ΤΙΝΤΖΟΓΛΙΔΟΥ
& ΣΥΝΕΡΓΑΤΕΣ
ΔΙΚΗΓΟΡΙΚΟ ΓΡΑΦΕΙΟ

Οι ενέργειες του νομικού συμβούλου για τη συμμόρφωση των επιχειρήσεων με τον Κανονισμό GDPR

Εισηγήτρια: Νόπη Τιντζογλίδου, Δικηγόρος, τέως Δ/ντρια νομικών θεμάτων συνδρομητών και προσωπικών δεδομένων Ομίλου ΟΤΕ.

ΤΙΝΤΖΟΓΛΙΔΟΥ & ΣΥΝΕΡΓΑΤΕΣ
ΔΙΚΗΓΟΡΙΚΟ ΓΡΑΦΕΙΟ

Τι θα πρέπει να διαθέτει ο κατάλληλος νομικός σύμβουλος που θα συμμορφώσει την επιχείρηση

1. Γνώση και εμπειρία ζητημάτων που άπτονται της προστασίας των προσωπικών δεδομένων.
2. Επικοινωνιακές ικανότητες και εξοικείωση με τεχνικούς όρους και όρους μάρκετινγκ που να του επιτρέπουν να επικοινωνεί εύκολα με πρόσωπα που ανήκουν σε άλλους επαγγελματικούς χώρους (marketing, IT, management).

προκειμένου να:

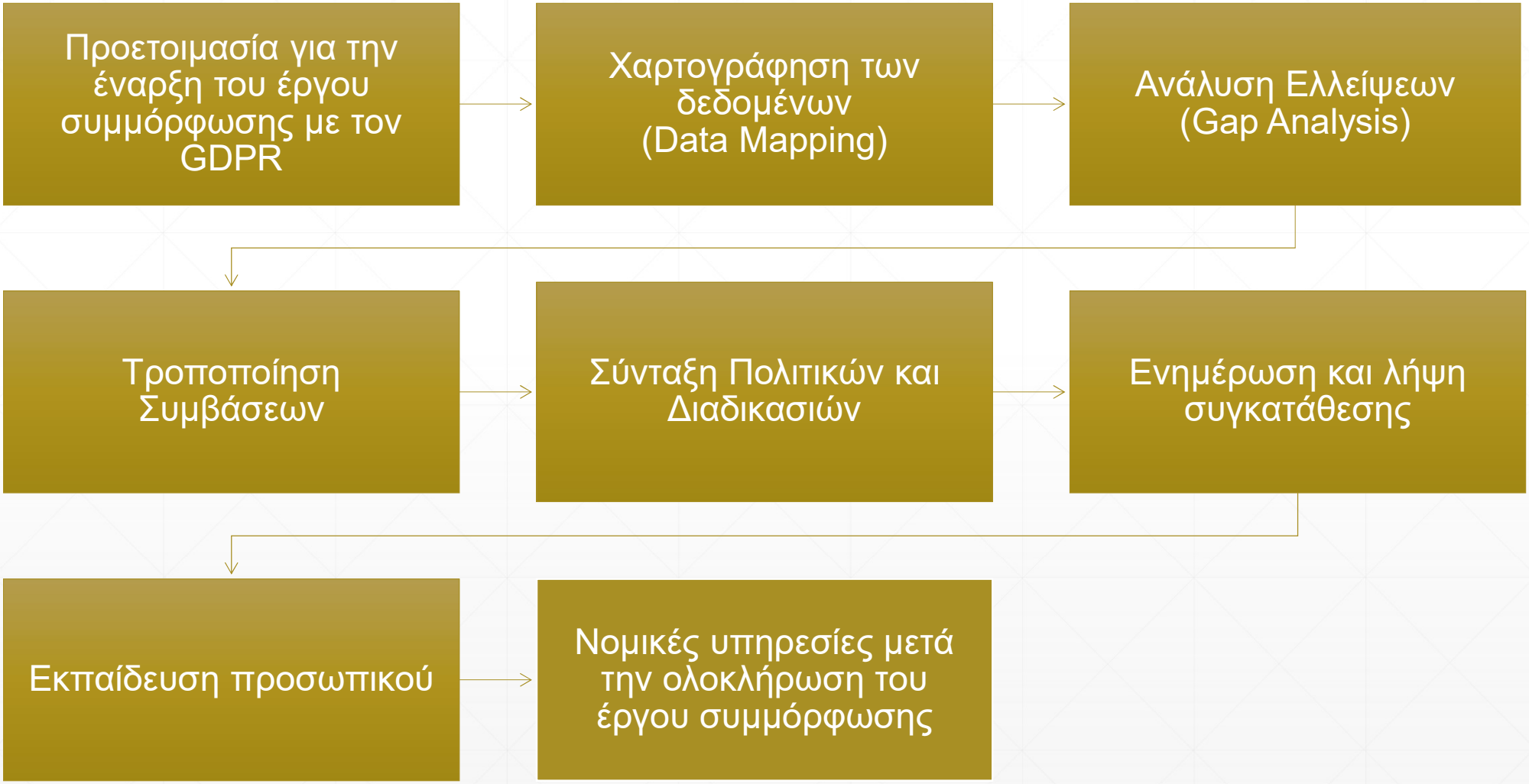
- να κατανοήσει τον τρόπο λειτουργίας της επιχείρησης.
- να συνεργαστεί επιτυχώς με πρόσωπα άλλων ειδικοτήτων.
- να δώσει στην επιχείρηση την αίσθηση ασφάλειας.
- να κατευθύνει σωστά την επιχείρηση βρίσκοντας τις κατάλληλες, αλλά και συνάμα πιο εύκολα υλοποιήσιμες λύσεις.

