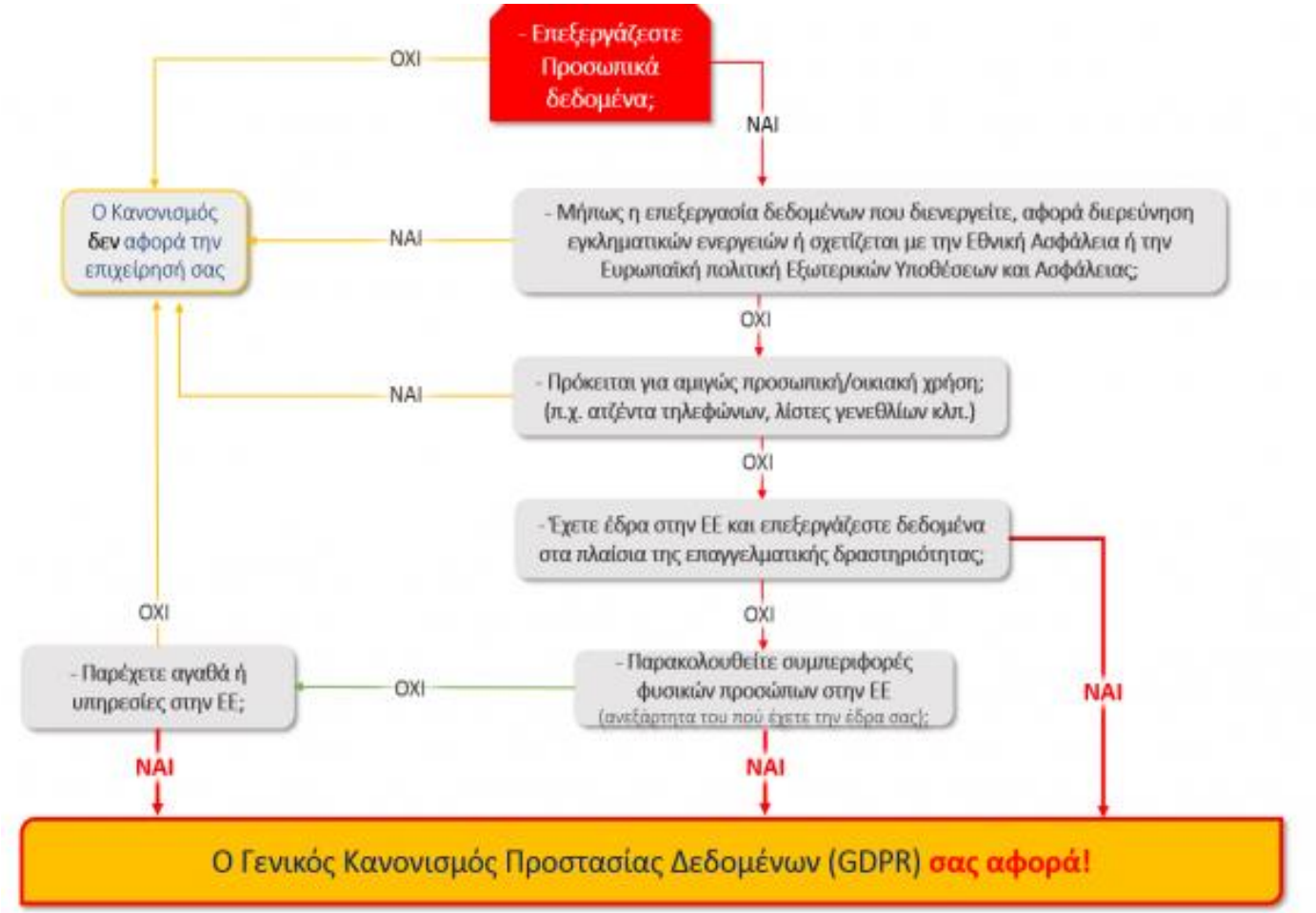
GDPR: έλεγχος 20 σημείων – για μικρές και μεσαίες επιχειρήσεις

Ο νέος Γενικός Κανονισμός Προστασίας Δεδομένων (EU GDPR 2016/679, στο εξής GDPR) **προστατεύει τα φυσικά πρόσωπα** από κινδύνους που σχετίζονται με την ανεξέλεγκτη -μέχρι σήμερα- επεξεργασία των προσωπικών τους δεδομένων. Θέτει λοιπόν αυστηρότερους κανόνες στους οργανισμούς, για να περιορίσει την ανεξέλεγκτη επεξεργασία προσωπικών δεδομένων και να μειώσει τους κινδύνους για τα φυσικά πρόσωπα. Απώτερος σκοπός είναι να δημιουργηθεί τελικά ένα ευρύτερο ασφαλές περιβάλλον, ίδιο σε όλα τα κράτη-μέλη της Ευρώπης, κάτω από μία ενιαία νομοθεσία, που θα προστατεύει αποτελεσματικά τα φυσικά πρόσωπα, ώστε να **εξασφαλιστεί η ελεύθερη διακίνηση** των προσωπικών δεδομένων μεταξύ των κρατών, δίχως κινδύνους για τα φυσικά πρόσωπα.

