ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ
ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΕΕ 2016/679

Ευαγγελία Παλαιολόγου

Δικηγόρος

Την 27η Απριλίου 2016 εξεδόθη ο Νέος Γενικός Κανονισμός Προστασίας Δεδομένων της ΕΕ 2016/679 (General Data Protection Regulation – GDPR), από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της Ευρωπαϊκής Ένωσης, ο οποίος θα τεθεί σε ισχύ την 25η Μαΐου του 2018, καθιερώνοντας ενιαίο νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων σε όλα τα κράτη μέλη της ΕΕ, ως νομοθέτημα άμεσης εφαρμογής σε αυτά.

Το διάστημα που μεσολαβεί από την έκδοσή του μέχρι την θέση του σε ισχύ, αποτελεί περίοδο προσαρμογής για τους υπαγόμενους στο πεδίο εφαρμογής του. Κάθε κράτος μέλος οφείλει να κοινοποιήσει στην Επιτροπή τις διατάξεις που θεσπίζει στο δίκαιό του, έως την 25η Μαΐου 2018 καθώς και κάθε μεταγενέστερη τροποποίησή τους.

Εδώ παρατίθενται τα βασικότερα σημεία του Κανονισμού, με τον οποίο αντικαθίσταται η ισχύουσα οδηγία 95/46/ΕΚ και προβλέπονται ρυθμίσεις και καινοτομίες, οι οποίες αλλάζουν σταδιακά αλλά και ριζικά το νομικό καθεστώς των δεδομένων προσωπικού χαρακτήρα στην Ευρωπαϊκή Ένωση:

Ι. ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ-ΑΡΧΕΣ ΕΠΕΞΕΡΓΑΣΙΑΣ

Σύμφωνα με το άρθρο 2 «Ουσιαστικό πεδίο εφαρμογής» του Κεφαλαίου Ι, ο εν λόγω Κανονισμός εφαρμόζεται στην, εν όλω ή εν μέρει, αυτοματοποιημένη ή μη επεξεργασία δεδομένων προσωπικού χαρακτήρα, τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης στο πλαίσιο των δραστηριοτήτων μιας εγκατάστασης ενός Υπεύθυνου Επεξεργασίας ή Εκτελούντος την επεξεργασία στην Ένωση, ανεξάρτητα από το κατά πόσο η επεξεργασία πραγματοποιείται εντός της Ένωσης.

Αντιθέτως, «δεν εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα:

α) στο πλαίσιο δραστηριότητας η οποία δεν εμπίπτει στο πεδίο εφαρμογής του δικαίου της Ένωσης,

β) από τα κράτη μέλη κατά την άσκηση δραστηριοτήτων που εμπίπτουν στο πεδίο εφαρμογής του κεφαλαίου 2 του τίτλου V της ΣΕΕ,

γ) από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας,

δ) από αρμόδιες αρχές για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, συμπεριλαμβανομένης της προστασίας και πρόληψης έναντι κινδύνων που απειλούν τη δημόσια ασφάλεια».

Όλη η διαδικασία της επεξεργασίας δεδομένων προσωπικού χαρακτήρα πρέπει να διεξάγεται στο πλαίσιο των αρχών που προβλέπονται στο άρθρο 5 «Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα» του Κεφαλαίου ΙΙ:

- Αρχή νομιμότητας
- Αρχή αντικειμενικότητας
- Αρχή διαφάνειας
- Αρχή του σκοπού (και περιορισμού αυτού)
- Αρχή της ελαχιστοποίησης των δεδομένων
- Αρχή της ακρίβειας (δικαίωμα διόρθωσης ή διαγραφής)
- Αρχή του περιορισμού
- Αρχή της ακεραιότητας και εμπιστευτικότητας (ασφάλεια)
- Αρχή της λογοδοσίας

ΙΙ. ΝΕΑ ΔΙΚΑΙΩΜΑΤΑ ΤΟΥ ΥΠΟΚΕΙΜΕΝΟΥ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Μεταξύ άλλων, στα άρθρα 12-22 του Κεφαλαίου ΙΙΙ εισάγονται νέα δικαιώματα του υποκειμένου των δεδομένων, με στόχο την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Ειδικότερα:

1. Δικαίωμα σαφέστερης ενημέρωσης κατά τη συλλογή των δεδομένων και δικαίωμα πρόσβασης σε αυτά.