ΤΙΝΤΖΟΓΛΙΔΟΥ & ΣΥΝΕΡΓΑΤΕΣ
ΔΙΚΗΓΟΡΙΚΟ ΓΡΑΦΕΙΟ

ΤΙΝΤΖΟΓΛΙΔΟΥ
& ΣΥΝΕΡΓΑΤΕΣ
ΔΙΚΗΓΟΡΙΚΟ ΓΡΑΦΕΙΟ

Οι ενέργειες του νομικού συμβούλου στη συμμόρφωση της επιχείρησης

ΤΙΝΤΖΟΓΛΙΔΟΥ & ΣΥΝΕΡΓΑΤΕΣ
ΔΙΚΗΓΟΡΙΚΟ ΓΡΑΦΕΙΟ



ΤΙΝΤΖΟΓΛΙΔΟΥ
& ΣΥΝΕΡΓΑΤΕΣ
ΔΙΚΗΓΟΡΙΚΟ ΓΡΑΦΕΙΟ

Ας ξεκινήσουμε το ταξίδι της συμμόρφωσης!

ΤΙΝΤΖΟΓΛΙΔΟΥ
& ΣΥΝΕΡΓΑΤΕΣ
ΔΙΚΗΓΟΡΙΚΟ ΓΡΑΦΕΙΟ

1. Προετοιμασία για την έναρξη του έργου συμμόρφωσης με τον GDPR

- Ενημέρωση των στελεχών της επιχείρησης σχετικά με το αντικείμενο του έργου και εν γένει με τον Κανονισμό GDPR.
- Κατανόηση του αντικειμένου της επιχείρησης.
- Συναπόφαση για το πλάνο ενεργειών συμμόρφωσης της επιχείρησης.
- Δέσμευση της διοίκησης.

ΤΙΝΤΖΟΓΛΙΔΟΥ
& ΣΥΝΕΡΓΑΤΕΣ
ΔΙΚΗΓΟΡΙΚΟ ΓΡΑΦΕΙΟ

2. Χαρτογράφηση των δεδομένων (Data Mapping) σύμφωνα με το άρθρο 30 του GDPR

- Το πρώτο βήμα και ίσως και το κρισιμότερο κατά την εκτέλεση του έργου συμμόρφωσης μιας επιχείρησης με τον GDPR.
- Σκοπός της χαρτογράφησης είναι να μάθουμε τί είδους δεδομένα (πελάτων, προμηθευτών, εργαζομένων) συλλέγει και επεξεργάζεται η επιχείρηση, για ποιο σκοπό, πού υπάρχουν, ποιος έχει πρόσβαση σε αυτά και για πόσο χρόνο τα διατηρεί.
- Χρήση ερωτηματολογίων και πραγματοποίηση των λεγόμενων «συνεντεύξεων» με στελέχη της επιχείρησης.

