Πόσο έτοιμοι είμαστε για το νέο Κανονισμό περί Προστασίας Προσωπικών Δεδομένων; Οδηγός Βέλτιστων Πρακτικών.

Are we GDPR ready? Best Practices Guide.

Εβίτα Βαϊνανίδη

Δικηγόρος, LL.M.

ΔΙΚΗΓΟΡΙΚΗ ΕΤΑΙΡΕΙΑ
ΒΑΪΝΑΝΙΔΗΣ ΟΙΚΟΝΟΜΟΥ & ΣΥΝΕΡΓΑΤΕΣ

ΔΙΚΗΓΟΡΙΚΗ ΕΤΑΙΡΕΙΑ
ΒΑΪΝΑΝΙΔΗΣ ΟΙΚΟΝΟΜΟΥ & ΣΥΝΕΡΓΑΤΕΣ

ΔΙΚΗΓΟΡΙΚΗ ΕΤΑΙΡΕΙΑ
ΒΑΪΝΑΝΙΔΗΣ ΟΙΚΟΝΟΜΟΥ & ΣΥΝΕΡΓΑΤΕΣ

Πόσο έτοιμοι είμαστε για το νέο Κανονισμό περί Προστασίας Προσωπικών Δεδομένων; (Are we GDPR ready?)

- Στο τέλος του 2018, περισσότερες από το 50% των επιχειρήσεων που επηρεάζονται από το νέο Κανονισμό **δεν** θα έχουν συμμορφωθεί πλήρως με τις απαιτήσεις του.
- Δύο στις τρείς επιχειρήσεις **δεν** είναι έτοιμες να ξεχάσουν…
- Περισσότερες από τις μισές επιχειρήσεις **δεν** έχουν ξεκινήσει σήμερα οποιαδήποτε διεργασία, έστω και ελάχιστης συμμόρφωσης με το νέο Κανονισμό!

Οι συνέπειες και η πολυπλοκότητα της συμμόρφωσης με το νέο Κανονισμό **δεν** έχουν γίνει ακόμα απολύτως αντιληπτές από τις επιχειρήσεις

Η προετοιμασία είναι βέβαιο ότι θα διαρκέσει αρκετούς μήνες, πιθανότατα περισσότερο από χρόνο!

Οδηγός Βέλτιστων Πρακτικών (Best Practices Guide)

ΔΙΚΗΓΟΡΙΚΗ ΕΤΑΙΡΕΙΑ
ΒΑΪΝΑΝΙΔΗΣ ΟΙΚΟΝΟΜΟΥ & ΣΥΝΕΡΓΑΤΕΣ

Βήμα 1: Ενημέρωση & Εξοικείωση (Understanding the GDPR)

Μελέτη Κανονισμού ΕΕ 2016/679

- Κατανοούμε τις αλλαγές που επιφέρει & πώς επηρεάζουν την επιχείρηση
- Εξοικειωνόμαστε με βασικούς ορισμούς Κανονισμού (*περιορισμός επεξεργασίας, κατάρτιση προφίλ, ψευδωνυμοποίηση…*)

- Προσοχή στις 6+1 Αρχές:
  - ✓Νομιμότητας, αντικειμενικότητας & διαφάνειας
  - ✓Περιορισμού του σκοπού
  - ✓Ελαχιστοποίησης των δεδομένων
  - ✓Ακρίβειας δεδομένων
  - ✓Περιορισμός της περιόδου αποθήκευσης
  - ✓Ακεραιότητας & εμπιστευτικότητας

Λογοδοσία!

Βήμα 1: Ενημέρωση & Εξοικείωση (Understanding the GDPR)

- **Ενημέρωση ανώτατων στελεχών επιχείρησης**
  - ✓ Χρειαζόμαστε υποστήριξη διοίκησης
  - ✓ Χρειαζόμαστε πόρους (HR, τεχνολογία)

- **Επιμόρφωση υπαλλήλων επιχείρησης**
  - ✓ Ενημέρωση για επερχόμενες μεταβολές & πιθανές επιπτώσεις σε περίπτωση παραβίασης
  - ✓ Εκπαίδευση υποχρεωτική & στοχευμένη, κατά περίπτωση
  - ✓ Καλλιέργεια ευαισθησίας & δημιουργία κουλτούρας

Βήμα 2: Διορισμός Υπευθύνου Προστασίας Δεδομένων (Appointment of a Data Protection Officer)

- Παρέχει εχέγγυα ανεξαρτησίας & εμπειρία στον τομέα του δικαίου & των πρακτικών προστασίας δεδομένων
- Σχεδιάζει & παρακολουθεί εσωτερική συμμόρφωση με Κανονισμό, συμβουλεύει, συνδράμει (‘Pilot’)
- Αναπτύσσει δράσεις ευαισθητοποίησης
- Συνεργάζεται με εθνική ΑΠΔΠΧ & ενεργεί ως σημείο επικοινωνίας με την Αρχή και τα υποκείμενα

