HADPP ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ & ΙΔΙΩΤΙΚΟΤΗΤΑΣ

# Το Ηλεκτρονικό Εμπόριο στο νέο πλαίσιο προστασίας προσωπικών δεδομένων

eCommerce Expo 2017

www.dataprotection.gr

**Σπύρος Τάσσης**

**Δικηγόρος**

# Νέος Κανονισμός - Γενικά

- **Το νέο ιδιαίτερα αυστηρό πλαίσιο του Κανονισμού φαίνεται ότι αποτελεί και μία προσπάθεια κανονικοποίησης των οικονομικών/επιχειρηματικών όρων δραστηριοποίησης ιδίως στην ψηφιακή αγορά.**

- **Οι παραβάσεις ασφαλείας των δεδομένων είναι αναμενόμενες.**

- **Το ζητούμενο είναι κάθε υπεύθυνος να ενεργήσει σύμφωνα με τα όσα ορίζει ο Κανονισμός ώστε να ελαχιστοποιηθεί ο κίνδυνος.**

# Νέος Κανονισμός - Γενικά

**Είναι λοιπόν σημαντικό να ξεκινήσουμε με την παραδοχή ότι υπάρχει κίνδυνος για τα προσωπικά δεδομένα που οφείλεται κυρίως σε δύο παράγοντες:**

- **Οργανωτικό (ανεπαρκείς διαδικασίες, μη ασφαλή συστήματα και ελλιπής οργάνωση της επίβλεψης τους)**
- **Ανθρώπινο (ελλιπής εκπαίδευση του προσωπικού που τα χειρίζεται). Είναι εκπληκτικό το πόσα περιστατικά ασφαλείας οφείλονται στον ανθρώπινο παράγοντα.**

# Υποχρεώσεις Υπευθύνων Επεξεργασίας

**Οι υποχρεώσεις είναι διάσπαρτες στον Κανονισμό (κυρίως όμως άρθρα 28-37)**

- **Υποχρέωση Λογοδοσίας**
- **Ενημέρωση (awareness)**
- **Προστασία Ανηλίκων**
- **Συγκατάθεση**
- **Καταγραφή (διαδικασίες και συμβάντα)**
- **Εκτίμηση Επιπτώσεων**
- **Ανασχεδιασμός Διαδικασιών και Συστημάτων**
- **Υπεύθυνος Προστασίας Δεδομένων**
- **Πολιτικές Ασφαλείας**
- **Σεβασμός στα δικαιώματα**
- **Συνεργασία με τις Εποπτικές Αρχές**
- **Διαχείριση Παραβάσεων**
- **Ενημέρωση Αρχής και Υποκειμένων (γνωστοποίηση/ανακοίνωση)**
- **Διασυνοριακή Ροή (επάρκεια, δεσμευτικοί εταιρικοί κανόνες κλπ.)**

# Υπεύθυνος Προστασίας Δεδομένων (DPO)

- **Μέρος του συστήματος Λογοδοσίας**

- **Υποχρεωτικός όταν:**
  **α) η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα,**
  **β) οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες, λόγω της φύσης, του πεδίου εφαρμογής και/ή των σκοπών τους, απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα,**
  **γ) οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών**

- **Εθελοντικός (voluntarily)ως ένδειξη υπεύθυνης διαχείρισης των διαδικασιών και μηχανισμών.**

