GDPR: Στόχος και Σκοπός εφαρμογής του Ευρωπαϊκού Κανονισμού General Data Protection Regulation .

Περιεχόμενα

Στόχος και σκοπός του GDPR είναι να προστατεύσει όλους τους πολίτες της ΕΕ από την ιδιωτική ζωή και τις παραβιάσεις των δεδομένων σε έναν κόσμο όλο και περισσότερο βασισμένο στις πληροφορίες, ο οποίος είναι πολύ διαφορετικός από τον χρόνο σύστασης της αρχικής οδηγίας του 1995.

Μολονότι οι βασικές αρχές της ιδιωτικής ζωής των δεδομένων εξακολουθούν να ισχύουν από την προηγούμενη οδηγία, ο GDPR έχει πολλές αλλαγές οι οποίες έχουν ενταχθεί στις κανονιστικές πολιτικές. Τα βασικά σημεία του GDPR καθώς και πληροφορίες για τις επιπτώσεις/αλλαγές που θα έχει στις επιχειρήσεις μπορούν να βρεθούν παρακάτω.

GDPR: Βασική Αλλαγή σχετικά με το αυξημένο εδαφικό πεδίο εφαρμογής (εξωεδαφική εφαρμογή)

Αναμφισβήτητα η μεγαλύτερη αλλαγή στο ρυθμιστικό περιβάλλον της ιδιωτικής ζωής των δεδομένων έρχεται με την εκτεταμένη αρμοδιότητα του GDPR, καθώς ισχύει για όλες τις εταιρείες που επεξεργάζονται τα προσωπικά δεδομένα των υποκειμένων των δεδομένων που διαμένουν στην Ένωση, ανεξάρτητα από την τοποθεσία της εταιρείας.

Προηγουμένως, η εδαφική εφαρμογή της οδηγίας ήταν διφορούμενη και αναφέρεται σε διαδικασία επεξεργασίας δεδομένων «στο πλαίσιο εγκατάστασης». Αυτό το θέμα έχει προκύψει σε πολλές δικαστικές υποθέσεις υψηλού προφίλ.

Το GPDR καθιστά σαφή την εφαρμογή του - θα εφαρμόζεται στην επεξεργασία προσωπικών δεδομένων από ελεγκτές και μεταποιητές στην ΕΕ, ανεξάρτητα από το εάν η επεξεργασία πραγματοποιείται στην ΕΕ ή όχι.

Το GDPR θα ισχύει επίσης για την επεξεργασία δεδομένων προσωπικού χαρακτήρα των υποκειμένων των δεδομένων στην ΕΕ από υπεύθυνο επεξεργασίας ή μεταποιητή μη εγκατεστημένο στην ΕΕ, όπου οι δραστηριότητες αφορούν: προσφορά αγαθών ή υπηρεσιών σε πολίτες της ΕΕ (ανεξάρτητα από το αν απαιτείται πληρωμή) και την παρακολούθηση της συμπεριφοράς που λαμβάνει χώρα εντός της ΕΕ.

Οι επιχειρήσεις εκτός ΕΕ που επεξεργάζονται τα δεδομένα των πολιτών της ΕΕ θα πρέπει επίσης να διορίσουν έναν εκπρόσωπο στην ΕΕ.

GDPR: Βασική Αλλαγή σχετικά με τις Ποινικές ρήτρες

Σύμφωνα με τον κανονισμό GDPR, οι οργανισμοί που παραβιάζουν το GDPR, μπορεί να υποχρεωθούν σε πρόστιμο μέχρι 4% του ετήσιου συνολικού κύκλου εργασιών ή € 20 εκατ. (Όποιο είναι μεγαλύτερο).

Πρόκειται για το μέγιστο πρόστιμο που μπορεί να επιβληθεί για τις πιο σοβαρές παραβάσεις, π.χ. χωρίς τη δέουσα συγκατάθεση του πελάτη για επεξεργασία δεδομένων ή παραβίαση του πυρήνα των εννοιών «Απόρρητο από το σχεδιασμό».

Υπάρχει μια κλιμακωτή προσέγγιση στα πρόστιμα, π.χ. μια επιχείρηση μπορεί να επιβληθεί πρόστιμο ύψους 2% για μη τήρηση των αρχείων της (άρθρο 28), χωρίς να ενημερώνει την εποπτεύουσα αρχή και το υποκείμενο των δεδομένων για παραβίαση ή μη διενέργεια εκτιμήσεων αντικτύπου.