Ο GDPR ψηφίστηκε στις 27 Απριλίου 2016 κι έχει καθολική ισχύ σε όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης. Έχει δοθεί μια διετής περίοδος προσαρμογής στους οργανισμούς, μέχρι 25 Μαΐου 2018, οπότε τίθεται σε **πλήρη εφαρμογή** ο Κανονισμός, καθώς και τα πολύ υψηλά πρόστιμα για τους παραβάτες. Περισσότερα εδώ: GDPR – Απλές απαντήσεις στις συχνότερες ερωτήσεις.

Ο GDPR **αφορά κάθε οργανισμό** που "επεξεργάζεται" προσωπικά δεδομένα φυσικών προσώπων που βρίσκονται στην Ευρωπαϊκή Ένωση. Ως "επεξεργασία" νοείται κάθε πράξη που πραγματοποιείται σε προσωπικά δεδομένα, με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, όπως π.χ. συλλογή, καταχώριση, οργάνωση, διάρθρωση, αποθήκευση, προσαρμογή, μεταβολή, ανάκτηση, αναζήτηση πληροφοριών, χρήση, κοινολόγηση με διαβίβαση, διάδοση ή κάθε άλλη μορφή διάθεσης, συσχέτιση ή συνδυασμός, περιορισμός, διαγραφή ή καταστροφή.



Τα φυσικά πρόσωπα που σχετίζονται με την εταιρία σας είναι -ενδεικτικά – όλοι σας οι **υπάλληλοι**, παλαιοί και νέοι, ακόμη κι όσοι εργάζονται εξ αποστάσεως, οι **Πελάτες** και οι **υποψήφιοι** Πελάτες σας, οι

Συνεργάτες και **Προμηθευτές** σας, μέσα στα χρόνια λειτουργίας της εταιρίας σας. Είναι επίσης όλοι όσοι έχουν αφήσει τα στοιχεία τους κατά καιρούς στο σύστημα **Chat** ή **Ticketing**, συμπλήρωσαν μια **online φόρμα** στο **website** ή στο **Newsletter** σας. Είναι φυσικά πρόσωπα με τα οποία συναλλάσσεστε καθημερινά κι άλλα, πολύ περισσότερα, που συμπλήρωσαν τα στοιχεία τους για **συμμετοχή σε κλήρωση** δώρου, ή σε εκδήλωση της εταιρίας σας. Και είναι ακόμη αμέτρητα τα φυσικά πρόσωπα που δεν γνωρίσατε ποτέ, αλλά παρ΄όλα αυτά έχετε στα χέρια σας πλήθος προσωπικά τους δεδομένα: τα **βιογραφικά** των υποψηφίων. Η λίστα δεν εξαντλείται εδώ. Μάλλον το αντίστροφο: τα παραπάνω παραδείγματα αποτελούν μια πολύ περιορισμένη ένδειξη της πληθώρας προσωπικών δεδομένων που επεξεργάζεται μια εταιρία μέσα στα χρόνια.

Συνεπώς, **κατά πάσα πιθανότητα ο GDPR σας αφορά.** Πώς θα το ανακαλύψετε και τι πρέπει να κάνετε; Ο εξειδικευμένος σας σύμβουλος, σε θέματα προστασίας προσωπικών δεδομένων, είναι ο πλέον αρμόδιος για να σας κατατοπίσει. Αν θέλετε όμως μια πρώτη εκτίμηση, ο παρακάτω έλεγχος των 20 σημείων ελπίζουμε να σας διαφωτίσει: τα 20 σημεία καλύπτουν 1- προς-1 τα άρθρα του GDPR που αφορούν στη συμμόρφωση επιχειρήσεων και οργανισμών.

Προτού ξεκινήσετε τον έλεγχο, καλό είναι να αποκτήσετε μια εξοικείωση με τις βασικότερες έννοιες και ορισμούς, όπως π.χ. τί είναι προσωπικά δεδομένα, πότε είναι νόμιμη η συγκατάθεση, κλπ. διότι ο GDPR ορίζει νέες, αυστηρότερες απαιτήσεις. Για ευκολία, δείτε συγκεντρωμένους τους ορισμούς εδώ (Άρθρο 4).

Προτείνουμε να διεξάγετε τον παρακάτω έλεγχο **μαζί** με βασικά στελέχη από κάθε τμήμα της εταιρίας σας. Επιπλέον:

Ένας έμπειρος σύμβουλος, κατά προτίμηση πιστοποιημένος DPO (Υπεύθυνος Προστασίας Δεδομένων) ή εξειδικευμένος νομικός σε θέματα προστασίας δεδομένων, είναι απαραίτητος για να αποσαφηνιστούν λεπτομέρειες νομικής φύσεως.

