

**Προετοιμασία των Δημόσιων Οργανισμών για
την εφαρμογή του νέου Κανονισμού**
Τα εργαλεία συμμόρφωσης για τη μετάβαση από το ν.2472/1997 στον ΓΚΠΔ



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Γεώργιος Ρουσόπουλος

Δρ. Μηχ. Η/Υ & Πληροφορικής
Ε.Ε.Π. - Α.Π.Δ.Π.Χ.

[grousopoulos at dpa.gr](mailto:grousopoulos@dpa.gr)

Κωνσταντίνος Λιμνιώτης

Δρ. Πληροφορικής και Τηλ/νιών
Ε.Ε.Π. - Α.Π.Δ.Π.Χ.

[klimniotis at dpa.gr](mailto:klimniotis@dpa.gr)

Δομή παρουσίασης

- Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ως Αρχή Εφαρμογής του ΓΚΠΔ
- ΓΚΠΔ: Τα νέα εργαλεία για τη συμμόρφωση με τη νομοθεσία
- Προετοιμάζοντας τη συμμόρφωση - Βασικά βήματα

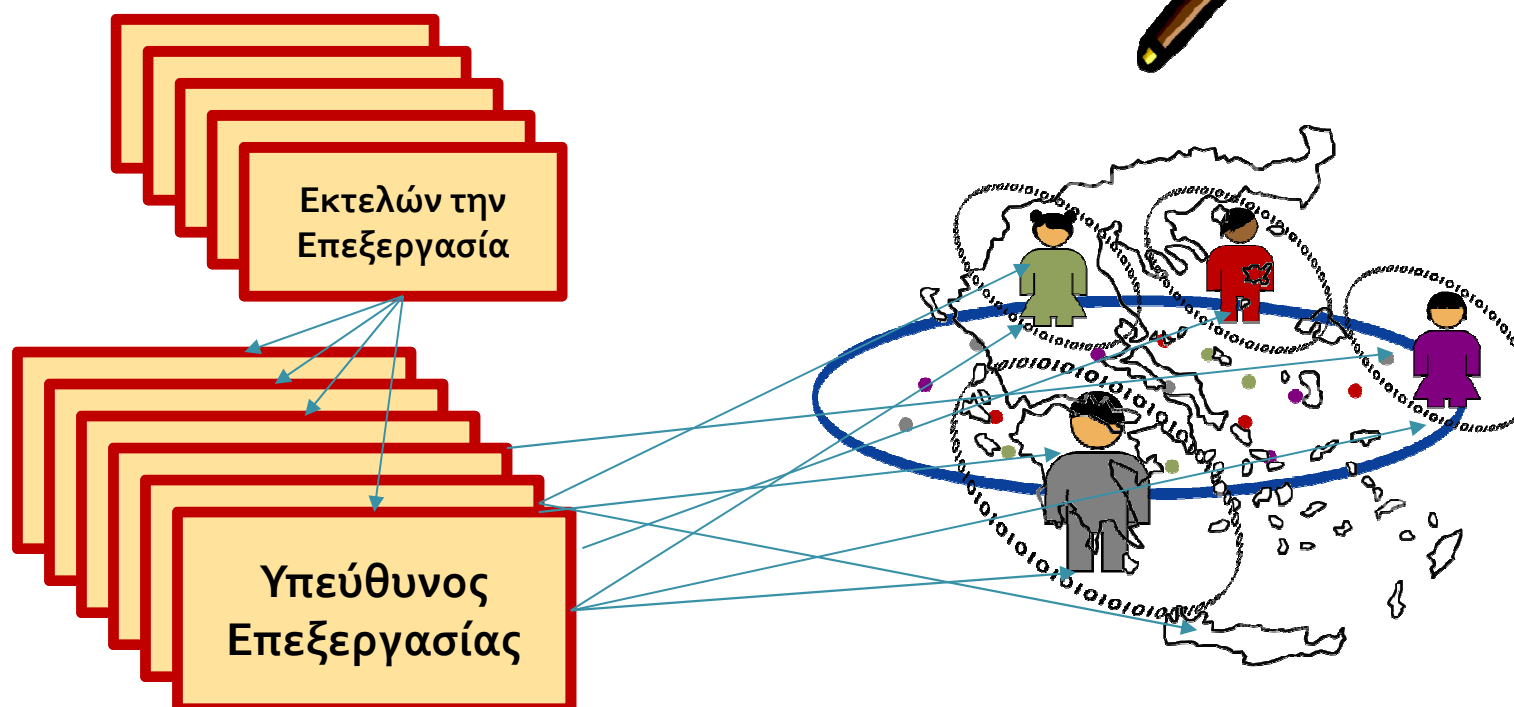


ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Ας ξανασυστηθούμε

Η Αρχή του ν. 2472/1997 και οι αλληλεπιδράσεις της...



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr



- Ρυθμιστικό
- Ελεγκτικό
- Ενημερωτικό

Η Αρχή και τα Φυσικά Πρόσωπα



Παράπονα (καταγγελίες, προσφυγές)

Σχετικά με:

- εφαρμογή του νόμου
- προστασία δικαιωμάτων



Καταγγελίες

- Μπορεί να υποβάλλονται και από φορέα, οργάνωση ή ένωση
- Στην Αρχή της χώρας κατοικίας ή του υπευθύνου
- Ακόμα και για υπεύθυνο εκτός Ε.Ε.
- Ενημέρωση εντός τριμήνου

Ενημέρωση - ευαισθητοποίηση

Ετήσια έκθεση προς Βουλή
Οδηγίες και δημοσιότητα
«Άτυπη» δράση

Ενημέρωση

Ατομικά μετά από αίτημα:

- Πληροφορίες για την **άσκηση των δικαιωμάτων**

Ευαισθητοποίηση

- Επαπειλούμενοι κίνδυνοι
- Κανόνες επεξεργασίας
- Θεσμικές εγγυήσεις
- Άσκηση δικαιωμάτων
- Ειδική αναφορά στα παιδιά

Ο πολίτης «αλληλεπιδρά» με μία Αρχή κάθε φορά



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Η Αρχή και οι Υπεύθυνοι Επεξεργασίας (ν. 2472/1997)



Ρυθμιστικές

Οδηγίες

Καθοδήγηση: Ενιαία εφαρμογή ρυθμίσεων σε εθνικό επίπεδο

Γνώμες ΟΕ αρ. 29

Προσπάθεια συνεκτικής εφαρμογής ρυθμίσεων σε επίπεδο Ε.Ε.

