ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

ΕΙΣΑΓΩΓΗ

Ο Χάρτης των Θεμελιωδών Δικαιωμάτων της ΕΕ προβλέπει ότι οι πολίτες της ΕΕ έχουν το δικαίωμα προστασίας των προσωπικών τους δεδομένων. Ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων (Κανονισμός (ΕΕ) 2016/679) της Ευρωπαϊκής Ένωσης (ΕΕ), για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, τέθηκε σε ισχύ στις 24 Μαΐου 2016 και θα αρχίσει να εφαρμόζεται από τις 25 Μαΐου 2018.

Ο κανονισμός αποκτά αυτομάτως δεσμευτικό χαρακτήρα σε όλη την ΕΕ από την ημερομηνία έναρξης ισχύος του και αντικαθιστά την παλαιότερη Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου. Οι κανονισμοί της Ε.Ε. δεν απαιτούν εθνική νομοθεσία για την εφαρμογή τους, ωστόσο υπάρχει η δυνατότητα έκδοσης εφαρμοστικού νόμου, ο οποίος θα παρέχει ερμηνεία σε θέματα υλοποίησης του κανονισμού.

Ο ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 έχει σκοπό να προστατεύσει **τα φυσικά πρόσωπα** έναντι της επεξεργασίας των προσωπικών τους δεδομένων και **την ελεύθερη κυκλοφορία των δεδομένων** αυτών και να **καταργήσει την οδηγία 95/46/ΕΚ**. Ρυθμίζει επίσης θέματα διαβίβασης δεδομένων εκτός Ευρωπαϊκών συνόρων. Ο Κανονισμός προστατεύει φυσικά πρόσωπα που βρίσκονται στην Ένωση, ανεξαρτήτως ιθαγένειας ή τόπου διαμονής τους.

Υπόχρεοι σε εφαρμογή του κανονισμού

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) εφαρμόζεται:

α) σε κάθε εταιρεία ή οντότητα η οποία επεξεργάζεται δεδομένα προσωπικού χαρακτήρα στο πλαίσιο των δραστηριοτήτων ενός από τα υποκαταστήματά της που έχουν έδρα στην ΕΕ, ανεξάρτητα από το πού γίνεται η επεξεργασία των δεδομένων ή

β) σε κάθε εταιρεία η οποία έχει έδρα εκτός της ΕΕ και προσφέρει αγαθά/υπηρεσίες (επί πληρωμή ή δωρεάν) ή παρακολουθεί τη συμπεριφορά φυσικών προσώπων στην ΕΕ.

Μεγάλη προσοχή !!!

Η επεξεργασία ευαίσθητων προσωπικών δεδομένων καταρχήν απαγορεύεται εκτός αν γίνεται για νόμιμους σκοπούς και κάτω από συγκεκριμένες προϋποθέσεις και εγγυήσεις

Τα παρακάτω δεδομένα προσωπικού χαρακτήρα θεωρούνται «ευαίσθητα» βάση της νέας ευρωπαικής νομοθεσίας και υπόκεινται σε συγκεκριμένες προϋποθέσεις επεξεργασίας:

- δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν φυλετική ή εθνική καταγωγή, πολιτικά φρονήματα, θρησκευτικές ή φιλοσοφικές πεποιθήσεις·
- συμμετοχή σε συνδικαλιστική οργάνωση·
- γενετικά δεδομένα, βιομετρικά δεδομένα που υποβάλλονται σε επεξεργασία αποκλειστικά για την ταυτοποίηση ενός ατόμου·
- δεδομένα σχετικά με την υγεία·
- δεδομένα σχετικά με τη σεξουαλική ζωή ή τον γενετήσιο προσανατολισμό ενός ατόμου.

Μη υπαγόμενοι σε προστασία των δεδομένων τους

- **τα νομικά πρόσωπα** και ιδίως επιχειρήσεις συσταθείσες ως νομικά πρόσωπα (δεν καλύπτει δηλαδή την επωνυμία, τον τύπο και τα στοιχεία επικοινωνίας του νομικού προσώπου).
- την επεξεργασία προσωπικών δεδομένων η οποία διενεργείται από φυσικά πρόσωπα και αποκλειστικά στα πλαίσια **προσωπικής ή οικιακής δραστηριότητας** και χωρίς σύνδεση με κάποια επαγγελματική ή εμπορική δραστηριότητα. Ωστόσο, ο παρών κανονισμός εφαρμόζεται σε υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία (αυτοί δεν είναι φυσικά πρόσωπα!), οι οποίοι παρέχουν τα μέσα επεξεργασίας δεδομένων προσωπικού χαρακτήρα για τέτοιες προσωπικές ή οικιακές δραστηριότητες
- **τους θανόντες**.

