Ο ΝΕΟΣ ΚΑΝΟΝΙΣΜΟΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ

ΙΩΑΝΝΗΣ Δ. ΙΓΓΛΕΖΑΚΗΣ

ΑΝ. ΚΑΘΗΓΗΤΗΣ ΝΟΜΙΚΗΣ ΣΧΟΛΗΣ ΑΠΘ

Ψήφιση Κανονισμού

Ο Κανονισμός (ΕΕ) 2016/679 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 (Γενικός Κανονισμός για την Προστασία Δεδομένων)» αντικαθιστά την οδηγία, η οποία δεν ήταν προσαρμοσμένη στην τεχνολογική πραγματικότητα του Διαδικτύου.

Ο Κανονισμός κατατέθηκε το 2012 και μετά από τέσσερα έτη διαπραγματεύσεων ψηφίσθηκε και πρόκειται να τεθεί σε ισχύ τον Μάϊο του 2018 (25/5/18).

Νομική φύση του Κανονισμού

Ο Κανονισμός ισχύει απευθείας, ωστόσο, τα εθνικά κράτη πρέπει να ψηφίσουν διατάξεις κατ’ εξουσιόδοτηση, σε τομείς όπου προβλέπονται μερικές παρεκκλίσεις ή εξειδικεύσεις.

Άμεση συνέπεια είναι ότι καταργείται ο Ν. 2472/97.

Η ψήφιση εφαρμοστικού νόμου στην Ελλάδα αναμένεται πριν την έναρξη ισχύος του Κανονισμού.

Κανονισμός & Οδηγία 95/46

Ο Κανονισμός στηρίζεται στο οικοδόμημα της Οδηγίας, αλλά εισάγει νέες καινοτομίες, νέα δικαιώματα, όπως το δικαίωμα στη λήθη και στη φορητότητα δεδομένων.

Καταργείται ο προληπτικός έλεγχος με τις γνωστοποιήσεις και άδειες από τις εποπτικές αρχές. Αντικαθίσταται από την υποχρέωση εκπόνησης μελέτης αντικτύπου.

Εισάγεται η υποχρέωση διορισμού υπευθύνου για την προστασία δεδομένων.

Ανάγκη προσαρμογής στον νέο Κανονισμό για τις δημόσιες αρχές, στις βασικές δραστηριότητες των οποίων ανήκει η επεξεργασία ευαίσθητων δεδομένων (π.χ. δεδομένων υγείας) και επεξεργασία σε μεγάλη κλίμακα.

Νεωτερισμοί του Κανονισμού

- Ενισχύεται η νομική θέση των πολιτών, με τη θέσπιση δικαιωμάτων
- Επιβάλλονται νέες υποχρεώσεις στους υπεύθυνους επεξεργασίας
- Νέα μοντέλα (privacy by design)
- Γνωστοποίηση παραβιάσεων δεδομένων
- Στο άρθρο 83 προβλέπονται βαρύτατες κυρώσεις για τους παραβάτες και δρακόντεια πρόστιμα (λ.χ. έως €20.000.000 ή έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους μιας επιχείρησης, ανάλογα με το ποιο είναι υψηλότερο).

Βασικά δικαιώματα

- **1. Δικαίωμα ενημέρωσης:**
- Ο υπεύθυνος επεξεργασίας λαμβάνει τα κατάλληλα μέτρα για να παρέχει στο υποκείμενο των δεδομένων κάθε πληροφορία και κάθε ανακοίνωση σχετικά με την επεξεργασία σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση, ιδίως όταν πρόκειται για πληροφορία απευθυνόμενη ειδικά σε παιδιά.
- Ο υπεύθυνος επεξεργασίας διευκολύνει την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων (αρθρ. 15-22)
- Ο υπεύθυνος επεξεργασίας παρέχει στο υποκείμενο των δεδομένων πληροφορίες για την ενέργεια που πραγματοποιείται κατόπιν αιτήματος δυνάμει των άρθρων 15 έως 22 χωρίς καθυστέρηση και σε κάθε περίπτωση εντός μηνός από την παραλαβή του αιτήματος.

Βασικά δικαιώματα

2. Δικαίωμα πρόσβασης στα δεδομένα

Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει από τον υπεύθυνο επεξεργασίας επιβεβαίωση για το κατά πόσον ή όχι τα δεδομένα προσωπικού χαρακτήρα που το αφορούν υφίστανται επεξεργασία και έχει πρόσβαση σε πλήθος πληροφοριών που προβλέπονται στο άρθρο 15

Βασικά δικαιώματα

3. Δικαίωμα διόρθωσης

Το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει από τον υπεύθυνο επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν. Έχοντας υπόψη τους σκοπούς της επεξεργασίας, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει τη συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων μέσω συμπληρωματικής δήλωσης.