ΤΙΝΤΖΟΓΛΙΔΟΥ & ΣΥΝΕΡΓΑΤΕΣ
ΔΙΚΗΓΟΡΙΚΟ ΓΡΑΦΕΙΟ

Παράδειγμα ερωτήσεων ερωτηματολογίου

1) Το αντικείμενο της εταιρίας
2) Κατηγορίες υποκειμένων των δεδομένων (π.χ. πελάτες, καταναλωτές, εργαζόμενοι, προμηθευτές κ.λ.π)
3) Κατηγορίες προσωπικών δεδομένων
4) Ειδικές κατηγορίες δεδομένων
5) Χρήση των δεδομένων
6) Ποιοι εργαζόμενοι (υπό ποία ιδιότητα) έχουν πρόσβαση στα δεδομένα
7) Αποδέκτες των δεδομένων
8) Διαβίβαση δεδομένων εκτός Ε.Ε.
9) Χρόνος Τήρησης
10) Τεχνικά και οργανωτικά Μέτρα
11) Εκτελούντες την επεξεργασία
12) Ύπαρξη Πολιτικών και Διαδικασιών
13) Τρόπος ενημέρωσης υποκειμένων
14) Δικαιώματα και άσκηση τους από τα υποκείμενα
15) Ειδικό νομικό καθεστώς που διέπει την επιχείρηση

ΤΙΝΤΖΟΓΛΙΔΟΥ
& ΣΥΝΕΡΓΑΤΕΣ
ΔΙΚΗΓΟΡΙΚΟ ΓΡΑΦΕΙΟ

- Στην πράξη, στο στάδιο αυτό, δημιουργείται το Αρχείο Δραστηριοτήτων Επεξεργασίας, για το οποίο γίνεται λόγος στο άρθρο 30 του GDPR και το οποίο συνήθως τηρείται σε ηλεκτρονική μορφή (αρχείο excel). Στο στάδιο αυτό αποτυπώνεται η **υφιστάμενη κατάσταση της επιχείρησης.**

- **Μετά την συμμόρφωση της επιχείρησης με τον GDPR το αρχείο αυτό πρέπει να επικαιροποιηθεί**, ώστε, σε ενδεχόμενο έλεγχο, να αποτελεί στοιχείο απόδειξης της συμμόρφωσης της επιχείρησης. Η επιχείρηση είναι υποχρεωμένη να διαθέτει **πάντοτε επικαιροποιημένο** το αρχείο αυτό και οφείλει να το τροποποιεί/ συμπληρώνει, όποτε απαιτείται.

ΤΙΝΤΖΟΓΛΙΔΟΥ
& ΣΥΝΕΡΓΑΤΕΣ
ΔΙΚΗΓΟΡΙΚΟ ΓΡΑΦΕΙΟ

ΥΠΕΥΘΥΝΟΣ ΕΠΕΞΕΡΓΑΣΙΑΣ					
Όνομα και στοιχεία επικοινωνίας		Υπεύθυνος Προστασίας Δεδομένων (αν υφίσταται)		Εκπρόσωπος (αν υφίσταται)	
Όνομα		Όνομα		Όνομα	
Ταχυδρομική Διεύθυνση		Ταχυδρομική Διεύθυνση		Ταχυδρομική Διεύθυνση	
Διεύθυνση Ηλεκτρονικού Ταχυδρομείου		Διεύθυνση Ηλεκτρονικού Ταχυδρομείου		Διεύθυνση Ηλεκτρονικού Ταχυδρομείου	
Τηλέφωνο		Τηλέφωνο		Τηλέφωνο	

Άρθρο 30 Αρχείο δραστηριοτήτων επεξεργασίας

Λειτουργία Επιχείρησης	Σκοπός της Επεξεργασίας	Όνομα και στοιχεία επικοινωνίας από κοινού υπεύθυνου επεξεργασίας (αν υφίσταται)	Κατηγορίες Υποκειμένων	Κατηγορίες Προσωπικών Δεδομένων	Κατηγορίες Αποδεκτών	Σύνδεσμο Εκτελούν