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (EU GDPR) αφορά **κάθε επιχείρηση και οργανισμό** που διατηρεί ή επεξεργάζεται προσωπικά δεδομένα φυσικών προσώπων που βρίσκονται στην Ευρώπη, ανεξαρτήτως ιθαγένειας ή τόπου διαμονής τους. Αφορά όλους τους οργανισμούς, από τις πιο μικρές εταιρίες έως τους πιο μεγάλους ομίλους, δημοσίου και ιδιωτικού δικαίου. Αφορά τόσο τους υπευθύνους επεξεργασίας, όσο και τους εκτελούντες την επεξεργασία δεδομένων (δείτε παρακάτω – data controllers και data processors).

Ο Κανονισμός **είναι σε ισχύ**. Δεν απαιτείται επιπλέον έγκριση από κυβερνήσεις κρατών. ‘Εχει ήδη ψηφιστεί από το Ευρωκοινοβούλιο τον Απρίλιο του 2016 και δημοσιεύθηκε στην εφημερίδα της ΕΕ. Δόθηκε απλώς μια 2-ετής περίοδος προσαρμογής μέχρι τις **25 Μαΐου 2018,** οπότε ο Κανονισμός τίθεται σε πλήρη εφαρμογή, καθώς και τα υψηλά πρόστιμα. Ο Γενικός Κανονισμός Προστασίας Δεδομένων δεν είναι ένας εντελώς καινούργιος νόμος. Αποτελεί μια ισχυρότερη και εκσυγχρονισμένη εκδοχή της Οδηγίας του 1995 (Data Protection Directive 95/46/EC), με τη **διαφορά** ότι τώρα ο Κανονισμός έχει **καθολική ισχύ** στα κράτη μέλη, ορίζει **αυστηρότερες απαιτήσεις** και προβλέπει **υψηλά πρόστιμα** για τους παραβάτες.

ΠΡΟΣΤΙΜΑ

Τα πρόστιμα που προβλέπει ο Γενικός Κανονισμός είναι υψηλά. Το ανώτερο ανέρχεται στα **€20.000.000** ή στο **4% του παγκόσμιου ετήσιου κύκλου εργασιών** του προηγούμενου οικονομικού έτους, εφόσον πρόκειται για επιχείρηση – όποιο είναι υψηλότερο. Το πρόστιμο αυτό δύναται να επιβληθεί σε σοβαρές παραβιάσεις του Κανονισμού, όπως: παραβιάσεις που αφορούν την συγκατάθεση του ατόμου, τις βασικές αρχές προστασίας δεδομένων, τη μεταφορά δεδομένων Ευρωπαίων πολιτών εκτός Ευρώπης, τη μη συμμόρφωση με τις υποδείξεις των Εποπτικών Αρχών. Υπάρχουν και περιπτώσεις όπου προβλέπεται πρόστιμο **€10 εκατομμύρια**, ή το **2% του παγκόσμιου ετήσιου κύκλου εργασιών** – όποιο είναι υψηλότερο – για παράδειγμα: για τη μη τήρηση οργανωμένων αρχείων, τη μη γνωστοποίηση για παραβίαση ασφαλείας, την παράλειψη ορισμού DPO στις περιπτώσεις που επιβάλλεται, την παράλειψη διενέργειας Εκτίμησης Αντικτύπου, την ατελή εφαρμογή ή απουσία τεχνικών και οργανωτικών μέτρων για την εξασφάλιση της προστασίας δεδομένων από το σχεδιασμό και εξ' ορισμού – data privacy by design and by default.

