ΣΥΝΔΕΣΜΟΣ ΦΑΡΜΑΚΕΥΤΙΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ ΕΛΛΑΔΟΣ

**Βαϊνανίδης, Οικονόμου & Συνεργάτες**
***Δικηγορική Εταιρεία***

# Ζητήματα για τις Φαρμακευτικές Εταιρείες από το νέο Κανονισμό περί Προστασίας Προσωπικών Δεδομένων και από τη Συμφωνία Ε.Ε.-Η.Π.Α. για τη διατλαντική ροή αυτών

**Εβίτα Βαϊνανίδη**

# Επισκόπηση

**Οδηγία 95/46/ΕΚ**

Ραγδαίες τεχνολογικές εξελίξεις & ύπαρξη αποκλίσεων

κατά την εκτέλεση και εφαρμογή της Οδηγίας

Ανάγκη για μεταρρύθμιση θεσμικού πλαισίου

προστασίας προσωπικών δεδομένων

**Κανονισμός (ΕΕ) 2016/679**

**(Γενικός Κανονισμός για την Προστασία Δεδομένων)**

Τέθηκε σε ισχύ στις 24 Μαΐου 2016

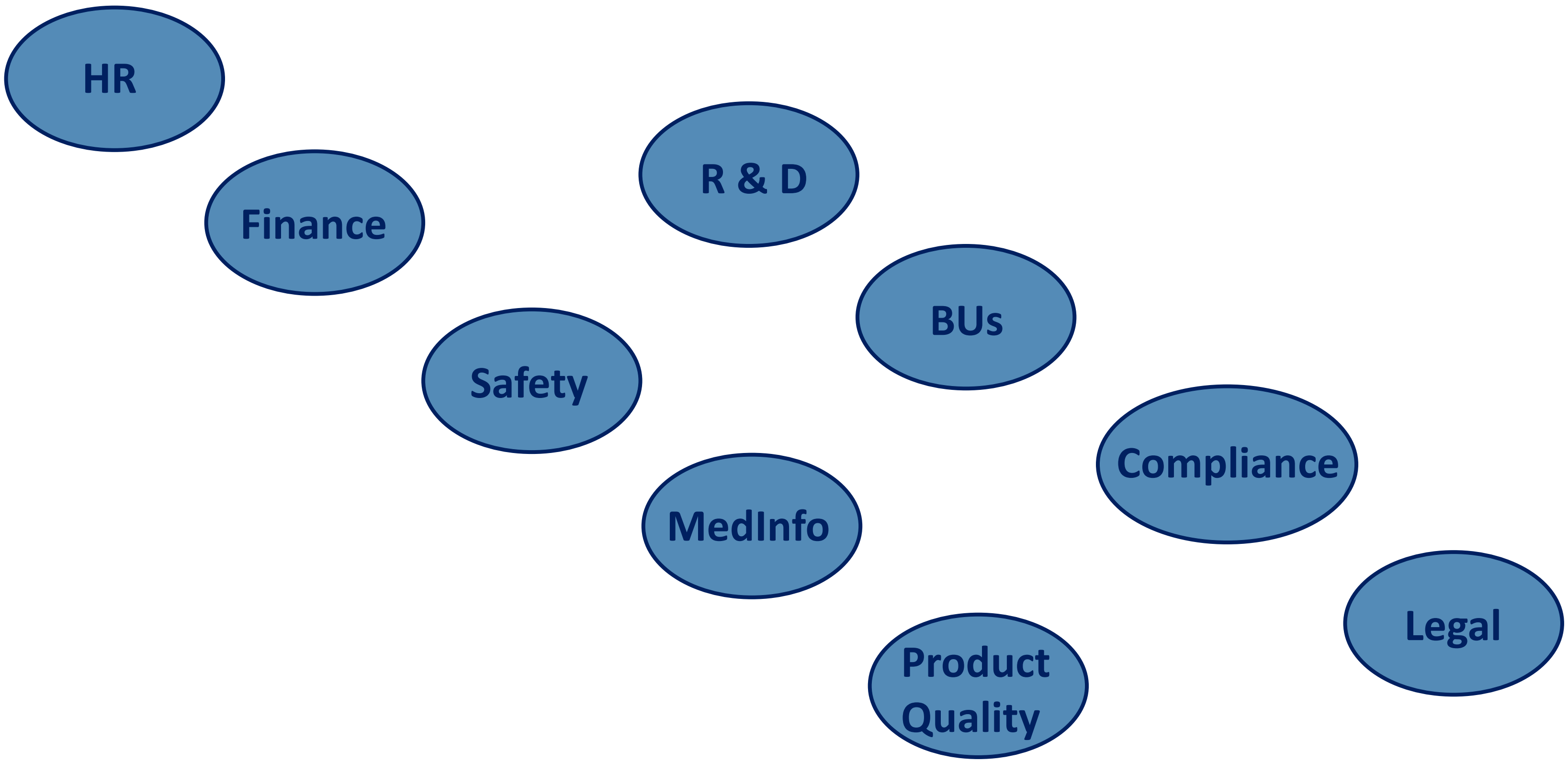
Τίθεται σε εφαρμογή από τις **25 Μαΐου 2018**

