Προετοιμασία για τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) σε 12 βήματα

Το παρόν κείμενο βασίστηκε σε έγγραφο οδηγιών του Γραφείου της Επιτρόπου για την Προστασία Δεδομένων του Ηνωμένου Βασιλείου (ICO), μίας εκ των πλέον δραστήριων εποπτικών αρχών για την προστασία δεδομένων στην Ευρωπαϊκή Ένωση. Σκοπός του κειμένου δεν είναι η παροχή νομικών συμβουλών, αλλά η ενημέρωση των πολιτών και των επιχειρήσεων, ειδικά των πολύ μικρών, των μικρών και των μεσαίων, σε σχέση με ορισμένα βασικά σημεία του Γενικού Κανονισμού για την Προστασία των Δεδομένων.

Μετάφραση - Επιμέλεια: Μαρία Κακαβά, Φοιτήτρια Νομικής Σχολής ΕΚΠΑ

Βασίλης Καρκατζούνης, Δικηγόρος, CIPP/E

Εισαγωγή

Ο παρών οδηγός περιλαμβάνει 12 βήματα που μπορείτε να κάνετε με σκοπό τη συμμόρφωση προς τις διατάξεις του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR), ο οποίος τέθηκε σε εφαρμογή στις 25 Μαΐου 2018.

Πολλές από τις βασικές έννοιες και αρχές του GDPR είναι οι ίδιες με αυτές του ισχύοντος νόμου περί προστασίας δεδομένων (Νόμος 2472/1997). Επομένως, εάν συμμορφώνεστε ορθά με τον προϊσχύοντα νόμο, τότε οι πρακτικές σας θα παραμείνουν, κατά ένα μεγάλο μέρος τους, σύμφωνες με τις διατάξεις του GDPR, αποτελώντας το σημείο εκκίνησης για περαιτέρω πρόοδο. Ωστόσο, υπάρχουν ορισμένα νέα στοιχεία και σημαντικές βελτιώσεις ως προς την προστασία δεδομένων στον GDPR, συνεπώς θα πρέπει να προβείτε σε ορισμένες ενέργειες για πρώτη φορά, αλλά και να κάνετε κάποια πράγματα τελείως διαφορετικά απ' ό,τι μέχρι σήμερα.

Χρησιμοποιήστε την παρούσα λίστα καθώς και τις οδηγίες που εκδίδουν οι ευρωπαϊκές αρχές για την προστασία δεδομένων, προκειμένου να

κατανοήσετε τις κύριες διαφορές μεταξύ του ισχύοντος πλαισίου και του GDPR. Είναι σημαντικό να σχεδιάσετε το συντομότερο δυνατό την συμμόρφωσή σας προς τις προβλέψεις του GDPR, και να εξασφαλίσετε το συντονισμό βασικών στελεχών του οργανισμού σας. Για παράδειγμα, μπορεί να χρειαστεί να θέσετε σε εφαρμογή νέες διαδικασίες για να αντεπεξέλθετε στις νέες απαιτήσεις διαφάνειας και της προστασίας των δικαιωμάτων των προσώπων που περιλαμβάνονται στον GDPR. Σε μια μεγάλη ή σύνθετη επιχείρηση αυτό θα μπορούσε να έχει σημαντικές επιπτώσεις από πλευράς προϋπολογισμού, αξιοποίησης συστημάτων πληροφορικής, προσωπικού, εταιρικής διακυβέρνησης και marketing.

Ο GDPR δίνει μεγάλη έμφαση στα έγγραφα που οφείλουν να κατέχουν οι υπεύθυνοι επεξεργασίας προκειμένου να αποδείξουν τον βαθμό συμμόρφωσής τους (τεκμηρίωση).

Το παρόν έγγραφο έχει ως στόχο να παρέχει στους οργανισμούς μία πρώτη εικόνα σχετικά με τις παραμέτρους που πρέπει να ληφθούν υπόψη για τη συμμόρφωση με το νέο πλαίσιο για την προστασία δεδομένων, οδηγώντας τους στην επανεξέταση της προσέγγισής τους αναφορικά με τις μεθόδους επεξεργασίας προσωπικών δεδομένων.