2. Δικαίωμα διόρθωσης από τον υπεύθυνο επεξεργασίας ανακριβών δεδομένων καθώς και συμπλήρωση ελλιπών δεδομένων.
3. Δικαίωμα περιορισμού της επεξεργασίας από τον υπεύθυνο επεξεργασίας υπό συγκεκριμένες προϋποθέσεις.
4. Δικαίωμα εναντίωσης στην επεξεργασία υπό συγκεκριμένες προϋποθέσεις, ιδίως όταν πρόκειται για κατάρτιση «προφίλ» ή για σκοπούς απευθείας εμπορικής προώθησης.
5. Δικαίωμα στη λήθη, δηλ. δικαίωμα διαγραφή τους, υπό την προϋπόθεση ότι τα δεδομένα δεν τηρούνται για κάποιο συγκεκριμένο νόμιμο και δηλωμένο σκοπό.
6. Δικαίωμα στη φορητότητα των δεδομένων: δηλ. δικαίωμα υποβολής αιτήματος μεταφοράς των δεδομένων σε μηχαναγνώσιμη μορφή, από έναν υπεύθυνο επεξεργασίας σε άλλον, υπό συγκεκριμένες προϋποθέσεις.

III. ΒΑΣΙΚΕΣ ΥΠΟΧΡΕΩΣΕΙΣ ΓΙΑ ΤΟΝ ΥΠΕΥΘΥΝΟ ΕΠΕΞΕΡΓΑΣΙΑΣ – ΟΡΙΣΜΟΣ *ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ*

Α. Στα άρθρα 24-39 του Κεφαλαίου IV ο Κανονισμός επιβάλλει μια σειρά νέων υποχρεώσεων στον υπεύθυνο 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. Ειδικότερα:

Ευθύνη: Ο υπεύθυνος επεξεργασίας υποχρεούται να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τα προβλεπόμενα στον Κανονισμό.

Προστασία δεδομένων κατά τον σχεδιασμό («Data protection by design»): Ο Κανονισμός επιβάλλει την εφαρμογή προϊόντων και υπηρεσιών (ηλεκτρονικών και μη) που κατά τον αρχικό σχεδιασμό τους δημιουργούν φιλικές συνθήκες για την προστασία των δεδομένων σας.

Προστασία δεδομένων εξ ορισμού («Data protection by default»): Ο Κανονισμός επιβάλλει την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων που να

διασφαλίζουν ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα που είναι απαραίτητα για τον σκοπό της επεξεργασίας.

Ασφάλεια επεξεργασίας: Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία πρέπει να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το ενδεδειγμένο επίπεδο ασφάλειας.

Γνωστοποίηση παραβιάσεων δεδομένων: Ο υπεύθυνος επεξεργασίας έχει υποχρέωση, μόλις αντιληφθεί παραβίαση, να ενημερώσει αμελλητί και, εάν είναι δυνατό, εντός 72 ωρών από τη στιγμή της γνώσεως του γεγονότος της παραβίασης, την αρμόδια εποπτική Αρχή αλλά και το υποκείμενο των δεδομένων, εφ' όσον η παραβίαση αυτή θέτει σε σοβαρό κίνδυνο τα δικαιώματά του.

