ΚΕΝΤΡΙΚΗ ΕΝΩΣΗ ΕΠΙΜΕΛΗΤΗΡΙΩΝ ΕΛΛΑΔΟΣ

ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

ΚΑΝΟΝΙΣΜΟΣ ΕΕ 2016/679

ΕΝΑΣ ΣΥΝΤΟΜΟΣ ΟΔΗΓΟΣ ΕΦΑΡΜΟΓΗΣ

4/2018

Σε ποιες περιπτώσεις εφαρμόζονται οι διατάξεις του Κανονισμού;

- Ο Κανονισμός εφαρμόζεται σε κάθε περίπτωση αυτοματοποιημένης ή μη επεξεργασίας δεδομένων προσωπικού χαρακτήρα (ΔΠΧ), εφόσον ο υπεύθυνος επεξεργασίας, ο εκτελών την επεξεργασία ή το υποκείμενο των ΔΠΧ είναι εγκατεστημένοι ενός της Ευρωπαϊκής Ένωσης (ΕΕ). Εξαιρούνται περιπτώσεις όπου η επεξεργασία αυτή λαμβάνει χώρα:
- α) στο πλαίσιο δραστηριότητας η οποία δεν εμπίπτει στο πεδίο εφαρμογής του δικαίου της Ένωσης,
- β) από τα κράτη μέλη κατά την άσκηση δραστηριοτήτων που αφορούν την κοινή εξωτερική πολιτική και την πολιτική ασφαλείας,
- γ) από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας και
- δ) από αρμόδιες αρχές για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, συμπεριλαμβανομένης της προστασίας και πρόληψης έναντι κινδύνων που απειλούν τη δημόσια ασφάλεια.

Ποια θεωρούνται «δεδομένα προσωπικού χαρακτήρα» ;

- Κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων») και ειδικότερα κάθε πληροφορία η οποία δύναται είτε μόνη της είτε σε συνδυασμό με άλλη πληροφορία να οδηγήσει στην εξακρίβωση της ταυτότητας ενός φυσικού προσώπου (ταυτοποίηση).

Ποια θεωρούνται «ευαίσθητα προσωπικά δεδομένα» ;

- Ευαίσθητα προσωπικά δεδομένα είναι αυτά που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και τα γενετικά δεδομένα, βιομετρικά δεδομένα με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένα που αφορούν την υγεία ή δεδομένα που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό του.

Ποια η σημασία της έννοιας «επεξεργασία»;

- 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

Ποιος είναι ο 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.

Πότε θεωρείται κάποιος ως εκτελών την επεξεργασία;

- Όταν επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας.

Ποιες αρχές πρέπει να τηρεί ο υπεύθυνος επεξεργασίας;

- α) η επεξεργασία πρέπει να είναι σύννομη και θεμιτή και να διεξάγεται με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων («νομιμότητα, αντικειμενικότητα και διαφάνεια»)
- β) τα ΔΠΧ συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς («περιορισμός του σκοπού»)
- γ) τα ΔΠΧ είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»)
- δ) τα ΔΠΧ είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται («ακρίβεια»)
- ε) τα ΔΠΧ διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας του («περιορισμός της περιόδου αποθήκευσης»)
- στ) τα ΔΠΧ υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλειά τους, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων («ακεραιότητα και εμπιστευτικότητα»)

Πότε θεωρείται η επεξεργασία ΔΠΧ σύννομη;

- Η επεξεργασία ΔΠΧ είναι σύννομη στις ακόλουθες περιπτώσεις:
- α) το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των ΔΠΧ 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,
- 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.

