Ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα (GDPR)

Ο νέος Γενικός 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» θα έχει άμεση εφαρμογή στις 25 Μαΐου 2018 σε όλα τα Κράτη-Μέλη της ΕΕ, αντικαθιστώντας την ισχύουσα Οδηγία **95/46/ΕΚ** και την εθνική νομοθεσία που την ενσωμάτωσε, δηλαδή το ν. 2472/1997, όπως ισχύει.

Ποια είναι η βασική διαφοροποίησή του σε σχέση με το ισχύον νομικό καθεστώς προστασίας των προσωπικών δεδομένων:

Ο νέος Γενικός Κανονισμός **(ΕΕ) 2016/679** δεν παρεκκλίνει ουσιωδώς από τις γενικές αρχές του υφιστάμενου πλαισίου προστασίας των προσωπικών δεδομένων, αλλά επιχειρεί να δημιουργήσει ένα αυστηρότερο θεσμικό πλαίσιο επεξεργασίας των προσωπικών δεδομένων και κατ' επέκταση προστασίας τους.

Χαρακτηρίζεται ιδίως από την ριζική αλλαγή του συστήματος ευθύνης για τήρηση της νομοθεσίας εισάγοντας την αρχή της Λογοδοσίας (Accountability Principle), σύμφωνα με τον οποίο οι εταιρείες που συλλέγουν και επεξεργάζονται προσωπικά δεδομένα οφείλουν να διαμορφώσουν τις διαδικασίες και τα τεχνικά και οργανωτικά συστήματα τους κατά τέτοιο τρόπο ώστε να είναι πλήρως συμμορφωμένες με όσα προβλέπει ο νέος Κανονισμός. Το βάρος απόδειξης μεταφέρεται από τις Αρχές Προστασίας Προσωπικών Δεδομένων στις εταιρείες, οι οποίες οφείλουν να αποδεικνύουν σε οποιαδήποτε περίπτωση ελέγχου ότι είναι πλήρως εναρμονισμένες με τις διατάξεις του Κανονισμού.

Περαιτέρω, ο Κανονισμός επιτάσσει την ύπαρξη ξεκάθαρης συναίνεσης του υποκειμένου των δεδομένων για κάθε σκοπό επεξεργασίας. Το γεγονός αυτό δημιουργεί την ανάγκη άμεσου εκσυγχρονισμού των μεθόδων και συστημάτων που εφαρμόζονται για την επεξεργασία των προσωπικών δεδομένων ούτως ώστε να τηρούνται οι αυστηρές προϋποθέσεις συγκατάθεσης και επεξεργασίας.

Ποια δεδομένα πρέπει να προστατεύονται

Τα δεδομένα προσωπικού χαρακτήρα κάθε εν ζωή φυσικού προσώπου, δηλαδή κάθε πληροφορία που αφορά ταυτοποιημένο φυσικό πρόσωπο ή κάθε πληροφορία που μπορεί άμεσα ή έμμεσα να ταυτοποιήσει ένα φυσικό πρόσωπο, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης ή σε στοιχεία που αφορούν τη σωματική, ψυχολογική, οικονομική ή κοινωνική κατάσταση του εν λόγω φυσικού προσώπου. Δεν αφορά λοιπόν τα δεδομένα των νομικών προσώπων (εταιρειών κ.λπ). Αφορά όμως τα δεδομένα μιας Μονοπρόσωπης εταιρίας ή μιας ατομικής επιχείρησης που νομικά αντιμετωπίζεται ως φυσικό πρόσωπο.

Τι σημαίνει «επεξεργασία» προσωπικών δεδομένων.

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.

Συνεπώς η επεξεργασία των προσωπικών δεδομένων είναι πολύ ευρεία έννοια και περιλαμβάνει ακόμη και τη συλλογή προσωπικών δεδομένων.

Προϋποθέσεις νόμιμης επεξεργασίας των προσωπικών δεδομένων:

Η επεξεργασία είναι νόμιμη εφόσον συντρέχουν 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.

Εμπλεκόμενα μέρη στην επεξεργασία των προσωπικών δεδομένων:

- «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.

- «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.

