



software **athensoft** solutions
software + hardware solutions

ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (GDPR)

Τι είναι ο Γενικός Κανονισμός για την Προστασία Δεδομένων;

Ο Ευρωπαϊκός Κανονισμός 2016/679 (General Data Protection Regulation, GDPR) ψηφίστηκε στις 27.04.2016 και τίθεται σε υποχρεωτική εφαρμογή για όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης στις 25.05.2018, διαμορφώνοντας ένα ενιαίο νομικό πλαίσιο, χωρίς την ανάγκη ψήφισης εθνικής νομοθεσίας και καταργώντας την υφιστάμενη νομοθεσία. Ο νέος κανονισμός αυξάνει σημαντικά τις υποχρεώσεις των επιχειρήσεων, ενώ το μέγεθος των προβλεπόμενων προστίμων τον τοποθετεί πολύ υψηλά στην ατζέντα της ανώτατης διοίκησης.

Ποιες επιχειρήσεις αφορά;

Όλες τις ιδιωτικές και δημόσιες επιχειρήσεις, καθώς και τις κρατικές αρχές που με οποιοδήποτε τρόπο διαχειρίζονται δεδομένα προσωπικού χαρακτήρα πελατών, πελατών των πελατών τους, εργαζομένων, συνεργατών ή άλλων φυσικών προσώπων. Ως εκ τούτου, ο GDPR αφορά πρακτικά όλες τις επιχειρήσεις, εντός και εκτός Ευρωπαϊκής Ένωσης, εφόσον τα δεδομένα αφορούν Ευρωπαίους πολίτες.

Ποιες υποχρεώσεις προβλέπονται για τις επιχειρήσεις;

Να τηρούν τις βασικές αρχές προστασίας των προσωπικών δεδομένων, δηλαδή να τα συλλέγουν για συγκεκριμένο νόμιμο σκοπό και μόνο όσα εξ' αυτών είναι απαραίτητα, να μην τα υποβάλουν σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο με το σκοπό, να τα επικαιροποιούν, να τα αποθηκεύουν για το ελάχιστο χρονικό διάστημα που απαιτείται, να λαμβάνουν κατά περίπτωση την ελεύθερη και σαφή συγκατάθεση των φυσικών προσώπων.

Να τα μεταφέρουν σε χώρες εκτός ΕΕ μόνον υπό συγκεκριμένες προϋποθέσεις.



software **athensoft** solutions
software + hardware solutions

Να δίνουν πρόσβαση στα προσωπικά δεδομένα σε συνεργάτες τους μόνον υπό συγκεκριμένες συνθήκες και εφόσον αυτοί αποδεικνύουν τη συμμόρφωσή τους με τον GDPR.

Να αναπτύξουν ηλεκτρονικά εργαλεία για την έγκαιρη και δωρεάν ανταπόκριση σε αιτήματα για:

- ανάκληση της συγκατάθεσης.
- πρόσβαση στα δεδομένα.
- διόρθωση των δεδομένων ή διαγραφή των δεδομένων.
- περιορισμό της επεξεργασίας.
- παράδοση των δεδομένων σε ηλεκτρονική μορφή.
- μεταφορά των δεδομένων σε άλλο φορέα.
- να γνωστοποιούν κατάλληλα και εγκαίρως στα φυσικά πρόσωπα τα δικαιώματά τους.
- να εξασφαλίζουν την ασφάλεια των προσωπικών δεδομένων σε όλο τον κύκλο ζωής τους.
- να τηρούν σε αρχείο και να γνωστοποιούν κάθε παραβίαση των δεδομένων εντός 72 ωρών στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και στα φυσικά πρόσωπα με απευθείας ενημέρωση ή δημόσια ανακοίνωση.
- να αποδεικνύουν ότι τηρούν όλες τις απαιτήσεις του Κανονισμού.

Για να ικανοποιήσουν όλα τα ανωτέρω οι επιχειρήσεις οφείλουν:

Να λαμβάνουν τα απαιτούμενα τεχνικά και οργανωτικά μέτρα που περιλαμβάνονται σε διεθνή πρότυπα, σε κώδικες δεοντολογίας και σε συστάσεις αρμοδίων κοινοτικών και εθνικών οργάνων.