Ένας έμπειρος σύμβουλος IT είναι επίσης απαραίτητος, για να αποτυπώσει με ακρίβεια όλα τα κενά ασφαλείας (GAP ANALYSIS) και τυχόν αδυναμίες σε διαθεσιμότητα, για το σύνολο των συστημάτων και υποδομών πληροφορικής σας και θα συμβάλλει στην ορθή εκτίμηση των κινδύνων.

Δίχως ορθή εκτίμηση των κινδύνων, η όποια “θεραπεία”, δηλαδή τα μέτρα που θα λάβετε, θα είναι κατά πάσα πιθανότητα λάθος: και χρήματα θα δαπανήσετε και εκτεθειμένοι σε κινδύνους θα παραμείνετε. Το χειρότερο είναι, ότι οι κίνδυνοι που σας απειλούν από κάθε κενό ασφαλείας, δεν περιορίζονται σε πρόστιμα ούτε σε δυσφήμιση, αλλά επεκτείνονται σε επιθέσεις ransomware, τη σύγχρονη μάστιγα που πλήττει καθημερινά εκατοντάδες χιλιάδες εταιρίες – χωρίς διακρίσεις! – και κοστίζει πλέον πολύ ακριβά …σε bitcoins.

Σκοπός είναι να αναγνωρίσετε αν και που βρίσκονται τα πιθανά “κενά” σας. Έχοντας μια ξεκάθαρη εικόνα των αναγκών σας, θα μπορέσετε να θέσετε τις δικές σας προτεραιότητες και να ορίσετε ένα χρονοδιάγραμμα συμμόρφωσης, μέχρι το Μάϊο του 2018.

1. Δέσμευση της διοίκησης

- Οι υπεύθυνοι λήψης αποφάσεων στην επιχείρησή σας έχουν ενημερωθεί για τον GDPR. Διαφορετικά, δείτε τα βασικά εδώ.
- Έχουν αποκτήσει όλοι μια σαφή εικόνα για την απόσταση που πρέπει να καλυφθεί προς τη συμμόρφωση. Έχετε καταγράψει δηλαδή τα κενά συμμόρφωσης (Gap Analysis).
- Η διοίκηση προωθεί έμπρακτα μια θετική κουλτούρα συμμόρφωσης σε ολόκληρη την επιχείρηση. Έχει δοθεί εντολή στα αρμόδια στελέχη, να προγραμματίσουν τις ενέργειές τους προς συμμόρφωση, σε ολόκληρη την οργάνωση, με συγκεκριμένο χρονοδιάγραμμα και παραδοτέα.

2. Καταγραφή προσωπικών δεδομένων

- Έχετε ολοκληρώσει την **χαρτογράφηση ροής** προσωπικών δεδομένων στην επιχείρησή σας.

- Έχει καταρτιστεί ο **πίνακας καταγραφής** όλων των κατηγοριών προσωπικών δεδομένων, με τα αντίστοιχα υποκείμενα, τους αποδέκτες, τους τρόπους απόκτησης & τήρησης, τους σκοπούς επεξεργασίας και τυχόν διαβιβάσεις σε τρίτους. Στη συνέχεια ο πίνακας αυτός θα συμπληρωθεί σε μεγαλύτερη λεπτομέρεια, ώστε να είναι σύμφωνος με τις "Επτά Αρχές" και τη "Νομιμότητα", καθώς και τις διατάξεις για τις "Ειδικές κατηγορίες" δεδομένων, όπως περιγράφεται αμέσως παρακάτω (στα σημεία 3 ως 6).

3. Επτά Αρχές και Νομιμότητα (Άρθρα 5, 6)