# Επισκόπηση

***18 μήνες για να προετοιμαστούμε, ξεκινώντας από…τώρα!***

# Προσωπικά Δεδομένα και Φαρμακευτικές Εταιρείες

- **Τα προσωπικά δεδομένα αφορούν <u>κάθε τμήμα</u> και συνδέονται σχεδόν με <u>κάθε δραστηριότητα</u> των φαρμακευτικών εταιρειών**



# Προσωπικά Δεδομένα και Φαρμακευτικές Εταιρείες

**Δεδομένα εντός & εκτός των τειχών των φαρμακευτικών εταιρειών**

**Σκληρός Δίσκος**

**Έγγραφα**

**Διακομιστές**


**Υπολογιστικό Νέφος**

**Εξωτερικοί Πάροχοι Υπηρεσιών**

**Εφαρμογές**


**Διαδικτυακοί Τόποι**

# Κανονισμός (ΕΕ) 2016/679

**Τι αλλάζει με το νέο Κανονισμό και**
**πώς επηρεάζονται οι φαρμακευτικές εταιρείες;**


**Βαϊνανίδης, Οικονόμου & Συνεργάτες**
***Δικηγορική Εταιρεία***

ΣfΕΕ
ΣΥΝΔΕΣΜΟΣ ΦΑΡΜΑΚΕΥΤΙΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ ΕΛΛΑΔΟΣ

# Κανονισμός (ΕΕ) 2016/679

## I. Διευρυμένο εδαφικό πεδίο εφαρμογής

Ο νέος Κανονισμός εφαρμόζεται σε δραστηριότητες υπευθύνων ή εκτελούντων την επεξεργασία εγκατεστημένων:

✓ Εντός Ε.Ε., ανεξάρτητα από το πού λαμβάνει χώρα η επεξεργασία.

✓ Εκτός Ε.Ε., εφόσον οι δραστηριότητες επεξεργασίας σχετίζονται με:

- Προσφορά αγαθών/υπηρεσιών σε υποκείμενα που διαμένουν στην Ε.Ε. ή
- Παρακολούθηση συμπεριφοράς υποκειμένων, στο βαθμό που η συμπεριφορά λαμβάνει χώρα εντός της Ε.Ε.

➢ Τελικά, αφορά ο σύνολο σχεδόν των εταιρειών παγκοσμίως!

# Κανονισμός (ΕΕ) 2016/679

## II. **Διευρύνεται η έννοια των προσωπικών δεδομένων**

- Κάθε πληροφορία που αφορά <u>ταυτοποιημένο ή ταυτοποιήσιμο</u> φυσικό πρόσωπο
- Ειδικές κατηγορίες δεδομένων = "παλιά" ευαίσθητα δεδομένα
- Ευρεία ερμηνεία δεδομένων υγείας
- Ρητή αναφορά σε <u>γενετικά</u> και <u>βιομετρικά</u> δεδομένα
- Εύρος των δεδομένων πολύ μεγάλο, περιλαμβάνει πλέον <u>κάθε αναγνωριστικό</u> π.χ. διευθύνσεις IP, αναγνωριστικά cookies, ετικέτες αναγνώρισης

