26 Μαΐου 2018

Πως θα προσαρμόσετε στον GDPR ιστοσελίδες, e-shop και web ή mobile εφαρμογές

/ Επιστήμες, Τέχνες & Πολιτισμός

Από τις 25 Μαΐου στην Ελλάδα και στις άλλες χώρες της Ευρωπαϊκής Ένωσης, τίθεται σε εφαρμογή ο νέος ευρωπαϊκός Γενικού Κανονισμός για την Προστασία των Δεδομένων (GDPR), ο οποίος αφορά τη συλλογή, χρήση και αποθήκευση των προσωπικών δεδομένων. Το σημαντικότερο βέβαια είναι ότι με τον GDPR καθορίζονται αυστηρά οι υποχρεώσεις φορέων και εταιρειών γύρω από την συλλογή, χρήση και αποθήκευση των προσωπικών δεδομένων αλλά και τα δικαιώματα των πολιτών – χρηστών.

Στόχος της ΕΕ είναι η εφαρμογή αυστηρότερων κανόνων, προκειμένου οι 250 εκατομμύρια καθημερινοί χρήστες του διαδικτύου στην Ευρώπη και γενικότερα οι πολίτες να ελέγχουν καλύτερα και ευκολότερα τα προσωπικά τους δεδομένα που βρίσκονται online, τα οποία άλλοι (επιχειρήσεις, οργανισμοί, μέσα κοινωνικής δικτύωσης) συλλέγουν, επεξεργάζονται και μοιράζονται με τρίτους.

Οι εταιρείες που επεξεργάζονται προσωπικά δεδομένα, πρέπει πλέον να παρέχουν σαφείς πληροφορίες για ποιους σκοπούς τα χρησιμοποιούν, για πόσο χρονικό διάστημα τα αποθηκεύουν, σε ποιους άλλους τα κοινοποιούν και εάν τα δεδομένα θα διαβιβασθούν εκτός της ΕΕ.

Οι εταιρείες πρέπει να παρέχουν στοιχεία επικοινωνίας των υπεύθυνων για την επεξεργασία και προστασία των δεδομένων. Όλες αυτές οι πληροφορίες θα πρέπει να διατυπώνονται με απόλυτη σαφήνεια.

Ταυτόχρονα κάθε εταιρεία (ή φορέας) που χρησιμοποιεί, επεξεργάζεται η αποθηκεύει τέτοια δεδομένα θα πρέπει να είναι έτοιμη να παραδώσει ή να τροποποιήσει ή να σβήσει προσωπικά δεδομένα οποιουδήποτε χρήστη, όταν ζητήσει.

Για να βοηθήσουμε στην κατανόηση εφαρμογής του GDPR μελετήσαμε:

Την αναλυτική παρουσίαση των κανόνων του GDPR στην ιστοσελίδα της ΕΕ,
Την Επισκόπηση του General Data Protection Regulation (GDPR) από την ESET Hellas με θέμα «Πως θα επηρεάσει την επιχείρησή σας»,
Την σχετική ανάλυση της Πανελλήνιας Ομοσπονδίας Φοροτεχνικών Ελευθέρων Επαγγελματιών (ΠΟΦΕΕ)
Και σας παρουσιάζουμε συνοπτικά, ειδικότερα για εταιρίες που διαθέτουν ιστοσελίδες ή e-shop ή web εφαρμογές ή mobile εφαρμογές που χρησιμοποιούν προσωπικά δεδομένα χρηστών, όσα πρέπει να προσέξουν και να εφαρμόσουν για την προσαρμογή τους στους κανόνες του GDPR.