Είναι σημαντικό να σημειωθεί ότι αυτοί οι κανόνες ισχύουν τόσο για τους υπεύθυνους επεξεργασίας όσο και για τους μεταποιητές - που σημαίνει ότι οι "cloud" υπηρεσίες δεν θα εξαιρούνται από την επιβολή του GDPR.

GDPR: Βασική Αλλαγή σχετικά με την Συγκατάθεση

Οι όροι για τη συναίνεση/ συγκατάθεση στο πλαίσιο του GDPR έχουν ενισχυθεί και οι εταιρείες δεν θα μπορούν πλέον να χρησιμοποιούν μακρούς δυσανάγνωστους όρους και προϋποθέσεις γεμάτες νομικίστικες έννοιες, καθώς η αίτηση συναίνεσης πρέπει να παρέχεται με κατανοητή και εύκολα προσπελάσιμη μορφή, με σκοπό την επεξεργασία δεδομένων που επισυνάπτεται αυτή τη συναίνεση.

Η συγκατάθεση πρέπει να είναι σαφής και διακριτή από άλλα θέματα και να παρέχεται με κατανοητή και εύκολα προσιτή μορφή, χρησιμοποιώντας σαφή και απλή γλώσσα. Πρέπει να είναι τόσο εύκολο να αποσύρετε τη συγκατάθεση σας, όσο εύκολο είναι να την δώσετε.

Δικαιώματα δεδομένων υποκειμένων

GDPR: Βασική Αλλαγή σχετικά με την Ειδοποίηση Παραβίασης

Σύμφωνα με το GDPR, η κοινοποίηση παραβίασης θα καταστεί υποχρεωτική σε όλα τα κράτη μέλη όπου μια παραβίαση δεδομένων ενδέχεται να "οδηγήσει σε κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων". Αυτό πρέπει να γίνει εντός 72 ωρών από την πρώτη στιγμή της συνειδητοποίησης της παραβίασης. Οι επεξεργαστές δεδομένων θα υποχρεούνται επίσης να ειδοποιούν τους πελάτες τους, τους ελεγκτές, "χωρίς αδικαιολόγητη καθυστέρηση", αφού καταλάβουν την παραβίαση δεδομένων.

GDPR: Βασική Αλλαγή σχετικά με το Δικαίωμα πρόσβασης

Μέρος των διευρυμένων δικαιωμάτων των προσώπων στα οποία αναφέρονται τα στοιχεία του GDPR είναι το δικαίωμα των υποκειμένων των δεδομένων να λαμβάνουν από τον υπεύθυνο επεξεργασίας δεδομένων την επιβεβαίωση του κατά πόσον τα δεδομένα προσωπικού χαρακτήρα που τους αφορούν υποβάλλονται σε επεξεργασία, πού και για ποιο σκοπό.

Επιπλέον, ο ελεγκτής παρέχει δωρεάν αντίγραφο των δεδομένων προσωπικού χαρακτήρα σε ηλεκτρονική μορφή. Αυτή η αλλαγή είναι μια δραματική αλλαγή στη διαφάνεια των δεδομένων και την ενδυνάμωση των υποκειμένων των δεδομένων.

GDPR: Βασική Αλλαγή στο "Δικαίωμα στη Λήθη"

Επίσης γνωστό ως Data Erasure, το "δικαίωμα στη λήθη" παρέχει στο υποκείμενο των δεδομένων τη δυνατότητα να διαγράψει τα δεδομένα προσωπικού χαρακτήρα από τον ελεγκτή δεδομένων, να σταματήσει την περαιτέρω διάδοση των δεδομένων και ενδεχομένως να σταματήσει την επεξεργασία των δεδομένων από τρίτους.

Οι όροι για τη διαγραφή, όπως περιγράφονται στο άρθρο 17, περιλαμβάνουν τα δεδομένα που δεν έχουν πλέον σχέση με τους αρχικούς σκοπούς για επεξεργασία ή τα υποκείμενα των δεδομένων που αποσύρουν τη συναίνεση.

Πρέπει επίσης να σημειωθεί ότι το δικαίωμα αυτό απαιτεί από τους ελεγκτές να συγκρίνουν τα δικαιώματα των υποκειμένων με το "δημόσιο συμφέρον για τη διαθεσιμότητα των δεδομένων" κατά την εξέταση αυτών των αιτήσεων.

