυναμικό των δεδομένων για την υγεία, η Ευρωπαϊκή Επιτροπή παρουσίασε πρόσφατα κανονισμό για τη δημιουργία του ευρωπαϊκού χώρου δεδομένων για την υγεία (European Health Data Space).

Σύμφωνα με την Ευρωπαϊκή Επιτροπή αυτή η πρόταση:

- στηρίζει τα άτομα ώστε να αναλάβουν τον έλεγχο των δικών τους δεδομένων υγείας
- στηρίζει τη χρήση δεδομένων υγείας για τη βελτίωση της παροχής υγειονομικής περίθαλψης, της έρευνας, της καινοτομίας και της χάραξης πολιτικής και
- επιτρέπει στην ΕΕ να αξιοποιήσει πλήρως τις δυνατότητες που προσφέρει η ασφαλής και προστατευμένη ανταλλαγή, χρήση και επαναχρησιμοποίηση δεδομένων υγείας.

Καθώς η πρόταση Κανονισμού αφορά μεταξύ άλλων και στην επεξεργασία ευαίσθητων προσωπικών δεδομένων, Ο Ευρωπαίος Επόπτης Προστασίας Προσωπικών Δεδομένων (EDPS) και το Ευρωπαϊκό Συμβούλιο Προστασίας Προσωπικών Δεδομένων (EDPB) εξέδωσαν Κοινή Γνώμη για τον εν λόγω Κανονισμό.

Στην ουσία εξέτασαν κατά πόσο η δημιουργία μιας τέτοιας πλατφόρμας είναι σύννομη και παρουσίασαν συγκεκριμένες προτάσεις για τη βελτίωση της έτσι ώστε να διασφαλίζεται η προστασίας προσωπικών δεδομένων των ευρωπαίων πολιτών.

Για παράδειγμα, ο Κανονισμός περιλαμβάνει τις ελάχιστες κατηγορίες ηλεκτρονικών δεδομένων για δευτερογενή χρήση που θα καθίστανται διαθέσιμες. Στις κατηγορίες αυτές περιλαμβάνονται “ηλεκτρονικά δεδομένα υγείας που παράγονται από το άτομο, συμπεριλαμβανομένων των ιατροτεχνολογικών προϊόντων, των εφαρμογών ευεξίας ή άλλων εφαρμογών ψηφιακής υγείας”.

Παραδείγματα Νόμιμης Βάσης Επεξεργασίας για Δεδομένα Υγείας

European Health Data Space

Η Κοινή Γνώμη του EDPB και του EDPS προτείνει την αφαίρεση αυτής της κατηγορίας δεδομένων απο τον Κανονισμό και τόνισε ότι σε περίπτωση που τα δεδομένα αυτά παραμείνουν στον Κανονισμό η δευτερογενής χρήση των δεδομένων απαιτεί τη λήψη της προηγούμενής συγκατάθεσής αυτών σύμφωνα με το GDPR.

Ο λόγος είναι ότι το EDPS και το EDPB έκριναν ότι εκτός από την παρακολούθηση των πράξεων και των αποφάσεων των ανθρώπων, είναι πλέον δυνατή η παρακολούθηση του σώματος, του μυαλού και των συναισθημάτων των ανθρώπων σε ένα επίπεδο που ακόμη και οι ίδιοι οι άνθρωποι μπορεί να μην μπορούν να κάνουν. Αυτά τα δεδομένα μπορούν στη συνέχεια να χρησιμοποιηθούν για να προβλέψουν τις ενέργειες των ανθρώπων και να χειραγωγήσουν τη συμπεριφορά τους, ακόμη και σε ομαδικό επίπεδο.

Επίσης, το EDPB και ο EDPS τόνισαν αυτά τα δεδομένα υγείας που δημιουργούνται από εφαρμογές ευεξίας και άλλες ψηφιακές εφαρμογές υγείας δεν έχουν τις ίδιες απαιτήσεις ποιότητας δεδομένων και χαρακτηριστικά αυτών που παράγονται από ιατροτεχνολογικά προϊόντα (τα τελευταία υπόκεινται σε υφιστάμενα ειδικά πρότυπα και νομοθεσία).

Παραδείγματα Νόμιμης Βάσης Επεξεργασίας για Δεδομένα Υγείας

<u>Χρήση ρητής συγκατάθεσης</u>

Μπορεί να λαμβάνεται πάντοτε η ρητή συγκατάθεση του ασθενή σαν νόμιμη βάση επεξεργασίας για τη συλλογή των ευαίσθητων δεδομένων του?

Η χρήση της ρητής συγκατάθεσης υπόκειται σε περιορισμούς.