Τι ισχύει για την επεξεργασία ευαίσθητων προσωπικών δεδομένων;

Απαγορεύεται η εν γένει επεξεργασία ευαίσθητων προσωπικών δεδομένων.
Η απαγόρευση αυτή αίρεται στις ακόλουθες περιπτώσεις:

- α) όταν το υποκείμενο των δεδομένων έχει παράσχει ρητή συγκατάθεση για την επεξεργασία τους,
- β) η επεξεργασία είναι απαραίτητη για την εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων στον τομέα του εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας,
- γ) η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, εάν το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να συγκατατεθεί,
- δ) η επεξεργασία διενεργείται, με κατάλληλες εγγυήσεις, στο πλαίσιο των νόμιμων δραστηριοτήτων ιδρύματος, οργάνωσης ή άλλου μη κερδοσκοπικού φορέα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό στόχο και υπό την προϋπόθεση ότι η επεξεργασία αφορά αποκλειστικά τα μέλη ή τα πρώην μέλη του φορέα ή πρόσωπα τα οποία έχουν τακτική επικοινωνία μαζί του σε σχέση με τους σκοπούς του,
- ε) η επεξεργασία αφορά δεδομένα προσωπικού χαρακτήρα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων,
- στ) η επεξεργασία είναι απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων,
- ζ) η επεξεργασία είναι απαραίτητη για λόγους ουσιαστικού δημόσιου συμφέροντος,
- η) η επεξεργασία είναι απαραίτητη για σκοπούς προληπτικής ή επαγγελματικής ιατρικής, εκτίμησης της ικανότητας προς εργασία του εργαζομένου, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους ή δυνάμει σύμβασης με επαγγελματία του τομέα της υγείας,
  θ) η επεξεργασία είναι απαραίτητη για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας,
- ι) η επεξεργασία είναι απαραίτητη για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς.

Ποια είναι τα δικαιώματα του υποκειμένου των ΔΠΧ;

- Το υποκείμενο των ΔΠΧ δικαιούται:
- α) να λαμβάνει από τον υπεύθυνο επεξεργασίας κάθε πληροφορία σχετικά με την επεξεργασία σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή,
- β) να λαμβάνει από τον υπεύθυνο επεξεργασίας επιβεβαίωση για το κατά πόσον ή όχι τα ΔΠΧ που το αφορούν υφίστανται επεξεργασία και, εάν συμβαίνει τούτο, το δικαίωμα πρόσβασης σε αυτά,
- γ) να απαιτήσει από τον υπεύθυνο επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν,
- δ) να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση,
- ε) να εξασφαλίζει από τον υπεύθυνο επεξεργασίας τον περιορισμό της επεξεργασίας,
- στ) να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και το δικαίωμα να διαβιβάζει τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας χωρίς αντίρρηση από τον υπεύθυνο επεξεργασίας στον οποίο παρασχέθηκαν τα δεδομένα προσωπικού χαρακτήρα,
- ζ) να αντιτάσσεται, ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν, η) να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο.

Ποιες είναι οι υποχρεώσεις του υπεύθυνου επεξεργασίας;

- Ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με την ισχύουσα εθνική και ευρωπαϊκή νομοθεσία και ότι εξασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων. Τα εν λόγω μέτρα επανεξετάζονται και επικαιροποιούνται όταν κρίνεται απαραίτητο. Στο πλαίσιο αυτό ο υπεύθυνος επεξεργασίας οφείλει να εφαρμόζει κατάλληλες πολιτικές για την προστασία των δεδομένων. Η τήρηση εγκεκριμένων κωδίκων δεοντολογίας ή εγκεκριμένου μηχανισμού πιστοποίησης, δύναται επίσης να χρησιμοποιηθεί ως στοιχείο για την απόδειξη της συμμόρφωσης του υπεύθυνου επεξεργασίας με τις υποχρεώσεις του, όπως αυτές απορρέουν από την ισχύουσα εθνική και ευρωπαϊκή νομοθεσία. Επίσης, ο υπεύθυνος επεξεργασίας τηρεί αρχείο των δραστηριοτήτων επεξεργασίας, για τις οποίες είναι υπεύθυνος, με όλες τις πληροφορίες που προβλέπονται στην εκάστοτε ισχύουσα νομοθεσία. Ο υπεύθυνος επεξεργασίας συνεργάζεται, κατόπιν αιτήματος, με την εποπτική αρχή για την άσκηση των καθηκόντων της.

