Προετοιμασία για μια νέα σχέση με την Αρχή Προστασίας Δεδομένων

Η ενίσχυση των δικαιωμάτων στην πράξη & τα εργαλεία συμμόρφωσης για τη μετάβαση από το ν.2472/1997 στον ΓΚΠΔ

Β: ΓΚΠΔ: Τα νέα εργαλεία για τη συμμόρφωση με τη νομοθεσία

Γεώργιος Ρουσόπουλος
Δρ. Μηχ. Η/Υ & Πληροφορικής
Ε.Ε.Π. - Α.Π.Δ.Π.Χ.
grousopoulos at dpa.gr

Κωνσταντίνος Λιμνιώτης
Δρ. Πληροφορικής & Τηλεπικοινωνιών
Ε.Ε.Π. - Α.Π.Δ.Π.Χ.
klimniotis at dpa.gr

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

«Νέα» Εργαλεία Συμμόρφωσης

- **Αρχεία Δραστηριοτήτων Επεξεργασίας**

- **Υπεύθυνος Προστασίας Δεδομένων**

  (Data Protection Officer - DPO)

- **Προστασία των δεδομένων ήδη από το σχεδιασμό & εξ ορισμού**

  (Privacy by Design – Privacy by Default)

- **Αναλυτικότερα μέτρα ασφάλειας**

  (εξειδίκευση)

- **Διαχείριση περιστατικών παραβίασης προσωπικών δεδομένων**

  (κοινοποίηση – ανακοίνωση)

- **Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων**

  (Data Protection Impact Assessment - DPIA)

- **Εγκεκριμένοι Κώδικες Δεοντολογίας**

- **Αναγνωρισμένες Πιστοποιήσεις**

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Αρχεία Δραστηριοτήτων Επεξεργασίας

Τεκμηρίωση κάθε πράξης επεξεργασίας

Καταργείται η υποχρέωση γνωστοποίησης στις εποπτικές Αρχές.

Τα αρχεία αυτά περιλαμβάνουν

- **Ποιος**; (ταυτότητα υπευθύνου, τρόπος επικοινωνίας, εκπρόσωπος και DPO)
- **Γιατί**; (σκοπός επεξεργασίας)
- **Τι**; (κατηγορίες υποκειμένων δεδομένων, κατηγορίες δεδομένων)
- **Σε ποιον**; (κατηγορίες αποδεκτών)
- **Διαβιβάσεις**: (σε χώρες εκτός Ε.Ε.)
- **Για πόσο**; (προθεσμία διαγραφής κάθε κατηγορίας δεδομένων)
- **Πώς**; (γενική περιγραφή μέτρων ασφάλειας)

> 250 εργαζόμενοι => Εσωτερικά αρχεία κάθε επεξεργασίας

< 250 εργαζόμενοι => Αρχεία επεξεργασιών με διακινδύνευση

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Υπεύθυνος Προστασίας Δεδομένων

- **Υποχρέωση ορισμού Υπεύθυνου Προστασίας Δεδομένων (DPO):**
  - Δημόσιες αρχές
  - Τακτική και συστηματική παρακολούθηση υποκειμένων σε μεγάλη κλίμακα
  - Μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων (και ποινικών)
- **Ρόλος DPO:**
  - Συμβουλεύει τον υπεύθυνο/εκτελούντα
  - Εκπαίδευση – ευαισθητοποίηση προσωπικού
  - Εσωτερικοί έλεγχου σε ζητήματα προσωπικών δεδομένων – παρακολούθηση συμμόρφωσης
  - Σημείο επαφής με Εποπτική Αρχή – συνεργασία μαζί της
  - Τα υποκείμενα των δεδομένων μπορούν να επικοινωνούν μαζί του
- **Το προφίλ ενός DPO:**
  - Εμπειρία στον τομέα του Δικαίου και των πρακτικών περί προστασίας δεδομένων
  - Λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο
  - Ενεργεί ανεξάρτητα – δεν λαμβάνει εντολές για την εκτέλεση των καθηκόντων του
  - Διαθέτει επαρκείς πόρους
  - Μπορεί να είναι υπάλληλος ή εξωτερικός συνεργάτης