Μια πτυχή αυτού του ζητήματος ενδέχεται να είναι και η αναθεώρηση των συμβάσεων ή και άλλων ρυθμίσεων που έχουν εφαρμόσει κατά την ανταλλαγή δεδομένων με άλλους οργανισμούς.

Ορισμένα τμήματα του GDPR θα έχουν μεγαλύτερο αντίκτυπο σε ορισμένους οργανισμούς απ' ότι σε άλλους (π.χ. πληροφορίες σχετικά με την κατάρτιση προφίλ ή δεδομένα ανηλίκων), συνεπώς θα ήταν χρήσιμο να καταγράψετε ποια κομμάτια του GDPR θα έχουν τον μεγαλύτερο αντίκτυπο στο δικό σας επιχειρηματικό μοντέλο και να δώσετε ιδιαίτερη σημασία σε αυτά κατά τον σχεδιασμό σας.

1. Ενημέρωση

Θα πρέπει να φροντίσετε να ενημερωθούν για τις ρυθμίσεις του νέου Κανονισμού και τις αλλαγές που συνεπάγεται, όλοι όσοι λαμβάνουν αποφάσεις και στελεχώνουν θέσεις-κλειδιά στον οργανισμό σας. Θα πρέπει να συνειδητοποιήσουν τις επιπτώσεις του και να βρουν σε ποιους τομείς ενδέχεται να παρουσιαστεί πρόβλημα συμμόρφωσης με αυτόν. Χρήσιμο θα ήταν να ξεκινούσατε ανατρέχοντας στο αρχείο καταγραφής και διαχείρισης κινδύνων, εάν φυσικά διαθέτει τέτοιο ο οργανισμός σας. Η εφαρμογή του GDPR ενδέχεται να έχει σημαντικές επιπτώσεις στους πόρους ενός μεγάλου και σύνθετου οργανισμού.

Η συμμόρφωση με τον Κανονισμό θα είναι πιο δύσκολη, εάν αφήσετε τις προετοιμασίες σας την τελευταία στιγμή.

2. Πληροφορίες που βρίσκονται στην κατοχή σας

Θα πρέπει να καταγράψετε όσα προσωπικά δεδομένα κατέχετε, από πού προήλθαν, και με ποιόν τα μοιράζεστε. Ενδέχεται να χρειαστεί να οργανώσετε έναν έλεγχο πληροφοριών που θα αφορά ολόκληρο τον οργανισμό σας ή και μόνο ορισμένους τομείς της επιχείρησης.

Ο Κανονισμός επιτάσσει να τηρείτε αρχείο με όλες τις πράξεις επεξεργασίας δεδομένων που πραγματοποιείτε. Αναβαθμίζει έτσι την προστασία των ατομικών δικαιωμάτων σε έναν "ψηφιακό κόσμο". Για παράδειγμα, εάν έχετε μοιραστεί ανακριβή προσωπικά δεδομένα με ένα άλλο οργανισμό, θα πρέπει να τον ενημερώσετε σχετικά, ούτως ώστε να διορθώσει τα αρχεία του. Αυτό όμως δεν θα είναι εφικτό, εάν δεν γνωρίζετε τι είδους δεδομένα κατέχετε, από πού προήλθαν και με ποιόν τα μοιράζεστε. Θα πρέπει, λοιπόν, να τηρείτε ένα σχετικό αρχείο. Αυτό θα σας βοηθήσει να συμμορφωθείτε με την «αρχή της λογοδοσίας» του Κανονισμού, σύμφωνα με την οποία όλοι οι

οργανισμοί θα πρέπει να είναι σε θέση να αποδεικνύουν με ποιους τρόπους συμμορφώνονται με τις αρχές προστασίας δεδομένων, π.χ. θέτοντας σε εφαρμογή αποτελεσματικές πολιτικές και διαδικασίες.