- «Αποδέκτης»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, στα οποία κοινοποιούνται τα δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για τρίτον είτε όχι. Ωστόσο, οι δημόσιες αρχές που ενδέχεται να λάβουν δεδομένα προσωπικού χαρακτήρα στο πλαίσιο συγκεκριμένης έρευνας σύμφωνα με το δίκαιο της Ένωσης ή κράτους μέλους δεν θεωρούνται ως αποδέκτες.

- «Τρίτος»: οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέας, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα.

Εδαφικό πεδίο εφαρμογής του Κανονισμού:

Ο Νέος Κανονισμός εφαρμόζεται όταν ο υπεύθυνος ή ο εκτελών την επεξεργασία των δεδομένων προσωπικού χαρακτήρα έχει την εγκατάστασή του στην ΕΕ, ανεξάρτητα από το κατά πόσο η επεξεργασία πραγματοποιείται εντός της Ένωσης.

Εφαρμόζεται επίσης στην επεξεργασία δεδομένων προσωπικού χαρακτήρα υποκειμένων των δεδομένων που βρίσκονται στην Ένωση από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία μη εγκατεστημένο στην Ένωση, εάν οι δραστηριότητες επεξεργασίας 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.

Επιπροσθέτως, ο Κανονισμός εφαρμόζεται για την επεξεργασία δεδομένων προσωπικού χαρακτήρα από υπεύθυνο επεξεργασίας μη εγκατεστημένο στην Ένωση, αλλά σε τόπο όπου εφαρμόζεται το δίκαιο κράτους μέλους δυνάμει του δημόσιου διεθνούς δικαίου.

Ποιες είναι οι βασικές καινοτομίες του Κανονισμού:

Ι) Η κατάργηση της γενικής υποχρέωσης γνωστοποίησης προς την εποπτική αρχή (δηλ. την εκάστοτε αρμόδια Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) της επεξεργασίας, η οποία βάρυνε τους υπευθύνους επεξεργασίας και μόνο.

Την καταργούμενη αυτή υποχρέωση ο νέος ΓΚΠΔ αντικαθιστά με την υποχρέωση για τους υπευθύνους επεξεργασίας να τηρούν αρχεία των δραστηριοτήτων επεξεργασίας όλων των δεδομένων προσωπικού χαρακτήρα, για τις οποίες είναι υπεύθυνοι, καθώς και με την υποχρέωση για τους εκτελούντες την επεξεργασία να τηρούν αρχεία όλων των κατηγοριών δραστηριοτήτων επεξεργασίας, που διεξάγονται για λογαριασμό υπευθύνου επεξεργασίας (Βλ. άρθρο 30 του ΓΚΠΔ).

Ένας ικανοποιητικός τρόπος προετοιμασίας ήδη από σήμερα, τόσο για τους υπευθύνους, όσο και για τους εκτελούντες επεξεργασία, είναι α) η κατανόηση των ζητημάτων που ανακύπτουν από τον ΓΚΠΔ (awareness), β) η καταγραφή των δεδομένων (data inventory) και των διαδικασιών, συστημάτων και αρχείων (φυσικών και ψηφιακών) που τα περιέχουν (data mapping), γ) η ανάλυση της απόκλισης από την συμμόρφωση με τον ΓΚΠΔ (Gap Analysis), δ) ο σχεδιασμός (ή ανασχεδιασμός) των κατάλληλων πολιτικών ροών δεδομένων και των επεξεργασιών που διενεργούνται, ώστε ο φορέας να είναι σε θέση να παρακολουθεί και να δημιουργήσει σύστημα τήρησης αρχείων.

ΙΙ) Εισάγεται η υποχρέωση του υπεύθυνου επεξεργασίας προς διενέργεια εκτίμησης αντικτύπου (Data protection impact assessment – DPIA) σχετικά με την προστασία δεδομένων σε συγκεκριμένες κατηγορίες επεξεργασιών. Ειδικότερα, ο υπεύθυνος επεξεργασίας υποχρεούται ρητά σε διενέργεια DPIA πριν από την κρίσιμη επεξεργασία κάθε φορά που ένα είδος επεξεργασίας, ιδίως με τη χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας αυτής, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. (Βλ. άρθρο 35 παρ. 1 ΓΚΠΔ).