Βασικά δικαιώματα

4. Δικαίωμα στη λήθη

Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν, εφόσον τα δεδομένα δεν είναι πλέον απαραίτητα ή το υποκείμενο ανακαλεί τη συγκατάθεση ή αντιτίθεται στην επεξεργασία και δεν υπάρχουν επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία, ή τα δεδομένα υποβλήθηκαν σε επεξεργασία παράνομα ή για να τηρηθεί νομική υποχρέωση ή έχουν συλλεχθεί όταν το υποκείμενο ήταν παιδί.

Υποχρέωση ενημέρωσης όσων έχουν δημιουργήσει συνδέσμους ή αντίγραφα των δεδομένων ότι πρέπει να διαγράψουν τα δεδομένα

Βασικά Δικαιώματα

5. Δικαίωμα περιορισμού της επεξεργασίας

Το υποκείμενο των δεδομένων μπορεί να ζητήσει από τον υπεύθυνο της επεξεργασίας τον περιορισμό της επεξεργασίας όταν η ακρίβεια των δεδομένων αμφισβητείται ή είναι παράνομη ή ο υπεύθυνος επεξεργασίας δεν χρειάζεται πλέον τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από το υποκείμενο των δεδομένων για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων, ή το υποκείμενο των δεδομένων έχει αντιρρήσεις για την επεξεργασία, εν αναμονή της επαλήθευσης του κατά πόσον οι νόμιμοι λόγοι του υπευθύνου επεξεργασίας υπερισχύουν έναντι των λόγων του υποκειμένου των δεδομένων.

Βασικά δικαιώματα

6. Δικαίωμα στη φορητότητα δεδομένων

Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και το δικαίωμα να διαβιβάζει τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας

Βασικά δικαιώματα

7. Δικαίωμα εναντίωσης

Το υποκείμενο των δεδομένων δικαιούται να αντιτάσσεται, ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν (επεξεργασία από δημόσιες αρχές ή από ιδιώτες), περιλαμβανομένης της κατάρτισης προφίλ βάσει των εν λόγω διατάξεων.

Εάν τα δεδομένα υποβάλλονται σε επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης, το υποκείμενο των δεδομένων δικαιούται να αντιταχθεί ανά πάσα στιγμή στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν για την εν λόγω εμπορική προώθηση, περιλαμβανομένης της κατάρτισης προφίλ, εάν σχετίζεται με αυτήν την απευθείας εμπορική προώθηση.

Βασικές υποχρεώσεις του υπεύθυνου επεξεργασίας

Κανονισμός επιβάλλει μια σειρά νέων υποχρεώσεων στους υπευθύνους επεξεργασίας, οι οποίες απορρέουν από τις βασικές αρχές και ιδίως την ενισχυμένη **αρχή της διαφάνειας** στον τρόπο συλλογής, επεξεργασίας και τήρησης δεδομένων και τη νέα **αρχή της λογοδοσίας**, σύμφωνα με την οποία ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωσή του με όλες τις αρχές που διέπουν την επεξεργασία προσωπικών δεδομένων:

Ευθύνη

Λαμβάνοντας υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό.

Κάθε υπεύθυνος επεξεργασίας και, κατά περίπτωση, ο εκπρόσωπός του, τηρεί αρχείο των δραστηριοτήτων επεξεργασίας για τις οποίες είναι υπεύθυνος.

Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού

Ο υπεύθυνος επεξεργασίας εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων, και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία κατά τρόπο ώστε να πληρούνται οι απαιτήσεις του παρόντος κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων.

Ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας.

Ασφάλεια επεξεργασίας

Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση: α) της ψευδωνυμοποίησης και της κρυπτογράφησης δεδομένων προσωπικού χαρακτήρα, β) της δυνατότητας διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση, γ) της δυνατότητας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος, δ) διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.

Γνωστοποίηση παραβίασης δεδομένων

Α) Στην εποπτική αρχή.

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

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.

Υπεύθυνος προστασίας δεδομένων

Προβλέπεται, υπό προϋποθέσεις, ο ορισμός «υπευθύνου προστασίας δεδομένων» (ΥΠΔ), ο οποίος έχει εχέγγυα ανεξαρτησίας και παρακολουθεί τη συμμόρφωση με τον νόμο αποτελώντας, συγχρόνως, το σημείο επαφής με την εποπτική αρχή

Υποχρεωτικός είναι ο διορισμός υπεύθυνου επεξεργασίας όταν η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα.

Ο ΥΠΔ ενημερώνει τον υπεύθυνο επεξεργασίας για τις υποχρεώσεις του, παρακολουθεί τη συμμόρφωση με τον κανονισμό, παρέχει συμβουλές όσον αφορά την εκτίμηση αντικτύπου, συνεργάζεται με την εποπτική αρχή και ενεργεί ως σημείο επικοινωνίας για αυτήν, για ζητήματα που αφορούν την επεξεργασία.

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων και προηγούμενη διαβούλευση

Όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα.

Ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη της εποπτικής αρχής πριν από την επεξεργασία, όταν η δυνάμει του άρθρου 35 εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων υποδεικνύει ότι η επεξεργασία θα προκαλούσε υψηλό κίνδυνο ελλείψει μέτρων μετριασμού του κινδύνου από τον υπεύθυνο επεξεργασίας. Όταν η εποπτική αρχή φρονεί ότι η σχεδιαζόμενη επεξεργασία παραβαίνει τον παρόντα κανονισμό, ιδίως εάν ο υπεύθυνος επεξεργασίας δεν έχει προσδιορίσει ή μετριάσει επαρκώς τον κίνδυνο, παρέχει γραπτώς συμβουλές στον υπεύθυνο επεξεργασίας.

Οργανισμοί Δημόσιου Τομέα

Νομιμοποιητική βάση για την επεξεργασία:

Δεν αλλάζει

Υποχρέωση ορισμού ΥΠΔ:

Αποφυγή σύγκρουσης συμφερόντων

Ευθύνη και διαφάνεια:

Η ευθύνη του υπεύθυνου επεξεργασίας είναι αυξημένη. Πρέπει να διασφαλίζεται η διαφάνεια της επεξεργασίας

Οργανισμοί Δημόσιου Τομέα - Βήματα προετοιμασίας *(Οδηγίες της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)*

1. ΕΝΗΜΕΡΩΣΗ - ΕΤΟΙΜΟΤΗΤΑ:

Ενημερώστε το ανθρώπινο δυναμικό του οργανισμού σας για τις επερχόμενες μεταβολές, υπογραμμίζοντας τις σημαντικές επιπτώσεις σε περίπτωση παραβιάσεων. Αξιολογήστε τους πιθανούς κινδύνους για τα προσωπικά δεδομένα που συλλέγετε και επεξεργάζεστε. Διαμορφώστε στρατηγική αντιμετώπισης των πιθανών κινδύνων με τεχνικά και οργανωτικά μέτρα.

Οργανισμοί Δημόσιου Τομέα - Βήματα προετοιμασίας *(Οδηγίες της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)*

2. ΚΑΤΑΓΡΑΦΗ:

Οφείλετε να τηρείτε ειδικά αρχεία επεξεργασιών; Αν ναι, καταγράψτε ενδελεχώς τα δεδομένα που τηρείτε και μεταβιβάζετε, τις επεξεργασίες στις οποίες προβαίνετε, τον σκοπό τους και τη νομική βάση.

Οργανισμοί Δημόσιου Τομέα - Βήματα προετοιμασίας (Οδηγίες της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)

3. ΕΛΕΓΧΟΣ ΤΗΡΗΣΗΣ ΤΗΣ ΣΥΜΜΟΡΦΩΣΗΣ:

Εξετάζετε συνεχώς αν κατά την επεξεργασία των δεδομένων τηρούνται οι αρχές που διέπουν τη νόμιμη επεξεργασία των δεδομένων και αν γίνονται σεβαστά τα δικαιώματα των υποκειμένων.

Οργανισμοί Δημόσιου Τομέα - Βήματα προετοιμασίας (Οδηγίες της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)

4. ΑΝΑΘΕΩΡΗΣΗ ΠΟΛΙΤΙΚΩΝ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΔΙΑΔΙΚΑΣΙΩΝ:

Επικαιροποιήστε τις διαδικασίες για τον χειρισμό των αιτημάτων και την ικανοποίηση των δικαιωμάτων των πολιτών, ιδίως ως προς τη διαγραφή δεδομένων (δικαίωμα στη λήθη) ή την παροχή τους σε αναγνώσιμο ηλεκτρονικό μορφότυπο (φορητότητα δεδομένων).

*Οργανισμοί Δημόσιου Τομέα - **Βήματα προετοιμασίας** (Οδηγίες της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)*

5. ΕΚΤΙΜΗΣΗ ΕΠΙΠΤΩΣΕΩΝ:

Θα πρέπει να είστε σε θέση να εκτιμήσετε τις πιθανότητες επέλευσης κινδύνων και τις συνέπειες στα προσωπικά δεδομένα.

Οργανισμοί Δημόσιου Τομέα - Βήματα προετοιμασίας (Οδηγίες της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)

6. ΠΑΡΑΒΙΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ:

Υιοθετήστε μεθόδους για την ανίχνευση, την καταγραφή και τη διερεύνηση περιστατικών παραβιάσεων. Διαθέτετε διαδικασία για τις γνωστοποιήσεις παραβιάσεων προς την Αρχή και τα υποκείμενα;

*Οργανισμοί Δημόσιου Τομέα - **Βήματα προετοιμασίας** (Οδηγίες της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)*

7. ΔΙΑΒΙΒΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ ΕΚΤΟΣ ΕΕ:

Αν διαβιβάζετε δεδομένα και σε τρίτες χώρες, επιλέξτε κάποιο μηχανισμό διαβίβασης, όπως δεσμευτικούς εταιρικούς κανόνες (BCRs), τυποποιημένες συμβατικές ρήτρες (SCCs), πιστοποιήσεις στο Privacy Shield (για τις ΗΠΑ).