Οι βασικοί κανόνες του GDPR

Συναίνεση χρήσης προσωπικών δεδομένων
α)Αρχή περιορισμού του πεδίου εφαρμογής:

τα προσωπικά δεδομένα θα πρέπει να συλλέγονται μόνο για συγκεκριμένους, ρητούς και νόμιμους σκοπούς και δε θα πρέπει να επεξεργάζονται περαιτέρω κατά τρόπο ασύμβατο με αυτούς τους σκοπούς

β)Αρχή της ελαχιστοποίησης των προσωπικών δεδομένων:

Μόνο τα προσωπικά δεδομένα που είναι αναγκαία για τους αρχικούς σκοπούς θα πρέπει να υπόκεινται σε επεξεργασία

Δικαίωμα εναντίωσης και δικαίωμα διαγραφής δεδομένων
Αφορά το δικαίωμα του χρήστη να ζητήσει την διαγραφή ή την τροποποίηση των προσωπικών δεδομένων του

Δικαίωμα μεταφοράς δεδομένων
Αφορά το δικαίωμα του χρήστη να ζητήσει μεταφορά των δεδομένων του όπου επιθυμεί.

Ενημέρωση της Αρχής Προστασίας Προσωπικών Δεδομένων εντός 72 ωρών εάν εντοπιστεί παραβίαση δεδομένων.
Αφορά την υποχρέωση κάθε εταιρίας ή Οργανισμού να ενημερώσει εντός 72 ωρών την Αρχή Προστασίας Προσωπικών Δεδομένων σε περίπτωση που

εντοπίσει παραβίαση του Αρχείου δεδομένων είτε μέσω hacking είτε με οποιοδήποτε άλλο τρόπο.

Αυξημένες υποχρεώσεις συμμόρφωσης για τους υπεύθυνους επεξεργασίας οι οποίο θα πρέπει να ελέγχουν κατά πόσο οι λειτουργίες της εταιρίας ή του φορέα τηρούν τους κανονισμούς του GDPR.
Παραδείγματα δεδομένων προσωπικού χαρακτήρα:

όνομα και επώνυμο
διεύθυνση κατοικίας
ηλεκτρονική διεύθυνση ταχυδρομείου, π.χ. όνομα.επώνυμο@εταιρεία.com (όχι τύπου info@εταιρεία.com)
αριθμός εγγράφου ταυτοποίησης (π.χ. αριθμός ταυτότητας, διαβατηρίου, διπλώματος οδήγησης, κ.λπ.)
δεδομένα τοποθεσίας (π.χ. η λειτουργία δεδομένων τοποθεσίας σε κινητό

τηλέφωνο)
διεύθυνση διαδικτυακού πρωτοκόλλου (IP address)
αναγνωριστικό διαδικτυακής περιήγησης (π.χ. cookie)
το αναγνωριστικό διαφήμισης του τηλεφώνου σας
δεδομένα που φυλάσσονται από νοσοκομείο ή γιατρό, που θα μπορούσαν να είναι ένα σύμβολο που προσδιορίζει αποκλειστικά ένα άτομο (ανήκουν στην κατηγορία των ευαίσθητων προσωπικών δεδομένων).
Τι πρέπει να κάνετε για την προσαρμογή στον κανονισμό GDPR

Προσαρμογή για την προστασία των δεδομένων από τον σχεδιασμό της ιστοσελίδας, e–shop ή εφαρμογής.

Αναπτύξτε όλα τα ηλεκτρονικά εργαλεία για την εφαρμογή μέτρων προστασίας των προσωπικών δεδομένων στα προϊόντα, τις υπηρεσίες ή τα αρχεία σας από τα αρχικά στάδια ανάπτυξης της ιστοσελίδας, του e–shop ή της εφαρμογής σας.