GDPR: Βασική Αλλαγή σχετικά με την Φορητότητα δεδομένων

Το GDPR εισάγει τη φορητότητα δεδομένων - το δικαίωμα για ένα υποκείμενο των δεδομένων να λαμβάνει τα προσωπικά δεδομένα που τα αφορούν, τα οποία παρείχαν προηγουμένως σε μια «ευρέως χρησιμοποιούμενη και μηχανικά αναγνώσιμη μορφή» και έχουν το δικαίωμα να διαβιβάσουν τα δεδομένα αυτά σε άλλο ελεγκτή.

GDPR: Βασική Αλλαγή σχετικά με την Προστασία δεδομένων από το σχεδιασμό

Η προστασία της ιδιωτικής ζωής από τη σχεδίαση ως έννοια έχει υπάρξει εδώ και χρόνια, αλλά γίνεται μέρος μιας νομικής απαίτησης στον GDPR. Στον πυρήνα της, η προστασία της ιδιωτικής ζωής από το σχεδιασμό απαιτεί την ενσωμάτωση της προστασίας των δεδομένων από την εμφάνιση του σχεδιασμού των συστημάτων, και όχι από την προσθήκη.

Συγκεκριμένα: «Ο υπεύθυνος επεξεργασίας πρέπει να εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα με αποτελεσματικό τρόπο ώστε να ανταποκρίνεται στις απαιτήσεις του παρόντος κανονισμού και να προστατεύει τα δικαιώματα των υποκειμένων των δεδομένων».

Το άρθρο 23 ζητεί από τους ελεγκτές να διατηρούν και να επεξεργάζονται μόνο τα δεδομένα που είναι απολύτως απαραίτητα για την εκπλήρωση των καθηκόντων τους (ελαχιστοποίηση των δεδομένων), καθώς και τον περιορισμό της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε όσους χρειάζονται στη διεξαγωγή της επεξεργασίας.

Οι υπεύθυνοι επεξεργασίας υποχρεούνται να κοινοποιούν τις δραστηριότητές επεξεργασίας δεδομένων σε τοπικές αρχές προστασίας δεδομένων, οι οποίες, για τις πολυεθνικές εταιρείες, ενδέχεται να αποτελούν γραφειοκρατικό εφιάλτη με τα περισσότερα κράτη μέλη να έχουν διαφορετικές απαιτήσεις κοινοποίησης.

Σύμφωνα με το GDPR, δεν θα είναι απαραίτητο να υποβάλλονται κοινοποιήσεις / καταχωρήσεις σε κάθε τοπική αρχή των δραστηριοτήτων επεξεργασίας δεδομένων ούτε να απαιτείται η κοινοποίηση / απόκτηση έγκρισης για μεταφορές βάσει των πρότυπων ρητρών σύμβασης (MCC). Αντ 'αυτού, θα υπάρξουν απαιτήσεις εσωτερικής τήρησης αρχείων, όπως εξηγείται περαιτέρω παρακάτω, και ο διορισμός των DPO θα είναι υποχρεωτικός μόνο για τους ελεγκτές και τους μεταποιητές των οποίων οι βασικές δραστηριότητες συνίστανται σε επεξεργασίες που απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα ή σε ειδικές κατηγορίες δεδομένων ή δεδομένων σχετικά με ποινικές καταδίκες και αξιόποινες πράξεις. Είναι σημαντικό να διορίζεται ο ΥΠΔ με βάση τα επαγγελματικά προσόντα και ειδικότερα τις γνώσεις σχετικά με το δίκαιο και τις πρακτικές προστασίας των δεδομένων. Μπορεί να

είναι μέλος του προσωπικού ή εξωτερικός πάροχος υπηρεσιών. Πρέπει να παρέχονται λεπτομερή στοιχεία στο σχετικό DPAM με τους κατάλληλους πόρους να εκπληρώνουν τα καθήκοντά τους και να διατηρούν τις ειδικές γνώσεις τους. Να υποβάλλουν απευθείας αναφορά στο ανώτατο επίπεδο διαχείρισης. Να μην εκτελούν άλλα καθήκοντα που θα μπορούσαν να οδηγήσουν σε σύγκρουση συμφερόντων.