ΕΙΣΗΓΗΣΗ

ΠΡΟΣ :

ΕΝΤΑΥΘΑ

Θέμα : «Έγκριση Διαδικασίας Συμμόρφωσης με το Νέο Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων 2016/679, (General Data Protection Regulation (GDPR) της Ε.Ε».

Βάσει του νέου Ευρωπαϊκού Κανονισμού 2016/679 (General Data Protection Regulation, G.D.P.R) της Ευρωπαϊκής Ένωσης, που ψηφίστηκε στις 27.04.2016 τίθεται σε υποχρεωτική εφαρμογή η εν λόγω οδηγία για όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης από τις 25.05.2018, διαμορφώνοντας ένα ενιαίο νομικό πλαίσιο, χωρίς την ανάγκη ψήφισης εθνικής νομοθεσίας που αφορά τις ιδιωτικές και δημόσιες επιχειρήσεις, καθώς και τις κρατικές αρχές που με οποιοδήποτε τρόπο συγκεντρώνουν, επεξεργάζονται και εν γένει διαχειρίζονται δεδομένα προσωπικού χαρακτήρα πελατών, σχετιζόμενων με τους πελάτες τους, εργαζομένων, συνεργατών ή άλλων φυσικών προσώπων.

Ο κανονισμός αυτός καταργεί την οδηγία 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) που ισχύει σήμερα και βάσει του οποίου έχει προκύψει ο Νόμος 2472/1997 του Ελληνικού κράτους. Βάσει του νομικού συστήματος της ΕΕ οι Ευρωπαϊκοί Κανονισμοί είναι γενικής εφαρμογής, υποχρεωτικοί και άμεσα εφαρμόσιμοι σε όλα τα κράτη μέλη, χωρίς να υπάρχει υποχρέωση για ενσωμάτωση στην εθνική νομοθεσία εκάστου κράτους μέλους.

Ο νέος Γενικός Κανονισμός Προστασίας Δεδομένων της ΕΕ αποτελεί τη μεγαλύτερη αλλαγή στην νομοθεσία περί προστασίας των δεδομένων τα τελευταία σχεδόν 20 χρόνια. Ο νέος κανονισμός αυξάνει σημαντικά τις υποχρεώσεις των επιχειρήσεων, ενώ το μέγεθος των προβλεπόμενων προστίμων τον τοποθετεί πολύ υψηλά στην ατζέντα της ανώτατης διοίκησης
Ο κανονισμός θέτει μία σειρά περιορισμών και νέων υποχρεώσεων στις επιχειρήσεις σχετικά με την επεξεργασία των προσωπικών δεδομένων σε όλο τον κύκλο ζωής τους, από τη συλλογή έως και την καταστροφή τους, τη δυνατότητα μεταφοράς τους σε άλλες χώρες, την προστασία των δικαιωμάτων των φυσικών προσώπων, την ασφάλεια (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα) των προσωπικών δεδομένων και τις ενέργειες γνωστοποίησης που οφείλει να κάνει η επιχείρηση σε περίπτωση παραβίασης.

Ο Κανονισμός 2016/679 έχει εφαρμογή σε όλες τις κρατικές αρχές που με οποιοδήποτε τρόπο συγκεντρώνουν, επεξεργάζονται και εν γένει διαχειρίζονται δεδομένα προσωπικού χαρακτήρα πελατών, σχετιζόμενων με τους πελάτες τους, εργαζομένων, συνεργατών ή άλλων φυσικών προσώπων, είτε έχουν έδρα και δραστηριότητα σε χώρα της Ευρωπαϊκής Ένωσης είτε όχι, εφόσον τα δεδομένα αφορούν Ευρωπαίους πολίτες ή σχετίζονται με οποιουδήποτε είδους υπηρεσίες και αγαθά προς Ευρωπαίους πολίτες.