Κανονιστικές πράξεις

Ρύθμιση ειδικών, τεχνικών και λεπτομερειακών θεμάτων

Κώδικες δεοντολογίας

Καλεί και επικουρεί επαγγελματικά σωματεία και ενώσεις

Ερωτήματα

Απαντά σε αιτήσεις υπευθύνου

Έλεγχος και εξακρίβωση της νομιμότητας της επεξεργασίας

Ελεγκτικές

Γνωστοποιήσεις

Τήρηση μητρώου – Δυνατότητα (όχι υποχρέωση) εξέτασης

Άδειες

Υποχρέωση εξέτασης στα ευαίσθητα δεδομένα

Διαβιβάσεις

Περιορισμός – εργαλεία διευκόλυνσης –αδειοδότηση

Έλεγχοι

Δυνατότητα ελέγχου κάθε αρχείου εντός Ελλάδας

Συστάσεις/υποδείξεις

Εργαλεία επιβολής νομοθεσίας

Κυρώσεις



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Η Αρχή και οι Υπεύθυνοι Επεξεργασίας (ΓΚΠΔ)



Ρυθμιστικές

Κατευθυντήριες γραμμές, Συστάσεις, βέλτιστες πρακτικές

Αρμοδιότητα στο **Ε.Σ.Π.Δ.** με σκοπό την ενθάρρυνση της συνεκτικής εφαρμογής του ΓΚΠΔ. Οι Αρχές προτείνουν και εισηγούνται.

Κανονιστικές πράξεις

Κώδικες δεοντολογίας

Ενθαρρύνει τους φορείς και **εγκρίνει** τους κώδικες

D.P.O.

Συνεργάζονται με τους **DPO** ώστε αυτοί να παρέχουν τις απαραίτητες συμβουλές και κατευθύνσεις

Πιστοποιήσεις

Μηχανισμοί πιστοποίησης – σφραγίδες – σήματα: νέα εργαλεία

Αρχεία δραστηριοτήτων

Τηρούνται εσωτερικά – διαθέσιμα στις Αρχές

DPIA - Διαβούλευση

Κατάλογοι δραστηριοτήτων υψηλού κινδύνου - Συμβουλές

Διαβιβάσεις

Περιορισμός αδειών - Έμφαση στα εργαλεία νομιμότητας

Περιστατικά παραβίασης

Υποχρέωση τήρησης / γνωστοποίησης / κοινοποίησης

Έλεγχοι

Δυνατότητα συνεργασίας για έλεγχο και εντός Ε.Ε.

Διορθωτικές εξουσίες

Ευρύτερη γκάμα επανορθωτικών εξουσιών στις Αρχές.

Αρχεία παραβάσεων – Εντολές για «επανόρθωση»

Πρόστιμα: αποτελεσματικά, αναλογικά και αποτρεπτικά

Ελεγκτικές



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Η Αρχή και ο Δημόσιος Τομέας

(ως Υπεύθυνος Επεξεργασίας)



Γνωμοδοτεί

για κάθε ρύθμιση που αφορά την επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr



- Κοινοβούλιο
- Κυβέρνηση
- Άλλα όργανα και οργανισμούς

Για νομοθετικά και διοικητικά μέτρα, σύμφωνα με το εθνικό δίκαιο



Απαραίτητη πριν την εφαρμογή κάθε νέου μέτρου

- ως μέρος γενικής εκτίμησης αντικτύπου στο πλαίσιο έγκρισης της νομικής βάσης ή ...
- πριν τη θέση σε εφαρμογή μιας διάταξης



Υποχρέωση DPO για κάθε Δημόσιο Φορέα

Ο ΓΚΠΔ προσπαθεί να επιβάλλει **διαβούλευση** με την Αρχή **κατά την εκπόνηση** ενός νομοθετικού ή κανονιστικού μέτρου

Η Αρχή και οι Εκτελούντες την επεξεργασία

Ευθύνη του Υπεύθυνου Επεξεργασίας

οι υποχρεώσεις των εκτελούντων (π.χ. υπεργολάβοι) ρυθμίζονται από τη μεταξύ τους σύμβαση



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Ευθύνη του Υπεύθυνου Επεξεργασίας

Η βασική ευθύνη για τη νομιμότητα της επεξεργασίας διατηρείται στον Υπεύθυνο

Ευθύνη του Εκτελούντος την Επεξεργασία

Οφείλουν να «βοηθούν» τον Υπεύθυνο στην εκτέλεση των υποχρεώσεων του ΓΚΠΔ

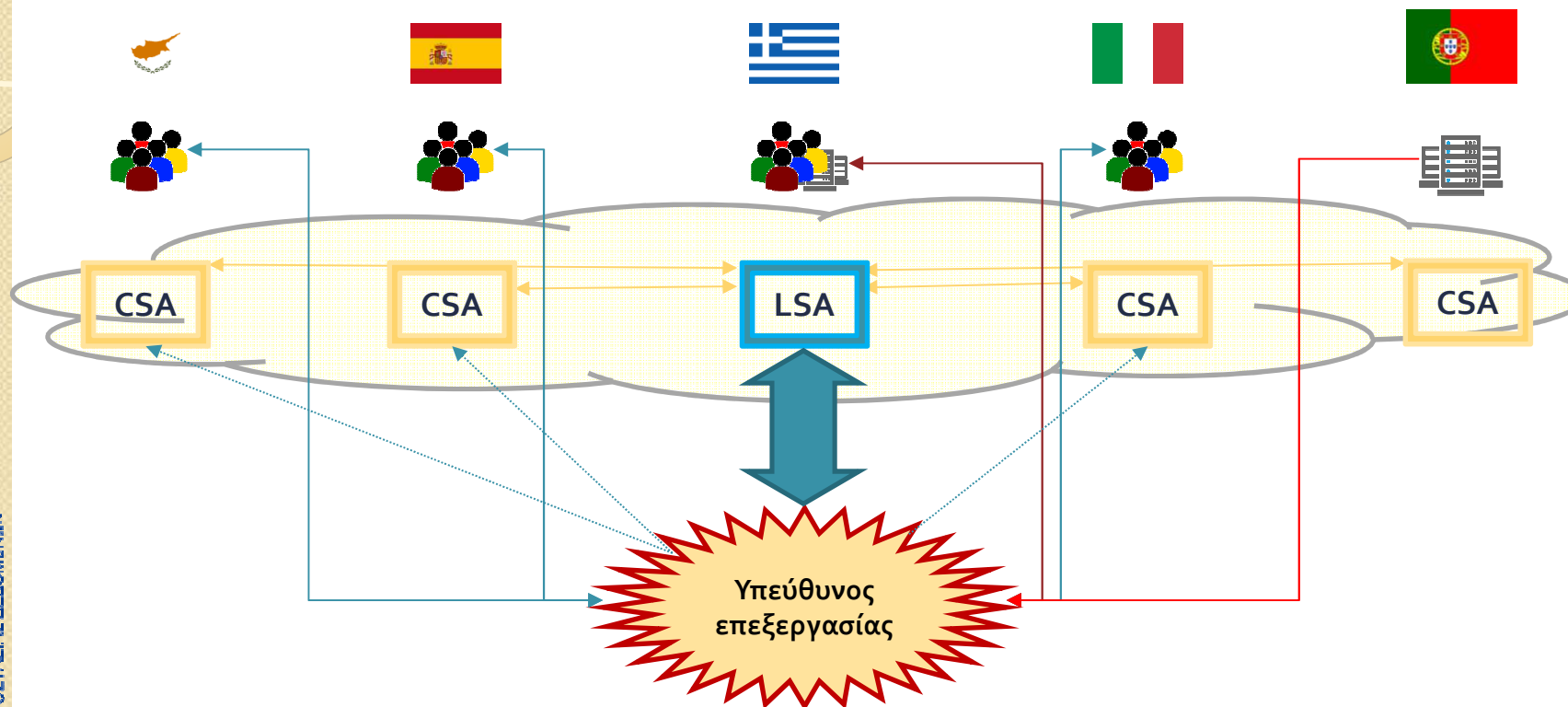
- Μέτρα ασφάλειας
- Ικανοποίηση δικαιωμάτων
- ...