- Ο GDPR εισάγει **επτά "αρχές"** (για την ακρίβεια 6 αρχές και 1 "αρχή-ομπρέλα", αυτή της "λογοδοσίας") και απαιτεί να τηρούνται **όλες** για κάθε κατηγορία προσωπικών δεδομένων που επεξεργάζεστε (Άρθρο 5). Βεβαιωθείτε ότι τις κατανοείτε και ότι τις **τηρείτε όλες**:
    1. νομιμότητα, αντικειμενικότητα και διαφάνεια,
    2. περιορισμός του σκοπού,
    3. ελαχιστοποίηση,
    4. ακρίβεια,
    5. περιορισμός περιόδου αποθήκευσης,
    6. ασφάλεια, ακεραιότητα, εμπιστευτικότητα,
    7. λογοδοσία: εσείς ευθύνεστε, ως υπεύθυνος επεξεργασίας, κι επιπλέον πρέπει να είστε σε θέση να αποδείξετε πλήρη συμμόρφωση.
- Ο GDPR ορίζει **έξι προϋποθέσεις "νομιμότητας"** της επεξεργασίας και απαιτεί να ισχύει **τουλάχιστον μία** (Άρθρο 6). Βεβαιωθείτε λοιπόν ότι ισχύει τουλάχιστον μία από τις έξι προϋποθέσεις νομιμότητας, για κάθε κατηγορία προσωπικών δεδομένων και σημειώστε την στον πίνακα καταγραφής:
    1. το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία,
    2. η επεξεργασία είναι απαραίτητη για εκτέλεση σύμβασης (όπου το υποκείμενο είναι συμβαλλόμενος) ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου πριν τη σύναψη σύμβασης
    3. η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας,
    4. η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος (του υποκειμένου ή άλλου φυσικού προσώπου),
    5. η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας (που έχει ανατεθεί στον υπεύθυνο επεξεργασίας),
    6. 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 που επιβάλλουν την προστασία των προσωπικών δεδομένων, ιδίως εάν το υποκείμενο είναι παιδί). Εξαιρούνται οι δημόσιες αρχές κατά την άσκηση των καθηκόντων τους.
- Καταγράψτε στον πίνακα και οπωσδήποτε **τεκμηριώστε** το νόμιμο σκοπό, για κάθε επεξεργασία προσωπικών δεδομένων που διενεργείτε.

4. Λήψη συγκατάθεσης (Άρθρο 7)

- Η λήψη συγκατάθεσης του υποκειμένου κατ' αρχήν δύναται να αποτελεί μία από τις έξι "νόμιμες βάσεις" για την επεξεργασία προσωπικών δεδομένων, όπως είδαμε παραπάνω, στο σημείο 3. Βεβαιωθείτε όμως ότι πράγματι αρμόζει στην περίπτωση, ή μήπως θα ήταν προτιμότερο να στηρίξετε την επεξεργασία σε κάποια από τις υπόλοιπες "νόμιμες βάσεις". Εξάλλου, **η συγκατάθεση μπορεί να αρθεί ανά πάσα στιγμή**. Επίσης, έχει ιδιαίτερη σημασία για τις ειδικές κατηγορίες προσωπικών δεδομένων. Συγκεκριμένα, αποτελεί μία εκ των νομικών βάσεων για άρση της απαγόρευσης επεξεργασίας **ειδικών κατηγοριών** προσωπικών δεδομένων, όπως ορίζει το Άρθρο 9.
- Βεβαιωθείτε ότι ισχύουν ακριβώς όσα ορίζει ο GDPR στο Άρθρο 4 (στους ορισμούς, σημείο 11), ότι δηλαδή η συγκατάθεση που λαμβάνετε είναι μια **πράξη** του υποκειμένου "…ως 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 από πλευράς

του…”. Άρα, η σιωπηρή αποδοχή, δίχως σαφή ενέργεια επιβεβαίωσης, δεν αποτελεί συγκατάθεση, όπως πιστεύαμε μέχρι σήμερα.
- Επίσης, η συγκατάθεση δεν σας απαλλάσσει από την υποχρέωση τήρησης των επτά “Αρχών” που είδαμε παραπάνω, στο σημείο 3.
- Ελέγξτε ότι είστε σε θέση να **αποδείξετε** ανά πάσα στιγμή, ότι έχετε λάβει τη συγκατάθεση του υποκειμένου, στις περιπτώσεις που απαιτείται.
- Παρέχετε στα υποκείμενα των δεδομένων τους μηχανισμούς καταγραφής και διαρκούς διαχείρισης, καθώς και αναίρεσης της συγκατάθεσής τους.

5. Παιδιά (Άρθρο 8)

- Αν η επιχείρησή σας προσφέρει υπηρεσίες απευθείας σε ανήλικους κάτω των 16 ετών, πρέπει να έχετε εγκατεστημένα τα προβλεπόμενα από το νόμο συστήματα διαχείρισης της συγκατάθεσης του γονέα ή κηδεμόνα.
- Επιπλέον, φροντίστε ώστε οι πληροφορίες προστασίας απορρήτου (Πολιτική Απορρήτου) να δίνονται με τρόπο **εύκολα αντιληπτό** από παιδιά.

6. Ειδικές κατηγορίες, ποινικές καταδίκες και αδικήματα (Άρθρα 9 και 10)

- Καταγράψτε – αν υπάρχουν – τις “ειδικές κατηγορίες” προσωπικών δεδομένων του Άρθρου 9. Δείτε αναλυτικά εδώ. Ο GDPR **απαγορεύει** την επεξεργασία τους, πλην ορισμένων εξαιρέσεων και πάλι υπό αυστηρές προϋποθέσεις.
- Γνωρίζετε ποια είναι κατά τον GDPR τα προσωπικά δεδομένα που αφορούν **ποινικές καταδίκες και αδικήματα** και τηρείτε τις σχετικές διατάξεις.