Σύμφωνα με τον GDPR, θα πρέπει να εφαρμόσετε ένα ευρύ φάσμα μέτρων, προκειμένου να διασφαλίσετε ότι θα μειωθεί ο κίνδυνος υπέρβασης του Κανονισμού και να σας επιτρέψει να αποδείξετε ότι λαμβάνετε τη διαχείριση των δεδομένων προσωπικού χαρακτήρα πολύ σοβαρά.

Μεταξύ των αναγκαίων μέτρων λογοδοσίας είναι: αξιολόγηση των επιπτώσεων προσωπικών δεδομένων, έλεγχος, αξιολόγηση της πολιτικής, διατήρηση αρχείων δραστηριότητα και διορισμός υπεύθυνου προστασίας δεδομένων (DPO).

Ο Γενικός Κανονισμός Προστασίας Δεδομένων είναι ένα ενιαίο νομικό πλαίσιο για την επεξεργασία προσωπικών δεδομένων στα κράτη μέλη της Ευρωπαϊκής Ένωσης, που θέτει μία σειρά περιορισμών και νέων υποχρεώσεων στις επιχειρήσεις σχετικά με:

α. την επεξεργασία των προσωπικών δεδομένων σε όλο τον κύκλο ζωής τους, από τη συλλογή έως και την καταστροφή τους,

β. τη δυνατότητα μεταφοράς τους σε άλλες χώρες,

γ. την προστασία των δικαιωμάτων των φυσικών προσώπων,

δ. την ασφάλεια (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα) των προσωπικών δεδομένων και τις ενέργειες γνωστοποίησης που οφείλει να κάνει η επιχείρηση σε περίπτωση παραβίασης.

Οι οργανισμοί που υπόκεινται στην τήρηση του κανονισμού θα πρέπει:

1. Να τηρούν τις βασικές αρχές προστασίας των προσωπικών δεδομένων, δηλαδή να τα συλλέγουν για συγκεκριμένο νόμιμο σκοπό και μόνο όσα εξ' αυτών είναι απαραίτητα,

2. να μην τα υποβάλουν σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο με το σκοπό, να τα επικαιροποιούν,

3. να τα αποθηκεύουν για το μικρότερο δυνατό χρονικό διάστημα που απαιτείται, να λαμβάνουν - κατά περίπτωση - την ελεύθερη και σαφή συγκατάθεση των φυσικών προσώπων,

4. να τα μεταφέρουν σε χώρες εκτός ΕΕ μόνον υπό συγκεκριμένες προϋποθέσεις, να δίνουν πρόσβαση στα προσωπικά δεδομένα σε συνεργάτες τους μόνον υπό συγκεκριμένες συνθήκες και εφόσον αυτοί αποδεικνύουν τη συμμόρφωσή τους με τον νέο κανονισμό,
5. να αναπτύξουν ηλεκτρονικά εργαλεία για την έγκαιρη και δωρεάν ανταπόκριση σε αιτήματα που θα ανακύπτουν.
6. να γνωστοποιούν κατάλληλα και εγκαίρως στα φυσικά πρόσωπα τα δικαιώματά τους να εξασφαλίζουν την ασφάλεια των προσωπικών δεδομένων σε όλο τον κύκλο ζωής τους,
7. 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,
8. να αποδεικνύουν ότι τηρούν όλες τις απαιτήσεις του Κανονισμού. Οι οργανισμοί που υπόκεινται στην τήρηση του κανονισμού έχουν να αντιμετωπίσουν στα πλαίσια του νέου κανονισμού τα ακόλουθα προβλήματα:
   α. Ακριβής γνώση για το ποια δεδομένα συλλέγουν και επεξεργάζονται σε κάθε φάση των δραστηριοτήτων τους, ποιοι εμπλέκονται και με ποια εργαλεία και με ποιες διαδικασίες γίνεται η επεξεργασία αυτή,
   β. Ακριβής καθορισμός και διαχωρισμός των επιχειρησιακών αναγκών, ώστε να διασφαλίζονται όλες οι απαιτούμενες συγκαταθέσεις του υποκειμένου και να μη γίνεται πλεονάζουσα επεξεργασία,
   γ. Συστηματικός έλεγχος για την κάλυψη των απαιτήσεων του κανονισμού σε κάθε στάδιο επεξεργασίας των δεδομένων,
   δ. Αξιολόγηση των κινδύνων που ενδέχεται να οδηγήσουν σε παραβίαση των προσωπικών δεδομένων, με αποτέλεσμα βαρύτατες οικονομικές κυρώσεις και επιπτώσεις στην εταιρική φήμη.