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ
www.dpa.gr

Data protection by Design by Default

- **…από το σχεδιασμό** :
  - Τεχνολογίες ιδιωτικότητας και προστασία προσωπικών δεδομένων κατά το σχεδιασμό συστήματος/επεξεργασίας και όχι εκ των υστέρων
  - **Λαμβάνοντας υπόψη:**
    - Τελευταίες εξελίξεις τεχνολογίας
    - Κόστος εφαρμογής μέτρων
    - Φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας,
    - Ελαχιστοποίηση πιθανότητας κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων από την επεξεργασία
  - **Μέσα επίτευξης:**
    - Ελαχιστοποίηση δεδομένων
    - Ψευδωνυμοποίηση
- **…εξ ορισμού**:
  - Οι «προ-καθορισμένες» ρυθμίσεις πρέπει να είναι οι πιο φιλικές προς την ιδιωτικότητα

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

PRIVACY BY DESIGN

Ασφάλεια επεξεργασίας

Όπως και με το νυν νομικό πλαίσιο, απαιτήσεις για ασφαλή επεξεργασία και με το ΓΚΠΔ. Αλλά…

- **Νέες ρυθμίσεις:**
  - Εξειδίκευση, με πρόταση «ενδεδειγμένων» τεχνικών και οργανωτικών μέτρων:
    - ***Ψευδωνυμοποίηση*** και ***Κρυπτογράφηση***
    - Διασφάλιση **Απορρήτου, Ακεραιότητας, *Διαθεσιμότητας*** και ***Αξιοπιστίας***
    - Αποκατάσταση ***Διαθεσιμότητας*** και της πρόσβασης σε περίπτωση συμβάντος
    - Δοκιμή, εκτίμηση και ***διαρκής αξιολόγηση*** της αποτελεσματικότητας των μέτρων
  - Χρήση εγκεκριμένου κώδικα δεοντολογίας ή μηχανισμού πιστοποίησης (προαιρετικά μεν, αλλά ο ΓΚΠΔ σαφώς ενθαρρύνει)
  - «Αναβαθμίζεται» η σχετική υποχρέωση ασφαλείας και για τους εκτελούντες την επεξεργασία
  - Κοινοποίηση περιστατικών παραβίασης……

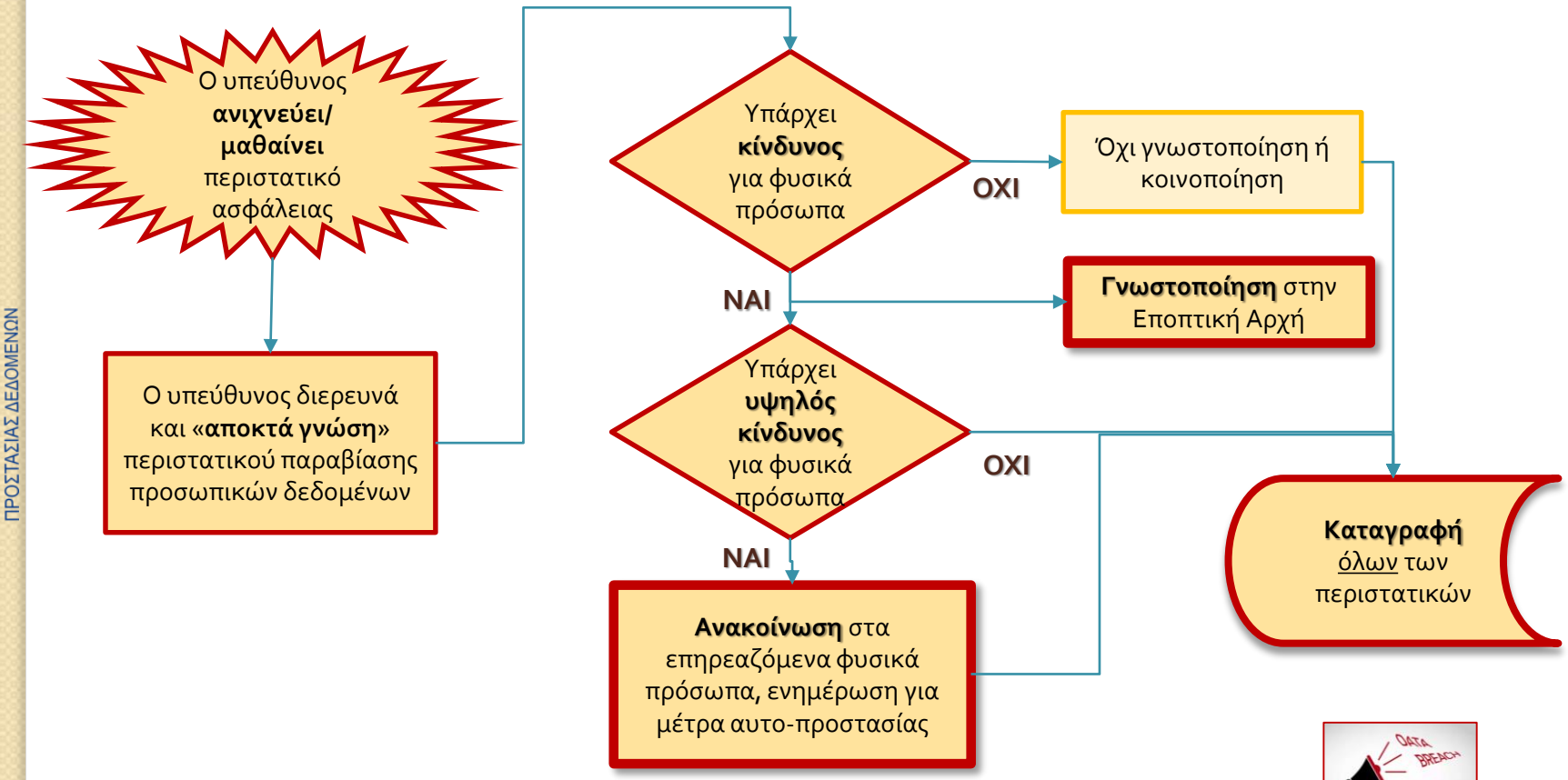
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Περιστατικά Παραβίασης Προσωπικών Δεδομένων