3. Πληροφορίες σχετικά με την προστασία δεδομένων

Θα πρέπει να ελέγξετε τις τρέχουσες πολιτικές απορρήτου του οργανισμού σας (privacy policies) και να καταρτίσετε ένα σχέδιο, προκειμένου να πραγματοποιήσετε όλες τις απαραίτητες αλλαγές, έως ότου αρχίσει να εφαρμόζεται ο GDPR.

Προς το παρόν, όταν συλλέγετε προσωπικά δεδομένα οφείλετε να δίνετε στα υποκείμενα των δεδομένων ορισμένα στοιχεία σας, όπως η ταυτότητά σας, και ο τρόπος με τον οποίο σκοπεύετε να χρησιμοποιήσετε τα δεδομένα τους. Αυτό γίνεται συνήθως μέσω μιας ειδοποίησης απορρήτου.

Με την εφαρμογή του GDPR θα πρέπει να παρέχετε και κάποιες ακόμα πληροφορίες στα υποκείμενα.

Για παράδειγμα, θα χρειαστεί να αναφέρετε την νομική βάση που έχετε για την επεξεργασία των δεδομένων τους, την περίοδο αποθήκευσης των δεδομένων, καθώς και ότι έχουν το δικαίωμα να προσφύγουν στην ΑΠΔΠΧ, εφόσον θεωρήσουν ότι υπάρχει κάποιο πρόβλημα με τον τρόπο που χειρίζεστε τα δεδομένα τους.

Ο Κανονισμός επιτάσσει οι εν λόγω πληροφορίες να παρέχονται με καθαρή, απλή, και συνοπτική διατύπωση.

4. Δικαιώματα υποκειμένων των δεδομένων

Θα πρέπει να ελέγξετε τις διαδικασίες σας για να βεβαιωθείτε πως καλύπτουν όλα τα δικαιώματα που έχουν τα φυσικά πρόσωπα, συμπεριλαμβανομένου του τρόπου διαγραφής προσωπικών δεδομένων ή παροχής προσωπικών δεδομένων ηλεκτρονικά, στην μορφή που χρησιμοποιείται συνήθως. Ο Κανονισμός περιλαμβάνει τα ακόλουθα δικαιώματα των προσώπων:

- δικαίωμα ενημέρωσης
- δικαίωμα πρόσβασης
- δικαίωμα διόρθωσης
- δικαίωμα διαγραφής («δικαίωμα στην λήθη»)
- δικαίωμα περιορισμού της επεξεργασίας
- δικαίωμα στην φορητότητα των δεδομένων
- δικαίωμα εναντίωσης και
- το δικαίωμα να μην λαμβάνεται καμία απόφαση που τα αφορά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ.

Γενικά, τα δικαιώματα που απολαμβάνουν τα υποκείμενα υπό τον νέο Κανονισμό θα είναι τα ίδια με εκείνα που απολάμβαναν υπό το παλαιό καθεστώς, αλλά με κάποιες σημαντικές βελτιώσεις. Εάν προσανατολίζεστε ήδη προς μια κατεύθυνση παροχής αυξημένων δικαιωμάτων στα υποκείμενα, τότε η μετάβαση στον Κανονισμό θα είναι σχετικά εύκολη. Τώρα είναι μια καλή στιγμή για να ελέγξετε τις διαδικασίες που εφαρμόζετε, και για να σχεδιάσετε π.χ. πώς θα δράσετε εάν ένα υποκείμενο ζητήσει να διαγραφούν τα δεδομένα του. Θα σας βοηθούσε το σύστημά σας να

εντοπίσετε και να διαγράψετε τα σχετικά δεδομένα; Ποιος θα είναι ο υπεύθυνος για την λήψη της σχετικής απόφασης;

Το δικαίωμα στην φορητότητα των δεδομένων είναι καινούργιο. Εφαρμόζεται μόνο:

- σε προσωπικά δεδομένα που ένα υποκείμενο έχει παράσχει σε υπεύθυνο επεξεργασίας
- όπου η επεξεργασία είναι βασισμένη στην συγκατάθεση του υποκειμένου ή για την εκτέλεση μιας σύμβασης και
- όταν η επεξεργασία διενεργείται με αυτοματοποιημένα μέσα.