# Κανονισμός (ΕΕ) 2016/679

III. **Ενίσχυση δικαιωμάτων υποκειμένων δεδομένων**

# Κανονισμός (ΕΕ) 2016/679

## III. Ενίσχυση δικαιωμάτων υποκειμένων δεδομένων

**Εκτενής ενημέρωση υποκειμένων:**

- Στοιχεία υπευθύνου επεξεργασίας
- Σκοποί επεξεργασίας
- Αποδέκτες ή κατηγορίες αποδεκτών
- Δικαιώματα υποκειμένου
- Κατηγορίες δεδομένων
- Πηγές προέλευσης
- Πρόθεση διαβίβασης σε τρίτη χώρα, εγγυήσεις/απόφαση επάρκειας
- Νομική βάση επεξεργασίας & έννομα συμφέροντα
- Στοιχεία επικοινωνίας Υπευθύνου Προστασίας Δεδομένων
- Χρονικό διάστημα αποθήκευσης
- Εάν αποτελεί προϋπόθεση για τη σύμβαση και ποιες οι συνέπειες άρνησης/μη παροχής
- Πρόθεση κατάρτισης προφίλ

# Κανονισμός (ΕΕ) 2016/679

## IV. Αυστηρότερες προϋποθέσεις λήψης συγκατάθεσης

- Ελεύθερη, συγκεκριμένη, ρητή & εν πλήρει επιγνώσει ένδειξη συμφωνίας, παρέχεται με δήλωση ή με σαφή θετική ενέργεια
- Για **ειδικές κατηγορίες** δεδομένων απαιτείται **ρητή συγκατάθεση** των υποκειμένων, εκτός εάν συντρέχουν άλλοι λόγοι
- Βάρος απόδειξης → υπεύθυνος επεξεργασίας
- Προσοχή στη διατύπωση των δηλώσεων συγκατάθεσης
- Αίτημα για συγκατάθεση <u>σαφώς διακριτό</u>
- Ανάκληση εξίσου εύκολη με παροχή!

☒ Δεν συνιστούν συγκατάθεση:

Σιωπή, αδράνεια, προσυμπληρωμένα τετραγωνίδια…

# Κανονισμός (ΕΕ) 2016/679

## V. Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ)


- Παρακολουθεί εσωτερική συμμόρφωση με Κανονισμό, συμβουλεύει
- Ενεργεί ως σημείο επικοινωνίας με εποπτική αρχή και υποκείμενα
- Πότε υπάρχει υποχρέωση να διοριστεί ΥΠΔ;
  - Όταν η επεξεργασία διενεργείται από δημόσια αρχή/φορέα (εξαιρούνται δικαστήρια) ή
  - Όταν οι πράξεις επεξεργασίας, λόγω φύσης, πεδίου ή σκοπού, απαιτούν τακτική & συστηματική παρακολούθηση υποκειμένων σε μεγάλη κλίμακα ή
  - Όταν οι βασικές δραστηριότητες του υπευθύνου/εκτελούντος αφορούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων .

# Κανονισμός (ΕΕ) 2016/679

- Όμιλος εταιρειών μπορεί να ορίσει έναν μόνο ΥΠΔ (προϋπόθεση εύκολη πρόσβαση)
- Υπάλληλος ή εξωτερικός συνεργάτης
- Εμπειρία στον τομέα του δικαίου & των πρακτικών προστασίας δεδομένων
- Δεν λαμβάνει εντολές για την άσκηση των καθηκόντων του
- Λογοδοτεί απευθείας σε ανώτατο διοικητικό επίπεδο
- Δεσμεύεται από τήρηση απορρήτου
- Προσοχή: Μπορεί να επιτελεί και άλλα καθήκοντα,
  <u>εφόσον δεν συνεπάγονται σύγκρουση συμφερόντων</u> !

# Κανονισμός (ΕΕ) 2016/679

## VI. Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων (risk assessment)

- 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
- Εάν υψηλός κίνδυνος ελλείψει μέτρων μετριασμού → διαβούλευση με εποπτική αρχή πριν την επεξεργασία
- *Παραδείγματα*: πράξεις επεξεργασίας μεγάλης κλίμακας, χρήση νέας τεχνολογίας, κατάρτιση προφίλ