Θα πρέπει να μπορείτε αν ανταποκριθείτε άμεσα, ολοκληρωμένα και δωρεάν σε αιτήματα για:

Συγκατάθεση τήρησης δεδομένων ή ενημέρωσης των χρηστών
Ανάκληση της συγκατάθεσης
Πρόσβαση στα δεδομένα (όπου είναι δυνατόν)
Διόρθωση των δεδομένων
Διαγραφή των δεδομένων
Περιορισμό της επεξεργασίας
Παράδοση των δεδομένων σε ηλεκτρονική μορφή
Μεταφορά των δεδομένων σε άλλο φορέα
Θα πρέπει επίσης να μεριμνήσετε για:

Ενημέρωση

Διαρκή ενημέρωση (πρωτίστως στους όρους χρήσης) για τους όρους που εφαρμόζετε και τηρείτε σε ότι αφορά την αποθήκευση ή διαχείριση προσωπικών δεδομένων καθώς και για τα δικαιώματα των ατόμων που αφορούν αυτά

Security

Εξασφάλιση αυστηρών security μέτρων για την διαδικτυακή προστασία των προσωπικών δεδομένων

Επικοινωνία

Εάν ζητάτε προσωπικά δεδομένα θα πρέπει να γνωρίζουν οι αποδέκτες του αιτήματος με σαφήνεια: Ποιοι είστε . Γιατί χρειάζεστε τα συγκεκριμένα δεδομένα. Εάν θα τα επεξεργαστείτε, τον λόγο που επεξεργάζεστε τα δεδομένα τους, για πόσο καιρό θα τα φυλάξετε και ποιος τα λαμβάνει.

Πρόσβαση και δυνατότητα μεταφοράς

Δώστε στα άτομα πρόσβαση (αμέσως ή εμμέσως) στα δεδομένα τους και επιτρέψτε τους να τα δώσουν σε άλλη εταιρεία.

Διαγραφή δεδομένων

Δώστε τους το «δικαίωμα στη λήθη». Διαγράψτε τα προσωπικά τους δεδομένα αν το ζητήσουν, αλλά μόνο αν δεν θίγεται η ελευθερία έκφρασης, όπως προβλέπει ο GDPR

Μάρκετινγκ

Δώστε στα άτομα το δικαίωμα να εξαιρεθούν από πρακτικές άμεσου μάρκετινγκ που χρησιμοποιούν τα δεδομένα τους.

Διαβίβαση δεδομένων εκτός της ΕΕ

Συνάψτε νομικές συμφωνίες όταν πρόκειται να διαβιβάσετε δεδομένα σε χώρες που δεν έχουν λάβει έγκριση από τις αρχές της ΕΕ.

Συγκατάθεση

Λάβετε τη ρητή συγκατάθεσή τους για την επεξεργασία των δεδομένων ή την διαβίβασή τους οπουδήποτε

Προειδοποιήσεις

Ενημερώστε τα άτομα σχετικά με παραβιάσεις δεδομένων αν ενέχει σοβαρός κίνδυνος για αυτούς.

Δημιουργία προφίλ

Αν χρησιμοποιείτε προφίλ για την επεξεργασία αιτήσεων ατόμων για νομικά δεσμευτικές συμφωνίες, πρέπει:

Να ενημερώνετε τους πελάτες σας
Να ορίζετε ένα πρόσωπο και όχι μια μηχανή να ελέγχει τη διαδικασία αν η αίτηση τελικά απορρίπτεται
Να χορηγείτε στον αιτούντα το δικαίωμα να προσβάλλει την απόφαση ή να ζητήση αιτιολόγησή της.
Προστασία ευαίσθητων προσωπικών δεδομένων

Χρησιμοποιήστε πρόσθετα αυξημένα μέτρα προστασίας εάν ταξινομείτε, επεξεργάζεστε ή χρησιμοποιείτε με οποιοδήποτε τρόπο πληροφορίες που αφορούν την υγεία, τη φυλή, τον σεξουαλικό προσανατολισμό, τη θρησκεία ή τις πολιτικές πεποιθήσεις ατόμων.

Πρόσβαση σε τρίτους

Δίνετε πρόσβαση στα προσωπικά δεδομένα τρίτων σε συνεργάτες σας μόνον υπό συγκεκριμένες συνθήκες και εφόσον αυτοί αποδεικνύουν τη συμμόρφωσή τους με τον GDPR