Δείτε τις κατευθυντήριες γραμμές της Ομάδας Εργασίας του άρθρου 29 σχετικά με το δικαίωμα στη φορητότητα των δεδομένων.

Θα πρέπει να αναλογιστείτε εάν είναι απαραίτητο να αναβαθμίσετε τις διαδικασίες σας ή να πραγματοποιήσετε αλλαγές. Θα χρειαστεί να παράσχετε τα προσωπικά δεδομένα σε δομημένο, κοινώς χρησιμοποιούμενο, αναγνώσιμο από μηχανήματα μορφότυπο, και χωρίς χρέωση.

> Δείτε το infographic του Lawspot σχετικά με τα δικαιώματα που προβλέπονται στον GDPR εδώ.

5. Αιτήματα πρόσβασης

Θα πρέπει να αναβαθμίσετε τις διαδικασίες σας και να σχεδιάσετε πώς θα χειριστείτε τα νέα αιτήματα για άσκηση δικαιωμάτων εκ μέρους των υποκειμένων των δεδομένων, λαμβάνοντας υπόψη τους νέους κανόνες:

- Στις περισσότερες περιπτώσεις δεν θα μπορείτε να επιβάλλετε κάποια χρέωση προκειμένου να ανταποκριθείτε στα αιτήματα
- Θα έχετε στην διάθεσή σας ένα μήνα για να ανταποκριθείτε στα αιτήματα
- Έχετε το δικαίωμα να αρνηθείτε να παράσχετε πρόσβαση εάν τα αιτήματα είναι προδήλως αβάσιμα ή υπερβολικά
- Εάν αρνηθείτε το αίτημα θα πρέπει να αιτιολογήσετε την άρνησή σας στον αιτούντα και να τον ενημερώσετε, δίχως υπερβολική καθυστέρηση (και σε κάθε περίπτωση μέσα σε ένα μήνα) πως έχει το δικαίωμα να προσφύγει στην εποπτική αρχή ή να ζητήσει δικαστική προστασία.

Εάν ο οργανισμός σας χειρίζεται μεγάλο αριθμό αιτημάτων, καλό θα ήταν να φροντίσετε να επιταχύνετε τις σχετικές διαδικασίες. Ενδεχομένως να είναι πιο αποτελεσματική η διαδικασία, εάν τα υποκείμενα έχουν πρόσβαση στα δεδομένα τους μέσω του διαδικτύου.

6. Νομική βάση για την επεξεργασία προσωπικών δεδομένων

Θα πρέπει να προσδιορίσετε την νομική βάση για τη επεξεργασία δεδομένων που πραγματοποιείτε στον GDPR, να την καταγράψετε και να αναβαθμίσετε την πολιτική απορρήτου σας, έτσι ώστε να την εξηγεί επαρκώς.

Πολλοί οργανισμοί δεν έχουν εξετάσει τη νομική βάση για την επεξεργασία προσωπικών δεδομένων που πραγματοποιούν. Με το παλαιό νομοθετικό καθεστώς αυτό δεν είχε σημαντικές συνέπειες στην πράξη. Ωστόσο, δεν ισχύει το ίδιο υπό το καθεστώς του GDPR, καθώς τα δικαιώματα των υποκειμένων θα τροποποιούνται ανάλογα με την νομική βάση που επικαλείστε για την επεξεργασία των δεδομένων τους. Το πιο προφανές παράδειγμα είναι ότι θα ισχυροποιηθεί το δικαίωμα των υποκειμένων στην

διαγραφή των δεδομένων τους, στις περιπτώσεις όπου νομική βάση είναι η συγκατάθεσή τους.