- Έχει κριθεί από τον Ευρωπαίο Επόπτη Προστασίας Προσωπικών Δεδομένων (EDPB) ότι σε ερευνητικές δραστηριότητες (λ.χ. κλινικές μελέτες) η συγκατάθεση δεν αποτελεί πάντοτε την κατάλληλη νομική βάση για την επεξεργασία των ευαίσθητων δεδομένων των ασθενών ιδίως όπου υπάρχει **σαφής ανισορροπία δυνάμεων** μεταξύ του υποκειμένου των δεδομένων (ασθενούς) και του υπεύθυνου επεξεργασίας (π.χ. του Χορηγού σε μια κλινική μελέτη).
- Αναγνωρίζεται ότι σε κλινικές δοκιμές μια τέτοια ανισορροπία μπορεί να υπάρχει ανάλογα με τις περιστάσεις, **για παράδειγμα, όταν το υποκείμενο των δεδομένων δεν είναι σε καλή κατάσταση υγείας και δεν υπάρχει διαθέσιμη θεραπευτική αγωγή εκτός της κλινικής δοκιμής.**
- Ως εκ τούτου, προκειμένου ο υπεύθυνος επεξεργασίας να βασίζεται στη συγκατάθεση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα σε κλινικές δοκιμές, πρέπει πρώτα να πραγματοποιηθεί «ιδιαίτερα ενδελεχής αξιολόγηση» των περιστάσεων της κλινικής δοκιμής για να καθοριστεί εάν η συγκατάθεση είναι κατάλληλη».
- Η απαίτηση λήψης ενημερωμένης συγκατάθεσης για τη συμμετοχή ασθενούς σε κλινικές μελέτες πρέπει να διακρίνεται από τη ρητή συγκατάθεση ως νόμιμη βάση επεξεργασίας δεδομένων προσωπικού χαρακτήρα για σκοπούς επιστημονικής έρευνας

Παραδείγματα Νόμιμης Βάσης Επεξεργασίας για Δεδομένα Υγείας

Αποστολή ενημερώσεων χωρίς νόμιμη βάση

Ένας ασθενής επισκέπτεται ιδιωτική κλινική για σκοπούς διενέργειας προληπτικών εξετάσεων. Σε αυτή την περίπτωση η νόμιμη βάση επεξεργασίας είναι η ότι η "επεξεργασία είναι απαραίτητη για σκοπούς προληπτικής ή επαγγελματικής ιατρικής, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών". Μπορεί η Κλινική να αποστείλει στην συνέχεια ενημερωτικές προσφορές στον ασθενή για δράσεις και νέα της Κλινικής? Όχι! Τα προσωπικά δεδομένα συνελέχθησαν με σκοπό την διενέργειας προληπτικών εξετάσεων, η χρήση των δεδομένων αυτών για άλλο σκοπό απαιτεί την εξασφάλιση νόμιμης βάσης επεξεργασίας και την κατάλληλη ενημέρωση του ασθενή.

Αποστολή εξετάσεων σε τρίτο

- Εισαγγελική Παραγγελία: Μπορεί ένας γιατρός να αποστείλει αποτελέσματα ιατρικών εξετάσεων σε τρίτο πρόσωπο π.χ. σύζυγο του ασθενούς κατόπιν εισαγγελικής παραγγελίας? Ως προς την εισαγγελική παραγγελία, η Αρχή Προστασίας Προσωπικών Δεδομένων έχει κατ' επανάληψη κρίνει ότι αυτή δεν δεσμεύει το φορέα παροχής υπηρεσιών υγείας, ως υπεύθυνο επεξεργασίας, ως προς τη διαβίβαση. Ο φορέας παροχής υπηρεσιών υγείας, ως υπεύθυνος επεξεργασίας, οφείλει σε κάθε περίπτωση να εξετάζει τη συνδρομή όλων των αναγκαίων προϋποθέσεων για τη νομιμότητα της διαβίβασης στον αιτούντα τρίτο. Εάν κρίνει ότι τα ζητηθέντα δεδομένα προσωπικού χαρακτήρα για οποιονδήποτε νόμιμο λόγο δεν επιτρέπεται να διαβιβαστούν στον αιτούντα τρίτο, οφείλει να απορρίπτει αιτιολογημένα τη σχετική αίτηση, κονιοποιώντας την απορριπτική αυτή απάντηση και στην εισαγγελία που είχε εκδώσει τη σχετική παραγγελία.

