

# Η εφαρμογή του GDPR στον Ιδιωτικό τομέα- Πρακτικός Οδηγός Ενσωμάτωσης

**Γρηγόρης Λαζαράκος**



**Δ.Ν., Δικηγόρος, πιστοποιημένος νομικός εμπειρογνώμονας για την προστασία δεδομένων (CEPE L PS) σε ηλεκτρονικά προϊόντα και υπηρεσίες (IT based products and services) στο γερμανικό φορέα πιστοποίησης European Privacy Seal GmbH (EuroPriSe), πρώην αν. μέλος της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα**

Παρουσίαση στην διημερίδα του ΕΚΔΔΑ με θέμα:  
**«Προστασία Προσωπικών Δεδομένων, Κανονισμός (ΕΕ) 2016/679»**

# Στόχος εισήγησης



- Παρουσίαση ενός χρηστικού Οδηγού για την ενσωμάτωση των νέων απαιτήσεων του Κανονισμού.



- Χρήση παραδειγμάτων από την πράξη.



# Απλά και Ευαίσθητα δεδομένα προσωπικού χαρακτήρα

## Απλά

προσωπικά δεδομένα



Κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο, δηλαδή πρόσωπο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, αριθμός ταυτότητας, δεδομένα θέσης, επιγραμμικό (online) αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου

## Ευαίσθητα

προσωπικά δεδομένα



Δεδομένα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό.

# Επεξεργασία Προσωπικών Δεδομένων

Κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.



# Τριπλή πρόκληση για τις περισσότερες επιχειρήσεις

1. Ελάχιστες επιχειρήσεις γνωρίζουν πραγματικά που βρίσκονται τα προσωπικά δεδομένα που συλλέγουν και επεξεργάζονται.
2. Ασάφειες του Γενικού Κανονισμού σε σχέση με αρκετές διατάξεις, που προσπαθεί να καλύψει η Ομάδα του άρθρου 29.
3. Δυσκολία των επιχειρήσεων να βρουν εξειδικευμένους επαγγελματίες με γνώση και εμπειρία στο δίκαιο και στην πράξη των προσωπικών δεδομένων  
Την ίδια δυσκολία αντιμετωπίζουν οι εταιρείες και στην ανεύρεση DPO, ο οποίος αποτελεί έναν χρήσιμο και σε πολλές περιπτώσεις, απαραίτητο συνεργάτη του Υπεύθυνου Επεξεργασίας.

# Υποχρεώσεις επιχειρήσεων και οργανισμών ως υπεύθυνοι επεξεργασίας

- Τήρηση αρχείου δραστηριοτήτων επεξεργασίας (άρθρο 30)
- Ορισμός υπεύθυνου προστασίας δεδομένων (DPO) (άρθρα 37 – 39)
- Υποχρέωση εκπόνησης εκτίμησης αντικτύπου σχετικά με την προστασία των προσωπικών δεδομένων (άρθρα 35 και 36)
- Ασφάλεια επεξεργασίας (άρθρα 5 παρ. 1 στοιχ. στ' και 32)
- Προστασία των δεδομένων ήδη από το σχεδιασμό ή εξ ορισμού (άρθρο 4 παρ. 5, άρθρο 5 παρ.1 στοιχ. γ' και άρθρο 25)
- Γνωστοποίηση τυχόν παραβίασης προσωπικών δεδομένων στην εποπτική αρχή (υπό προϋποθέσεις και στα θιγόμενα πρόσωπα) (άρθρα 33 και 34)
- Εποπτεία του εκτελούντος την επεξεργασία (άρθρα 4 παρ. 8, 28 και 29)



# Υπεύθυνος προστασίας δεδομένων *Data Protection Officer (DPO)*

- Ορισμός υπευθύνου προστασίας δεδομένων
  - Δημόσιες αρχές ή φορείς
  - Τακτική και συστηματική παρακολούθηση σε ευρεία κλίμακα
  - Ειδικές κατηγορίες δεδομένων
- Θέση υπευθύνου
- Καθήκοντα υπευθύνου προστασίας δεδομένων

# *Εκτίμηση αντικτύπου και προηγούμενη διαβούλευση*

Για επεξεργασίες υψηλού κινδύνου, πριν την εφαρμογή τους, υποχρέωση εκτίμησης αντικτύπου