Επίσης, θα πρέπει να εξηγείτε την νομική βάση προς επεξεργασία προσωπικών δεδομένων στην πολιτική απορρήτου σας, καθώς και όταν εξετάζετε το αίτημα πρόσβασης ενός υποκειμένου. Οι νομικές βάσεις επεξεργασίας στον GDPR είναι σε γενικές γραμμές οι ίδιες με αυτές προέβλεπε η έως τώρα νομοθεσία. Λογικά, η διαδικασία κατηγοριοποίησης των ειδών επεξεργασίας που πραγματοποιείτε έως τώρα, και η αναζήτηση των νομικών βάσεών τους δεν θα είναι ιδιαίτερα απαιτητική. Μια τέτοια κατηγοριοποίηση θα σας βοηθήσει να συμμορφωθείτε με τις προϋποθέσεις λογοδοσίας του GDPR.

7. Συγκατάθεση

Θα πρέπει να επανεξετάσετε τον τρόπο με τον οποίο ζητάτε, καταγράφετε και διαχειρίζεστε τη συγκατάθεση και εάν κριθεί αναγκαίο να κάνετε αλλαγές. Φροντίστε να λάβετε εκ νέου όποια συγκατάθεση δεν πληροί τις προϋποθέσεις του GDPR.

Η συγκατάθεση των υποκειμένων θα πρέπει να είναι ελεύθερη, συγκεκριμένη, ρητή, και να παρέχεται ύστερα από ενημέρωσή τους σχετικά με την επικείμενη επεξεργασία των δεδομένων τους. Θα πρέπει να εκφράζεται με θετικό τρόπο - η συγκατάθεση δεν μπορεί να συναχθεί από την σιωπή του υποκειμένου, από προ-συμπληρωμένα τετραγωνίδια, ή από την αδράνειά του. Επίσης, θα πρέπει να τίθεται ξεχωριστά από άλλους όρους και προϋποθέσεις, επίσης, θα χρειαστεί να παρέχετε μια εύκολη διαδικασία απόσυρσης της συγκατάθεσης των υποκειμένων. Ιδιαίτερη προσοχή θα πρέπει να δείξουν οι δημόσιες αρχές και οι εργοδότες. Άλλωστε, θα πρέπει να μπορεί εύκολα να διαπιστωθεί η παροχή της, καθώς γενικά τα υποκείμενα έχουν περισσότερα

δικαιώματα όταν απαιτείται συγκατάθεση για την επεξεργασία των δεδομένων τους.

Δεν είστε υποχρεωμένοι να αναδιοργανώσετε αυτόματα, ή να ανανεώσετε όλες τις συγκαταθέσεις που σας έχουν δοθεί για επεξεργασία δεδομένων, προκειμένου να είστε συμμορφωμένοι με τον GDPR. Ωστόσο, εάν βασίζεστε στη συγκατάθεση των υποκειμένων προκειμένου να επεξεργαστείτε τα δεδομένα τους, φροντίστε να τηρείτε τα πρότυπα του GDPR, έτσι ώστε να είναι συγκεκριμένη, λεπτομερής, σαφής, εμφανής, κατάλληλα καταγεγραμμένη και μπορεί να ανακληθεί εύκολα. Εάν δεν βασίζεστε σε αυτήν για την επεξεργασία σας, αλλάξτε τον μηχανισμό συγκατάθεσης που χρησιμοποιείτε και αναζητήστε έναν νέο, σύμφωνο με τον GDPR ή βρείτε μια εναλλακτική λύση για τη νομική σας βάση.

Δείτε το infographic του Lawspot σχετικά με τη συγκατάθεση στον GDPR εδώ.

8. Ανήλικοι

Θα πρέπει να εξετάσετε κατά πόσο θα πρέπει να θέσετε σε εφαρμογή συστήματα επαλήθευσης της ηλικίας των χρηστών, και λήψης της συγκατάθεσης των γονέων ή των κηδεμόνων τους για οποιαδήποτε δραστηριότητα επεξεργασίας δεδομένων.