ΒΑΣΙΚΕΣ ΑΡΧΕΣ

1. **Αρχές επεξεργασίας**: α) «**Νομιμότητα, αντικειμενικότητα και διαφάνεια**», β) «**Περιορισμός του σκοπού**» δηλ. κάθε οργανισμός οφείλει να προσδιορίζει ρητά – και να είναι σε θέση να τεκμηριώσει – τους νόμιμους σκοπούς, για τους οποίους συλλέγει και επεξεργάζεται προσωπικά δεδομένα. Οφείλει επίσης να μην διενεργεί περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς, γ) «**Ελαχιστοποίηση των δεδομένων»**: τα δεδομένα που συλλέγονται οφείλουν να είναι κατάλληλα, συναφή και απολύτως αναγκαία για τους συγκεκριμένους σκοπούς που ορίστηκαν, δ) «**Ακρίβεια**», δηλ. τα δεδομένα να είναι ορθά κι επίκαιρα, ε) «**Περιορισμός περιόδου αποθήκευσης**»: να τηρούνται μόνο για όσο χρονικό διάστημα απαιτείται σύμφωνα με το νόμιμο σκοπό, στ) «**Ακεραιότητα και εμπιστευτικότητα**», να διασφαλίζεται η προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με χρήση κατάλληλων τεχνικών ή οργανωτικών μέτρων, ζ) «**Λογοδοσία**» του υπευθύνου επεξεργασίας, ο οποίος φέρει την ευθύνη και επιπλέον πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωση με τα όλα παραπάνω.
2. **Ρητή συγκατάθεση**: απαιτείται η συγκατάθεση του ατόμου, η οποία ορίζεται ως "κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν". Είναι σαφές ότι η μη αντίδραση του ατόμου, όπως π.χ. η παθητική παραμονή του σε λίστες, δεν ισοδυναμεί με συγκατάθεση, σύμφωνα με τον νέο Κανονισμό. Για προσωπικά δεδομένα ανηλίκων κάτω των 16 ετών, απαιτείται σαφής συγκατάθεση γονέα ή κηδεμόνα. Ο οργανισμός οφείλει να τηρεί αρχείο και διαδικασία η οποία να επιτρέπει στο άτομο να διαφοροποιήσει τη συγκατάθεση που έδωσε για μια συγκεκριμένη χρήση, όσες φορές αλλάξει γνώμη.
3. **Σαφής Πολιτική Απορρήτου**: οι οργανισμοί απαιτούνται να δηλώνουν με διαφάνεια, σαφή γλώσσα και κατανοητό τρόπο την πολιτική απορρήτου που εφαρμόζουν. Δηλαδή, να δηλώνουν αναλυτικά ποια δεδομένα συλλέγουν, για ποιο νόμιμο σκοπό, πώς τα διαχειρίζονται, για πόσο χρονικό διάστημα τα διατηρούν, με ποιες μεθόδους ασφαλείας τα προστατεύουν κλπ.
4. **Πλήθος νέα Ατομικά δικαιώματα**: όλα τα άτομα έχουν δικαίωμα να επεμβαίνουν στα δεδομένα τους προκειμένου να τα διορθώσουν (**Δικαίωμα Διόρθωσης**), να ζητήσουν την παραλαβή των δεδομένων τους, σε δομημένο, συμβατό και διαλειτουργικό μορφότυπο, αναγνώσιμο από μηχανήματα, προκειμένου να τα διαβιβάσουν σε άλλον υπεύθυνο επεξεργασίας (**Δικαίωμα**

στη Φορητότητα), ακόμη και τη διαγραφή (**Δικαίωμα στη Λήθη**) των προσωπικών τους δεδομένων υπό προϋποθέσεις.