Αυτοτελής Ευθύνη του Εκτελούντος

- Οφείλουν να ενημερώνουν τον υπεύθυνο όταν εκτιμούν ότι τους ζητείται παράνομη ενέργεια
- Αρχεία δραστηριοτήτων
- DPO
- Περιστατικά παραβίασης
- Συνεργάζονται με τις Αρχές

Οι Αρχές μπορούν, πλέον, να επιβάλουν διορθωτικά μέτρα και σε εκτελούντες της επεξεργασία

One Stop Shop



Κάθε Υπεύθυνος Επεξεργασίας «συνεργάζεται» με μια Εποπτική Αρχή
Οι πολίτες «απευθύνονται» σε μια Εποπτική Αρχή

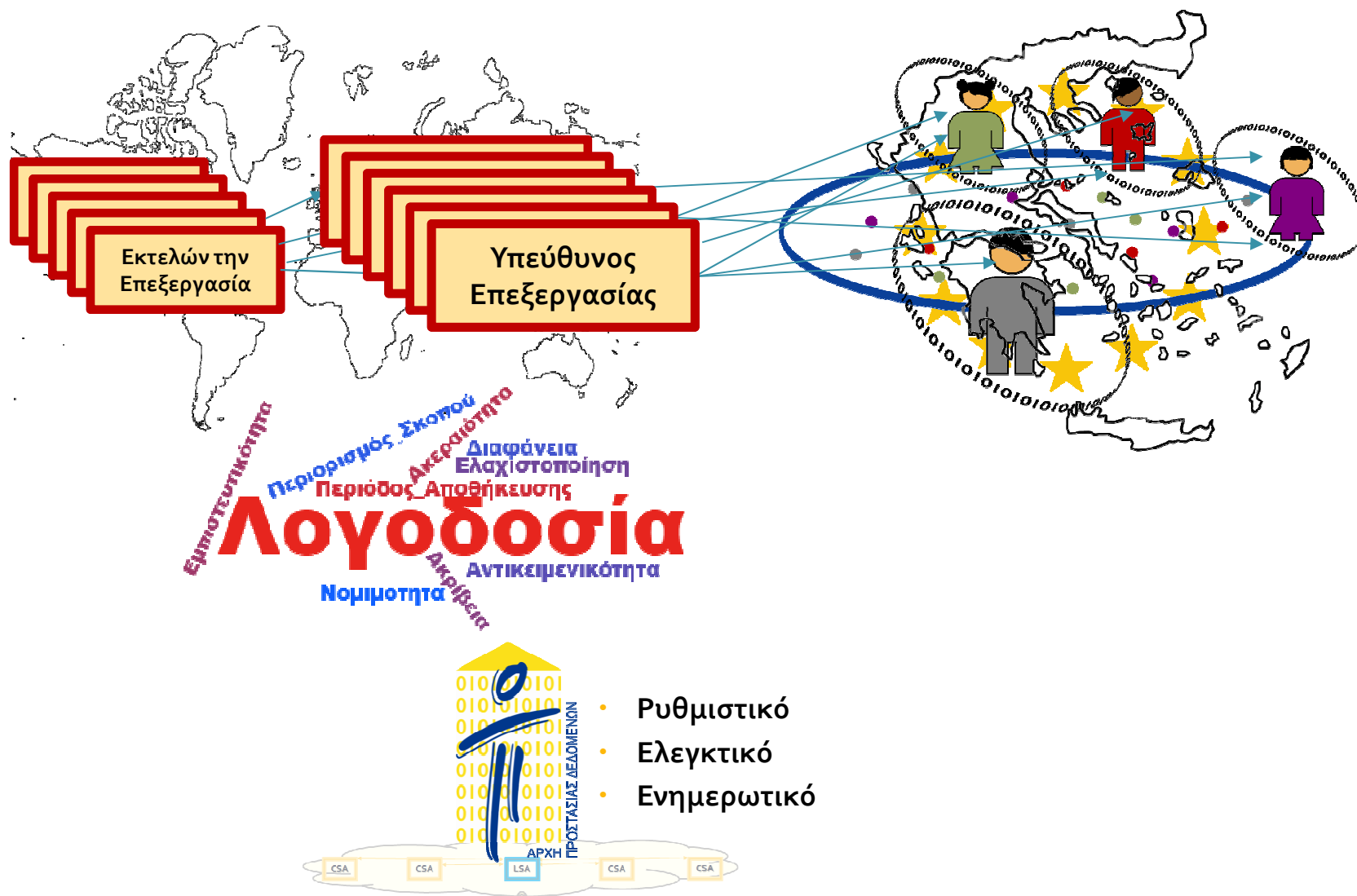


ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Τελικά...