Για πρώτη φορά, ο νέος Κανονισμός θα προσφέρει ειδική προστασία για τα προσωπικά δεδομένα των ανηλίκων, ιδίως στο πλαίσιο εμπορικών υπηρεσιών του διαδικτύου, όπως τα μέσα κοινωνικής δικτύωσης. Εάν ο οργανισμός σας παρέχει διαδικτυακές υπηρεσίες («υπηρεσίες της κοινωνίας της πληροφορίας») σε ανήλικους, και στηρίζεται στην λήψη συγκατάθεσης

προκειμένου να συγκεντρώσει πληροφορίες για αυτούς, τότε θα χρειαστείτε την συγκατάθεση ενός γονέα ή κηδεμόνα για να επεξεργαστείτε νομίμως τα προσωπικά τους δεδομένα.

Ο νέος Κανονισμός ορίζει τον τρόπο με τον οποίο ένας ανήλικος μπορεί να δώσει ο ίδιος την εν λόγω συγκατάθεση για επεξεργασία, εάν έχει συμπληρώσει το 16ο έτος της ηλικίας του. Εάν ένα παιδί είναι μικρότερο, θα πρέπει να λάβετε την συγκατάθεση ενός ατόμου που έχει την γονική του μέριμνα (Σημαντική σημείωση: το όριο θα τεθεί ανάμεσα στα 16 και 13 έτη από εθνική νομοθεσία των κρατών-μελών. Με βάση το ελληνικό σχέδιο νόμου, η ηλικία αυτή θα είναι τα 15 έτη).

Αυτό θα μπορούσε να έχει σημαντικές επιπτώσεις, εάν ο οργανισμός σας προσφέρει διαδικτυακές υπηρεσίες σε παιδιά, και συλλέγει τα προσωπικά τους δεδομένα. Να θυμάστε ότι η συγκατάθεση πρέπει να είναι επαληθεύσιμη, και ότι κατά τη συλλογή των δεδομένων των ανηλίκων, η ειδοποίηση περί απορρήτου θα πρέπει να είναι γραμμένη σε γλώσσα που τα παιδιά θα κατανοήσουν.

9. Παραβιάσεις δεδομένων

Θα πρέπει να βεβαιωθείτε ότι έχετε θέσει τις σωστές διαδικασίες προκειμένου να ανιχνεύσετε, να αναφέρετε και να ερευνήσετε μια παραβίαση προσωπικών δεδομένων.

Κάποιοι οργανισμοί είναι ήδη υποχρεωμένοι να ενημερώνουν την ΑΠΔΠΧ (και πιθανόν κάποια άλλα όργανα) σε περίπτωση παραβίασης προσωπικών δεδομένων. Ο νέος Κανονισμός υποχρεώνει όλους τους οργανισμούς να αναφέρουν ορισμένες μορφές παραβίασης στην ΑΠΔΠΧ, και σε ορισμένες περιπτώσεις, στα υποκείμενα. Το μόνο που έχετε να κάνετε είναι να ενημερώσετε την ΑΠΔΠΧ για μια παραβίαση, όταν είναι πιθανόν να

οδηγήσει στην διακινδύνευση των δικαιωμάτων, και των ελευθεριών των υποκειμένων - εάν, για παράδειγμα, θα μπορούσε να οδηγήσει σε διακρίσεις, δυσφήμηση, περιουσιακή ζημία, απώλεια εμπιστευτικότητας, ή οποιοδήποτε άλλο οικονομικό, ή κοινωνικό μειονέκτημα.

Όταν μια παραβίαση είναι πιθανό να οδηγήσει σε σημαντική διακινδύνευση των δικαιωμάτων και των ελευθεριών των ατόμων, θα πρέπει, στις περισσότερες περιπτώσεις, να ενημερώσετε άμεσα τους ενδιαφερομένους.