Ορισμός:

- παραβίαση της ασφάλειας (C-I-A) που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα.



ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

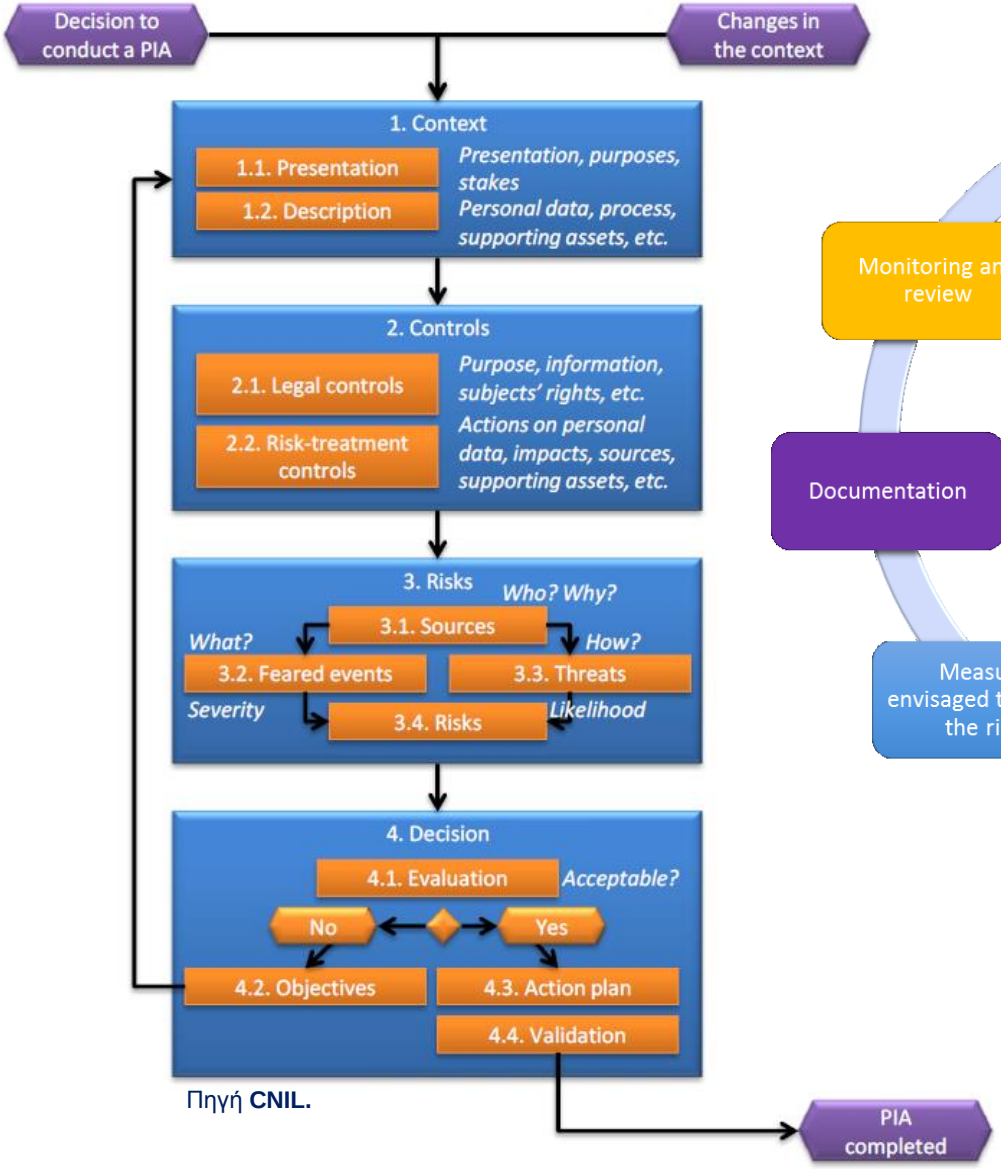
- **Data Protection Impact Assessment (DPIA)**
  - συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας, των σκοπών της επεξεργασίας και της νομικής βάσης
  - εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας
  - εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων
  - τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων

DPIA : εργαλείο ελέγχου & απόδειξης συμμόρφωσης με GDPR

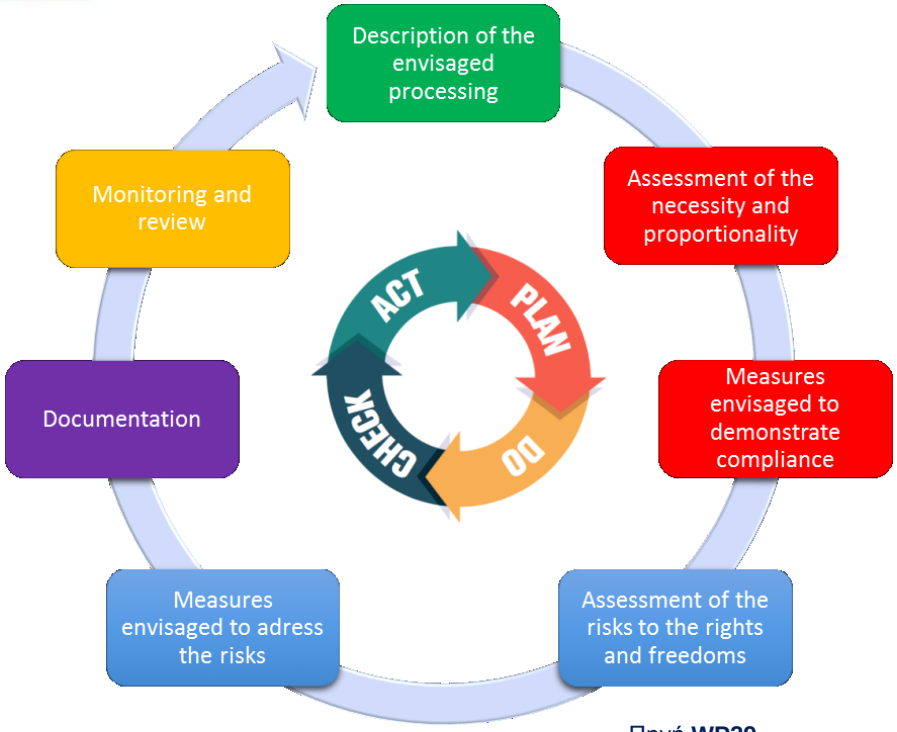
- Υποχρεωτικό όταν "*...ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων*"
- Οι Αρχές θα ορίσουν καταλόγους με επεξεργασίες που απαιτείται DPIA
- Αν μετά την εκπόνηση της DPIA προκύπτει ακόμα «υψηλός κίνδυνος» => Διαβούλευση με την Εποπτική Αρχή