5. **Ευθύνη και Λογοδοσία**: οι οργανισμοί είναι διαρκώς υπόλογοι στα άτομα και στις Αρχές. Οφείλουν, όχι απλώς να εφαρμόζουν το νέο Κανονισμό, αλλά και να είναι κάθε στιγμή σε θέση να αποδείξουν ότι συμμορφώνονται με όλες τις απαιτήσεις του.
6. **Προστασία ήδη από τον αρχικό σχεδιασμό και εξ' ορισμού** (Privacy by Design and by Default): ο οργανισμός οφείλει να εφαρμόζει αποτελεσματικά, τα κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, η ελαχιστοποίηση των δεδομένων και η ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία τους, κατά τρόπο ώστε να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων. Για παράδειγμα, πρέπει να υπάρχουν ρυθμίσεις ασφάλειας δεδομένων ενσωματωμένες στις υπηρεσίες του οργανισμού και αυτές οι ρυθμίσεις ασφαλείας να είναι κατανοητές και φιλικές προς το χρήστη, είτε πρόκειται για υπάλληλο, είτε για Πελάτη, ή εξωτερικό Συνεργάτη ή Προμηθευτή. Επίσης, πρέπει να είναι εξ' ορισμού (by default) ενεργοποιημένες οι ρυθμίσεις στην ύψιστη προστασία απορρήτου και πάντα σύμφωνα με τις αρχές της ελαχιστοποίησης και της νομιμότητας του σκοπού. Για παράδειγμα, στις "φόρμες επικοινωνίας" που υπάρχουν συνήθως στον ιστότοπο ενός οργανισμού, να συλλέγονται αυστηρά και μόνο τα δεδομένα που είναι απαραίτητα για τον νόμιμο σκοπό της επικοινωνίας και όχι περισσότερα.
7. **Ασφάλεια Επεξεργασίας**: ο οργανισμός που τηρεί και διαχειρίζεται προσωπικά δεδομένα οφείλει να εφαρμόζει τα απαραίτητα συστήματα, πολιτικές και διαδικασίες που εξασφαλίζουν τα απαιτούμενα επίπεδα προστασίας των δεδομένων αυτών, συμπεριλαμβανομένης της προστασίας από την παράνομη πρόσβαση κι επεξεργασία, τόσο από το προσωπικό του οργανισμού, όσο και από τρίτους, την κατά λάθος απώλεια, καταστροφή ή αλλοίωσή τους. Οφείλει επίσης να διασφαλίζει ότι τα δεδομένα που τηρεί είναι ορθά και επίκαιρα.
8. **Γνωστοποίηση παραβίασης εντός 72 ωρών**: Σε περίπτωση παραβίασης ασφαλείας που αφορά προσωπικά δεδομένα, οι οργανισμοί οφείλουν να ενημερώνουν εντός 72 ωρών – από τη στιγμή που αποκτούν γνώση του γεγονότος – τις αρμόδιες Αρχές. Υπό προϋποθέσεις, οφείλουν να ενημερώνουν και τα ίδια τα άτομα (Υποκείμενα) των οποίων τα προσωπικά δεδομένα έχουν τεθεί σε κίνδυνο. Οφείλουν επίσης να τηρούν αρχείο με όλα τα περιστατικά παραβίασης ασφαλείας προσωπικών δεδομένων.
9. **Εκτίμηση αντικτύπου**: οι οργανισμοί οφείλουν να διεξάγουν μελέτες εκτίμησης αντικτύπου, με σκοπό την εκτίμηση των επιπτώσεων της επεξεργασίας προσωπικών δεδομένων, τον εντοπισμό των κινδύνων ασφάλειας και τον σχεδιασμό της αντιμετώπισης αυτών.
10. **Υπεύθυνος Προστασίας Δεδομένων** (Data Protection Officer, εν συντομία "DPO"): οι οργανισμοί οφείλουν υπό προϋποθέσεις να ορίσουν έναν Υπεύθυνο Προστασίας Δεδομένων. Ο ρόλος του είναι να παρακολουθεί τη διαρκή και επαρκή συμμόρφωση του οργανισμού με τον νόμο, ενώ παράλληλα αποτελεί τον σύνδεσμο του οργανισμού με την αρμόδια εποπτική Αρχή. **Υποχρέωση για διορισμό DPO** έχουν: α) όσοι διενεργούν μεγάλης κλίμακας συστηματική επεξεργασία και παρακολούθηση, β) όσοι διενεργούν μεγάλης κλίμακας επεξεργασία ευαίσθητων προσωπικών δεδομένων και δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα, και γ) το δημόσιο. Ο DPO δύναται να είναι μέλος του προσωπικού υπό προϋποθέσεις, ή εξωτερικός Συνεργάτης, με δελτίο παροχής υπηρεσιών,
11. **Εκπαίδευση προσωπικού**: οι οργανισμοί οφείλουν να εκπαιδεύσουν το προσωπικό τους στο πως να εφαρμόζει καθημερινά την πολιτική προστασίας προσωπικών δεδομένων.

ΟΡΙΣΜΟΙ

Οποιοδήποτε στοιχείο πληροφορίας συνδέεται με ένα άτομο (Το Υποκείμενο των δεδομένων) και μπορεί να χρησιμοποιηθεί άμεσα ή έμμεσα για την ταυτοποίησή του, αποτελεί σύμφωνα με τον Κανονισμό προσωπικό δεδομένο. Μπορεί να είναι ένα όνομα, αριθμός ταυτότητας, δεδομένα θέσης, ακόμη και online ID, ή ένα ή περισσότερα στοιχεία που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα ενός φυσικού προσώπου. Υπάρχουν επίσης και οι **ειδικές κατηγορίες** προσωπικών δεδομένων, όπως η **φυλετική ή εθνική προέλευση, τα πολιτικά φρονήματα, οι θρησκευτικές ή φιλοσοφικές πεποιθήσεις, η συμμετοχή σε συνδικαλιστική οργάνωση, τα γενετικά και βιομετρικά δεδομένα, η κατάσταση της υγείας, η σεξουαλική ζωή και ο γενετήσιος προσανατολισμός του ατόμου**. Ο Κανονισμός απαγορεύει την επεξεργασία αυτών των ειδικών κατηγοριών, πλην ορισμένων περιπτώσεων και υπό συγκεκριμένες προϋποθέσεις, Επιπλέον, υπάρχει ειδική μέριμνα για την επεξεργασία προσωπικών δεδομένων που αφορούν **ποινικές καταδίκες και αδικήματα** του ατόμου. Γι' αυτό, είναι εξαιρετικά σημαντικό για την επιτυχή συμμόρφωση ενός οργανισμού, να προσδιορίζονται με ακρίβεια τα προσωπικά δεδομένα και οι ειδικότερες κατηγορίες δεδομένων που αυτός τηρεί και επεξεργάζεται. Για παράδειγμα, εάν γίνεται επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων σε μεγάλη κλίμακα, τότε ο οργανισμός οφείλει να διορίσει Υπεύθυνο Προστασίας Δεδομένων (DPO), όπως εξηγείται παρακάτω.