- Ζητείται η γνώμη του υπευθύνου προστασίας δεδομένων
- Εποπτική αρχή δημοσιοποιεί λίστα επεξεργασιών υψηλού κινδύνου
- Διαβούλευση με την εποπτική αρχή αν παραμένει υψηλός κίνδυνος



# Πότε μία επεξεργασία είναι υψηλού κινδύνου (οπότε απαιτείται DPIA);

Σε περίπτωση:

ή

Συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών που βασίζεται σε αυτοματοποιημένη επεξεργασία (κατάρτιση προφίλ) και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα ή επηρεάζουν σημαντικά το φυσικό πρόσωπο

ή

Μεγάλης κλίμακας επεξεργασίας των ευαίσθητων δεδομένων του άρθρου 9 ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10

Συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα

Επεξεργασίες για τις οποίες απαιτείται εκπόνηση εκτίμησης αντικτύπου (DPIA)

[illegible]



# Καταγραφή Επεξεργασιών

Παραδείγματα πράξεων επεξεργασίας	Πιθανά συναφή κριτήρια	Ενδέχεται να απαιτείται διενέργεια ΕΑΠΔ;
Νοσοκομείο που επεξεργάζεται τα γενετικά δεδομένα και τα δεδομένα υγείας των ασθενών του (πληροφοριακό σύστημα του νοσοκομείου).	<ul style="list-style-type: none"> <li>- Ευαίσθητα δεδομένα ή δεδομένα εξαιρετικά προσωπικού χαρακτήρα.</li> <li>- Δεδομένα που αφορούν ευάλωτα υποκείμενα δεδομένων.</li> <li>- Δεδομένα μεγάλης κλίμακας επεξεργασίας.</li> </ul>	Ναι
Χρήση συστήματος Βιντεοσκόπησης για την παρακολούθηση της οδικής συμπεριφοράς σε αυτοκινητοδρόμους. Ο υπεύθυνος επεξεργασίας σκοπεύει να χρησιμοποιεί έξυπνο σύστημα ανάλυσης βίντεο για να απομονώνει τα οχήματα και να αναγνωρίζει αυτόματα τις πινακίδες τους.	<ul style="list-style-type: none"> <li>- Συστηματική παρακολούθηση.</li> <li>- Καινοτόμος χρήση ή εφαρμογή τεχνολογικών ή οργανωτικών λύσεων.</li> </ul>	
Εταιρεία που παρακολουθεί συστηματικά τις δραστηριότητες των εργαζομένων της, καθώς και τον σταθμό εργασίας τους, τη δραστηριότητά τους στο διαδίκτυο κ.ο.κ.	<ul style="list-style-type: none"> <li>- Συστηματική παρακολούθηση.</li> <li>- Δεδομένα που αφορούν ευάλωτα υποκείμενα δεδομένων.</li> </ul>	
Συλλογή δημόσιων δεδομένων στα μέσα κοινωνικής δικτύωσης για την κατάρτιση προφίλ.	<ul style="list-style-type: none"> <li>- Αξιολόγηση ή βαθμολόγηση.</li> <li>- Δεδομένα μεγάλης κλίμακας επεξεργασίας.</li> <li>- Αντιστοίχιση ή συνδυασμός συνόλων δεδομένων.</li> <li>- Ευαίσθητα δεδομένα ή δεδομένα εξαιρετικά προσωπικού χαρακτήρα</li> </ul>	
Ηλεκτρονικό περιοδικό που χρησιμοποιεί κατάλογο ηλεκτρονικών διευθύνσεων για να αποστέλλει γενικές ημερήσιες συνόψεις στους συνδρομητές του.	<ul style="list-style-type: none"> <li>- Δεδομένα μεγάλης κλίμακας επεξεργασίας.</li> </ul>	Όχι