Ποιες είναι οι υποχρεώσεις του εκτελούντος την επεξεργασία;

- Η επεξεργασία από τον εκτελούντα την επεξεργασία διέπεται από σύμβαση, που δεσμεύει τον εκτελούντα την επεξεργασία σε σχέση με τον υπεύθυνο επεξεργασίας και καθορίζει το αντικείμενο και τη διάρκεια της επεξεργασίας, τη φύση και τον σκοπό της επεξεργασίας, το είδος των δεδομένων προσωπικού χαρακτήρα και τις κατηγορίες των υποκειμένων των δεδομένων και τις υποχρεώσεις και τα δικαιώματα του υπευθύνου επεξεργασίας. Η εν λόγω σύμβαση προβλέπει κατ' ελάχιστον ότι ο εκτελών την επεξεργασία: α) επεξεργάζεται τα ΔΠΧ μόνο βάσει καταγεγραμμένων εντολών του υπευθύνου επεξεργασίας, β) διασφαλίζει ότι τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα έχουν αναλάβει δέσμευση τήρησης εμπιστευτικότητας ή τελούν υπό τη δέουσα κανονιστική υποχρέωση τήρησης εμπιστευτικότητας, γ) λαμβάνει όλα τα απαιτούμενα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, δ) δεν προσλαμβάνει άλλον εκτελούντα την επεξεργασία χωρίς προηγούμενη ειδική ή γενική γραπτή άδεια του υπευθύνου επεξεργασίας, και εφόσον προσλάβει, οι ίδιες υποχρεώσεις όσον αφορά την προστασία των δεδομένων που προβλέπονται στη σύμβαση μεταξύ υπευθύνου επεξεργασίας και εκτελούντος την επεξεργασία, επιβάλλονται στον άλλον αυτόν εκτελούντα μέσω σύμβασης, ιδίως ώστε να παρέχονται επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων, ούτως ώστε η επεξεργασία να πληροί τις απαιτήσεις του ισχύοντος νομοθετικού πλαισίου, ε) λαμβάνει υπόψη τη φύση της επεξεργασίας και επικουρεί τον υπεύθυνο επεξεργασίας με τα κατάλληλα τεχνικά και οργανωτικά μέτρα, στον βαθμό που αυτό είναι δυνατό, για την εκπλήρωση της υποχρέωσης του υπευθύνου επεξεργασίας να απαντά σε αιτήματα για άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων, στ) συνδράμει τον υπεύθυνο επεξεργασίας στη διασφάλιση της συμμόρφωσης προς τις υποχρεώσεις του, λαμβάνοντας υπόψη τη φύση της επεξεργασίας και τις πληροφορίες που διαθέτει ο εκτελών την επεξεργασία, ζ) κατ' επιλογή του υπευθύνου επεξεργασίας, διαγράφει ή επιστρέφει όλα τα δεδομένα προσωπικού χαρακτήρα στον υπεύθυνο επεξεργασίας μετά το πέρας της παροχής υπηρεσιών επεξεργασίας και διαγράφει τα υφιστάμενα αντίγραφα, η) θέτει στη διάθεση του υπευθύνου επεξεργασίας κάθε απαραίτητη πληροφορία προς απόδειξη της συμμόρφωσης προς τις υποχρεώσεις του και επιτρέπει και διευκολύνει τους ελέγχους, περιλαμβανομένων των επιθεωρήσεων, που διενεργούνται από τον υπεύθυνο επεξεργασίας ή από άλλον ελεγκτή εντεταλμένο από τον υπεύθυνο επεξεργασίας, θ) τηρεί αρχείο όλων των κατηγοριών δραστηριοτήτων επεξεργασίας που διεξάγονται εκ μέρους του υπευθύνου επεξεργασίας, το οποίο περιλαμβάνει τις πληροφορίες που ορίζονται από την εκάστοτε ισχύουσα νομοθεσία, ι) συνεργάζεται, κατόπιν αιτήματος, με την εποπτική αρχή για την άσκηση των καθηκόντων της.