7. Διαφανής ενημέρωση (Άρθρα 12-14)

- Η επιχείρησή σας διαθέτει σαφή και κατανοητή **Πολιτική Απορρήτου** (η γνωστή και ως Privacy Policy ή Privacy Notice).
- Βεβαιωθείτε ότι μέσα από την Πολιτική Απορρήτου σας, ***παρέχετε στο υποκείμενο*** όλες τις πληροφορίες που απαιτεί ο GDPR να του δώσετε με σαφήνεια, τόσο α) για την επεξεργασία που διενεργείτε, δηλαδή ποιος είναι ο υπεύθυνος επεξεργασίας, στοιχεία επικοινωνίας αυτού, σκοποί επεξεργασίας, χρόνοι διατήρησης κλπ., καθώς και β) για τα δικαιώματά του (διόρθωση, διαγραφή, εναντίωση, φορητότητα, κλπ. (δείτε επόμενο σημείο 8) και τέλος γ) για να υποβάλλει καταγγελία σε εποπτική αρχή.

8. Δικαιώματα του υποκειμένου (Άρθρα 15-22)

- Γνωρίζετε και **αποδεδειγμένα προστατεύετε** και τα **οκτώ δικαιώματα** του υποκειμένου, μερικά εκ των οποίων μάλιστα προστατεύονται για πρώτη φορά από τον GDPR:
    1. Δικαίωμα πρόσβασης στα δεδομένα, Άρθρο 15
    2. Δικαίωμα διόρθωσης, Άρθρο 16
    3. Δικαίωμα διαγραφής, Άρθρο 17
    4. Δικαίωμα περιορισμού της επεξεργασίας, Άρθρο 18
    5. Υποχρέωση γνωστοποίησης όσον αφορά τη διόρθωση ή διαγραφή ή περιορισμό επεξεργασίας, Άρθρο 19
    6. Δικαίωμα φορητότητας σε δομημένο, συμβατό και μηχαναγνώσιμο μορφότυπο, Άρθρο 20
    7. Δικαίωμα εναντίωσης στην επεξεργασία, Άρθρο 21
    8. Σχετικά με την αυτοματοποιημένη ατομική λήψη αποφάσεων συμπεριλαμβανομένης της κατάρτισης **προφίλ** (την οποία θα έχετε ήδη εντοπίσει, όπως περιγράφεται παραπάνω, υπό το σημείο 2: “Καταγραφή προσωπικών δεδομένων”), έχετε θεσπίσει **διαδικασίες** για την ικανοποίηση του **δικαιώματος εναντίωσης** των υποκειμένων σε λήψη αυτοματοποιημένων αποφάσεων και προφιλοποίησης, Άρθρο 22.

Σημ. Τα άρθρα 15 ως 20 δεν εφαρμόζονται, όταν αποδεδειγμένα δεν μπορείτε να εξακριβώσετε την ταυτότητα του υποκειμένου, εκτός εάν το ίδιο το υποκείμενο, για τον σκοπό της άσκησης των δικαιωμάτων του που απορρέουν από τα εν λόγω άρθρα, σας παρέχει συμπληρωματικές πληροφορίες που επιτρέπουν την εξακρίβωση της ταυτότητάς του (Άρθρο 11).

- Βεβαιωθείτε ότι διαθέτετε διαδικασία για να ανταποκρίνεστε εντός του **προβλεπόμενου χρονικού πλαισίου** στα αιτήματα των υποκειμένων (δηλαδή, εντός **1 μηνός** από την παραλαβή του αιτήματος και με περιθώριο για παράταση κατά 2 ακόμη μήνες, εφόσον αυτό απαιτείται και δικαιολογείται, λαμβάνοντας υπόψη την πολυπλοκότητα του κάθε αιτήματος και τον μεγάλο αριθμό των αιτημάτων). Σε περίπτωση παράτασης, πάλι πρέπει η εταιρία σας να είναι σε θέση να ενημερώσει το υποκείμενο εντός 1 μηνός για την παράταση καθώς και για τους λόγους της καθυστέρησης.

9. Ευθύνη της επιχείρησης και λογοδοσία (Άρθρο 24)

- Η επιχείρησή σας γνωρίζει ότι είναι **διαρκώς υπόλογη** α) στα υποκείμενα των δεδομένων (φυσικά πρόσωπα) και β) στις εποπτικές αρχές.
- Γνωρίζει όλες τις απαιτήσεις του GDPR και είναι πάντα σε θέση να **αποδεικνύει** συμμόρφωση. Άρα, είναι απαραίτητο να υιοθετήσετε τους κατάλληλους μηχανισμούς και οργάνωση, με ξεκάθαρες πολιτικές και διαδικασίες, κατά τρόπον ώστε να έχετε τη δυνατότητα να αποδεικνύετε τη συμμόρφωσή σας. Στα πλαίσια αυτά, η Ομάδα Εργασίας του Άρθρου 2 (WP29) συστήνει την διενέργεια Εκτίμησης Αντικτύπου – ΕΑΠΔ (Data Privacy Impact Assessment, DPIA) ως το καταλληλότερο εργαλείο διαχείρησης κινδύνου.