Στα πλαίσια λοιπόν εφαρμογής του νέου κανονισμού θα πρέπει ο φορέας/οργανισμός:

1. Να σχεδιάσει διαδικασίες που αφορούν:
   - Δικαίωμα στη λήθη,
   - Ενίσχυση της παιδικής προστασίας,
   - Δικαίωμα στη φορητότητα,
   - Ενημέρωση σε περίπτωση παραβιάσεως,
   - Δικαίωμα στην ανθρώπινη παρέμβαση
2. Να κάνει αντίστοιχα προσαρμογές στα πληροφοριακά τους συστήματα ώστε να υλοποιηθούν οι ανωτέρω διαδικασίες.
3. Να λάβει μέτρα ασφάλειας που αφορούν π.χ Ασφάλεια Πληροφοριών, Asset Management (Διαχείριση Πόρων της Επιχείρησης), Data Classification (Κατ/ση Πληροφοριών),Κρυπτογράφηση δεδομένων (Cryptography), Ψευδονυμοποίηση δεδομένων (Pseudonymization) κ.α
4. Να εκπονήσει: Impact Assessment, Risk Assessment Data Protection Officer / Υπεύθυνος Προστασίας Δεδομένων
   Οι δημόσιες αρχές που εκτελούν πράξεις επεξεργασίας δεδομένων και ενέχουν κινδύνους θα πρέπει να έχουν ορίσει υπεύθυνο προστασίας δεδομένων (Data Protection officer). Ο κανονισμός GDPR θεσπίζει επίσης την υποχρέωση των υπεύθυνων επεξεργασίας των δεδομένων να παρέχουν διαφανείς και εύκολα προσβάσιμες πληροφορίες στα υποκείμενα των δεδομένων όσον αφορά την επεξεργασία των δεδομένων τους.

   Το άρθρο 37 του κανονισμού προβλέπει ότι υπεύθυνοι προστασίας δεδομένων (DPO) πρέπει να οριστούν για όλες τις δημόσιες αρχές εκτός των δικαστηρίων που ενεργούν στα πλαίσια των αρμοδιοτήτων τους. Ο ορισμός υπευθύνου προστασίας δεδομένων είναι υποχρεωτικός:

   - εάν η επεξεργασία διενεργείται από δημόσια αρχή ή δημόσιο φορέα (ανεξάρτητα από το είδος των δεδομένων που υφίστανται επεξεργασία),
   - εάν οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα,

- εάν οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα.

Ο υπεύθυνος προστασίας δεδομένων, συνεπικουρούμενος από ομάδα εφόσον απαιτείται, πρέπει να είναι σε θέση να επικοινωνεί με τα υποκείμενα των δεδομένων και να συνεργάζεται με τις ενδιαφερόμενες εποπτικές αρχές με αποτελεσματικό τρόπο. Η διαθεσιμότητα του υπευθύνου προστασίας δεδομένων (είτε με φυσική παρουσία στις ίδιες εγκαταστάσεις με τους υπαλλήλους, είτε μέσω ανοικτής τηλεφωνικής γραμμής ή άλλου ασφαλούς μέσου επικοινωνίας) είναι καθοριστικής σημασίας για τη διασφάλιση της δυνατότητας επικοινωνίας των υποκειμένων των δεδομένων μαζί του.