Θα πρέπει να τεθούν σε εφαρμογή διαδικασίες για την αποτελεσματική ανίχνευση, αναφορά και διερεύνηση μιας παραβίασης προσωπικών δεδομένων. Ενδέχεται να επιθυμείτε να αξιολογήσετε τους τύπους των προσωπικών δεδομένων που διατηρείτε, και να καταγράψετε σε ποιες περιπτώσεις θα χρειαστεί να ενημερώσετε την ΑΠΔΠΧ ή τα θιγόμενα υποκείμενα σε περίπτωση παραβίασης. Μεγαλύτεροι οργανισμοί θα πρέπει να αναπτύξουν πολιτικές και διαδικασίες για την διαχείριση παραβιάσεων δεδομένων. Η παράλειψη αναφοράς μιας παραβίασης, όταν απαιτείται να γίνει, θα μπορούσε να επιφέρει πρόστιμο, καθώς και πρόστιμο για την παραβίαση αυτή καθαυτή.

10. Προστασία δεδομένων ήδη από τον σχεδιασμό και εκτιμήσεις αντικτύπου (DPIA)

Ανέκαθεν ήταν χρήσιμο να υιοθετεί κανείς μια πολιτική προστασίας των προσωπικών δεδομένων κατά το στάδιο του σχεδιασμού της επεξεργασίας, αξιολογώντας ταυτόχρονα τις επιπτώσεις της επεξεργασίας στην προστασία τους. Ο νέος Κανονισμός, ωστόσο, αναγάγει ρητώς σε νομική υποχρέωση την προστασία δεδομένων ήδη από τον σχεδιασμό, με την ονομασία «προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού». Ακόμη, ορίζει πως η αξιολόγηση των επιπτώσεων της

επεξεργασίας στην προστασία των προσωπικών δεδομένων είναι υποχρεωτική σε ορισμένες περιπτώσεις.

Η αξιολόγηση των επιπτώσεων στην προστασία των προσωπικών δεδομένων απαιτείται σε περιπτώσεις, όπου η επεξεργασία τους ενδέχεται να οδηγήσει σε υψηλό κίνδυνο για τα υποκείμενα, για παράδειγμα:

- Όπου χρησιμοποιείται μια νέα τεχνολογία
- Όταν μια δραστηριότητα δημιουργίας προφίλ ενδέχεται να επηρεάσει σημαντικά τα υποκείμενα ή
- Όπου γίνεται επεξεργασία ειδικών κατηγοριών δεδομένων σε μεγάλη κλίμακα

Εάν η εν λόγω διαδικασία αξιολόγησης καταδεικνύει, πως η επεξεργασία των δεδομένων έχει υψηλό βαθμό επικινδυνότητας, και δεν είναι εύκολο να αντιμετωπιστεί ο κίνδυνος, θα πρέπει να συμβουλευτείτε την ΑΠΔΠΧ, και να λάβετε την γνώμη της, για το κατά πόσο η εν λόγω επεξεργασία είναι σύμφωνη με τον GDPR.

Συνεπώς, θα πρέπει να ξεκινήσετε να αναζητείτε τις περιπτώσεις όπου θα είναι απαραίτητο να πραγματοποιήσετε μια τέτοια αξιολόγηση επιπτώσεων. Ποιος θα την κάνει; Ποιος άλλος απαιτείται να εμπλακεί; Η διαδικασία θα πρέπει να γίνει από την κεντρική ή την τοπική διοίκηση του οργανισμού;

Επίσης, καλό θα ήταν να εξοικειωθείτε από τώρα με τις σχετικές οδηγίες της ΑΠΔΠΧ και της Ομάδας Εργασίας του Άρθρου 29 (πλέον Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, και να αναλογιστείτε πως θα τις εφαρμόσετε στον οργανισμό σας.

Αυτές οι οδηγίες δείχνουν πως οι εν λόγω αξιολογήσεις συνδέονται με άλλες οργανωτικές διαδικασίες, όπως η διαχείριση κινδύνων και η διαχείριση των projects.