ΙΙΙ) Εισάγεται η υποχρέωση για κατηγορίες υπευθύνων επεξεργασίας και εκτελούντων την επεξεργασία, να ορίσουν Υπεύθυνο Προστασίας Δεδομένων (Data Protection Officer-DPO) στη βάση συγκεκριμένων ποιοτικών κριτηρίων, που περιλαμβάνουν τη διενέργεια συγκεκριμένων τύπων επεξεργασιών. Επίσης ορίζονται οι περιπτώσεις υποχρεωτικού ορισμού DPO και παρέχεται η ευχέρεια όπως ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία ή ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπευθύνων ή εκτελούντων επεξεργασία, ορίσουν DPO και πέραν των περιπτώσεων του υποχρεωτικού ορισμού τούτου.

Η ύπαρξη και λειτουργία του DPO είναι εξαιρετικά σημαντική για τις εταιρείες διότι ουσιαστικά αυτός θα είναι το πρόσωπο που θα κατευθύνει τον οργανισμό προς την ολοκλήρωση και τήρηση ενός ικανού προγράμματος συμμόρφωσης με τον ΓΚΠΔ, θα διαχειριστεί τυχόν καταγγελίες και παραβάσεις και θα εκπροσωπήσει την εταιρεία στην εποπτική αρχή για κάθε σχετικό ζήτημα. Για το λόγο αυτό ακόμα και όταν δεν είναι υποχρεωτικός ο διορισμός DPO, θα ήταν ιδιαίτερα συμφέρον για κάθε εταιρεία να έχει εθελοντικά ορίσει έναν DPO. Ο ΓΚΠΔ δεν προβλέπει ειδικά κριτήρια ή πιστοποιήσεις για την επιλογή του DPO, θεωρεί όμως ότι θα πρέπει να είναι πρόσωπο με μεγάλη εμπειρία στη νομοθεσία των προσωπικών δεδομένων και τη διαχείριση τυχόν σχετικών παραβάσεων.

IV) Ενθαρρύνεται ιδιαιτέρως η σύνταξη κωδίκων δεοντολογίας από ενώσεις και άλλους φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία προκειμένου να προσδιορίσουν

την εφαρμογή του ΓΚΠΔ (αρθ. 40 ΓΚΠΔ), καθώς και η θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων, με σκοπό την απόδειξη συμμόρφωσης προς το ΓΚΠΔ (αρθ. 42). Σημειώνεται βέβαια, ότι αμφότερες οι περιπτώσεις αυτές δεν λειτουργούν ως απαλλακτικοί λόγοι ευθύνης.

Η εκτόξευση των διοικητικών προστίμων

Με το νέο Κανονισμό εκτοξεύεται το ύψος των επαπειλούμενων διοικητικών προστίμων σε περίπτωση διαπίστωσης παράβασης των διατάξεων του Κανονισμού, εφόσον δεν λαμβάνονται άλλα μέτρα.

Έτσι, συγκεκριμένες παραβάσεις των υποχρεώσεων των υπευθύνων και εκτελούντων επεξεργασία επισύρουν πρόστιμα έως 10.000.000 € ή σε περίπτωση επιχειρήσεων έως το 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους (όποιο είναι υψηλότερο). Είναι, δε, χαρακτηριστικό ότι και αυτή η απουσία των κατάλληλων οργανωτικών μέτρων για συμμόρφωση με τον ΓΚΠΔ δύναται να επισύρει το εν λόγω πρόστιμο, χωρίς καν να υφίσταται περίπτωση παράβασης.

Τα βαρύτερα πρόστιμα επιφυλάσσονται για τις παραβάσεις σε βάρος των δικαιωμάτων των υποκειμένων των δεδομένων, των βασικών αρχών για την επεξεργασία, της διαβίβασης δεδομένων προσωπικού χαρακτήρα σε αποδέκτη σε τρίτη χώρα ή σε διεθνή οργανισμό και τη μη συμμόρφωση προς εντολή ή προς προσωρινό ή οριστικό περιορισμό της επεξεργασίας ή προς αναστολή της κυκλοφορίας δεδομένων που επιβάλλει η εποπτική αρχή ή μη παροχή πρόσβασης. Στις περιπτώσεις αυτές επιβάλλονται διοικητικά πρόστιμα έως 20.000.000 € ή, σε περίπτωση επιχειρήσεων, έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο.