# Κανονισμός (ΕΕ) 2016/679

## VII. Τήρηση αρχείων δραστηριοτήτων επεξεργασίας (data mapping)

- Περιλαμβάνουν ακόλουθες πληροφορίες:
  - Στοιχεία υπευθύνου επεξεργασίας, τυχόν εκπροσώπου, υπευθύνου προστασίας δεδομένων
  - Σκοπούς επεξεργασίας
  - Κατηγορίες υποκειμένων, δεδομένων, αποδεκτών
  - Διαβίβαση δεδομένων σε τρίτες χώρες & τεκμηρίωση εγγυήσεων
  - Αναμενόμενο χρόνο διαγραφής
  - Περιγραφή τεχνικών & οργανωτικών μέτρα προστασίας

- Υποχρέωση δεν ισχύει για οργανισμούς που απασχολούν κάτω από 250 άτομα, εκτός εάν η επεξεργασία:
  - Ενέχει κινδύνους παραβίασης δικαιωμάτων & ελευθεριών υποκειμένου ή
  - Δεν είναι περιστασιακή ή
  - Αφορά ειδικές κατηγορίες  προσωπικών δεδομένων

# Κανονισμός (ΕΕ) 2016/679

## VIII. Υποχρέωση γνωστοποίησης παραβιάσεων ασφαλείας

- Γνωστοποίηση παραβίασης στην εποπτική αρχή αμελλητί, το αργότερο <u>εντός 72 ωρών</u>, ***εκτός εάν*** *η παραβίαση δεν ενδέχεται να προκαλέσει κίνδυνο.*


- Ανακοίνωση παραβίασης στο υποκείμενο των δεδομένων αμελλητί, **εκτός εάν**:
  - Δεν τίθενται σε κίνδυνο ελευθερίες και δικαιώματα υποκειμένων
  - Έχει ήδη λάβει μέτρα που καθιστούν δεδομένα ακατάληπτα
  - Απαιτείται δυσανάλογη προσπάθεια, τότε δημόσια ανακοίνωση

# Κανονισμός (ΕΕ) 2016/679

## IX. Ειδικές απαιτήσεις για τους εκτελούντες την επεξεργασία

- ✓ Να παρέχουν επαρκείς διαβεβαιώσεις, π.χ. προσχώρηση σε κώδικα συμπεριφοράς, μηχανισμό πιστοποίησης
- ✓ Υποχρεωτική σύμβαση με υπεύθυνο επεξεργασίας
- ✓ Σαφής καθορισμός σκοπών, μέσων επεξεργασίας, αντικειμένου, είδους δεδομένων, κατηγοριών υποκειμένων, διάρκειας επεξεργασίας
- ✓ Απαγορεύεται υπεργολαβία χωρίς προηγούμενη γραπτή άδεια υπευθύνου
- ✓ Ο υπεργολάβος έχει ακριβώς τις ίδιες υποχρεώσεις, ενώ στον αρχικό εκτελούντα παραμένουν όλες οι ευθύνες
- ✓ Υποχρέωση διαγραφής ή επιστροφής δεδομένων μετά το πέρας της επεξεργασίας

# Κανονισμός (ΕΕ) 2016/679

## X. Αυστηρότερα διοικητικά πρόστιμα

- Επιβάλλονται επιπροσθέτως ή αντί άλλων μέτρων που δύναται να διατάξει η εποπτική αρχή (προειδοποίηση, περιορισμό επεξεργασίας, διαγραφή, διόρθωση κλπ.)

- Έως 20.000.000 Ευρώ ή, σε περίπτωση επιχειρήσεων, έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, όποιο είναι υψηλότερο!

# Διασυνοριακή ροή δεδομένων & Privacy Shield

**Γενικά περί διαβίβασης δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες**

Διαβιβάσεις απαραίτητες για επέκταση διεθνούς εμπορίου & συνεργασίας

- Διαβιβάσεις **που δεν απαιτούν ειδική άδεια** της εποπτικής αρχής:
  - ✓ Διαβιβάσεις βάσει <u>απόφασης επάρκειας</u> της Ευρωπαϊκής Επιτροπής
  - ✓ Διαβιβάσεις που υπόκεινται σε <u>κατάλληλες εγγυήσεις</u> (νομικές δεσμεύσεις μεταξύ δημόσιων αρχών, BCRs, τυποποιημένες ρήτρες προστασίας κώδικας δεοντολογίας, μηχανισμός πιστοποίησης )