Εκτίμηση επιπτώσεων και προηγούμενη διαβούλευση: Όταν η επεξεργασία ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα των ατόμων, ιδίως επειδή είναι συστηματική, μεγάλης κλίμακας, αφορά ειδικές κατηγορίες δεδομένων και βασίζεται στη χρήση νέων τεχνολογιών, ο υπεύθυνος επεξεργασίας πρέπει να διενεργήσει, πριν την επεξεργασία, εκτίμηση επιπτώσεων σχετικά με την προστασία των δεδομένων («Data protection impact assessment»). Η προαναφερθείσα υποχρέωση της Εκτίμησης Αντικτύπου (DPIA), αποτελεί ουσιαστικά μια μορφή αξιολόγησης κινδύνου (Risk Assessment), στο πλαίσιο δε της διεξαγωγής της DPIA, ο Υπεύθυνος Επεξεργασίας διαβουλεύεται με την Εποπτική Αρχή και τον Υπεύθυνο Προστασίας Δεδομένων, ώστε να αποτραπούν οι υψηλοί κίνδυνοι σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα, ελλείψει μέτρων μετριασμού του κινδύνου από τον ίδιο τον Υπεύθυνο Επεξεργασίας.

Η δημοσίευση της διενεργηθείσας Εκτίμησης Αντικτύπου δεν είναι υποχρεωτική, καθώς δεν προβλέπεται στον Κανονισμό, αλλά εναπόκειται στη βούληση του Υπεύθυνου Επεξεργασίας. Μια όμως δημοσίευση ολόκληρης ή ακόμη και μέρους της DPIA, σταθμίζοντας πάντοτε το βαθμό του κινδύνου και το είδος των δεδομένων προσωπικού χαρακτήρα που υπόκεινται σε επεξεργασία, ενθαρρύνει και ενισχύει την εμπιστοσύνη μεταξύ του Υπεύθυνου Επεξεργασίας και των υποκειμένων των δεδομένων, ενώ παράλληλα εξυπηρετεί τη διαφάνεια της επεξεργασίας.

Κώδικες Δεοντολογίας: Ενθαρρύνεται η εκπόνηση Κωδίκων Δεοντολογίας από τους υπευθύνους επεξεργασίας, οι οποίοι υποβάλλονται προς έγκριση στην εποπτική Αρχή, με σκοπό να συμβάλουν στην ορθή εφαρμογή του Κανονισμού. Σε περίπτωση διευρωπαϊκής δραστηριότητας ζητείται και η γνώμη του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων.

Πιστοποίηση: Ενθαρρύνεται η θέσπιση μηχανισμών πιστοποίησης, σφραγίδων και σημάτων προστασίας δεδομένων για την απόδειξη της συμμόρφωσης προς τον Κανονισμό ή για την απόδειξη παροχής κατάλληλων εγγυήσεων κατά την επεξεργασία. Η πιστοποίηση είναι εθελοντική και μπορεί να παρέχεται και από την εποπτική Αρχή.

Β. *Ορισμός Υπευθύνου Προστασίας Δεδομένων***:** Ριζική καινοτομία εμφανίζεται με τον υποχρεωτικό ορισμό Υπεύθυνου Προστασίας Δεδομένων (Data Protection Officer – DPO) από τον Υπεύθυνο Επεξεργασίας και τον Εκτελούντα την Επεξεργασία στις αναλυτικά περιγραφόμενες περιπτώσεις του άρθρου 37 του Νέου Γενικού Κανονισμού.

Ο ρόλος του Data Protection Officer, ως εξειδικευμένου και *λειτουργικά ανεξάρτητου* στελέχους (άρθρο 38 παρ. 3) δεν περιορίζεται μόνο στην υποχρεωτική παρουσία του σε μια εταιρία, με την έννοια της τυπικής πλήρωσης μιας θέσης εργασίας (tick box), αλλά αναλαμβάνει ουσιαστικές αρμοδιότητες μεταξύ των οποίων η εκπροσώπηση της επιχείρησης έναντι εθνικών και ευρωπαϊκών Αρχών, η διασφάλιση της εναρμόνισης της λειτουργίας της επιχείρησης με τις πολιτικές πρακτικές και τη μεθοδολογία επεξεργασίας, αποθήκευσης και μεταφοράς Δεδομένων Προσωπικού Χαρακτήρα σύμφωνα με τον νέο αυστηρό νομοθετικό πλαίσιο, καθώς και η προστασία της επιχείρησης από τους κινδύνους επιβολής των σημαντικότατων και βαρύτατων διοικητικών προστίμων που προβλέπει ο Κανονισμός (άρθρα 38-39).