# Ασφάλεια επεξεργασίας



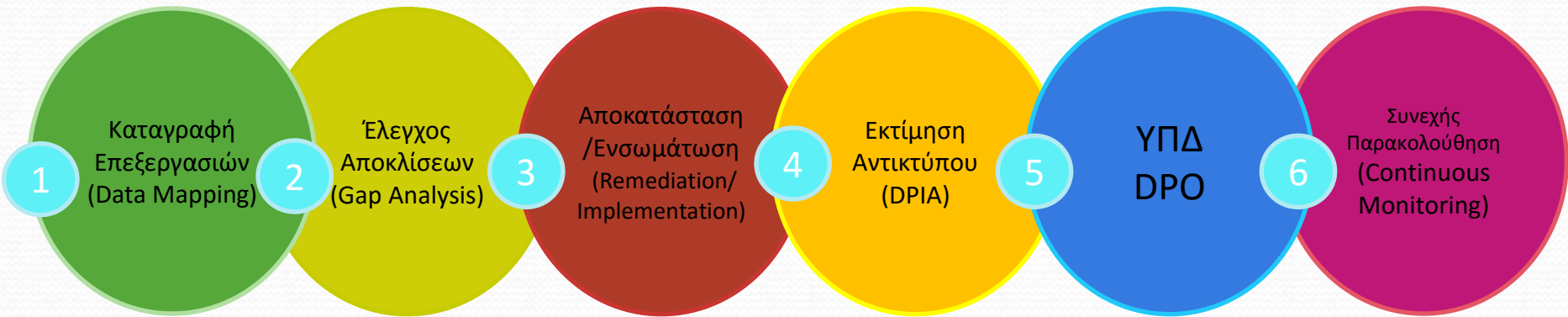
Κατάλληλο επίπεδο ασφάλειας

- Ψευδώνυμα, κρυπτογράφηση
- Διασφάλιση απορρήτου, ακεραιότητα, διαθεσιμότητα
- Αντιμετώπιση φυσικών ή τεχνικών συμβάντων
- Αξιολόγηση και αναθεώρηση μέτρων
- Διαχείριση κινδύνων
- Κώδικες δεοντολογίας και πιστοποίηση



- Ενθαρρύνεται η θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων, σφραγίδων και σημάτων
- Εφαρμογή από υπεύθυνους ή εκτελούντες την επεξεργασία
- Αποτελεί απόδειξη συμμόρφωσης με τον Γ. Κανονισμό, χωρίς όμως να περιορίζει τις υποχρεώσεις των υπ. ή εκτελ. την επεξεργασία
- Ούτε θίγονται οι αρμοδιότητες των εποπτικών αρχών
- Η πιστοποίηση γίνεται από φορέα πιστοποίησης ή την εποπτική αρχή
- Πιστοποίηση για μέγιστη περίοδο 3 ετών, δυνατότητα ανανέωσης, ανάκληση
- Μητρώο με μηχανισμούς πιστοποιήσεων, σφραγίδων και σημάτων τηρείται από το ΕΣΠΔ και είναι δημόσια προσβάσιμο

# *Βασικά Βήματα/Φάσεις Ενσωμάτωσης*





# Κατανόηση του περιβάλλοντος σε επίπεδο προσωπικών δεδομένων (1/2)

Η ακριβής κατανόηση του περιβάλλοντος των προσωπικών δεδομένων αποτελεί τη βάση, πάνω στην οποία θα πατήσουν όλες οι επόμενες ενέργειες της επιχείρησης για τη συμμόρφωσή της με τον Κανονισμό. Παραδείγματος χάριν:

Επιχείρηση ή οργανισμός που δεν γνωρίζει ποια προσωπικά δεδομένα και για ποιο σκοπό συλλέγει και επεξεργάζεται



δεν είναι σε θέση να αξιολογήσει τη νομιμότητα της όποιας επεξεργασίας

Όποιος επίσης δεν γνωρίζει ποια τρίτα – φυσικά ή νομικά- πρόσωπα επεξεργάζονται ή έχουν πρόσβαση σε προσωπικά δεδομένα που ο ίδιος συλλέγει



δεν θα μπορεί να αξιολογήσει αν πρέπει να συναφθεί σχετική σύμβαση ή αν η σύμβαση που πιθανόν να έχει ήδη συνάψει πρέπει να προσαρμοσθεί στις απαιτήσεις του άρθρου 28 GDPR,