Ένας μόνο υπεύθυνος προστασίας δεδομένων μπορεί να ορίζεται για πολλές δημόσιες αρχές ή δημόσιους φορείς, λαμβάνοντας υπόψη την οργανωτική τους δομή και το μέγεθός τους

Ο υπεύθυνος προστασίας δεδομένων μπορεί να είναι μέλος του προσωπικού του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία (εσωτερικός υπεύθυνος προστασίας δεδομένων) ή να ασκεί τα καθήκοντά του βάσει σύμβασης παροχής υπηρεσιών.

Ο υπεύθυνος προστασίας δεδομένων πρέπει να διαθέτει, μεταξύ άλλων, τις ακόλουθες δεξιότητες και εμπειρογνωμοσύνη:

- εμπειρογνωσία στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, τόσο σε εθνικό όσο και σε ευρωπαϊκό επίπεδο, καθώς και άριστη γνώση του ΓΚΠΔ,
- γνώση των πράξεων επεξεργασίας που διενεργούνται,
- γνώση του τομέα των τεχνολογιών πληροφοριών και της ασφάλειας δεδομένων,
- γνώση του τομέα δραστηριότητας και του οργανισμού,
- ικανότητα ανάπτυξης νοοτροπίας προστασίας των δεδομένων στους κόλπους του οργανισμού. (Άρθρο 37/ παράγραφος 5/ του ΓΚΠΔ)

**Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών**

Ένα σύστημα διαχείρισης ασφάλειας πληροφοριών βάση του προτύπου ISO/IEC 27001:2013 έχει να κάνει με όλες αυτές τις απαιτήσεις του άρθρου 32. Το ISO/IEC 27001:2013 είναι το διεθνές πρότυπο για την ασφάλεια πληροφοριών που έχει αυστηρές απαιτήσεις σε όλους τους τομείς που επηρεάζουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών και των δεδομένων, από τη
φυσική ασφάλεια των εγκαταστάσεων, τη διαχείριση του ανθρωπίνου δυναμικού, τις διαδικασίες λειτουργίας και οργάνωσης, τις σχέσεις με συνεργάτες, πελάτες και τρίτα μέρη, τη συμμόρφωση με νομικές και κανονιστικές απαιτήσεις, μέχρι την ασφάλεια των υποδομών πληροφορικής και επικοινωνιών, τη συνεχή εκπαίδευση και ευαισθητοποίηση του προσωπικού, τον χειρισμό περιστατικών ασφαλείας και τον σχεδιασμό επιχειρησιακής συνέχειας.

Όπως έχει αναφερθεί παραπάνω ο κανονισμός θα εφαρμοστεί το Μάιο του 2018, έτσι ώστε οι οργανισμοί/φορείς να έχουν δύο χρόνια για να προετοιμαστούν και να συμμορφωθούν πλήρως με το νέο πλαίσιο.

Η εφαρμογή και πιστοποίηση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών βάση του ISO/IEC 27001 για τους φορείς, αποτελεί ένα αποτελεσματικό εργαλείο συμμόρφωσης με σημαντικές απαιτήσεις του General Data Protection Regulation (GDPR).

Στο πλαίσιο αυτό σας στέλνουμε ένα ερωτηματολόγιο προκειμένου να διαστασιολογήσουμε τις ανάγκες του φορέα σας για την προσαρμογή στην νέα οδηγία και να σας καταθέσουμε την οικονομοτεχνική μας προσφορά, κατόπιν συμπλήρωσης του (ΣΕ ΠΕΡΙΠΤΩΣΗ ΠΟΥ ΘΕΛΕΤΕ ΒΟΗΘΕΙΑ ΓΙΑ ΤΗΝ ΣΥΜΠΛΗΡΩΣΗ ΕΠΙΚΟΙΝΩΝΗΣΕΤΕ ΜΑΖΙ Μ)ΑΣ

Παραμένουμε στην διάθεση σας για οποιαδήποτε πρόσθετη πληροφορία ή διευκρίνιση

Με σεβασμό & εκτίμηση

Κωνσταντίνος Κοτσιφάκης