- Καθοδηγεί την επιχείρηση στα επόμενα…

Βήμα 3: Χαρτογράφηση Δεδομένων (Data Mapping)

- **Κατανόηση κύκλου ζωής** των δεδομένων. Εξετάζουμε & καταγράφουμε:
  - ✓ Είδος δεδομένων που διατηρεί η εταιρεία
  - ✓ Πώς τα συλλέξαμε
  - ✓ Πού βρίσκονται αποθηκευμένα (και back-up)
  - ✓ Ποια συστήματα χρησιμοποιούμε για την επεξεργασία τους
  - ✓ Συνεργασία με εξωτερικούς παρόχους υπηρεσιών
  - ✓ Αποδέκτες των δεδομένων
  - ✓ Χρόνο διατήρησης κάθε κατηγορίας δεδομένων
  - ✓ Διαδικασίες καταστροφής δεδομένων

- Μόνο εάν έχουμε πλήρη εικόνα της ροής των δεδομένων, μπορούμε να:
  - ✓ Αξιολογήσουμε την ετοιμότητα της επιχείρησης
  - ✓ Δημιουργήσουμε έναν χάρτη, ώστε με ρεαλιστικά βήματα & στόχους να επιτύχουμε συμμόρφωση

Βήμα 3: Χαρτογράφηση Δεδομένων (Data Mapping)

- Μία από τις πρώτες & κυριότερες προκλήσεις του Νέου Κανονισμού
  - ✓ Απαιτείται ένα είδος εσωτερικού πληροφοριακού ελέγχου
  - ✓ Προϋποθέτει τη συμμετοχή όλων των τμημάτων της επιχείρησης
  - ✓ Εμπλέκονται πολλές τεχνολογίες και συστήματα
  - ✓ Δεδομένα συχνά δύσκολο να εντοπιστούν (dark data) – διασκορπισμένα σε διάφορα αποθηκευτικά μέσα, μη δομημένα
  - ✓ Χρονοβόρα διαδικασία, ανάλογα με βαθμό οργάνωσης επιχείρησης

Σκληρός Δίσκος

Έγγραφα

Διακομιστές

Υπολογιστικό Νέφος

Εξωτερικοί Πάροχοι Υπηρεσιών

Εφαρμογές

Διαδικτυακοί Τόποι

Βήμα 4: Δικαιώματα υποκειμένων (Individuals' rights)

Ο Κανονισμός **ενισχύει** τα υφιστάμενα & **δημιουργεί νέα** δικαιώματα για τα υποκείμενα

Βήμα 4: Δικαιώματα υποκειμένων (Individuals' Rights)

- Εξετάζουμε πώς τα δικαιώματα επηρεάζουν τις δραστηριότητες της επιχείρησης
- Σχεδιάζουμε τον τρόπο άσκησης από τα υποκείμενα των δικαιωμάτων τους
- Επικαιροποιούμε διαδικασίες χειρισμού αιτημάτων & ικανοποίησης δικαιωμάτων
- Εξετάζουμε εάν τα συστήματά μας μπορούν να ανταποκριθούν στα αιτήματα των υποκειμένων (δικαίωμα στη λήθη, πρόσβαση, διόρθωση ...)

Βήμα 5: Έλεγχος πληροφόρησης (Communicating Privacy Information)

- Επικαιροποιούμε πολιτικές ιδιωτικότητας & κείμενα ενημέρωσης υποκειμένων (έντυπα, ιστοσελίδες κλπ.), βάσει νέου Κανονισμού
- Αρχή διαφάνειας: Ενημέρωση σαφής, κατανοητή, εύκολα προσβάσιμη
- Υπάρχουν **πολλά** που πρέπει να πούμε στα υποκείμενα με **απλό τρόπο**!
- Περιλαμβάνει:

- Στοιχεία υπευθύνου επεξεργασίας
- Σκοπούς επεξεργασίας
- Αποδέκτες ή κατηγορίες αποδεκτών
- Δικαιώματα υποκειμένου
- Κατηγορίες δεδομένων
- Πηγές προέλευσης
- Πρόθεση διαβίβασης σε τρίτη χώρα & εγγυήσεις/απόφαση επάρκειας
- Νομική βάση επεξεργασίας
- Στοιχεία επικοινωνίας ΥΠΔ
- Χρονικό διάστημα αποθήκευσης
- Εάν αποτελεί προϋπόθεση για τη σύναψη σύμβασης & ποιες οι συνέπειες άρνησης
- Πρόθεση κατάρτισης προφίλ

Βήμα 6: Συγκατάθεση (Consent)