Επεξεργασία σημαίνει κάθε εργασία, τόσο με αυτοματοποιημένα ή ψηφιακά μέσα, όσο και με χειροκίνητα ή φυσικά μέσα (π.χ. φυσική αρχειοθήκη), που αφορά σε προσωπικά δεδομένα, όπως: συλλογή, καταγραφή, οργάνωση, διατήρηση, αποθήκευση, ολική ή μερική διόρθωση, ενημέρωση, τροποποίηση, εξαγωγή, χρήση, μεταβίβαση, διάδοση, συσχετισμός, διασύνδεση, δέσμευση, διαγραφή, καταστροφή.

Υπεύθυνος Επεξεργασίας - Data Controller

Εκτελών την Επεξεργασία - Data Processor

Ο Υπεύθυνος Επεξεργασίας (data controller) είναι η οντότητα (το φυσικό ή νομικό πρόσωπο δημοσίου ή ιδιωτικού δικαίου) που καθορίζει το σκοπό, τις προϋποθέσεις και τον τρόπο επεξεργασίας προσωπικών δεδομένων. Για παράδειγμα, Υπεύθυνος Επεξεργασίας είναι κάθε εταιρία, σωματείο, σύλλογος κλπ. που τηρεί προσωπικά δεδομένα τουλάχιστον ενός φυσικού προσώπου: των Υπαλλήλων **ή των υποψηφίων Υπαλλήλων της**, των Μελών, Πελατών, Προμηθευτών, Συνεργατών και Συμβούλων της, κλπ. Ο Εκτελών την Επεξεργασία (data processor) είναι αντίστοιχα η οντότητα που επεξεργάζεται προσωπικά δεδομένα **για λογαριασμό** του Υπευθύνου Επεξεργασίας. Στο ως άνω παράδειγμα, Εκτελών την Επεξεργασία είναι μεταξύ άλλων και ο Πάροχος ηλεκτρονικού ταχυδρομείου της εταιρίας, καθώς επεξεργάζεται και προσωπικά δεδομένα φυσικών προσώπων (π.χ. τα προσωπικά δεδομένα που υπάρχουν σε αφθονία μέσα στα βιογραφικά σημειώματα που οι υποψήφιοι αποστέλλουν στην εταιρία). Λέγοντας οντότητα, εννοούμε νομικό πρόσωπο του δημόσιου ή ιδιωτικού τομέα.

DATA PROTECTION OFFICER DPO

Οι παρακάτω οργανισμοί υποχρεούνται να διορίσουν DPO

Κάθε δημόσιος οργανισμός και ΔΕΚΟ, εκτός από δικαστήρια που ενεργούν στα πλαίσια της δικαιοδοσίας τους.

Κάθε οργανισμός του οποίου η βασική δραστηριότητα συνιστά:

I. **τακτική** και **συστηματική παρακολούθηση** φυσικών προσώπων (Υποκειμένων των δεδομένων) **σε μεγάλη κλίμακα**, ή
II. **μεγάλης κλίμακας** επεξεργασία **ειδικών** κατηγοριών προσωπικών δεδομένων : φυλετική ή εθνοτική καταγωγή, πολιτικά φρονήματα, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, συμμετοχή σε συνδικαλιστική οργάνωση, γενετικά ή βιομετρικά δεδομένα με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένα που αφορούν την υγεία, τη σεξουαλική ζωή και τον γενετήσιο προσανατολισμό φυσικού προσώπου, ή
III. **μεγάλης κλίμακας** επεξεργασία δεδομένων που αφορούν **ποινικές καταδίκες** και **αδικήματα**.