Αν επίσης η επιχείρηση δεν έχει σαφή εικόνα των χρησιμοποιούμενων συγκαταθέσεων



δεν θα είναι σε θέση να εξετάσει και να αξιολογήσει αν τα κείμενα των συγκαταθέσεων αυτών ανταποκρίνονται στις αυξημένες απαιτήσεις του Κανονισμού για τη συγκατάθεση

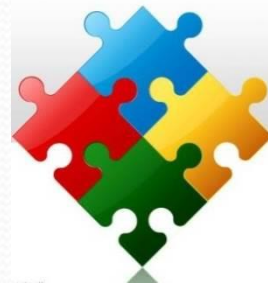
# Κατανόηση του περιβάλλοντος σε επίπεδο προσωπικών δεδομένων (2)

## Συμπέρασμα:

Πριν ξεκινήσει μια επιχείρηση ή ένας οργανισμός ασχοληθεί σε βάθος με τις απαιτήσεις του Κανονισμού και πριν καν καταπιαστεί με το “GAP ANALYSIS” είναι ΑΠΑΡΑΙΤΗΤΟ να καταγράψει με προσοχή τις επεξεργασίες, για τις οποίες η επιχείρηση είναι υπεύθυνη.

## Συνίσταται

Η δημιουργία Ομάδας Έργου εντός εταιρείας, που θα αποτελείται από περισσότερες περιοχές ευθύνης της επιχείρησης και της οποίας το έργο είναι συνθέσουν τα διαφορετικά κομμάτια του παζλ σε μία ενιαία και σαφή εικόνα για τις επεξεργασίες του συνόλου της επιχείρησης.





# *Καταγραφή Επεξεργασιών*



# Καταγραφή Επεξεργασιών

Υπεύθυνος επεξεργασίας με >250 συνεργατών ή για επεξεργασίες υψηλού κινδύνου

Για κάθε δραστηριότητα επεξεργασίας, καταγράφονται τα ακόλουθα στοιχεία:

- Σκοποί επεξεργασίας
- Δεδομένα και υποκείμενα
- Αποδέκτες δεδομένων
- Ενδεχόμενες διαβιβάσεις εκτός ΕΕ
- Χρόνος τήρησης
- Οργανωτικά και τεχνικά μέτρα προστασίας

Παρόμοια υποχρέωση για τον εκτελούντα της επεξεργασία

Κατόπιν αιτήματος, το αρχείο επεξεργασιών τίθεται στη διάθεση της εποπτικής αρχής

## Αρχείο Δραστηριοτήτων

[illegible]



## *Χρησιμότητα Αρχείου Δραστηριοτήτων στο στάδιο της συμμόρφωση (αλλά και μετά)*

Το αρχείο δραστηριοτήτων μπορεί να βοηθήσει την επιχείρηση να διαγνώσει τα κενά της και να λάβει τα ενδεικνυόμενα μέτρα σε σχέση με τις ακόλουθες απαιτήσεις του κανονισμού:

- 1.Υποχρέωση λογοδοσίας και τεκμηρίωσης (άρθρο 5 παρ. 2)
- 2.Υποχρέωση εκπόνησης εκτίμησης αντικτύπου για επεξεργασίες υψηλού κινδύνου για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων (άρθρο 35)
- 3.Εποπτεία του εκτελούντος την επεξεργασία (άρθρα 4 παρ. 8, 28 και 29)
- 4.Έλεγχος νομιμότητας της επεξεργασίας (άρθρο 6)
- 5.Υποχρέωση ενημέρωσης των υποκειμένων (άρθρα 12-14)