- Ελέγχουμε και αναθεωρούμε μεθόδους αναζήτησης, εξασφάλισης & καταγραφής συγκατάθεσης, για κάθε επιδιωκόμενο σκοπό επεξεργασίας
- Βάρος απόδειξης → υπεύθυνος επεξεργασίας
- Για **ειδικές κατηγορίες** δεδομένων απαιτείται **ρητή συγκατάθεση** των υποκειμένων
- Προσοχή στη διατύπωση των δηλώσεων συγκατάθεσης!
- Αίτημα για συγκατάθεση <u>σαφώς διακριτό</u>
- Ανάκληση εξίσου εύκολη με χορήγηση

☒ Δεν συνιστούν συγκατάθεση:

Σιωπή, αδράνεια, προσυμπληρωμένα τετραγωνίδια…

Βήμα 7: Έλεγχος Νομικής Βάσης (Identifying Lawful Basis)

- Κάθε δραστηριότητα μίας επιχείρησης πρέπει να υπακούει στις προϋποθέσεις για νόμιμη επεξεργασία που θέτει ο Κανονισμός
- Προσδιορίζουμε & καταγράφουμε τη νομική βάση για κάθε επεξεργασία
- Η νομική βάση επεξεργασίας πρέπει να δηλώνεται στα υποκείμενα!
- Επεξεργασία δεδομένων σύννομη όταν:
  - Στηρίζεται στη συναίνεση
  - Είναι απαραίτητη για εκτέλεση σύμβασης
  - Προβλέπεται από το νόμο
  - Είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος υποκειμένου ή τρίτου
  - Είναι απαραίτητη για την εκπλήρωση καθήκοντος προς το δημόσιο συμφέρον
  - Στηρίζεται σε έννομο συμφέρον υπό τον όρο ότι υπερέχει των συμφερόντων, δικαιωμάτων, θεμελιωδών ελευθεριών υποκειμένου
- Εάν επεξεργασία βασίζεται στη συγκατάθεση, εξετάζουμε εάν μπορεί να στηριχθεί και σε άλλη νομική βάση

Βήμα 8: Διαχείριση κινδύνου (Managing risk)

I. Προστασία δεδομένων ήδη από το σχεδιασμό και εξ' ορισμού (Privacy by Design & by Default)

➢Η επιχείρηση οφείλει κατά το σχεδιασμό και εξ' ορισμού να δημιουργεί δομή, τεχνολογία και διαδικασίες που θα ανταποκρίνονται στις απαιτήσεις του Κανονισμού

➢Απόδειξη συμμόρφωσης → θέσπιση εσωτερικών πολιτικών & λήψη μέτρων:

- Κατά τη στιγμή καθορισμού των μέσων επεξεργασίας, επιλογής, ανάπτυξης, σχεδιασμού υπηρεσιών, εφαρμογών...
- Κατά τη στιγμή της επεξεργασίας

➢Παραδείγματα: *ψευδωνυμοποίηση, ελαχιστοποίηση επεξεργασίας δεδομένων, ενσωμάτωση εγγυήσεων στην επεξεργασία*

Βήμα 8: Διαχείριση κινδύνου (Managing Risk)

ΙΙ. Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων (PIA)

- Όταν ένα είδος επεξεργασίας ενδέχεται να επιφέρει υψηλό κίνδυνο για δικαιώματα & ελευθερίες των υποκειμένων
- «Άσκηση» αξιολόγησης επιπτώσεων σχεδιαζόμενων πράξεων επεξεργασίας
- Περιέχει, κατ' ελάχιστο:
  - Περιγραφή πράξεων & σκοπών επεξεργασίας
  - Εκτίμηση αναγκαιότητας & αναλογικότητας των πράξεων
  - Εκτίμηση κινδύνων
  - Προβλεπόμενα μέτρα αντιμετώπισης κινδύνων
- Παραδείγματα: *πράξεις επεξεργασίας μεγάλης κλίμακας, χρήση νέας τεχνολογίας, κατάρτιση προφίλ*
- Σημαντική η απόδειξη εκτίμησης αντικτύπου σε περίπτωση περιστατικού παραβίασης δεδομένων

Βήμα 9: Παραβιάσεις δεδομένων (Data breaches)

- Η επιχείρηση οφείλει να λαμβάνει εκσυγχρονισμένα τεχνικά & οργανωτικά μέτρα για την προστασία των δεδομένων που επεξεργάζεται

- Σε περίπτωση παραβίασης, υποχρέωση γνωστοποίησης στην εποπτική αρχή και στο υποκείμενο αμελλητί, το αργότερο **εντός 72 ωρών** *από την ανακάλυψη του περιστατικού* (με εξαιρέσεις)