10. Προστασία ήδη από το σχεδιασμό και εξ' ορισμού (Άρθρο 25)

- Έχετε εφαρμόσει ήδη από το σχεδιασμό και εξ' ορισμού (Privacy by Design and by Default), τα κατάλληλα τεχνικά και οργανωτικά μέτρα τα οποία διασφαλίζουν ότι τα προσωπικά δεδομένα υφίστανται την εκάστοτε ελάχιστη νόμιμη και απαραίτητη επεξεργασία. Για να γίνει αυτό κατανοητό, δείτε παραδείγματα εδώ: Ποιες είναι οι κυριότερες απαιτήσεις, σημείο 6

11. Συμβάσεις με άλλους από κοινού Υπευθύνους Επεξεργασίας (Άρθρο 26)

- Αν η επιχείρησή σας επεξεργάζεται προσωπικά δεδομένα καθορίζοντας από κοινού με άλλο φορέα/επιχείρηση τους σκοπούς και τα μέσα της επεξεργασίας, τότε αποτελείτε "από κοινού Υπευθύνους Επεξεργασίας" και πρέπει να διασφαλίσετε ότι διαθέτετε τις κατάλληλες **γραπτές συμβάσεις** με κάθε από κοινού Υπεύθυνο Επεξεργασίας. Στις συμβάσεις αυτές επιτρέπεται, αν θέλετε, να αναφέρετε μόνο ένα σημείο επικοινωνίας με τα υποκείμενα των δεδομένων.

12. Διορισμός εκπροσώπου (Άρθρο 27)

- Αν η επιχείρησή σας δεν είναι εγκατεστημένη στην Ευρωπαϊκή Ένωση, αλλά επεξεργάζεται προσωπικά δεδομένα υποκειμένων που βρίσκονται στην Ένωση, τότε πρέπει να ορίσετε γραπτώς έναν εκπρόσωπο εντός της Ένωσης, εκτός αν υπάγεστε στις εξαιρέσεις του σχετικού άρθρου του GDPR.

13. Διακριτές υποχρεώσεις Υπευθύνου και Εκτελούντος την επεξεργασία και συνεργασία με την εποπτική αρχή (Άρθρα 28, 29 και 31)

- Βεβαιωθείτε ότι έχετε αντιληφθεί πλήρως το ρόλο σας, ως Υπευθύνου ή/και ως Εκτελούντος την επεξεργασία (διότι μπορεί να συντρέχουν και τα δύο). Συμμορφωθείτε ανάλογα, ακολουθώντας τις

διατάξεις των άρθρων 28 και 29 που σας αφορούν. Για να γίνει αυτό κατανοητό, δείτε παραδείγματα εδώ.

14. Τήρηση αρχείου επεξεργασίας – Εταιρίες άνω των 250 ατόμων (Άρθρο 30)

- Εξετάστε αν συντρέχουν οι προϋποθέσεις που υποχρεώνουν την εταιρία σας σε συστηματική τήρηση αρχείου επεξεργασίας προσωπικών δεδομένων. Αν ναι, τότε είστε υποχρεωμένοι επίσης να το θέτετε υπόψιν της εποπτικής αρχής, κατόπιν σχετικού αιτήματος. Εξαιρούνται -υπό τις προϋποθέσεις του Άρθρου 30 – οι εταιρίες που απασχολούν κάτω από 250 άτομα.

15. Λήψη μέτρων προστασίας (Άρθρο 32)

- Ελέγξτε ότι έχετε λάβει τα απαιτούμενα τεχνικά και οργανωτικά μέτρα για την εξασφάλιση της προστασίας των προσωπικών δεδομένων. Καταγράψτε τα στον πίνακα, δίπλα σε κάθε κατηγορία προσωπικών δεδομένων. Ο GDPR συνιστά τη λήψη συγκεκριμένων μέτρων, μεταξύ άλλων τα εξής (Άρθρο 32):
    - την κρυπτογράφηση και ψευδωνυμοποίηση προσωπικών δεδομένων,
    - τη διασφάλιση του τρίπτυχου “Απόρρητο, Ακεραιότητα, Διαθεσιμότητα” (CIA, Confidentiality, Integrity, Availability),
    - τη θέσπιση διαδικασιών γρήγορης αποκατάστασης της διαθεσιμότητας
    - τη θέσπιση διαδικασιών τακτικής δοκιμής κι αξιολόγησης της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων ασφαλείας
    - την τήρηση εγκεκριμένων κωδίκων δεοντολογίας του Άρθρου 40, ή μηχανισμού πιστοποίησης του Άρθρου 42 για την απόδειξη συμμόρφωσης.