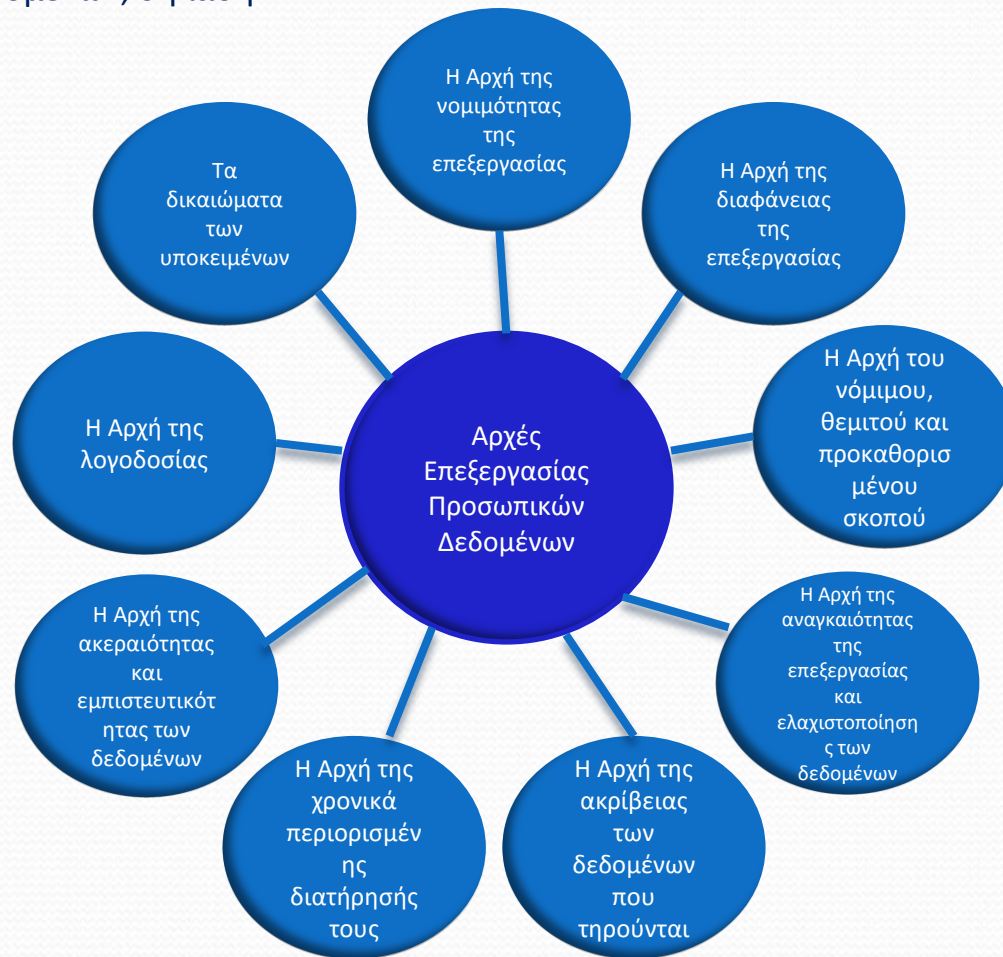
# Έλεγχος Αποκλίσεων (Gap Analysis)





# Έλεγχος Αποκλίσεων (Gap Analysis)

Εξετάζεται η συμμόρφωση της εταιρείας στη βάση των αρχών που διέπουν την επεξεργασία των προσωπικών δεδομένων, δηλαδή:



Όλες αυτές οι αρχές εξειδικεύονται στη συνέχεια στα επιμέρους άρθρα του Κανονισμού, τα οποία θα πρέπει να ελεγχθούν σε σχέση με την κατάσταση της εταιρείας.



# Έλεγχος Αποκλίσεων (Gap Analysis) (1/3)

Προσαρμογή του ελέγχου στις ιδιαιτερότητες της εταιρείας.

Θα πρέπει καταρχάς να ελεγχθεί ποιος είναι ο πυρήνας των δραστηριοτήτων της εταιρείας και εκεί να ρίξει κανείς το βάρος του. Χωρίς βεβαίως να παραμελήσει τα υπόλοιπα θέματα.

## ΠΑΡΑΔΕΙΓΜΑ

Πυρήνας της δραστηριότητας ενός νοσοκομείου από άποψη προσωπικών δεδομένων είναι η επεξεργασία δεδομένων υγείας ασθενών, **δηλαδή η επεξεργασία ευαίσθητων δεδομένων.**

**Νομική βάση** είναι ως επί το πλείστον η **συγκατάθεση**. Άρα θα πρέπει να ελεγχθεί η συνδρομή των όρων και προϋποθέσεων του άρθρου 7 για τη συγκατάθεση.

## Έλεγχος Αποκλίσεων (Gap Analysis) (2/3)

Θα πρέπει επιπλέον να ελεγχθούν και οι υπόλοιπες απαιτήσεις του Κανονισμού, όπως λ.χ.