Ποιες είναι οι ουσιαστικές αλλαγές;



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

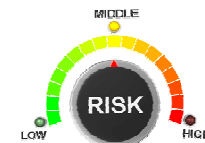
www.dpa.gr

- Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ως Αρχή Εφαρμογής του ΓΚΠΔ
- ΓΚΠΔ: Τα νέα εργαλεία για τη συμμόρφωση με τη νομοθεσία
- Προετοιμάζοντας τη συμμόρφωση σε 10 βήματα



«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
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 έλεγχοι 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
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



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
- **Γνωστοποίηση περιστατικών παραβίασης.....**



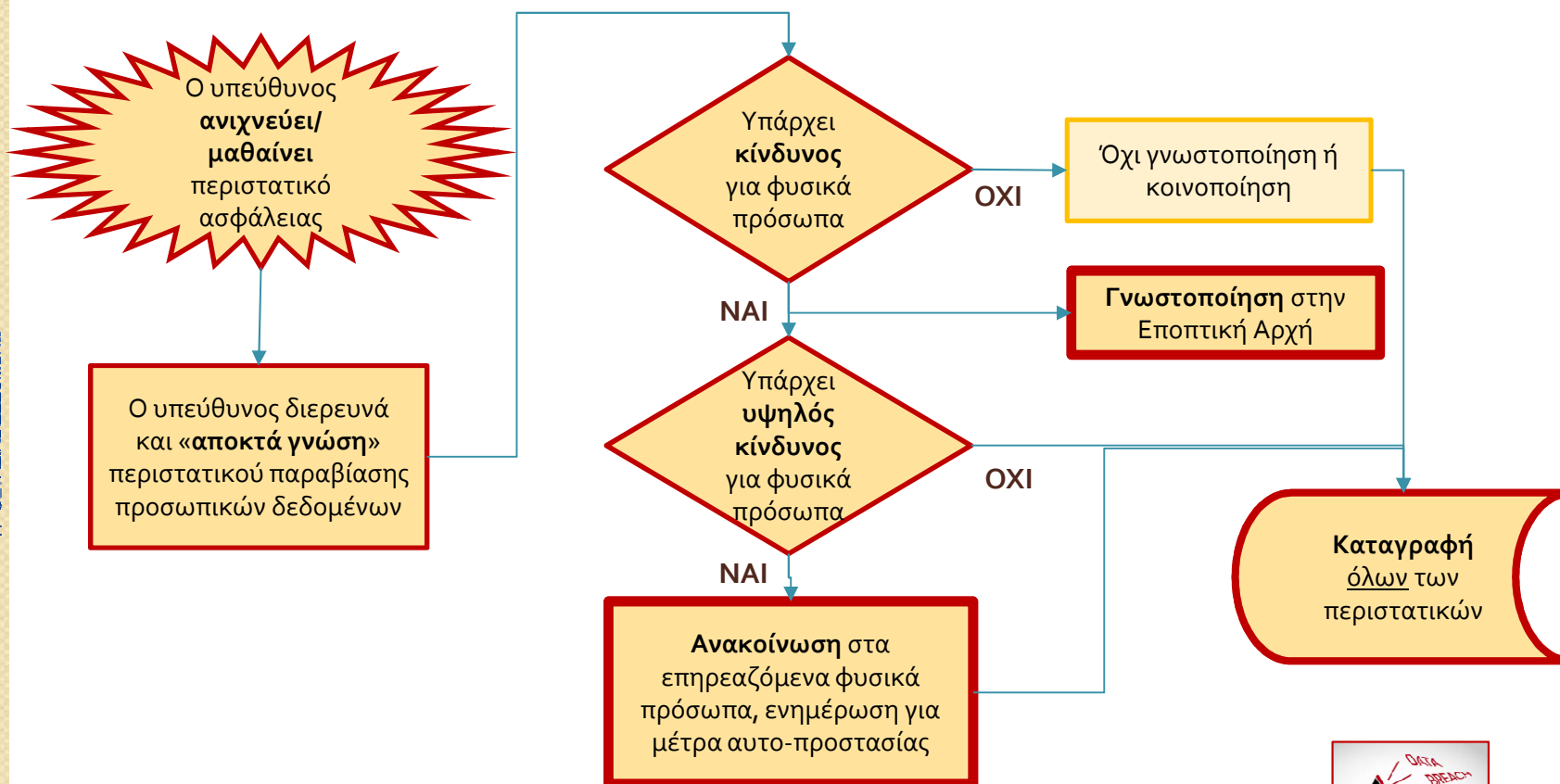
ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

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.



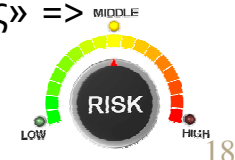
Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