16. Γνωστοποίηση παραβίασης εντός 72 ωρών (Άρθρα 33-34)

- Ελέγξτε ότι εφαρμόζετε κατάλληλα μέτρα, ώστε να αντιληφθείτε **εγκαίρως** τυχόν παραβίαση ασφαλείας που αφορά προσωπικά δεδομένα, αλλά και να ενεργοποιηθεί άμεσα ο μηχανισμός αντιμετώπισης. Δηλαδή, έχετε εφαρμόσει τα κατάλληλα συστήματα και έχετε ορίσει τους κατάλληλους ανθρώπους για να παρακολουθούν και να ενημερώνουν αρμοδίως, για κάθε εσωτερική ή εξωτερική παραβίαση ασφαλείας.
- Έχετε **έτοιμες** διαδικασίες διαχείρισης κινδύνου, σε περίπτωση παραβίασης (Risk Management). Διαθέτετε ενημερωμένη **Incident Response Team** και επικαιροποιημένο **Insident Response Plan**.Έχετε πλάνο τακτικών **δοκιμών** αυτών των διαδικασιών, ώστε να επιβεβαιώνετε την αποτελεσματικότητά τους.
- Διαθέτετε τα σχετικά **έντυπα** Γνωστοποίησης παραβίασης (με τη διατύπωση που επιβάλλει ο GDPR) για να τα υποβάλετε εμπρόθεσμα στην αρμόδια εποπτική αρχή και (εφόσον απαιτείται) και στα υποκείμενα, τα δεδομένα των οποίων θίγονται.

17. Εκτίμηση Αντικτύπου – ΕΑΠΔ (Data Privacy Impact Assessment, DPIA) και Διαβούλευση (Άρθρα 35-36 & 83, αιτ.σκέψεις 84, 89, 96)

Η διενέργεια ΕΑΠΔ αποτελεί **ουσιώδες μέρος της συμμόρφωσης** με τον Κανονισμό (Άρθρο 24, αιτιολογική σκέψη 90), όποτε σχεδιάζεται ή υλοποιείται επεξεργασία δεδομένων με υψηλό κίνδυνο. Αυτό σημαίνει ότι, ως υπεύθυνοι επεξεργασίας θα πρέπει να διαπιστώνετε αν οφείλετε να διενεργήσετε ΕΑΠΔ. Για τη διαπίσωση, θα χρησιμοποιείτε τα κριτήρια που ορίζονται σε σχετική οδηγία της Ομάδας Εργασίας του Άρθρου 29 (WP29).

- Διερευνήστε μήπως συντρέχουν και για σας, οι προϋποθέσεις που **υποχρεώνουν** μια επιχείρηση να διενεργεί συστηματικά Εκτιμήσεις Αντικτύπου, σύμφωνα με τον Κανονισμό. Αν ναι, τότε

βεβαιωθείτε ότι διαθέτετε το κατάλληλο πλαίσιο DPIA, που συνδέεται με τις υφιστάμενες διαδικασίες διαχείρισης κινδύνων (Risk Management).

- Εάν τελικά, ο αντίκτυπος που προκύπτει από την εκτίμηση είναι μεγάλος, οφείλετε να ζητήσετε τη **γνώμη της εποπτικής αρχής** πριν προβείτε σε επεξεργασία προσωπικών δεδομένων (προηγούμενη διαβούλευση).
- Ως ορθή πρακτική, μια ΕΑΠΔ θα πρέπει να επανεξετάζεται συνεχώς και να επαναξιολογείται τακτικά. Συνεπώς, ακόμη και αν μια ΕΑΠΔ δεν είναι αναγκαία στις 25 Μαΐου 2018, ο υπεύθυνος επεξεργασίας θα υποχρεωθεί, στον ενδεδειγμένο χρόνο, να διενεργήσει μια τέτοια εκτίμηση στο πλαίσιο των γενικών υποχρεώσεων λογοδοσίας που υπέχει.

18. Διορισμός Υπευθύνου Προστασίας Δεδομένων (Data Protection Officer, DPO) (Άρθρα 37-39)

- Διερευνήστε και βεβαιωθείτε, αν συντρέχουν οι λόγοι που σας υποχρεώνουν να διορίσετε DPO.
- Δύνασθε να διορίσετε DPO ακόμη και αν δεν είστε υποχρεωμένοι γι΄αυτό από τον GDPR.