Ο Υπεύθυνος Προστασίας δεδομένων μπορεί να είναι μέλος του προσωπικού του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία ή να ασκεί τα καθήκοντά του, βάσει σύμβασης παροχής υπηρεσιών.

Η λειτουργική του ανεξαρτησία έγκειται στο γεγονός ότι διαθέτει αυτονομία στην άσκηση των καθηκόντων του και δε φέρει προσωπική ευθύνη, αλλά η ευθύνη για παραβίαση της νομοθεσίας σχετικά με τα δεδομένα προσωπικού χαρακτήρα, παραμένει στη Διοίκηση.

IV. ΕΠΟΠΤΙΚΕΣ ΑΡΧΕΣ-ΣΥΝΕΡΓΑΣΙΑ ΚΑΙ ΣΥΝΕΚΤΙΚΟΤΗΤΑ

Ανεξάρτητα από τα δικαιώματα που αναγνωρίζονται στο υποκείμενο των δεδομένων, κάθε Εποπτική Αρχή θα πρέπει να διασφαλίζει την αποτελεσματική προστασία των δεδομένων προσωπικού χαρακτήρα, μέσα από το διαρκή έλεγχο τήρησης του Κανονισμού και των επιταγών του, καθόλη τη διάρκεια της επεξεργασίας (άρθρο 58). Όταν κάποιος υπεύθυνος επεξεργασίας είναι εγκατεστημένος σε περισσότερα του ενός κράτη μέλη και προβαίνει σε διασυνοριακή επεξεργασία δεδομένων εντός ΕΕ, είναι σκόπιμο να καθορίσει το κράτος μέλος της κύριας εγκατάστασής του στην ΕΕ, ώστε να μπορεί να απευθύνεται στην εποπτική Αρχή του κράτους αυτού -η οποία θεωρείται η επικεφαλής εποπτική Αρχή- σε σχέση με τις διάφορες υποχρεώσεις συμμόρφωσης που πηγάζουν από τον Κανονισμό. Αυτό αποτελεί τον λεγόμενο μηχανισμό μίας στάσης («One stop shop»), σύμφωνα με τον οποίο προβλέπεται συνεργασία μεταξύ της επικεφαλής εποπτικής Αρχής και των ενδιαφερόμενων εθνικών Αρχών στην αρμοδιότητα των οποίων μπορεί να εμπίπτει μια υπόθεση ώστε να διασφαλίζεται ομοιογένεια στην αντιμετώπιση υποθέσεων διευρωπαϊκού ενδιαφέροντος και ασφάλεια δικαίου τόσο για τους υπευθύνους επεξεργασίας όσο και για τους πολίτες της Ένωσης.

Μία εξίσου σημαντική τροποποίηση που επιφέρει το άρθρο 94 του Κανονισμού, η οποία κρίνεται απαραίτητο να αναφερθεί, αποτελεί η αντικατάσταση της Ομάδας εργασίας του άρθρου 29 με το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, ο τρόπος σύστασης και οι αρμοδιότητες του οποίου προβλέπονται αναλυτικά στα άρθρα 68-76 του Νέου Γενικού Κανονισμού.

V. ΕΛΕΓΚΤΙΚΟΙ & ΚΥΡΩΤΙΚΟΙ ΜΗΧΑΝΙΣΜΟΙ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΥΠΟΚΕΙΜΕΝΩΝ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Α. Στο Κεφάλαιο VIII (άρθρα 77 επ.) του Κανονισμού προβλέπεται ένα πλαίσιο προστασίας των δικαιωμάτων των υποκειμένων, ως προς την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, τόσο σε διοικητικό όσο και σε δικαστικό επίπεδο.