ΤΙΝΤΖΟΓΛΙΔΟΥ
& ΣΥΝΕΡΓΑΤΕΣ
ΔΙΚΗΓΟΡΙΚΟ ΓΡΑΦΕΙΟ

Το Αρχείο Δραστηριοτήτων Επεξεργασίας (Data Mapping) επιχείρησης που ενεργεί ως Υπεύθυνος Επεξεργασίας θα πρέπει να περιλαμβάνει:

- το όνομα και τα στοιχεία επικοινωνίας του Υπευθύνου Επεξεργασίας.
- τυχόν Από Κοινού Υπευθύνου Επεξεργασίας.
- τυχόν εκπροσώπου του Υπευθύνου Επεξεργασίας και τυχόν Υπευθύνου Προστασίας δεδομένων.
- τους σκοπούς της επεξεργασίας.
- τις κατηγορίες υποκειμένων των δεδομένων.
- τις κατηγορίες προσωπικών δεδομένων.
- τις κατηγορίες αποδεκτών στους οποίους πρόκειται να γνωστοποιηθούν ή γνωστοποιήθηκαν τα προσωπικά δεδομένα.
- τις κατηγορίες αποδεκτών σε τρίτες χώρες ή διεθνείς οργανισμούς, συμπεριλαμβανομένων του προσδιορισμού της εν λόγω τρίτης χώρας ή του διεθνούς οργανισμού.
- σε περίπτωση διαβιβάσεων τρίτες χώρες της τεκμηρίωσης των κατάλληλων εγγυήσεων.
- τις προβλεπόμενες προθεσμίες διαγραφής των διάφορων κατηγοριών δεδομένων.
- γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφάλειας.

ΤΙΝΤΖΟΓΛΙΔΟΥ
& ΣΥΝΕΡΓΑΤΕΣ
ΔΙΚΗΓΟΡΙΚΟ ΓΡΑΦΕΙΟ

Το Αρχείο Δραστηριοτήτων Επεξεργασίας (Data Mapping) επιχείρησης που ενεργεί ως <u>Εκτελών την Επεξεργασία</u> θα πρέπει να περιλαμβάνει:

- το όνομα και τα στοιχεία επικοινωνίας του εκτελούντος ή των εκτελούντων την επεξεργασία.
- των υπευθύνων επεξεργασίας εκ μέρους των οποίων ενεργεί ο εκτελών.
- τυχόν εκπροσώπου του υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία.
- του υπευθύνου προστασίας δεδομένων.
- τις κατηγορίες επεξεργασιών που διεξάγονται εκ μέρους κάθε υπευθύνου επεξεργασίας.
- σε περίπτωση διαβιβάσεων τρίτες χώρες της τεκμηρίωσης των κατάλληλων εγγυήσεων.
- όπου είναι δυνατό, γενική περιγραφή των κατάλληλων τεχνικών και οργανωτικών μέτρων προκειμένου να διασφαλιστεί το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων.

ΤΙΝΤΖΟΓΛΙΔΟΥ
& ΣΥΝΕΡΓΑΤΕΣ
ΔΙΚΗΓΟΡΙΚΟ ΓΡΑΦΕΙΟ

3. Gap Analysis (Ανάλυση Ελλείψεων)
Ο προσδιορισμός της υφιστάμενης κατάστασης της επιχείρησης και η απόσταση της από τη συμμόρφωση

- Νομοτεχνική και αιτιολογημένη αναλυτική έκθεση ελλείψεων, ορθών πρακτικών και προτάσεων βελτίωσης συμμόρφωσης με τον GDPR.
- Στο Gap Analysis καταγράφεται:
  I. Η υφιστάμενη κατάσταση, δηλαδή ο τρόπος που επεξεργάζεται η επιχείρηση τα δεδομένα σήμερα
  II. Η έλλειψη απόκλιση από τις απαιτήσεις του Κανονισμού και
  III. Οι αναγκαίες ενέργειες συμμόρφωσης με τον Κανονισμό.
- Ο «οδικός χάρτης» για το τι πρέπει να αλλάξουμε στην επιχείρηση