Η άλλη όψη του νομίσματος - Η περαιτέρω ενίσχυση των δικαιωμάτων των φυσικών προσώπων τα προσωπικά δεδομένα των οποίων επεξεργάζονται.

Ο νέος Γενικός Κανονισμός επιχειρεί να διασφαλίσει την ισορροπία, μεταξύ της συνεχούς ροής, συλλογής και επεξεργασίας προσωπικών δεδομένων αλλά και των αναφαίρετων δικαιωμάτων προστασίας τους που πρέπει να διατηρούνται αλλά και να «επικαιροποιούνται».

Βασική στόχευση των σχετικών ρυθμίσεων του Κανονισμού είναι η διευκόλυνση του υποκειμένου στην πρόσβαση σε διοικητικές και δικαστικές διαδικασίες προκειμένου είτε να προσβάλλουν μη νόμιμες επεξεργασίες είτε να διεκδικήσουν την επανόρθωση της βλάβης που έχουν υποστεί.

Ο Κανονισμός υιοθετεί την αρχή της εγγύτητας προς το υποκείμενο των δεδομένων, προβλέποντας ρητά ότι κάθε πρόσωπο που θεωρεί ότι παραβιάζονται τα δικαιώματα του στην προστασία των δεδομένων του, έχει το δικαίωμα να υποβάλει καταγγελία σε οποιαδήποτε εποπτική αρχή (βλ. ενδεικτικά τόπος συνήθους διαμονής υποκειμένου, ή τόπος εργασίας του ή τόπος εικαζόμενης παράβασης).

Τα δικαιώματα του υποκειμένου επίσης διευρύνονται. Ενδεικτική είναι η ρητή νομοθετική κατοχύρωση του δικαιώματος στη λήθη, δηλαδή του δικαιώματος του φυσικού προσώπου να διαγραφούν προσωπικά του δεδομένα. Αποτελεί ένα βασικό δικαίωμα του υποκειμένου να διατηρεί τον έλεγχο των προσωπικών πληροφοριών του κυρίως στον ψηφιακό κόσμο (βλ. μηχανές αναζήτησης). Πρόκειται για ένα δικαίωμα που είχε νομολογιακά αναγνωριστεί από το ΔΕΕ στην υπόθεση Google v. Spain (14.5.2014) και μάλιστα υπό το καθεστώς της Οδηγίας 96/46/ΕΚ.

Περαιτέρω, το υποκείμενο των προσωπικών δεδομένων μπορεί πλέον να στραφεί δικαστικά τόσο κατά του υπευθύνου επεξεργασίας, όσο και κατά του εκτελούντος της επεξεργασία. Εισάγεται λοιπόν εις ολόκληρον ευθύνη του υπεύθυνου και του εκτελούντος την επεξεργασία, κάτι που μέχρι σήμερα δεν υπήρχε, καθώς ευθύνη αναγνωριζόταν μόνο για τον υπεύθυνο της επεξεργασίας.

Επιπλέον, ειδική πρόβλεψη υπάρχει στον Κανονισμό (άρ. 80) για το συλλογική υποστήριξη των δικαιωμάτων του υποκειμένου, ήτοι το δικαίωμα του υποκειμένου να αναθέτει σε μη κερδοσκοπικό φορέα, οργάνωση ή ένωση, να υποβάλλει την καταγγελία για λογαριασμό του και να ασκήσει τα δικαιώματα ενώπιον δικαστηρίου.

Η ρύθμιση της επεξεργασίας και της προστασίας των προσωπικών δεδομένων ισοδυναμεί με επαναπλαισίωση της οικονομικής δραστηριότητας των επιχειρήσεων, αλλά και της καθημερινότητας όλων μας για την προάσπιση του κεκτημένου διαφύλαξης των προσωπικών δεδομένων. Στην κατεύθυνση αυτή, ο νέος Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων αποτελεί ένα νέο και αναγκαίο συνάμα βήμα προόδου, τόσο προς την ενίσχυση του δικαίου προστασίας των προσωπικών δεδομένων όσο και προς την καλλιέργεια μιας κουλτούρας αυτορρύθμισης των επιχειρήσεων και φορέων για την προστασία της προσωπικότητας του ατόμου.