# Πολιτική Ασφαλείας

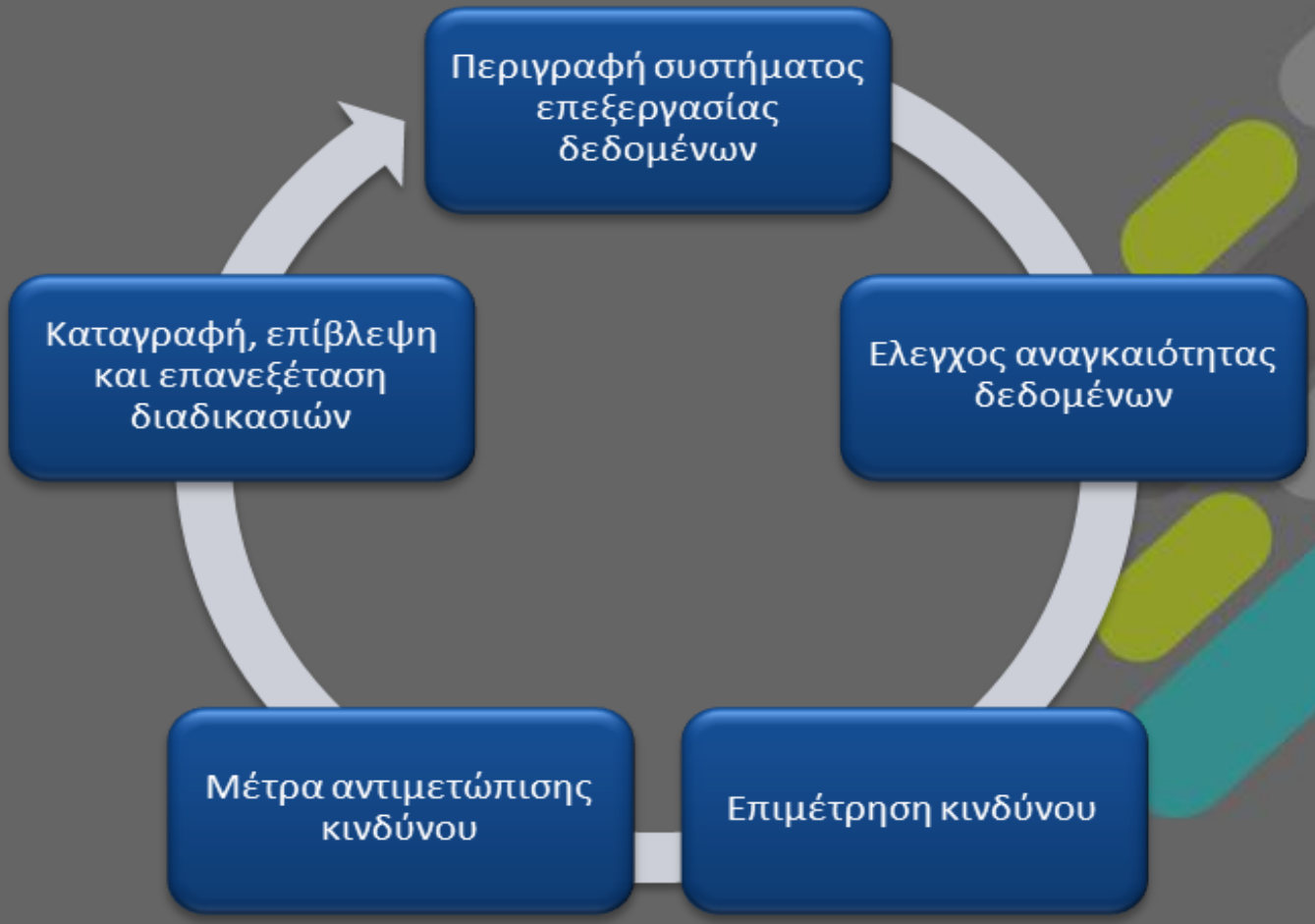
**Ανάλυση κινδύνου:**

- **πιθανές απειλές (τεχνολογικά κενά, ελλιπείς διαδικασίες, ακόμα και … δυσαρεστημένοι υπάλληλοι)**
- **κατηγοριοποίηση των δεδομένων ανάλογα με την κρισιμότητα τους**
- **αποτελεσματικές διαδικασίες μείωσης του αντικτύπου (DPIA)**

**Δραστηριότητες επεξεργασίας:**

- **Υψηλού κινδύνου (DPIA, διαβούλευση, γνωστοποιήσεις άρθρου 33)**
- **Κινδύνου (DPIA, γνωστοποιήσεις)**
- **Χαμηλού κινδύνου (προαιρετικό DPIA, χωρίς υποχρέωση γνωστοποιήσεων)**

# Ανάλυση Κινδύνου



# Privacy by Design – Privacy by Default

- ο υπεύθυνος επεξεργασίας εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων, και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία

- ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας. Αυτή η υποχρέωση ισχύει για το εύρος των δεδομένων προσωπικού χαρακτήρα που συλλέγονται, τον βαθμό της επεξεργασίας τους, την περίοδο αποθήκευσης και την προσβασιμότητά τους. Ειδικότερα, τα εν λόγω μέτρα διασφαλίζουν ότι, εξ ορισμού, τα δεδομένα προσωπικού χαρακτήρα δεν καθίστανται προσβάσιμα χωρίς την παρέμβαση του φυσικού προσώπου σε αόριστο αριθμό φυσικών προσώπων.

Σπύρος Τάσσης

# Προσωπικά Δεδομένα και Διαδίκτυο

## ➢ Cookies (ePrivacy)

- Απλούστεροι κανόνες για τα cookies με πιο φιλική προς το χρήστη διαδικασία, καθώς οι ρυθμίσεις του προγράμματος περιήγησης θα παρέχουν έναν εύκολο τρόπο αποδοχής ή απόρριψης των cookie παρακολούθησης και άλλων αναγνωριστικών.
- δεν απαιτείται συγκατάθεση για τα cookies που δεν επηρεάζουν την ιδιωτική ζωή και βελτιώνουν την εμπειρία του διαδικτύου (π.χ. να θυμάται το ιστορικό του καλαθιού αγορών, Google Analytics) ή τα cookies που χρησιμοποιούνται από έναν ιστότοπο για τον υπολογισμό του αριθμού των επισκεπτών.
- Προστασία από ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου: η πρόταση απαγορεύει ανεπιθύμητες ηλεκτρονικές επικοινωνίες μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου, SMS και αυτόματων τηλεφωνητών.
- Αποτελεσματικότερη επιβολή: η επιβολή των κανόνων εμπιστευτικότητας στον κανονισμό θα είναι αρμοδιότητα των αρχών προστασίας δεδομένων, οι οποίες είναι ήδη αρμόδιες για τους κανόνες του γενικού κανονισμού για την προστασία των δεδομένων.

Σπύρος Τάσσης

# Εποπτικές Αρχές

- Συνεργασία μεταξύ της επικεφαλής εποπτικής αρχής και των άλλων ενδιαφερόμενων εποπτικών αρχών
- Αμοιβαία συνδρομή (ιδίως, αιτήματα παροχής πληροφοριών και μέτρα ελέγχου, παραδείγματος χάρη αιτήματα για προηγούμενες διαβουλεύσεις και εγκρίσεις, ελέγχους και έρευνες)
- Κοινές επιχειρήσεις αρχών ελέγχου (κυρίως όταν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι εγκατεστημένος σε πολλά κράτη μέλη)
- Μηχανισμός συνεκτικότητας (οι εποπτικές αρχές συνεργάζονται μεταξύ τους και, εφόσον απαιτείται, με την Επιτροπή, μέσω του μηχανισμού συνεκτικότητας)
- Ανταλλαγή πληροφοριών (εκτελεστικές πράξεις γενικής εμβέλειας της Επιτροπής)
- Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

# Ευχαριστώ

Σπύρος Τάσσης

HADPP

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΠΡΟΣΤΑΣΙΑΣ
ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ & ΙΔΙΩΤΙΚΟΤΗΤΑΣ