- Διαβίβασή σε συγγενή λόγω αδυναμίας του ασθενούς: Αν ο ασθενής δεν είναι σε θέση να παραλάβει τις εξετάσεις και δεν είναι σε θέση να εξουσιοδοτήσει αρμόδιο πρόσωπο να παραλάβει τότε η παραλαβή στηρίζεται στο άρθρο 9 παρ. 2 του ΓΚΠΔ: (1) εφόσον πρόκειται για επεξεργασία που είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, εάν το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να συγκατατεθεί (άρθρο 9 παρ. 2 στοιχ. (γ΄) του ΓΚΠΔ)

Δικαιώματα

- Δικαίωμα ενημέρωσης & Πρόσβασης
- Δικαίωμα διόρθωσης
- Δικαίωμα διαγραφής (δικαίωμα στη λήθη)
- Δικαίωμα περιορισμού της επεξεργασίας
- Δικαίωμα στην φορητότητα των δεδομένων
- Δικαίωμα εναντίωσης στην επεξεργασία (λ.χ. σε περιπτώσεις direct marketing)
- Δικαίωμα σχετικά με την λήψη αυτοματοποιημένων αποφάσεων (automated decision making)

Υπεύθυνος Προστασίας Δεδομένων (DPO)

Υποχρέωση Ορισμού DPO

- η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα (εκτός από δικαστήρια που ενεργούν στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας)
- πράξεις επεξεργασίας οι οποίες, λόγω της φύσης, του πεδίου εφαρμογής και/ή των σκοπών τους, απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα, ή
- οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα.

Ο ρόλος του DPO

- Συμμετέχει σε όλα τα ζητήματα τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα.
- Τα υποκείμενα των δεδομένων μπορούν να επικοινωνούν με τον υπεύθυνο προστασίας δεδομένων για κάθε ζήτημα σχετικό με την επεξεργασία των δεδομένων τους προσωπικού χαρακτήρα και με την άσκηση των δικαιωμάτων τους.
- Ενημερώνει και συμβουλεύει για τις υποχρεώσεις σχετικά με την προστασίας προσωπικών δεδομένων.
- Παρακολουθεί τη συμμόρφωση με τον κανονισμό, συμπεριλαμβανομένων της ανάθεσης αρμοδιοτήτων, της ευαισθητοποίησης και της κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας, και των σχετικών ελέγχων.
- Παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και παρακολουθεί την υλοποίησή της σύμφωνα με το άρθρο 35.
- Συνεργάζεται με την εποπτική αρχή.
- Ενεργεί ως σημείο επικοινωνίας για την εποπτική αρχή για ζητήματα που σχετίζονται με την επεξεργασία, περιλαμβανομένης της προηγούμενης διαβούλευσης που αναφέρεται στο άρθρο 36, και πραγματοποιεί διαβουλεύσεις, ανάλογα με την περίπτωση, για οποιοδήποτε άλλο θέμα.

Γνωστοποίηση παραβίασης δεδομένων

Παραδείγματα Παραβίασης

- Απώλεια αρχείου ασθενών επειδή κλάπηκε ο ηλεκτρονικός υπολογιστής.
- Απώλεια usb-stick με γνωματεύσεις.
- Αποστολή αποτελεσμάτων σε άλλο ασθενή.
- Αποκάλυψη δεδομένων ασθενών σε μη εξουσιοδοτημένα τρίτα πρόσωπα.
- Καταστροφή φυσικού αρχείου ασθενών.

Α) Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας γνωστοποιεί αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή.

Στη γνωστοποίηση αυτή αναφέρεται, κατ’ ελάχιστο:

α) η περιγραφή της φύσης της παραβίασης προσωπικών δεδομένων,

β) το όνομα και τα στοιχεία επικοινωνίας του υπεύθυνου προστασίας δεδομένων ή άλλου σημείου επικοινωνίας για πληροφορίες,

γ) η περιγραφή των ενδεχόμενων συνεπειών από την παραβίαση δεδομένων,

δ) η περιγραφή των μέτρων που ελήφθησαν ή πρόκειται να ληφθούν για την αντιμετώπιση της παραβίαση

Β) Στο υποκείμενο των δεδομένων

Όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας ανακοινώνει αμελλητί την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων.

Πρόστιμα

Α) 1η κατηγορία παραβάσεων

Έως 10.000.000 ή για επιχειρήσεις το 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο

Β) 2η κατηγορία παραβάσεων

Έως 20.000.000 ή για επιχειρήσεις το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο

Η υψηλότερη κλίμακα περιλαμβάνει πρόστιμα για παραβίαση βασικών αρχών επεξεργασίας (αρχές επεξεργασίας και νόμιμη βάση) άρθρα 5, 6, 7 και 9, τα δικαιώματα των υποκειμένων των δεδομένων και τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε αποδέκτη σε τρίτη χώρα ή σε διεθνή οργανισμό.

Ευχαριστώ Πολύ

Αναστασία Παύλου

Attorney at Law (Athens Bar Association)

LL.M., CIPP-E