- Περιεχόμενο:
  - ✓ Φύση παραβίασης
  - ✓ Τρόπος αναγνώρισης της παραβίασης
  - ✓ Κατηγορίες δεδομένων
  - ✓ Αριθμός επηρεαζόμενων υποκειμένων & αρχείων
  - ✓ Στοιχεία ΥΠΔ
  - ✓ Ενδεχόμενες συνέπειες παραβίασης
  - ✓ Διορθωτικά & υπάρχοντα μέτρα ασφαλείας

Βήμα 9: Παραβιάσεις δεδομένων (Data breaches)

- **Δημιουργία Πλάνου Αντιμετώπισης Περιστατικών Παραβίασης**
  - ✓ Ύπαρξη κατάλληλων διαδικασιών εντοπισμού, αναφοράς & έρευνας περιστατικών
  - ✓ Έλεγχος μέτρων ασφαλείας που εφαρμόζει σήμερα η επιχείρηση – ανταποκρίνονται στις απαιτήσεις του νέου Κανονισμού;

- **Δημιουργία Ομάδας Αντιμετώπισης Περιστατικών Παραβίασης**
  - ✓ Στελέχη από διάφορα τμήματα επιχείρησης (Legal, IT, Compliance, Risk Management…)
  - ✓ Δημιουργία λίστας επαφών με εμπλεκόμενους στη διαχείριση περιστατικών παραβίασης

Βήμα 10: Διασυνοριακή ροή δεδομένων (International data transfers)

- Εξετάζουμε & καταγράφουμε σε ποιες χώρες η επιχείρηση διαβιβάζει δεδομένα
- Εάν διαβίβαση προς τρίτες χώρες που δεν παρέχουν ικανοποιητικό επίπεδο προστασίας δεδομένων, χρησιμοποιούμε κυρίως ως μηχανισμό διαβίβασης:
  - Πρότυπες συμβατικές ρήτρες (SCCs)
  - Δεσμευτικούς εταιρικούς κανόνες (BCRs)
  - Ασπίδα προστασίας (Privacy Shield, αφορά Η.Π.Α.)

Βήμα 11: Επικεφαλής εποπτική αρχή (Lead data protection supervisory authority)

- Μηχανισμός Μιας Στάσης:

  Επιτρέπει σε επιχείρηση που δραστηριοποιείται σε πολλά κράτη μέλη, να συνομιλεί με μία μόνο εποπτική αρχή, στο κράτος μέλος της κύριας εγκατάστασής της

- Αφορά επιχείρηση:
  - ✓ Εγκατεστημένη σε περισσότερα του ενός κράτη μέλη
  - ✓ Που διενεργεί διασυνοριακές πράξεις επεξεργασίας δεδομένων

- Κράτος μέλος κύριας εγκατάστασης:
  - Τόπος κεντρικής διοίκησης στην Ε.Ε. ή
  - Τόπος λήψης αποφάσεων για σκοπούς & μέσα επεξεργασίας (ουσιαστική & πραγματική άσκηση δραστηριοτήτων διαχείρισης)

- Όμιλος επιχειρήσεων: κύρια εγκατάσταση ελέγχουσας επιχείρησης, εκτός εάν σκοποί & μέσα επεξεργασίας καθορίζονται από άλλη επιχείρηση

Βήμα 12: Επίδειξη διαρκούς συμμόρφωσης (Demonstrate ongoing compliance)

- Αρχή της Λογοδοσίας ↔ Αρχή της Διαφάνειας
- Η εταιρεία οφείλει αφενός να συμμορφώνεται, αφετέρου να αποδεικνύει της συμμόρφωσή της

- Η εταιρεία πρέπει να:
  - ✓ Χτίσει ένα πρόγραμμα συμμόρφωσης
  - ✓ Τηρεί λεπτομερή αρχεία δραστηριοτήτων επεξεργασίας
  - ✓ Εφαρμόζει κατάλληλα τεχνικά & οργανωτικά μέτρα προστασίας
  - ✓ Επανεξετάζει πολιτικές & διαδικασίες διαχείρισης δεδομένων
  - ✓ Να εκπονεί εσωτερικούς ελέγχους, ώστε να εντοπίζονται κενά και αδυναμίες

- Η ορθή τήρηση αρχείων δραστηριοτήτων & η ενδελεχής καταγραφή προσπαθειών εταιρείας να προστατεύσει τα δεδομένα που επεξεργάζεται, της επιτρέπει να αποδεικνύει ανά πάσα στιγμή τη συμμόρφωσή της με τις βασικές αρχές του νέου Κανονισμού.

You can't win unless you
first begin. So start now.
Robin Sharma

Ευχαριστώ για την προσοχή σας!

Εβίτα Βαϊνανίδη

evitavainanidi@ve-legal.com

ΔΙΚΗΓΟΡΙΚΗ ΕΤΑΙΡΕΙΑ
ΒΑΪΝΑΝΙΔΗΣ ΟΙΚΟΝΟΜΟΥ & ΣΥΝΕΡΓΑΤΕΣ