- **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

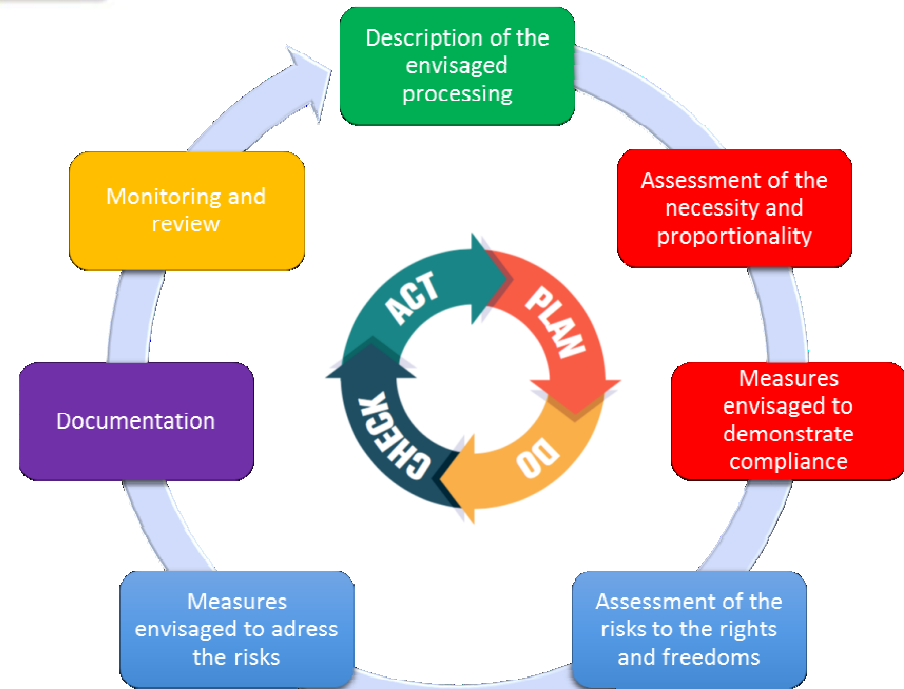
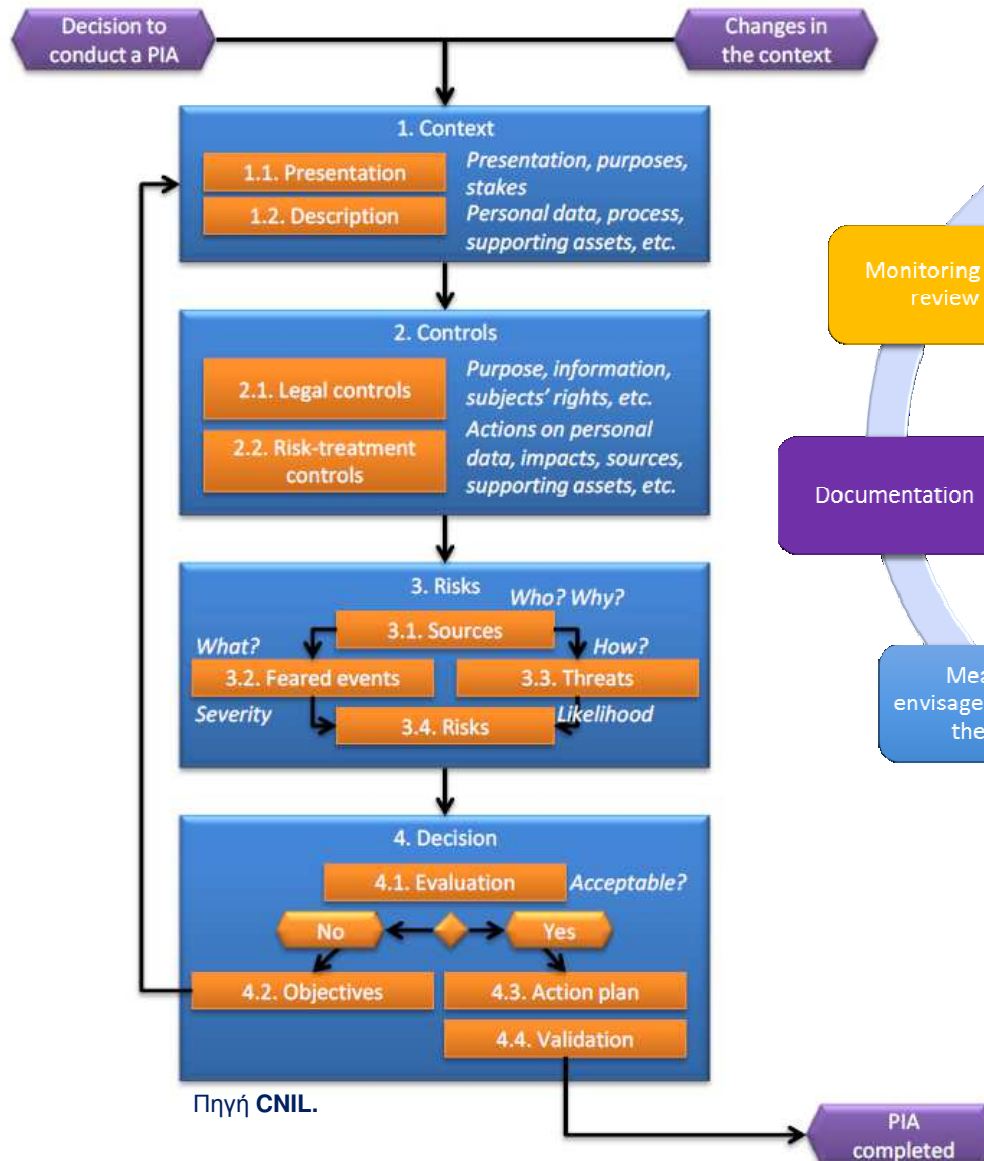
- Υποχρεωτικό όταν “...ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων”
- Οι Αρχές θα ορίσουν καταλόγους με επεξεργασίες που απαιτείται DPIA
 - Τα Κράτη-Μέλη μπορεί να κρίνουν αναγκαία την εκπόνηση DPIA για την έκδοση νομοθετήματος στο οποίο βασίζεται η άσκηση καθηκόντων δημόσιας αρχής ή φορέα
- Αν μετά την εκπόνηση της DPIA προκύπτει ακόμα «υψηλός κίνδυνος» =>
Διαβούλευση με την Εποπτική Αρχή



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

DPIA



Πηγή WP29



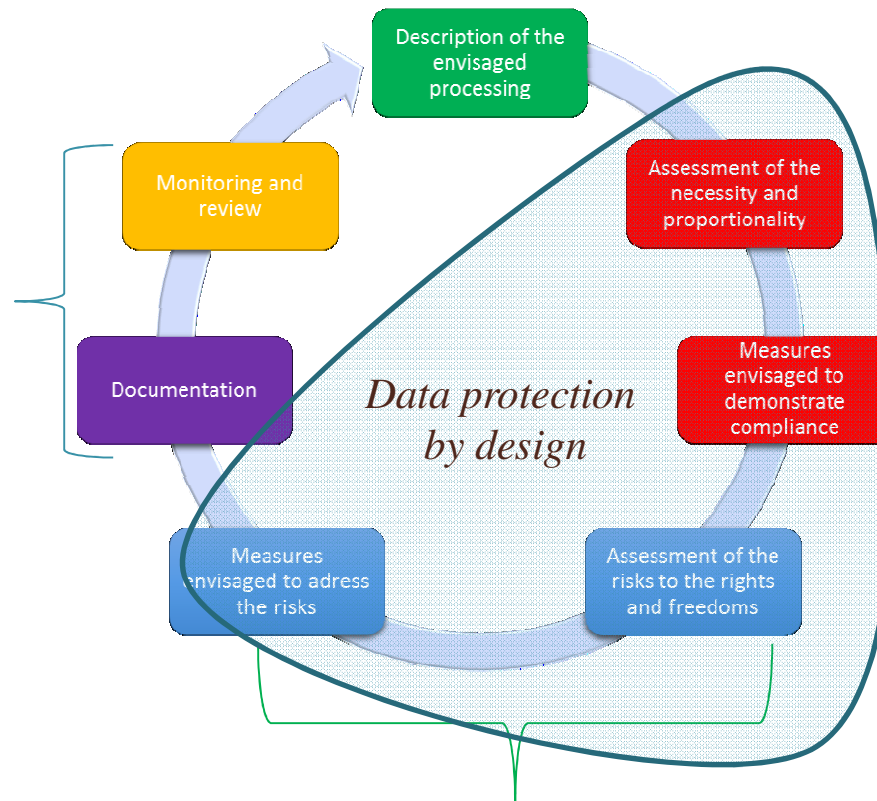
Πηγή CNIL.