Α/Α	Έλλειψη/Απόκλιση	Ενέργεια συμμόρφωσης	Υποχρεωτική Ενέργεια/ Πρόταση	Βάση απαίτησης	Προτεραιότητα υλοποίησης
1.	Στην είσοδο της Επιχείρησης έχει εγκατασταθεί σύστημα βιντεοεπιτήρησης, από το οποίο δεν γίνεται καταγραφή ήχου, χωρίς όμως να έχει τοποθετηθεί σχετική ενημερωτική πινακίδα.	Προτού ένα πρόσωπο εισέλθει στην εμβέλεια του συστήματος βιντεοεπιτήρησης, η Επιχείρηση, ως Υπεύθυνος Επεξεργασίας, οφείλει να το ενημερώνει, με τρόπο εμφανή και κατανοητό, ότι πρόκειται να εισέλθει σε χώρο που βιντεοσκοπείται. Προς τούτο, οφείλει να τοποθετήσει ευδιάκριτες πινακίδες στις οποίες θα αναγράφονται τα στοιχεία του Υπευθύνου Επεξεργασίας για λογαριασμό του οποίου γίνεται η βιντεοεπιτήρηση, δηλαδή της Επιχείρησης, ο σκοπός της επεξεργασίας, τυχόν έννομα συμφέροντα, τα δικαιώματα που έχουν τα πρόσωπα που καταγράφονται, οι αποδέκτες των δεδομένων, τυχόν διαβίβαση σε χώρα εκτός ΕΕ, το χρονικό διάστημα αποθήκευσης και τα στοιχεία επικοινωνίας του Υπευθύνου Προστασίας (Data Protection Officer). Επιπλέον θα πρέπει να εξεταστεί η εικόνα που λαμβάνεται, ούτως ώστε να βεβαιωθεί ότι δεν λαμβάνεται εικόνα από εισόδους ή εσωτερικό γειτονικών γραφείων, κατοικιών ή άλλων χώρων. Σε περίπτωση που λαμβάνεται εικόνα από τους ως άνω χώρους, πρέπει να τροποποιηθεί το πεδίο λήψης της κάμερας ώστε να εστιάζει μόνο στο χώρο της εισόδου.	Υ	Άρθρα GDPR: 5, 6, 12, 13 Άρθρο 5 του Σχεδίου Ελληνικού Νόμου για την προστασία δεδομένων προσωπικού χαρακτήρα	Υψηλή

ΤΙΝΤΖΟΓΛΙΔΟΥ & ΣΥΝΕΡΓΑΤΕΣ
ΔΙΚΗΓΟΡΙΚΟ ΓΡΑΦΕΙΟ

4. Τροποποίηση Συμβάσεων της επιχείρησης με πελάτες/προμηθευτές/ εργαζόμενους. Τι πρέπει να περιλαμβάνει;

- Νέες απαιτήσεις Κανονισμού → Ανάγκη τροποποίησης συμβάσεων.
- Συμβάσεις με εργαζόμενους/ πελάτες/ προμηθευτές.
- Τροποποίηση μόνο των σχετικών με τα προσωπικά δεδομένα άρθρων των συμβάσεων.
- Εύρεση σχέσης των συμβαλλομένων μερών.
- Συνήθως υπό μορφή παραρτήματος.

ΤΙΝΤΖΟΓΛΙΔΟΥ & ΣΥΝΕΡΓΑΤΕΣ
ΔΙΚΗΓΟΡΙΚΟ ΓΡΑΦΕΙΟ

5. Σύνταξη Πολιτικών και Διαδικασιών

- Πολιτική Προστασίας Προσωπικών Δεδομένων → «νόμος» για την επιχείρηση

Παρέχει πληροφορίες σχετικά με:

I. τη συλλογή, αποθήκευση, επεξεργασία και χρήση των προσωπικών δεδομένων των πελατών μιας επιχείρησης
II. τη νομιμοποιητική βάση επεξεργασίας για κάθε σκοπό επεξεργασίας
III. τα δικαιώματα των υποκειμένων
IV. τον τρόπο που μπορούν να ασκήσουν τα δικαιώματά τους τα υποκείμενα.