- Περιπτώσεις για τις οποίες **απαιτείται άδεια** της εποπτικής αρχής, ενδεικτικά:
  - ✓ Ρητή συγκατάθεση υποκειμένου
  - ✓ Διαβίβαση απαραίτητη για εκτέλεση σύμβασης
  - ✓ Σημαντικοί λόγοι δημοσίου συμφέροντος
  - ✓ Άσκηση ή υποστήριξη νομικών αξιώσεων
  - ✓ Προστασία ζωτικών συμφερόντων υποκειμένου ή τρίτου

# Διασυνοριακή ροή δεδομένων & Privacy Shield

**Ασπίδα προστασίας της Ιδιωτικής Ζωής Ε.Ε.-Η.Π.Α. (Privacy Shield)**

# Διασυνοριακή ροή δεδομένων & Privacy Shield

- Τέθηκε σε εφαρμογή 1 Αυγούστου 2016
- Αντικαθιστά αρχική συμφωνία Ε.Ε.-Η.Π.Α (Safe Harbor)
- Δέσμευση εταιρειών να τηρούν τις <u>αρχές</u> του πλαισίου της Ασπίδας Προστασίας
- Βασίζεται σε ένα σύστημα αυτοπιστοποίησης στο Υπουργείο Εμπορίου των Η.Π.Α.
- Ετήσια επαναπιστοποίηση συμμόρφωσης
- Η διαβίβαση στις Η.Π.Α. πραγματοποιείται <u>χωρίς άδεια</u> της εποπτικής Αρχής

# Διασυνοριακή ροή δεδομένων & Privacy Shield

- Βασικά στοιχεία:
  - Αυστηρές υποχρεώσεις επιχειρήσεων που χειρίζονται προσωπικά δεδομένα
  - Σαφείς διασφαλίσεις και υποχρεώσεις διαφάνειας όσον αφορά πρόσβαση κυβέρνησης των Η.Π.Α.
  - Αποτελεσματική προστασία ατομικών δικαιωμάτων μέσω προσιτών μηχανισμών επίλυσης διαφορών
  - Μηχανισμός κοινής επανεξέτασης λειτουργίας Ασπίδας Προστασίας
- Η Συμφωνία αντιμετωπίζει ήδη νομικές προκλήσεις:
  - ✓ *Υπόθεση T-670/16:* Προσφυγή της 16/9/2016 ενώπιον Γενικού Δικαστηρίου - Digital Rights Ireland Ltd. vs. Ευρωπαϊκής Επιτροπής, για την ακύρωση εκτελεστικής απόφασης 2016/1250 της Επιτροπής περί επάρκειας Privacy Shield.

# 10 + 1 Συμβουλές Συμμόρφωσης

① **Εξοικείωση με νέο Κανονισμό** (εκπαίδευση στελεχών, προσωπικού)

② **Καταγραφή κάθε δραστηριότητας επεξεργασίας** (data mapping)

③ **Διορισμός Υπευθύνου Προστασίας Δεδομένων**, εσωτερικές επιθεωρήσεις εφαρμογής

④ **Δικαιώματα υποκειμένων**: πώς επηρεάζουν τις δραστηριότητες της εταιρείας;

- ✓ **Επανέλεγχος και τροποποίηση πολιτικών προστασίας προσωπικών δεδομένων**
- ✓ **Υιοθέτηση εσωτερικών διαδικασιών** ανταπόκρισης σε αιτήματα & δικαιώματα υποκειμένων

⑤ **Συγκατάθεση**: πώς λαμβάνεται, τί καλύπτει, πώς αποδεικνύεται;

# 10 + 1 Συμβουλές Συμμόρφωσης

⑥ **Επανέλεγχος συμβάσεων με εκτελούντες την επεξεργασία**

⑦ **Ανάπτυξη μηχανισμών ανταπόκρισης σε & γνωστοποίησης παραβιάσεων**

⑧ **Αναβάθμιση τεχνολογικών υποδομών**

⑨ **Εντοπισμός δραστηριοτήτων υψηλού κινδύνου & διεξαγωγή εκτίμησης αντικτύπου**

⑩ **Ένταξη δαπανών συμμόρφωσης στον ετήσιο προϋπολογισμό!**

# 10 + 1 Συμβουλές Συμμόρφωσης

+①

# Ευχαριστώ για την προσοχή σας!

**Εβίτα Βαϊνανίδη**
**E-mail:** evitavainanidi@lawvse.gr