Ποια τα καθήκοντα του υπεύθυνου προστασίας δεδομένων;

- Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία ορίζουν υπεύθυνο προστασίας δεδομένων, τα στοιχεία του οποίου δημοσιεύονται και ανακοινώνονται στην εποπτική αρχή. Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία:
- α) διασφαλίζουν ότι ο υπεύθυνος προστασίας δεδομένων συμμετέχει, δεόντως και εγκαίρως, σε όλα τα ζητήματα τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα,
- β) στηρίζουν τον υπεύθυνο προστασίας δεδομένων στην άσκηση των καθηκόντων του, παρέχοντας απαραίτητους πόρους για την άσκηση των εν λόγω καθηκόντων και πρόσβαση σε δεδομένα προσωπικού χαρακτήρα,
- γ) διασφαλίζουν ότι ο υπεύθυνος προστασίας δεδομένων δεν λαμβάνει εντολές για την άσκηση των εν λόγω καθηκόντων. Ο υπεύθυνος προστασίας δεδομένων έχει τουλάχιστον τα ακόλουθα καθήκοντα: α) ενημερώνει και συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία, β) παρακολουθεί τη συμμόρφωση με τις ισχύουσες νομοθετικές διατάξεις και με τις πολιτικές του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σε σχέση με την προστασία των ΔΠΧ, γ) παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και παρακολουθεί την υλοποίησή της, δ) συνεργάζεται με την εποπτική αρχή και ε) ενεργεί ως σημείο επικοινωνίας για την εποπτική αρχή για ζητήματα που σχετίζονται με την επεξεργασία.

Είναι δυνατή η διαβίβαση προσωπικών δεδομένων σε τρίτη χώρα;

- Η διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτη χώρα μπορεί να πραγματοποιηθεί εφόσον η Επιτροπή έχει αποφασίσει ότι διασφαλίζεται επαρκές επίπεδο προστασίας από την τρίτη χώρα. Για μια τέτοια διαβίβαση δεν απαιτείται ειδική άδεια. Ελλείψει τέτοιας απόφασης, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία μπορεί να διαβιβάσει δεδομένα προσωπικού χαρακτήρα σε τρίτη χώρα μόνο εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία έχει παράσχει κατάλληλες εγγυήσεις και υπό την προϋπόθεση ότι υφίστανται εκτελεστά δικαιώματα και αποτελεσματικά ένδικα μέσα για τα υποκείμενα των δεδομένων.

Ποιες είναι οι κυρώσεις σε περίπτωση παράβασης των διατάξεων του Κανονισμού ;

- **Α.** Σε περίπτωση παράβασης των υποχρεώσεων του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία, επιβάλλονται διοικητικά πρόστιμα έως 10.000.000 ευρώ ή, σε περίπτωση επιχειρήσεων, έως το 2 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο.
- **Β.** Σε περίπτωση παράβασης των βασικών αρχών που διέπουν την επεξεργασία ΔΠΧ, των δικαιωμάτων των υποκειμένων των δεδομένων, των υποχρεώσεων σε περίπτωση διαβίβασης ΔΠΧ σε τρίτη χώρα, οιασδήποτε υποχρέωσης σύμφωνα με το εθνικό δίκαιο ή σε περίπτωση μη συμμόρφωσης σε εντολή, σε περιορισμό επεξεργασίας ή αναστολή της κυκλοφορίας προσωπικών δεδομένων της εποπτικής αρχής επιβάλλονται διοικητικά πρόστιμα έως 20.000.000 ευρώ ή, σε περίπτωση επιχειρήσεων, έως το 4 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο.

- 16