- Εάν τα δεδομένα υγείας του ασθενούς που συλλέχθηκαν προς το σκοπό της παροχής υπηρεσιών υγείας υποβάλλονται ενδεχομένως σε επεξεργασία και **για άλλους σκοπούς** (π.χ. εμπορικής προώθησης), χωρίς να έχει ενημερωθεί και χωρίς να έχει συγκατατεθεί ο ασθενής.
- Αν τα δεδομένα υγείας του ασθενούς **διαβιβάζονται και σε τρίτους** και, αν ναι, με ποια νομική βάση γίνεται η διαβίβαση.
- Εάν συλλέγονται μόνον όσα προσωπικά δεδομένα είναι **απαραίτητα για την εξυπηρέτηση του σκοπού** της παροχής υπηρεσιών υγείας και όχι παραπάνω.

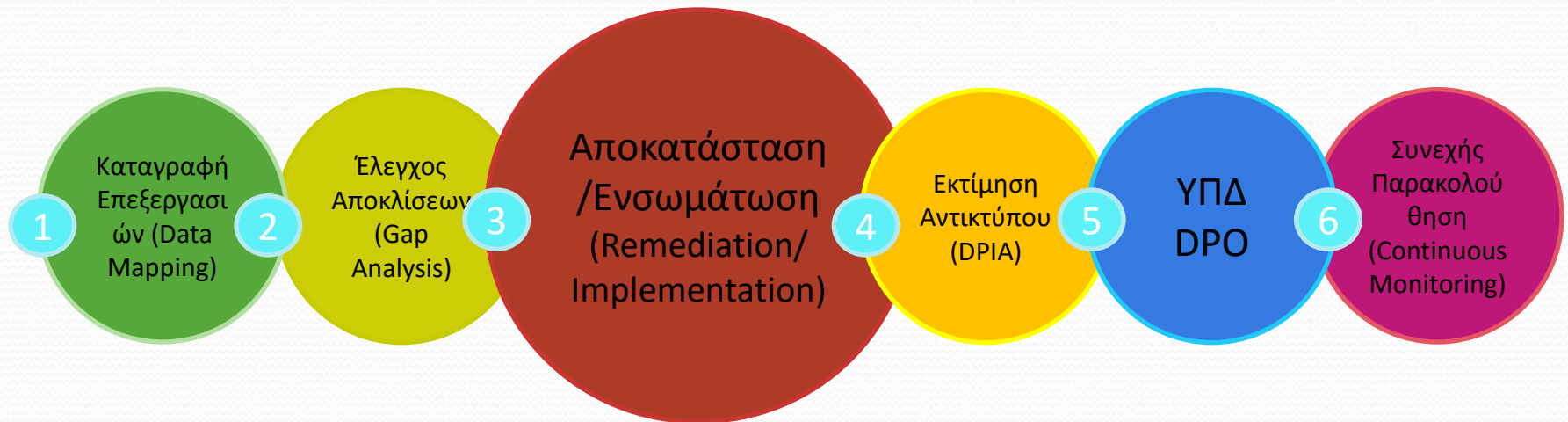


# Έλεγχος Αποκλίσεων (Gap Analysis) (3/3)

- Εάν τα δεδομένα που συλλέγονται είναι **ακριβή** και, μπορούν εύκολα να επικαιροποιηθούν.
- **Πόσο χρόνο τηρούνται τα δεδομένα που συλλέγονται και**
- Αν υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη **ασφάλεια** των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων.



# Αποκατάσταση/Ενσωμάτωση (Remediation/ Implementation)



# Αποκατάσταση/Ενσωμάτωση (Remediation/ Implementation)

➤ Υπάρχουν ζητήματα και κενά που συναντώνται (με ελάχιστες εξαιρέσεις) σε κάθε επιχείρηση, όπως είναι λ.χ. οι Πολιτικές που αφορούν ζητήματα:

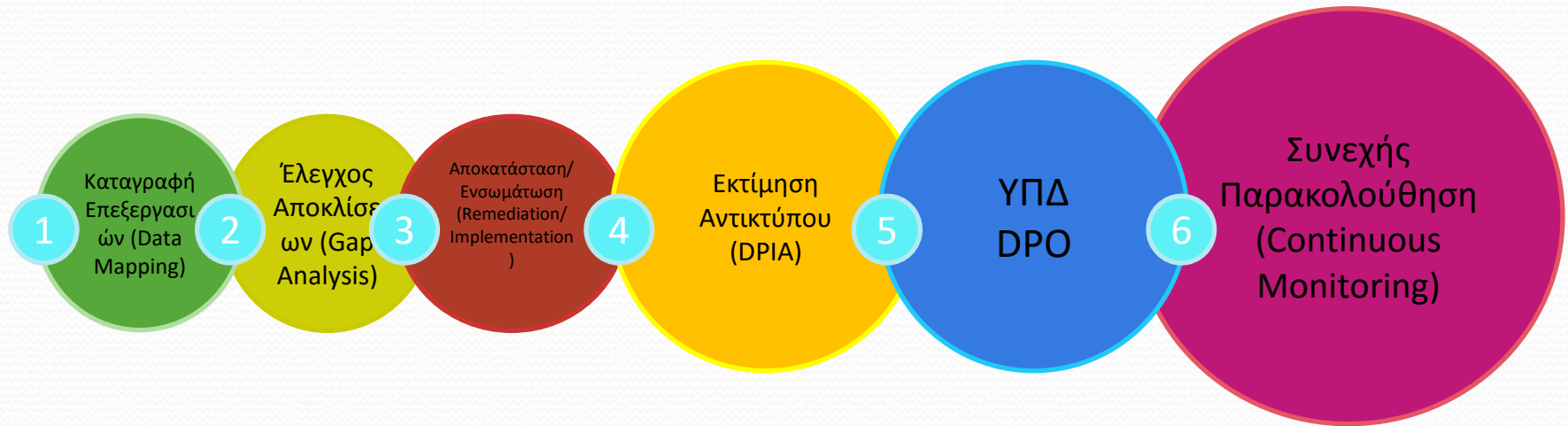
1. Γνωστοποίησης Περιστατικών Παραβίασης Δεδομένων,
2. Το χρόνο τήρησης των δεδομένων,
3. (Αποτελεσματικής) Ικανοποίησης των δικαιωμάτων των υποκειμένων.

Και αυτό είναι μάλλον αναμενόμενο διότι ο Κανονισμός περιέχει νέες διατάξεις, νέες απαιτήσεις.

➤ Πολλές αποκλίσεις όμως αφορούν παραδοσιακά ζητήματα προστασίας δεδομένων, όπως ζητήματα παραβίασης της αρχής του σκοπού, της ελαχιστοποίησης των δεδομένων, της διαφάνειας (με την έννοια της ενημέρωσης των υποκειμένων) ακόμη και της νομιμότητας της επεξεργασίας.



# Αποκατάσταση/Ενσωμάτωση (Remediation/ Implementation)



# Σημασία συμμόρφωσης με GDPR

## Ορθή και έγκαιρη συμμόρφωση επιχειρήσεων και οργανισμών

Θα αποβεί εις όφελος των φυσικών προσώπων, τα προσωπικά δεδομένα των οποίων θα πρέπει ούτως ή άλλως, να αποτελούν αντικείμενο νόμιμης και θεμιτής επεξεργασίας·

### ➤θα βοηθήσει τις επιχειρήσεις και τους οργανισμούς

- να «κτίσουν» -ή να αποκαταστήσουν- μία σχέση εμπιστοσύνης με τους πελάτες τους, να τους πλησιάσουν και να τους γνωρίσουν καλύτερα.
- να αποτρέψουν πιθανές παραβιάσεις της οικείας νομοθεσίας και, ακολούθως, να υποστούν τις αυστηρές – οικονομικής κυρίως φύσεως- κυρώσεις, που προβλέπει ο Κανονισμός σε περίπτωση παραβίασης των διατάξεών του.
- να προστατέψουν την αξιοπιστία τους και την εμπορική τους φήμη.



Σας ευχαριστώ πολύ!

Γρηγόρης Λαζαράκος

[grigorios@lazarakos.gr](mailto:grigorios@lazarakos.gr)