19. Κώδικες Δεοντολογίας και Πιστοποίηση (Άρθρα 40-43 & 83, αιτιολογικές σκέψεις 98-100 & 148-151)

- Ελέγξτε αν ο κλαδικός σας φορέας ή ένωση έχει εκπονήσει ή θα εκπονήσει Κώδικα Δεοντολογίας. Αν αυτός εγκριθεί από τα αρμόδια όργανα, σας βοηθά στην συμμόρφωση. Αν υπογράψατε έναν κώδικα δεοντολογίας, θα υποβληθείτε σε υποχρεωτική παρακολούθηση από οργανισμό διαπιστευμένο από την Εποπτική Αρχή. Εάν όμως παραβιάσετε τις απαιτήσεις του κώδικα δεοντολογίας, είναι σαν να παραβιάζετε τον Κανονισμό. Φυσικά θα ενημερωθεί η εποπτική αρχή και κινδυνεύετε με πρόστιμο ύψους έως 10 εκ ευρώ ή 2% του συνολικού κύκλου εργασιών σας. Από την άλλη, η υιοθέτηση ενός κώδικα δεοντολογίας μπορεί να χρησιμεύσει ως **ελαφρυντικός παράγοντας**, σε περίπτωση που μια εποπτική αρχή εξετάζει την επιβολή πραστίμου.
- Η πιστοποίηση ενθαρρύνεται επίσης από τον GDPR, αλλά είναι εθελοντική. Τα πλησιέστερα μέχρι σήμερα πρότυπα είναι κατ' αρχήν το παγκόσμιο πρότυπο ασφάλειας της πληροφορίας, δηλαδή το ISO 27001 καθώς κι άλλα πιο εξειδικευμένα κατά κλάδους, όπως για παράδειγμα το ISO 27018 για την ασφάλεια προσωπικών δεδομένω στο cloud, τα τραπεζικά πρότυπα PCI, ή αυτά των κλάδων υγείας. Ωστόσο, τα πρότυπα αυτά δεν καλύπτουν 100% τις απαιτήσεις για συμμόρφωση κατά GDPR, διότι σχεδιάστηκαν για άλλους σκοπούς, άλλοτε πιο γενικούς, άλλοτε πολύ πιο εξειδικευμένους. Κατά συνέπεια, η συμμόρφωσή σας με ένα τέτοιο πρότυπο, δεν ισοδυναμεί με συμμόρφωση κατά τον GDPR, αλλά απλά σας βοηθάει στην διαδικασία συμμόρφωσης: **διαρκή επίβλεψη** της τήρησης των προβλεπόμενων και **ετοιμότητα,** συνολική **διακυβένρηση** (Governance), καθώς **και λογοδοσία** (θα είστε πάντα σε θέση να αποδείξετε ότι συμμορφώνεστε).

20. Διαβιβάσεις σε τρίτες χώρες ή διεθνείς οργανισμούς (Άρθρα 44 – 50)

- Ελέγξτε αν η επιχείρησή σας διαβιβάζει προσωπικά δεδομένα εκτός ΕΕ, ώστε να φροντίσετε να τηρούνται οι ιδιαίτερες απαιτήσεις του GDPR και να εξασφαλίζει επαρκές επίπεδο προστασίας.

Το κλειδί της επιτυχίας

Η συμμόρφωση με τον GDPR είναι μια διαρκής διαδικασία. Γι' αυτό, είναι σωστό να γίνει εξ' αρχής ορθή υλοποίηση. Απολύτως απαραίτητο είναι, πάνω απ' όλα, να καλλιεργηθεί συστηματικά, σε κάθε τμήμα και υπάλληλο του οργανισμού, η **πολύτιμη κουλτούρα** που συνοψίζεται στη φράση: **«Σέβομαι τα προσωπικά δεδομένα»**.

Χρήσιμοι σύνδεσμοι:

- **Επίσημη Εφημερίδα** της Ευρωπαϊκής Ένωσης: http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016R0679
- **Ορισμός Μικρών και Μεσαίων Επιχειρήσεων**: http://www.imegsevee.gr/arhtrografia/221-orismos

Επιπλέον έγκυρες λίστες "προετοιμασίας"

Για λόγους αντικειμενικότητας και πληρότητας της πληροφόρησης, παραθέτουμε παρόμοιες λίστες και οδηγίες προετοιμασίας, όπως αυτές δημοσιεύονται από επίσημους φορείς με διεθνές κύρος (σε τυχαία σειρά):

1. **ΑΠΔΠΧ**, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Ελλάδα: http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/GDPR/FILES/FILLADIO%20GDPR.PDF
2. **CNIL**, επίσημη Αρχή Προστασίας Προσωπικών Δεδομένων της Γαλλίας: https://www.cnil.fr/en/home
3. **IAPP**, International Association of Privacy Professionals, Διεθνής οργανισμός: https://iapp.org/resources/article/gdpr-what-b2b-companies-need-to-know/