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

Χρήσιμα για την αποτίμηση
περιστατικών παραβίασης

Λήψη αποφάσεων για
μέτρα ασφάλειας



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.



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr



- Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ως Αρχή Εφαρμογής του ΓΚΠΔ
- ΓΚΠΔ: Τα νέα εργαλεία για τη συμμόρφωση με τη νομοθεσία
- Προετοιμάζοντας τη συμμόρφωση – Βασικά βήματα



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Προετοιμασία για τον ΓΚΠΔ

- Οι ακριβείς υποχρεώσεις για τον κάθε φορέα τελικά εξαρτώνται από διάφορους παράγοντες
 - Φύση της επεξεργασίας, εκτιμώμενοι κίνδυνοι,
- Ωστόσο, είναι σημαντικό ο κάθε φορέας να εντοπίσει έγκαιρα τις υποχρεώσεις του
- Συστηματικοποίηση των βασικών βημάτων που πρέπει να ακολουθηθούν από τους φορείς, για να είναι έτοιμοι για τον ΓΚΠΔ
 - Υπεύθυνοι επεξεργασίας
αλλά και
 - Εκτελούντες την επεξεργασία
- Στα βήματα εμπλέκονται:
 - Διοίκηση, Επιχειρησιακή λειτουργία, Νομικό τμήμα, Τμήμα Πληροφορικής κ.α.



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

1

Ενημέρωση – Ετοιμότητα



- Η συμμόρφωση με το ΓΚΠΔ θα πρέπει να αντιμετωπιστεί ως **μία συστηματική δράση**, με τον κατάλληλο σχεδιασμό
- Όλο το ανθρώπινο δυναμικό θα πρέπει να είναι ενήμερο για την αλλαγή του νομικού πλαισίου
 - Π.χ.: Περιστατικά παραβίασης δεδομένων ενδέχεται να υποπέσουν στην αντίληψη του οποιουδήποτε
- Τα **πρόσωπα-κλειδιά** του φορέα πρέπει να κατανοήσουν την αλλαγή στο νομικό πλαίσιο με τις συνέπειες που αυτή επιφέρει
 - : Ο ΓΠΚΔ μπορεί να επιφέρει αύξηση στο φόρτο εργασίας του φορέα
 - Π.χ. απλά και μόνο για την ικανοποίηση των δικαιωμάτων
 - Γρήγορη ανάθεση κατάλληλων ρόλων και αρμοδιοτήτων
- Μία **πρώτη αποτίμηση σημαντικών «ελλείψεων»**, με εύρεση τρόπων αντιμετώπισής τους, είναι σημαντικό να γίνει έγκαιρα, γιατί θα διευκολύνει τα επόμενα βήματα



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

2

Υπεύθυνος Προστασίας Δεδομένων



- Υποχρέωση για κάθε Δημόσιο φορέα, ανεξάρτητα του μεγέθους του
- Μπορεί να σας βοηθήσει για την υλοποίηση του ΓΚΠΔ.
 - Προσοχή: ο ρόλος του είναι **συμβουλευτικός**, όχι αποφασιστικός. Οι αποφάσεις λαμβάνονται πάντα από τη Διοίκηση. Μπορεί όμως να συνεισφέρει στην ταχύτερη συμμόρφωση με τις προτάσεις του.
- Μπορεί να είναι υπάλληλος ή με εξωτερική ανάθεση.
- Δύο ή περισσότεροι φορείς μπορεί να έχουν κοινό DPO
 - Αλλά πρέπει να μπορεί να απευθυνθεί κάποιος εύκολα στο DPO για κάθε φορέα.
- **Καινοφανής θέση** για το ελληνικό δημόσιο:
 - Λειτουργεί **εκτός ιεραρχίας** και δημοσιοϋπαλληλικής δομής
 - **Λογοδοτεί** απευθείας στο **υψηλότερο επίπεδο**.
 - Μπορεί να ασκεί τα **καθήκοντα με παράλληλη ανάθεση**, αρκεί να μην υπάρχει ασυμβίβαστο



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr



- **Αναγνώριση των δραστηριοτήτων**
 - **Προσοχή: Πολλές μπορεί να μην είναι άμεσα εμφανείς!**
 - Αρχείο εγγράφων, αρχείο προσωπικού, αρχείο πρωτοκόλλου, αρχεία από ηλεκτρονικές εφαρμογές, αρχεία επαφών για επικοινωνιακούς σκοπούς, αρχεία για σκοπούς ασφάλειας (π.χ. υλικό καμερών, καταγραφής προσβάσεων σε διαδικτυακές υπηρεσίες) κτλ.
 - Διαχωρισμός ανά σκοπό επεξεργασίας
- **Υπάρχει υποχρέωση καταγραφής αρχείων δραστηριοτήτων;**
 - Η επεξεργασία ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα των προσώπων;
 - Η επεξεργασία αφορά ειδικές κατηγορίες δεδομένων ή δεδομένα αναφορικά με ποινικές καταδίκες;
 - Προσοχή: Οι ειδικές κατηγορίες («ευαίσθητα» δεδομένα) διευρύνονται στο ΓΚΠΔ
 - Ο φορέας απασχολεί περισσότερα από 250 άτομα;
- **Καταγραφή αρχείων δραστηριοτήτων**
 - Ποιος; Γιατί; Τι; Σε ποιόν; Διαβιβάσεις; Για πόσο; Πως;
- Η καταγραφή των αρχείων βαρύνει και τον εκτελούντα την επεξεργασία, για τις δραστηριότητες που πραγματοποιεί για λογαριασμό του υπευθύνου





Έλεγχος τήρησης συμμόρφωσης

- **Για κάθε έναν από τους σκοπούς επεξεργασίας:**

- Είναι ο σκοπός σαφής; Υπάρχει νομική διάταξη για την επεξεργασία αυτή;
- Γίνεται επεξεργασία μόνο στο πλαίσιο αυτού του σκοπού;
- Πώς έχουν ληφθεί τα δεδομένα;
- Είναι τα απολύτως απαραίτητα δεδομένα για τον εν λόγω σκοπό;
- Πόσος χρόνος απαιτείται για την επεξεργασία των δεδομένων;