Παραδείγματα οργανισμών που έχουν υποχρέωση διορισμού DPO: Εταιρίες Τηλεπικοινωνιών, Πάροχοι ηλεκτρονικού ταχυδρομείου, εταιρίες Μισθοδοσίας, Ασφαλιστικές, Τράπεζες, υπηρεσιών Υγείας, Σωματεία, Οργανώσεις κλπ.

DPO μπορεί να οριστεί και υπάλληλος της οντότητας αλλά υπό την **προϋπόθεση ότι ΔΕΝ** υπάρχει σύγκρουση συμφερόντων. Αν ο ρόλος ενός υπαλλήλου στην εταιρεία περιλαμβάνει και το να ορίζει το σκοπό ή την μέθοδο επεξεργασίας προσωπικών δεδομένων, τότε αυτός ο υπάλληλος δεν πρέπει να διορισθεί DPO της εταιρίας. Συνήθως, σύγκρουση συμφερόντων παρατηρείται στις εξής θέσεις – αλλά όχι μόνο: CEO, COO, Επικεφαλής IT, HR, Οικονομικών, Marketing, κλπ. Αυτά αποτελούν ενδεικτικά μόνο παραδείγματα. Στην πραγματικότητα, η σύγκρουση συμφερόντων, σε ποιες βαθμίδες και σε ποιες θέσεις υπάρχει, εξαρτάται από την οργανωτική διάρθρωση της εκάστοτε εταιρείας.

ΑΛΛΑΓΕΣ ΣΕ ΣΧΕΣΗ ΜΕ ΤΗΝ ΗΔΗ ΙΣΧΥΟΥΣΑ ΟΔΗΓΙΑ (95/46/ΕΚ)

Κατ' αρχήν, ένας Κανονισμός έχει δεσμευτική ισχύ για όλα τα κράτη μέλη, ενώ μια Οδηγία είναι απλώς μια οδηγία, δηλαδή ένας «στόχος σύγκλισης» τον οποίο τα κράτη μέλη καλούνται να επιτύχουν, το καθένα όμως με την δική του, επιμέρους νομοθεσία. Είναι φανερό ότι μέχρι σήμερα, η Οδηγία άφηνε περιθώρια για επιμέρους ερμηνείες. Τώρα όμως, ο Γενικός Κανονισμός έχει καθολική ισχύ, ακόμη και στα πρόστιμα. Καταργεί την προηγούμενη και μέχρι τώρα ισχύουσα Οδηγία 95/46/ΕΚ. Η καθολική ισχύς του Κανονισμού αποτρέπει την δημιουργία «νομοθετικών παραδείσων» ανάμεσα στα κράτη μέλη της Ευρωπαϊκής ένωσης, όπου εκεί η νομοθεσία θα είχε μια πιο «χαλαρή» εφαρμογή, ευνοώντας τους παραβάτες. Συνοπτικά, ο νέος Κανονισμός διαφέρει στα εξής βασικά σημεία από την Οδηγία:

1. έχει **καθολική ισχύ** σε όλα τα κράτη μέλη, χωρίς να απαιτείται έγκριση από τα κοινοβούλιά τους
2. έχει **ευρύτερο πεδίο εφαρμογής** (ευρύτερη ερμηνεία προσωπικών δεδομένων, καθώς και εδαφική κάλυψη)
3. εισάγει **νέα δικαιώματα** για τα φυσικά πρόσωπα (Υποκείμενα των δεδομένων): Δικαίωμα διόρθωσης , Δικαίωμα στη Λήθη, Δικαίωμα περιορισμού της επεξεργασίας, Υποχρέωση γνωστοποίησης αλλαγής, Δικαίωμα Φορητότητας.
4. είναι **πιο αυστηρός** και **πιο σαφής** με στόχο την αποτελεσματική προστασία των προσωπικών δεδομένων. Ενδεικτικά, εισάγει και ρυθμίζει με πολύ αυστηρό τρόπο την **συγκατάθεση** του ατόμου, ως θετική ενέργεια, απαιτεί να τηρούνται **πάντα οι αρχές** και να ισχύει οπωσδήποτε **μία από τις προϋποθέσεις νομιμότητας**, η πιο κατάλληλη για κάθε περίσταση.
5. αναθέτει ξεκάθαρα πλέον την ευθύνη διαρκούς συμμόρφωσης και απόδειξης της συμμόρφωσης στα νομικά πρόσωπα (στους υπεύθυνους επεξεργασίας).
6. προβλέπει **υψηλά πρόστιμα**, που θα επιβάλλονται στους παραβάτες.