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ
www.dpa.gr

DPIA



Πηγή **CNIL.**



Πηγή **WP29**

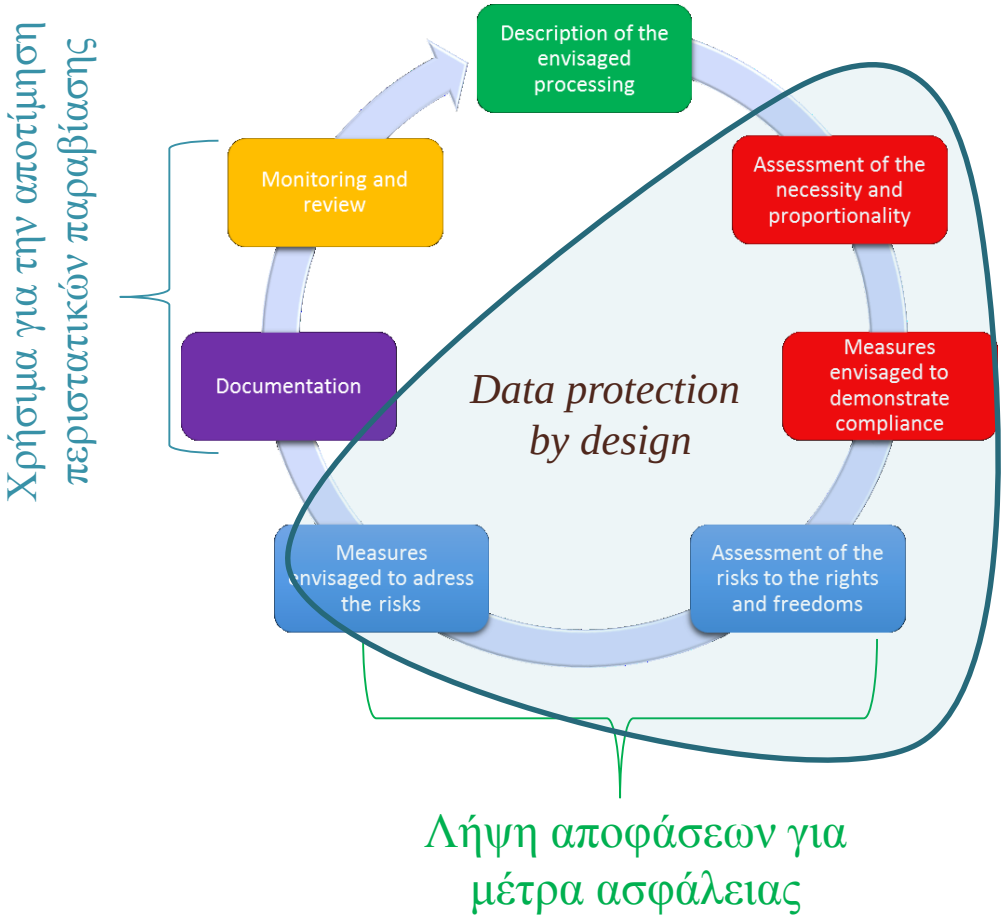
Πηγή **CNIL.**

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Πώς σχετίζονται;



- Μία DPIA ουσιαστικά μπορεί να διασφαλίσει την αρχή «data protection by design»
- Μία DPIA αναμένεται να καταδείξει (μεταξύ άλλων) τις τεχνολογικές λύσεις που απαιτούνται για την ασφάλεια της επεξεργασίας
- Η αποτίμηση κινδύνων και οι τρόποι αντιμετώπισής τους, που πραγματοποιούνται στο πλαίσιο της DPIA, διευκολύνουν την ορθή αποτίμηση / αξιολόγηση των περιστατικών παραβίασης δεδομένων

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Κώδικες Δεοντολογίας - Πιστοποιήσεις

- **Επιθυμητά για την απόδειξη της συμμόρφωσης**
  - Δεν είναι όμως de facto συμμόρφωση!
- Οι κώδικες δεοντολογίας καταρτίζονται από φορείς που εκπροσωπούν υπεύθυνους επεξεργασίας ή εκτελούντες την επεξεργασία και **εγκρίνονται** είτε από τις Εποπτικές Αρχές ενός κράτους μέλους, είτε από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (EDPB)
- Οι πιστοποιήσεις προβλέπονται για **πράξεις επεξεργασίας** (σε υπευθύνους και εκτελούντες)
  - Εκδίδονται από φορείς που διαπιστεύονται είτε από τους αρμόδιους φορείς διαπίστευσης (π.χ. ΕΣΥΔ), είτε από τις Εποπτικές Αρχές.
  - Οι πιστοποιήσεις χορηγούνται βάσει κριτηρίων που **εγκρίνουν** οι Εποπτικές Αρχές (ή το Συμβούλιο Προστασίας Δεδομένων)
  - Η διαπίστευση των φορέων πιστοποίησης πραγματοποιείται βάσει κριτηρίων που **εγκρίνουν** οι Εποπτικές Αρχές (ή το Συμβούλιο Προστασίας Δεδομένων).
- Παρέχουν (ως ένα βαθμό) «*ασφάλεια δικαίου*» καθώς δεν προβλέπεται πλέον η δυνατότητα γνωμοδοτήσεων των Αρχών.