Να δημιουργήσουν και να επικαιροποιούν το μητρώο επεξεργασίας, όπου θα απεικονίζουν τη ροή, τους αποδέκτες και το είδος των προσωπικών δεδομένων που διαχειρίζονται.

Να διενεργούν μελέτη εκτίμησης των επιπτώσεων (Privacy Impact Assessment), στην οποία θα αξιολογούν τους κινδύνους για τα προσωπικά δεδομένα που διαχειρίζονται και θα οδηγούνται στη λήψη των απαραίτητων μέτρων περιορισμού των κινδύνων.



software **athensoft** solutions
software + hardware solutions

Να αναπτύξουν πολιτικές και διαδικασίες προστασίας και ασφάλειας των προσωπικών δεδομένων.

Να ορίσουν Υπεύθυνο Προστασίας Δεδομένων (Data Protection Officer) να συμμορφώνονται με κώδικες δεοντολογίας ή να διαθέτουν πιστοποιήσεις που αποδεικνύουν τη συμμόρφωσή τους με τον Κανονισμό.

Τι προβλέπεται για τα ευαίσθητα προσωπικά δεδομένα;

Αλλάζει η ονομασία τους, καθώς ονομάζονται πλέον προσωπικά δεδομένα ειδικής κατηγορίας και διευρύνεται ο ορισμός τους, καθώς συμπεριλαμβάνονται τα γενετικά και βιομετρικά δεδομένα. Για τους οργανισμούς που χειρίζονται προσωπικά δεδομένα ειδικής κατηγορίας προβλέπονται επιπλέον απαιτήσεις.

Ποιες ποινές προβλέπονται;

Σε περίπτωση παράβασης προβλέπονται σημαντικά αυξημένα πρόστιμα, που ανάλογα με το είδος και το μέγεθός της, φθάνουν έως τα 20 εκατομμύρια ευρώ ή το 4% του παγκόσμιου ετήσιου κύκλου εργασιών.

Ποιες είναι οι κυριότερες δυσκολίες για τις επιχειρήσεις;

Η ακριβής γνώση για το ποια δεδομένα συλλέγουν και επεξεργάζονται σε κάθε φάση των δραστηριοτήτων τους, ποιοι εμπλέκονται και με ποια εργαλεία και διαδικασίες γίνεται η επεξεργασία.

Ο καθορισμός και διαχωρισμός των επιχειρησιακών αναγκών, ώστε να διασφαλίζονται όλες οι απαιτούμενες συγκαταθέσεις του υποκειμένου και να μη γίνεται πλεονάζουσα επεξεργασία.

Ο συστηματικός έλεγχος για την κάλυψη των απαιτήσεων του GDPR σε κάθε στάδιο επεξεργασίας των δεδομένων.

Η αξιολόγηση των κινδύνων που ενδέχεται να οδηγήσουν σε παραβίαση των προσωπικών δεδομένων, με αποτέλεσμα βαρύτερες οικονομικές κυρώσεις και επιπτώσεις στην εταιρική φήμη.



software **athensoft** solutions
software + hardware solutions

Η παρουσίαση των σημαντικότερων κινδύνων και των τρόπων αντιμετώπισής τους στη Διοίκηση με πρακτικό τρόπο, ώστε να αποφασισθεί ένα ρεαλιστικό πλάνο και προϋπολογισμός συμμόρφωσης.

Η λήψη αποτελεσματικών και οικονομικών μέτρων για τον περιορισμό του κινδύνου παραβιάσεων του GDPR, χωρίς να θίγονται οι επιχειρησιακές προτεραιότητες.

Η ATHENSOFΤ, με το κατάλληλα εκπαιδευμένο προσωπικό της, από την TUV AUSTRIA ACADEMY / DPO ACADEMY, διαθέτουν την γνώση έτσι ώστε να σας ενημερώσουν, να διασφαλίσουν και να εναρμονίσουν την λειτουργία της επιχείρησής σας, σε ότι αφορά τις πολιτικές πρακτικές και μεθοδολογία επεξεργασίας, αποθήκευσης και μεταφοράς δεδομένων προσωπικού χαρακτήρα.

Επικοινωνήστε μαζί μας, για οποιαδήποτε πληροφορία η διευκρίνηση και μαζί θα βρούμε κοινό τρόπο συνεργασίας στον τρόπο διαχείρισης προσωπικών δεδομένων.

www.athensoft.gr