Η προετοιμασία για τον GDPR είναι σημαντική και αποτελεί ένα μεγάλο βήμα προς την μελλοντική νομική εξασφάλιση της εταιρίας σου. Παράλληλα, είναι μια διαδικασία που θα απαιτήσει τη συνεχή παρακολούθηση και προστασία των δεδομένων.

Μην ξεχνάτε

Η συμμόρφωση προς τον κανονισμό προκειμένου να είναι δυνατή η απόδειξη εφαρμογής του προϋποθέτει όχι μόνο την εφαρμογή πολιτικής διασφάλισης του απορρήτου **αλλά και την καταγραφή αυτής σε εγχειρίδιο διαδικασιών** το οποίο η υπόχρεοι θα πρέπει να διαθέτουν και να θέτουν ενώπιον των αρχών σε κάθε περίπτωση ελέγχου.

Με αίσθημα ευθύνης παρέχουμε ολοκληρωμένες υπηρεσίες

ΟΔΗΓΟΣ ΠΡΟΕΤΟΙΜΑΣΙΑΣ

1. Ενημερώσου σχετικά με τον GDPR

Ο GDPR θα έχει αντίκτυπο στις εταιρίες που διατηρούν και επεξεργάζονται δεδομένα, οπότε αν η επιχείρησή σου κρατάει τα δεδομένα των πελατών, είναι καλό να ενημερωθείς σχετικά. Αρχικά θα χρειαστεί να αντιληφθείς πλήρως τους ορισμούς των προσωπικών δεδομένων που αναφέραμε παραπάνω, αλλά και τους περιορισμούς του Κανονισμού και έπειτα να εντοπίσεις τις αλλαγές που πρέπει να γίνουν στην εταιρία σου, ώστε να αρχίσεις να προσαρμόζεσαι στις νέες διατάξεις.

2. Χαρτογράφησε τα δεδομένα που λαμβάνεις και επεξεργάζεσαι

Το να αντιληφθείς ποια δεδομένα ορίζονται ως προσωπικά και το να βρεις πού και πώς αποθηκεύεις αυτά τα στοιχεία είναι δυο διαφορετικά πράγματα. Οι περισσότερες εταιρίες δεν αντιλαμβάνονται τις μισές πληροφορίες που αποθηκεύουν – οι πληροφορίες αυτές χαρακτηρίζονται ως “dark” data.

Αρχικό σου μέλημα είναι η εύρεση καθώς και η χαρτογράφηση των προσωπικών δεδομένων, ώστε να γνωρίζεις ανά πάσα στιγμή πού βρίσκονται και πώς καταλήγουν εκεί.

Μπορείς να ξεκινήσεις την έρευνα από:

- το site σου (για παράδειγμα, οι χρήστες του WordPress πρέπει να τσεκάρουν τα plugin τους όπως το Akismet και τις φόρμες επικοινωνίας)
- τα ηλεκτρονικά αρχεία που διατηρείς, όπως βάσεις δεδομένων σε excel, πληροφορίες σε pdf, ακόμα και αρχεία που αποθηκεύονται στο cloud
- και τέλος συνιστάται προσοχή στα:
- email & email marketing software
- social media
- messaging apps, όπως το Facebook
- managment software της εταιρίας

Αφού εντοπίσεις όλα τα δεδομένα που αποθηκεύεις, οργάνωσε ένα αρχείο με αυτά και διάγραψε ό,τι δεν χρειάζεται πλέον.

3. Επικοινωνία με τον πελάτη

Επικοινώνησε την πολιτική απορρήτου με απλή γλώσσα. Δώσε στους πελάτες σου όλες τις απαραίτητες πληροφορίες όταν ζητάς τα προσωπικά τους δεδομένα: τον σκοπό για τον οποίο τα επεξεργάζεσαι, για πόσο καιρό θα τα κρατήσεις και ποιος άλλος έχει τη δυνατότητα να τα επεξεργαστεί.

4. Δικαιώματα του πολίτη που είναι υποκείμενο επεξεργασίας δεδομένων

Τα προσωπικά δεδομένα θεωρούνται ένα πολύτιμο περιουσιακό στοιχείο και για τον λόγο αυτό ο GDPR δίνει τον έλεγχο στους πολίτες για τη διαχείριση αυτών. Τα δικαιώματα των πολιτών σχετικά με τα δεδομένα τους περιλαμβάνουν:

- την σωστή πληροφόρηση για την επεξεργασία τους
- την ανεμπόδιστη πρόσβαση του ιδιοκτήτη σε αυτά
- την άμεση διόρθωσή τους όταν παρατηρηθεί λάθος
- την διαγραφή τους όταν δεν είναι πια απαραίτητα
- την μεταφορά τους όταν το επιθυμεί ο ιδιοκτήτης
- το δικαίωμα στην ένσταση όταν αυτά χρησιμοποιούνται αθέμιτα
- τους περιορισμούς στην επεξεργασία τους

Η διαδικασία που επιτρέπει τις παραπάνω λειτουργίες θα πρέπει να είναι απλή και προσιτή στον πολίτη.