Ειδικότερα, στο υποκείμενο των δεδομένων παρέχεται:

α) Δικαίωμα υποβολής καταγγελίας σε Εποπτική Αρχή, σε περίπτωση παραβίασης των διατάξεων του Κανονισμού (άρθρο 77),

β) Δικαίωμα πραγματικής δικαστικής προσφυγής (άρθρα 78-79)

γ) Δικαίωμα αποζημίωσης, σε βάρος του Υπεύθυνου Επεξεργασίας ή του Εκτελούντος την επεξεργασία, σε περίπτωση που η παραβίαση του Κανονισμού είχε ως αποτέλεσμα την υλική ή μη υλική ζημία του υποκειμένου (άρθρο 82).

Β. Στην περίπτωση παράβασης των διατάξεων του Κανονισμού από τον Υπεύθυνο Επεξεργασίας ή τον Εκτελούντα την επεξεργασία, επιβάλλονται από την Εποπτική Αρχή διοικητικά πρόστιμα, ανάλογα με τις περιστάσεις κάθε μεμονωμένης περίπτωσης, ώστε η επιβολή τους να καθίσταται αποτελεσματική, αναλογική και αποτρεπτική για το μέλλον. Αποτελούν είτε αυτοτελές μέτρο είτε επιπρόσθετο, το οποίο επιβάλλεται ταυτοχρόνως με τις διορθωτικές εξουσίες των Εποπτικών Αρχών, όπως αυτές αναφέρονται στο άρθρο 58 του Κανονισμού.

Ενδεικτικά, ο Κανονισμός προβλέπει την επιβολή σημαντικότατων και *βαρύτατων διοικητικών προστίμων*, τα οποία εκκινούν από 10.000.000 ευρώ ή το 2% του παγκόσμιου τζίρου, εάν πρόκειται για διεθνή όμιλο και φτάνουν, σε περίπτωση παράβασης βασικών διατάξεων του Κανονισμού, σε 20.000.000 ευρώ ή στο 4% του παγκόσμιου τζίρου.

Όπως ορίζεται ρητά στο άρθρο 84 τα κράτη μέλη δύναται να προβλέπουν την επιβολή επιπρόσθετων μέτρων και κυρώσεων ιδίως για εκείνες τις παραβάσεις που δεν αποτελούν αντικείμενο διοικητικών προστίμων δυνάμει του άρθρου 83. Σε κάθε περίπτωση οι κυρώσεις αυτές θα πρέπει να είναι αποτελεσματικές, αναλογικές και αποτρεπτικές για το μέλλον.

VI. ΣΥΜΠΕΡΑΣΜΑ

Στο πλαίσιο συμμόρφωσης με το Νέο Γενικό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων (GDPR), κάθε επεργαζόμενος προσωπικά δεδομένα καλείται να προβεί από την 25^{η} Μαΐου του 2018 στη λήψη των ακόλουθων μέτρων: α) Ενημέρωση του προσωπικού για τις επερχόμενες μεταβολές, υπογραμμίζοντας τις σημαντικές επιπτώσεις σε περίπτωση παραβιάσεων, β) υποχρεωτικός διορισμός

DPO, γ) αναθεώρηση πολιτικών προστασίας δεδομένων και διαδικασιών με την επικαιροποίησή τους όσον αφορά στον χειρισμό των αιτημάτων και στην ικανοποίηση των δικαιωμάτων των πελατών, ιδίως ως προς τη διαγραφή δεδομένων (δικαίωμα στη λήθη) ή την παροχή τους σε αναγνώσιμο ηλεκτρονικό μορφότυπο (φορητότητα δεδομένων), δ) Αξιολόγηση των πιθανών κινδύνων από τη συλλογή προσωπικών δεδομένων, ε) Διαμόρφωση κατάλληλης στρατηγικής αντιμετώπισης των πιθανών κινδύνων με τεχνικά και οργανωτικά μέτρα, στ) Υιοθέτηση μεθόδων για την ανίχνευση, την καταγραφή και τη διερεύνηση περιστατικών παραβιάσεων, ζ) Θέσπιση διαδικασίας για τις γνωστοποιήσεις παραβιάσεων προς την Αρχή και τα υποκείμενα.