ΤΙΝΤΖΟΓΛΙΔΟΥ & ΣΥΝΕΡΓΑΤΕΣ
ΔΙΚΗΓΟΡΙΚΟ ΓΡΑΦΕΙΟ

6. Ενημέρωση Υποκειμένων των δεδομένων και λήψη συγκατάθεσης

- Η ενημέρωση του υποκειμένου των δεδομένων θα πρέπει να γίνεται σύμφωνα με την **αρχή της διαφάνειας** (άρθρα 12-22) (πληροφόρησης, πρόσβασης, διόρθωσης, διαγραφής, περιορισμού της επεξεργασίας, φορητότητας, εναντίωσης και κατάρτισης προφίλ) και να περιέχει τις **αναγκαίες πληροφορίες σύμφωνα με τα άρθρα 13 και 14.**
- Όταν χρησιμοποιείται ως νομιμοποιητική βάση η συγκατάθεση, αυτή θα πρέπει να δίνεται με **σαφή θετική ενέργεια**, να είναι **ελεύθερη**, **συγκεκριμένη** και **ρητή**.

Newsletter (βλ. Οδηγία για την ηλεκτρονική συγκατάθεση 2/2011 ΑΠΔΠΧ, αποφάσεις 50/2017 και 70/2017 της ΑΠΔΠΧ).

ΤΙΝΤΖΟΓΛΙΔΟΥ
& ΣΥΝΕΡΓΑΤΕΣ
ΔΙΚΗΓΟΡΙΚΟ ΓΡΑΦΕΙΟ

7. Εκπαίδευση προσωπικού

- Οι άνθρωποι ξεχνούν γρήγορα, γι' αυτό και απαιτείται περιοδική εκπαίδευση του προσωπικού μιας επιχείρησης σε τακτική βάση.
- Απλός και κατανοητός τρόπος παρουσίασης των θεμάτων.
- Παραδείγματα από τον συνήθη κύκλο εργασιών της επιχείρησης.
- Επίλυση όλων των βασικών απορριών των συμμετεχόντων που σχετίζονται, βεβαίως, με το αντικείμενο της επιχείρησης.
- Δεν αρκεί η λεκτική μεταφορά του Κανονισμού.

ΤΙΝΤΖΟΓΛΙΔΟΥ
& ΣΥΝΕΡΓΑΤΕΣ
ΔΙΚΗΓΟΡΙΚΟ ΓΡΑΦΕΙΟ

Πιστεύετε ότι τελείωσε η συμμόρφωση της επιχείρησης;

ΤΙΝΤΖΟΓΛΙΔΟΥ
& ΣΥΝΕΡΓΑΤΕΣ
ΔΙΚΗΓΟΡΙΚΟ ΓΡΑΦΕΙΟ

8. Παροχή υποστηρικτικών υπηρεσιών μετά την ολοκλήρωση του έργου συμμόρφωσης

- Παρακολούθηση των αλλαγών του νομικού πλαισίου → Ενημέρωση της επιχείρησης.
- Συνδρομή στον DPO.
- Επικαιροποίηση Πολιτικών και Διαδικασιών.
- Συμβουλευτική υποστήριξη για τη διαχείριση τυχόν περιστατικών παραβίασης του GDPR.

ΤΙΝΤΖΟΓΛΙΔΟΥ
& ΣΥΝΕΡΓΑΤΕΣ
ΔΙΚΗΓΟΡΙΚΟ ΓΡΑΦΕΙΟ

! Ο GDPR δεν είναι μόνο αρχεία, πολιτικές και διαδικασίες, αλλά δημιουργεί μία νέα εταιρική κουλτούρα.

! Η επιλογή της συμμόρφωσης ως επιχειρηματική στρατηγική προσφέρει στην επιχείρηση όχι μόνο προστασία αλλά και ανταγωνιστικό πλεονέκτημα.

ΤΙΝΤΖΟΓΛΙΔΟΥ
& ΣΥΝΕΡΓΑΤΕΣ
ΔΙΚΗΓΟΡΙΚΟ ΓΡΑΦΕΙΟ

Ευχαριστώ για την προσοχή σας!!

Νόπη Τιντζογλίδου