5. Πρόσεξε τις νομικές σου υποχρεώσεις
Όπως είδαμε παραπάνω, ένας πελάτης έχει το δικαίωμα να ζητήσει διαγραφή των προσωπικών του δεδομένων. Ταυτόχρονα, εσύ σαν επαγγελματίας ίσως χρειάζεται να διατηρείς κάποια από αυτά. Ένα χαρακτηριστικό παράδειγμα τέτοιας περίπτωσης είναι η διατήρηση ενός αρχείου πληρωμών για φορολογικούς λόγους, για ένα συγκεκριμένο χρονικό διάστημα. Από τη στιγμή που έχεις νομική υποχρέωση απέναντι σε φορολογικούς φορείς, μπορείς να διαγράψεις όλα τα στοιχεία του πελάτη εκτός από αυτά που χρειάζεσαι για το φορολογικό σου αρχείο και τα οποία δεν μπορείς να επεξεργαστείς για άλλους σκοπούς.
Υπάρχουν διάφοροι λόγοι που σε υποχρεώνουν νομικά να διατηρείς αρχείο με προσωπικά δεδομένα, οπότε φρόντισε να ενημερωθείς γι' αυτούς και στη συνέχεια να ενημερώσεις και τους πελάτες σου σχετικά.

6. Διαρροή δεδομένων
Σε περίπτωση παραβίασης των συστημάτων σου και διαρροής προσωπικών δεδομένων οφείλεις να γνωστοποιήσεις το γεγονός εντός 72 ωρών τις αρμόδιες Αρχές αλλά και στα ενδιαφερόμενα άτομα, εφόσον η παραβίαση αυτή μπορεί να αποτελέσει ρίσκο για τα δικαιώματα και τις ελευθερίες τους.

7. Προστάτευσε τα ευαίσθητα δεδομένα
Χρησιμοποίησε πρόσθετα μέτρα προστασίας για πληροφορίες που αφορούν την υγεία, τη φυλή, τον σεξουαλικό προσανατολισμό, τη θρησκεία και τις πολιτικές πεποιθήσεις. Σε αυτές τις περιπτώσεις θα χρειαστεί να πάρεις ειδική συγκατάθεση για την επεξεργασία των δεδομένων. Ενημέρωσε το κοινό σου σχετικά και διαβεβαίωσέ τους για την ασφάλεια των προσωπικών τους δεδομένων.

8. Όρισε έναν Υπεύθυνο Προστασίας Δεδομένων
Σε μερικές περιπτώσεις είναι αναγκαίος ο καθορισμός ενός Υπεύθυνου Προστασίας Δεδομένων (Data Protection Officer), κυρίως για τις δημόσιες αρχές, τους οργανισμούς που παρακολουθούν συστηματικά δεδομένα σε μεγάλη κλίμακα και τους οργανισμούς που παρακολουθούν ευαίσθητα δεδομένα σε μεγάλη κλίμακα ή επεξεργάζονται ποινικά μητρώα.

9. Διαβίβαση δεδομένων εκτός της Ε.Ε.
Η μεταφορά δεδομένων σε χώρες εκτός Ε.Ε. πρέπει να γίνεται υπό συγκεκριμένες προϋποθέσεις. Πριν διαβιβάσεις τα δεδομένα κάποιου πελάτη σου σε χώρα εκτός της Ε.Ε., σύναψε μαζί του μια συμφωνία, ώστε να καλυφθείς νομικά.

10. Διαμοιρασμός δεδομένων σε συνεργάτες
Οι συνεργάτες που εκτελούν εκ μέρους σου ενέργειες σχετιζόμενες με προσωπικά δεδομένα πελατών (όπως π.χ. ηλεκτρονικές πληρωμές) πρέπει να συμβαδίζουν με τους κανόνες του GDPR. Επανεξέτασε τις συνεργασίες σου, ελέγχοντας τις προθέσεις τους γύρω από τον κανονισμό και αν δεν έχουν ξεκινήσει να λαμβάνουν μέτρα για διαδικασίες συμμόρφωσης, ψάξε για άλλες εναλλακτικές.