11. Υπεύθυνος προστασίας δεδομένων (Data Protection Officer)

Θα πρέπει να επιλέξετε κάποιον, ο οποίος θα φέρει την ευθύνη για την συμμόρφωση με την νομοθεσία για την προστασία δεδομένων, και να καθορίσετε τη θέση του στην ιεραρχία του οργανισμού σας.

Αναλογιστείτε εάν οφείλετε εκ του νόμου να καθορίσετε έναν Υπεύθυνο Προστασίας Δεδομένων. Θα πρέπει να καθορίσετε έναν Υπεύθυνο Προστασίας Δεδομένων εάν είστε:

- Δημόσια αρχή (εκτός από τα δικαστήρια στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας)
- Οργανισμός που πραγματοποιεί τακτική και συστηματική παρακολούθηση υποκειμένων σε μεγάλη κλίμακα ή
- Οργανισμός που πραγματοποιεί εκτενή επεξεργασία ειδικών κατηγοριών δεδομένων, όπως ιατρικά δεδομένα ή πληροφορίες για ποινικές καταδίκες. Η Ομάδα Εργασίας του άρθρου 29 έχει εκδώσει κατευθυντήριες γραμμές για οργανισμούς, ως προς τον καθορισμό, την θέση και τα καθήκοντα των DPOs.

Είναι εξαιρετικά σημαντικό πως κάποιος στον οργανισμό σας, ή ένας εξωτερικός σύμβουλος προστασίας δεδομένων, θα αναλάβει την ευθύνη προς συμμόρφωση με τις διατάξεις για προστασία των δεδομένων, και θα έχει τις γνώσεις, την στήριξη, και την εξουσία να εκπληρώσει τον ρόλο του αποτελεσματικά.

12. Διασυνοριακή επεξεργασία δεδομένων

Εάν ο οργανισμός σας αναπτύσσει δραστηριότητες σε περισσότερα από ένα κράτη μέλη της Ε.Ε., θα πρέπει να προσδιορίσετε και να καταγράψετε ποια είναι η επικεφαλής εποπτική αρχή προστασίας προσωπικών δεδομένων.

Η επικεφαλής αρχή είναι η εποπτική αρχή του κράτους όπου έχετε την κύρια εγκατάστασή σας. Η κύρια εγκατάστασή σας είναι η τοποθεσία όπου βρίσκεται η κεντρική διοίκηση του οργανισμού στην Ε.Ε., ή αλλιώς η τοποθεσία όπου λαμβάνονται, και υλοποιούνται οι αποφάσεις για τους σκοπούς και τα μέσα της επεξεργασίας. Αυτό είναι σχετικό μόνο όταν πραγματοποιείτε διασυνοριακή επεξεργασία δεδομένων - δηλαδή έχετε εγκαταστάσεις σε περισσότερα από ένα κράτη μέλη της Ε.Ε. ή μία μοναδική εγκατάσταση στην Ε.Ε., η οποία πραγματοποιεί επεξεργασία δεδομένων που επηρεάζει σημαντικά υποκείμενα από άλλα κράτη μέλη της Ε.Ε..

Εάν αυτό ισχύει για τον οργανισμό σας, θα πρέπει να καταγράψετε σε ποιο μέρος λαμβάνει ο οργανισμός σας τις σημαντικότερες αποφάσεις σχετικά με την επεξεργασία. Γεγονός που θα σας βοηθήσει να καθορίσετε την «κύρια εγκατάστασή» σας, και συνεπώς την επικεφαλής εποπτική αρχή.

Η Ομάδα Εργασίας του άρθρου 29 έχει εκδώσει κατευθυντήριες γραμμές σχετικά με τον καθορισμό της επικεφαλής εποπτικής αρχής, του υπευθύνου ή του εκτελούντα την επεξεργασία των προσωπικών δεδομένων.

Δείτε επίσης τους Οδηγούς του Lawspot.gr/GDPR για:

Τα Διοικητικά Πρόστιμα με βάση τον GDPR

Τους Υπευθύνους Προστασίας Δεδομένων (Data Protection Officers)

Το Δικαίωμα στη λήθη

Τη Συγκατάθεση