- Πόσο ασφαλής είναι η τήρηση και περαιτέρω επεξεργασία των δεδομένων;
 - Κρυπτογραφούνται; Ψευδωνυμοποιούνται;
 - Ποια πρόσωπα είναι αυτά που πρέπει να έχουν πρόσβαση;
 -
- Οι συνεργαζόμενες εταιρείες παρέχουν εγγυήσεις για τη συμμόρφωση με το ΓΚΠΔ;
- Ο έλεγχος ως προς το αν τηρούνται οι αρχές που διέπουν τη νόμιμη επεξεργασία των δεδομένων και αν γίνονται σεβαστά τα δικαιώματα των προσώπων πρέπει να είναι **συνεχής**



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr



Έλεγχος τήρησης συμμόρφωσης

- **Για κάθε έναν από τους σκοπούς επεξεργασίας:**

- Γίνεται επεξεργασία αποκλειστικά πάνω στη βάση των καταγεγραμμένων εντολών του υπευθύνου επεξεργασίας;
- Επεξεργασία για άλλο σκοπό, με πρωτοβουλία του εκτελούντος, τον καθιστά υπεύθυνο επεξεργασίας και αποτελεί παράβαση
- Τα πρόσωπα που είναι εξουσιοδοτημένα, έχουν αναλάβει δέσμευση τήρησης εμπιστευτικότητας;

- Πόσο ασφαλής είναι η τήρηση και περαιτέρω επεξεργασία των δεδομένων;

- Κρυπτογραφούνται; Ψευδωνυμοποιούνται;
- Ποια πρόσωπα είναι αυτά που πρέπει να έχουν πρόσβαση;
-

- Οι συνεργαζόμενες εταιρείες παρέχουν εγγυήσεις για τη συμμόρφωση με το ΓΚΠΔ;

- Για την εν λόγω επεξεργασία, υπάρχει άδεια του υπευθύνου επεξεργασίας;

- Ο έλεγχος ως προς το αν τηρούνται οι αρχές που διέπουν τη νόμιμη επεξεργασία των δεδομένων και αν γίνονται σεβαστά τα δικαιώματα των προσώπων πρέπει να είναι **συνεχής**



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr



Αναθεώρηση πολιτικών προστασίας δεδομένων και διαδικασιών



- Δεν αρκεί να «κρύβετε» την ενημέρωση σε ένα κείμενο Πολιτικής Προστασίας Προσωπικών Δεδομένων ή Απορρήτου.
- Εξετάστε τι είδους ενημέρωση παρέχετε σήμερα στους πολίτες
 - Αλλαγή υποχρέωσης, απαιτούνται περισσότερα στοιχεία
 - Προστίθενται μεταξύ άλλων:
 - η νομική βάση για την επεξεργασία (που «δυσκολεύει» την ενημέρωση καθώς προϋποθέτει τη νομική ανάλυση)
 - το χρονικό διάστημα επεξεργασίας/αποθήκευσης.
 - Τα στοιχεία που ήταν απαραίτητα ως ενημέρωση με την «παλιά» νομοθεσία ήταν σε γενικές γραμμές 4, ενώ με το ΓΚΠΔ γίνονται 11 (δεν έχουν όλα πάντα εφαρμογή).
- Δημοσιοποιήστε τα στοιχεία του DPO σας
- Τι είδους ενημέρωση παρέχετε όταν συλλέγονται δεδομένα από πολίτες;
 - Μήπως τα σχετικά έντυπα χρειάζονται αναθώρηση;
- Πώς ικανοποιείται η ενημέρωση όταν συλλέγονται δεδομένα από τρίτες πηγές;

Αντιμετωπίστε ενιαία την καταγραφή, τη συμμόρφωση και την ενημέρωση των πολιτών.



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

6

Ορισμός εσωτερικών διαδικασιών για την ικανοποίηση των δικαιωμάτων του ΓΚΠΔ



- Ο ΓΚΠΔ προβλέπει νέα και επαυξημένα δικαιώματα για τους πολίτες και ικανοποίηση σε στενά χρονικά διαστήματα.
- Η υποχρέωση ισχύει και για το Δημόσιο
 - Οφείλετε να είστε έτοιμοι για να ανταπεξέλθετε στα αιτήματά τους
 - Οι πολίτες είναι πλέον πιο ενημερωμένοι για τα δικαιώματά τους
- Διαθέτετε τις κατάλληλες διαδικασίες;
 - Διαθέτετε το κατάλληλο προσωπικό;
- **Αναλύστε – εντοπίστε κενά – αναθεωρήστε**
- Υπολογίστε το **κόστος** για την άσκηση των δικαιωμάτων
 - Αναγνωρίστε πιθανά υπερβολικά κόστη και προετοιμαστείτε. Κατ' αρχήν η άσκηση των δικαιωμάτων είναι δωρεάν για τον πολίτη...
 - Ετοιμάστε πρότυπα έγγραφα (Παραδείγματα: για ικανοποίηση δικαιωμάτων - για άρνηση ικανοποίησης με αιτιολόγηση...)
- Επικοινωνήστε τις αλλαγές, στους κατάλληλους υπαλλήλους σας.
- Προετοιμαστείτε και για τις δύσκολες περιπτώσεις.
 - Πως χειριζόμαστε περιπτώσεις προβλημάτων;
 - Πως αντιμετωπίζουμε πολλαπλά αιτήματα;



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

7

Εκτίμηση αντικτύπου (DPIA)



- Γνωρίζετε πότε ένας δημόσιος φορέας πρέπει να κάνει DPIA;
 - Τίποτα δεν σας εμποδίζει να κάνετε και τώρα
 - Είναι μια ορθή πρακτική και μπορεί να αποκαλύψει «ατέλειες» του φορέα σας στην τήρηση της νομοθεσίας.
- Σε πράξεις επεξεργασίας μεγάλης κλίμακας που στοχεύουν στην επεξεργασία σημαντικής ποσότητας δεδομένων προσωπικού χαρακτήρα σε περιφερειακό, εθνικό ή υπερεθνικό επίπεδο, οι οποίες θα μπορούσαν να επηρεάσουν μεγάλο αριθμό υποκειμένων των δεδομένων και οι οποίες είναι πιθανόν να έχουν ως αποτέλεσμα υψηλό κίνδυνο (...)
- Υπάρχουν περιπτώσεις στις οποίες ενδέχεται να είναι λογικό το αντικείμενο μιας DPIA να υπερβαίνει ένα μεμονωμένο σχέδιο, για παράδειγμα εάν δημόσιες αρχές ή φορείς σκοπεύουν να εγκαθιδρύσουν μια κοινή εφαρμογή ή πλατφόρμα επεξεργασίας
- Διαβούλευση με την εποπτική αρχή θα πρέπει να πραγματοποιείται κατά την εκπόνηση ενός νομοθετικού ή κανονιστικού μέτρου που προβλέπει την επεξεργασία δεδομένων προσωπικού χαρακτήρα, προκειμένου να μετριάζονται οι κίνδυνοι για το υποκείμενο των δεδομένων.



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

7

Εκτίμηση αντικτύπου (DPIA)



- Όταν σε (νέα) διάταξη προβλέπονται μέτρα που συνεπάγονται επεξεργασία για την οποία απαιτείται εκτίμηση αντικτύπου (αρ. 35) χρήσιμο είναι αυτή να γίνεται πριν την ψήφιση της διάταξης.
 - Τότε πρέπει να αποτελεί τμήμα της γενικής εκτίμησης αντικτύπου της διάταξης (π.χ. στην αιτιολογική έκθεση ή σε ξεχωριστή έκθεση επιπτώσεων της διάταξης).
 - Προβλέπεται γνώμη της Αρχής πριν από νομοθετικά μέτρα (όπως και σήμερα...).
- Διαφορετικά, απαιτείται η διενέργεια DPIA πριν την έναρξη της επεξεργασίας.
 - Σε κάθε δημόσιο έργο, σε κάθε νέα επεξεργασία, η DPIA πρέπει να αποτελεί τμήμα της αρχικής μελέτης.
 - Εξασφαλίζεται τόσο το "Data Protection by Design" όσο και το "Data Protection by Default".
- Σε κάθε περίπτωση, αν υπάρχει αμφιβολία και προκύπτει υψηλός κίνδυνος, προβλέπεται **διαβούλευση με την Αρχή**.
- Εξετάστε:
 - Ποιος θα **πραγματοποιήσει** την DPIA;
 - Ποιοι **εργαζόμενοι** σας/τμήματά σας πρέπει να εμπλακούν;
 - Ποιος θα **αξιολογήσει** τα αποτελέσματα της DPIA;



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr



Παραβιάσεις δεδομένων

- Η ασφαλής επεξεργασία των προσωπικών δεδομένων, με κατάλληλα τεχνικά και οργανωτικά μέτρα, παραμένει ζητούμενο.
 - Εμπιστευτικότητα – Ακεραιότητα – Διαθεσιμότητα των προσωπικών δεδομένων
 - **Αναθεώρηση διαδικασιών** ώστε:
 - Να γίνεται έγκαιρη ανίχνευση και αξιολόγηση ενός περιστατικού παραβίασης δεδομένων, ώστε να **καταγράφεται εσωτερικά τεκμηρίωση αυτού**
 - Πρέπει να είναι σαφές τι συνιστά περιστατικό παραβίασης δεδομένων
 - Ενδεχομένως είναι πιο «ευρύς» ο όρος από ό,τι αρχικώς νομίζουμε
- **Γνωστοποίηση του περιστατικού στην ΑΠΔΠΧ**
 - Με συγκεκριμένες πληροφορίες επ' αυτού
 - Οι προθεσμίες είναι «πιεστικές»
 - **Ενημέρωση των προσώπων που αφορά το περιστατικό**, όταν αυτό ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες τους
- Οι κίνδυνοι για παραβίαση δεδομένων, από τυχαία ή εσκεμμένη αιτία, είναι πάντα πολύ πιθανοί – **Στόχος θα πρέπει να είναι η μέγιστη δυνατή ελαχιστοποίηση των κινδύνων**
 - Ενδεικτικά: Σωστά εφαρμοζόμενες τεχνικές κρυπτογράφησης ή/και ανωνυμοποίησης/ψευδωνυμοποίησης



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr



Παραβιάσεις δεδομένων

- Η ασφαλής επεξεργασία των προσωπικών δεδομένων, με κατάλληλα τεχνικά και οργανωτικά μέτρα, παραμένει ζητούμενο.
 - Εμπιστευτικότητα – Ακεραιότητα – Διαθεσιμότητα των προσωπικών δεδομένων
 - **Αναθεώρηση διαδικασιών** ώστε:
 - Να γίνεται έγκαιρη ανίχνευση και αξιολόγηση ενός περιστατικού παραβίασης δεδομένων, ώστε να **καταγράφεται εσωτερικά τεκμηρίωση αυτού**
 - Πρέπει να είναι σαφές τι συνιστά περιστατικό παραβίασης δεδομένων
 - Ενδεχομένως είναι πιο «ευρύς» ο όρος από ό,τι αρχικώς νομίζουμε
- Χωρίς καθυστέρηση ενημέρωση του υπεύθυνου επεξεργασίας για το περιστατικό
 - Συνδρομή στον υπεύθυνο επεξεργασίας
- Οι κίνδυνοι για παραβίαση δεδομένων, από τυχαία ή εσκεμμένη αιτία, είναι πάντα πολύ πιθανοί – **Στόχος θα πρέπει να είναι η μέγιστη δυνατή ελαχιστοποίηση των κινδύνων**
 - Ενδεικτικά: Σωστά εφαρμοζόμενες τεχνικές κρυπτογράφησης ή/και ανωνυμοποίησης/ψευδωνυμοποίησης



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Συμπεράσματα

- Ο ΓΚΠΔ ενισχύει το θεμελιώδες δικαίωμα της προστασίας προσωπικών δεδομένων
- Ενσωματώνει την προστασία δεδομένων στις επιχειρησιακές διαδικασίες
 - «Μεταφέρει» το βάρος στους ίδιους φορείς στο να αυτο-συμμορφώνονται και να μπορούν να το αποδεικνύουν όποτε χρειαστεί
 - Καταργούνται «γραφειοκρατικές» διαδικασίες που δεν παρείχαν ουσιαστικό επίπεδο προστασίας
- Νέα δικαιώματα για τα φυσικά πρόσωπα
 - Νέες υποχρεώσεις για υπευθύνους και εκτελούντες
- Νέος ρόλος της Αρχής Προστασίας Προσωπικών Δεδομένων
- Η προστασία προσωπικών δεδομένων δεν θα πρέπει να εκλαμβάνεται ως «εμπόδιο» στις δράσεις των φορέων
 - Όλοι θα είναι ωφελημένοι από την ορθή προστασία του δικαιώματος αυτού
 - Ο ΓΚΠΔ πρέπει να εκληφθεί ως ένα πολύτιμο εργαλείο για όλους



Ευχαριστούμε για την
προσοχή σας



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr