ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
(General Data Protection Regulation)

Κωνσταντίνος Λαμπρινουδάκης
Καθηγητής
Τμήμα Ψηφιακών Συστημάτων – Πανεπιστήμιο Πειραιώς

Τακτικό Μέλος Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Ορόσημα ΓΚΠΔ

- **Ιανουάριος 2012:** Η Ευρωπαϊκή Ένωση προτείνει μεταρρύθμιση των κανόνων προστασίας των δεδομένων
- **Μάρτιος 2014:** Το Ευρωπαϊκό Κοινοβούλιο εγκρίνει την πρόταση για τον νέο Κανονισμό (πρώτη ανάγνωση)
- **Απρίλιος 2016:** Το Ευρωπαϊκό Κοινοβούλιο ψηφίζει τον Κανονισμό 679/2016 – Γενικός Κανονισμός για την Προστασία Προσωπικών Δεδομένων (General Data Protection Regulation)
- **Μάιος 2016:** Ο Κανονισμός τίθεται σε ισχύ, με μεταβατική περίοδο δύο (2) ετών
- **25 Μαΐου 2018:** Ο Κανονισμός εφαρμόζεται, ως νομοθέτημα άμεσης εφαρμογής σε όλες τις χώρες – μέλη της Ευρωπαϊκής Ένωσης

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

ΓΚΠΔ

- Καθορίζει τις απαιτήσεις για την προστασία των φυσικών προσώπων όσον αφορά στην επεξεργασία δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών
- Είναι υποχρεωτικός για τους οργανισμούς που διαχειρίζονται προσωπικά δεδομένα Ευρωπαίων πολιτών

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
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……

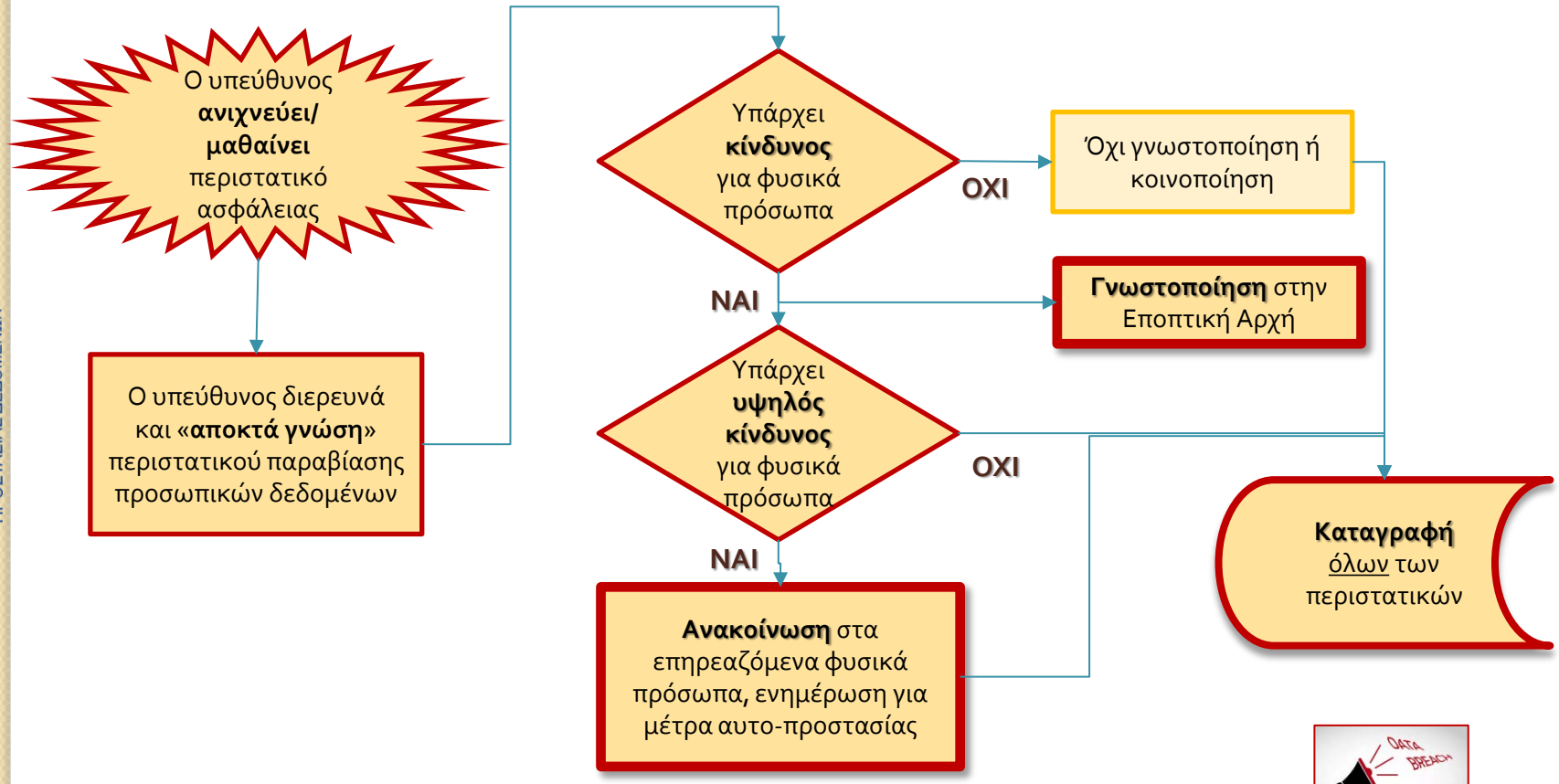
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

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

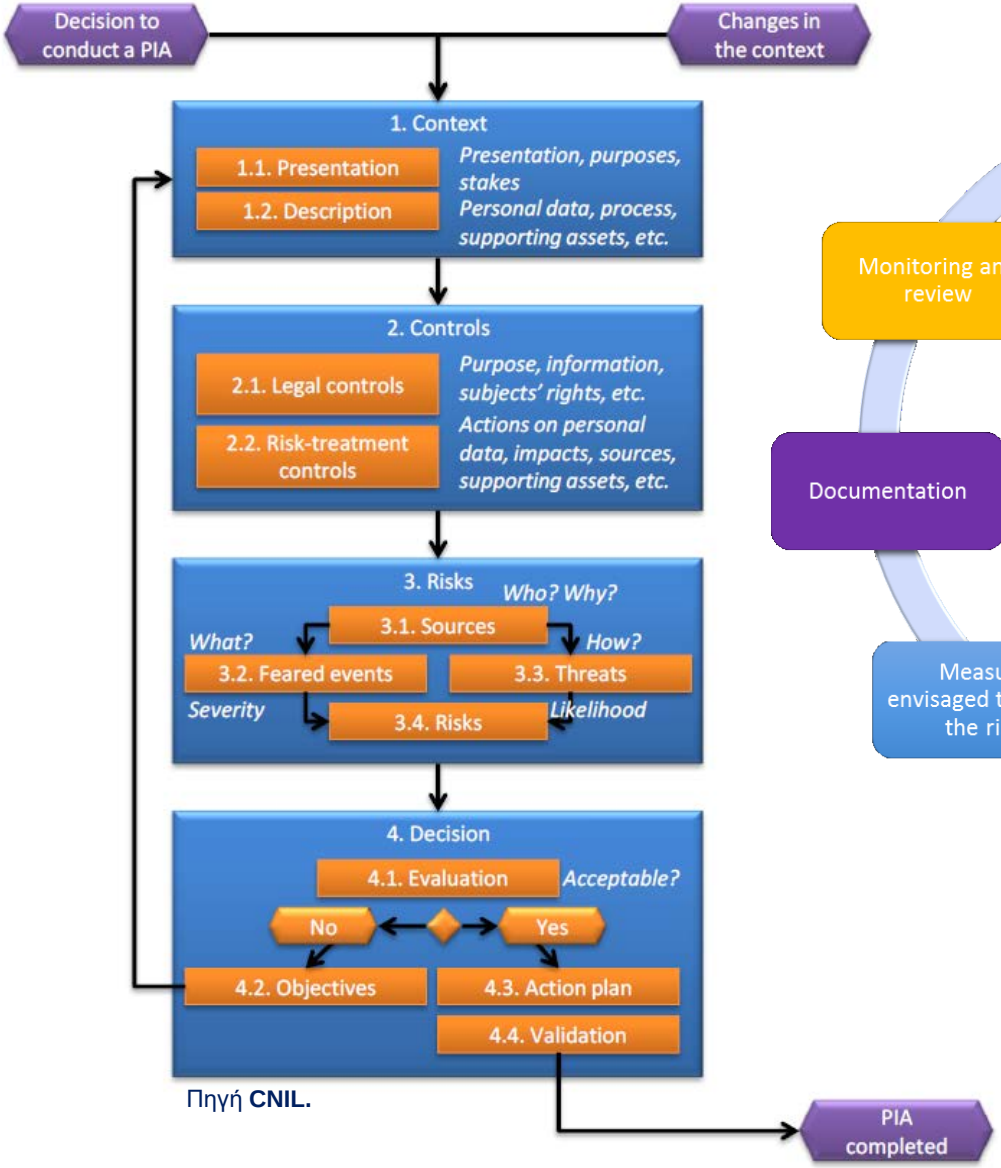
- **Data Protection Impact Assessment (DPIA)**
  - συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας, των σκοπών της επεξεργασίας και της νομικής βάσης
  - εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας
  - εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες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

DPIA : εργαλείο ελέγχου & απόδειξης συμμόρφωσης με GDPR

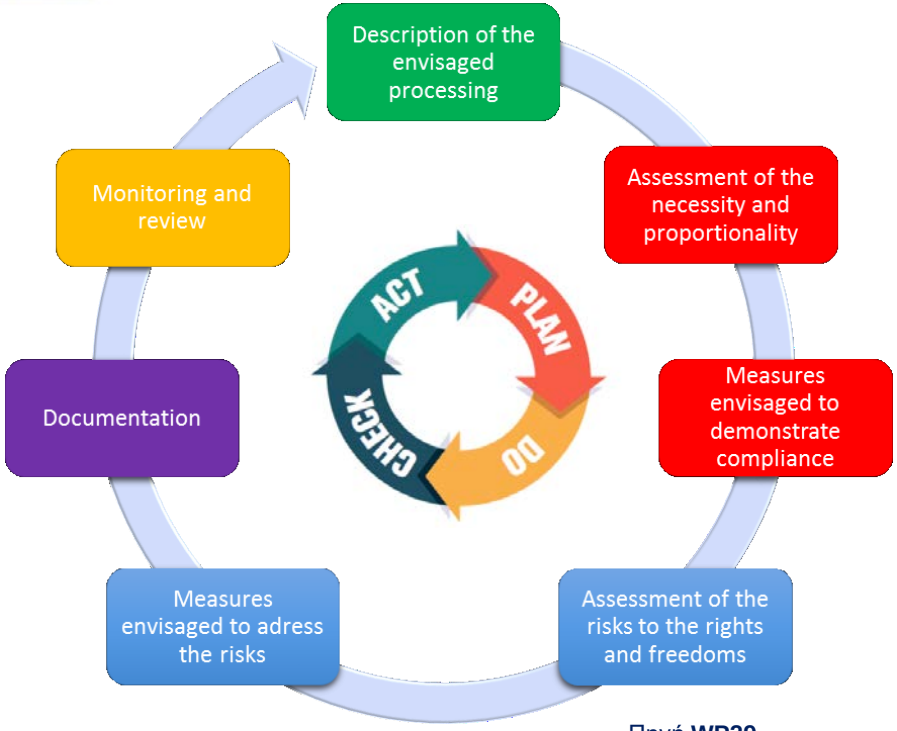
- Υποχρεωτικό όταν "*...ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων*"
- Οι Αρχές θα ορίσουν καταλόγους με επεξεργασίες που απαιτείται DPIA
- Αν μετά την εκπόνηση της DPIA προκύπτει ακόμα «υψηλός κίνδυνος» => Διαβούλευση με την Εποπτική Αρχή

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

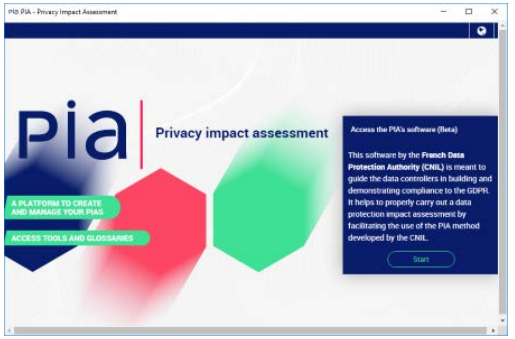
DPIA



Πηγή **CNIL.**



Πηγή **WP29**



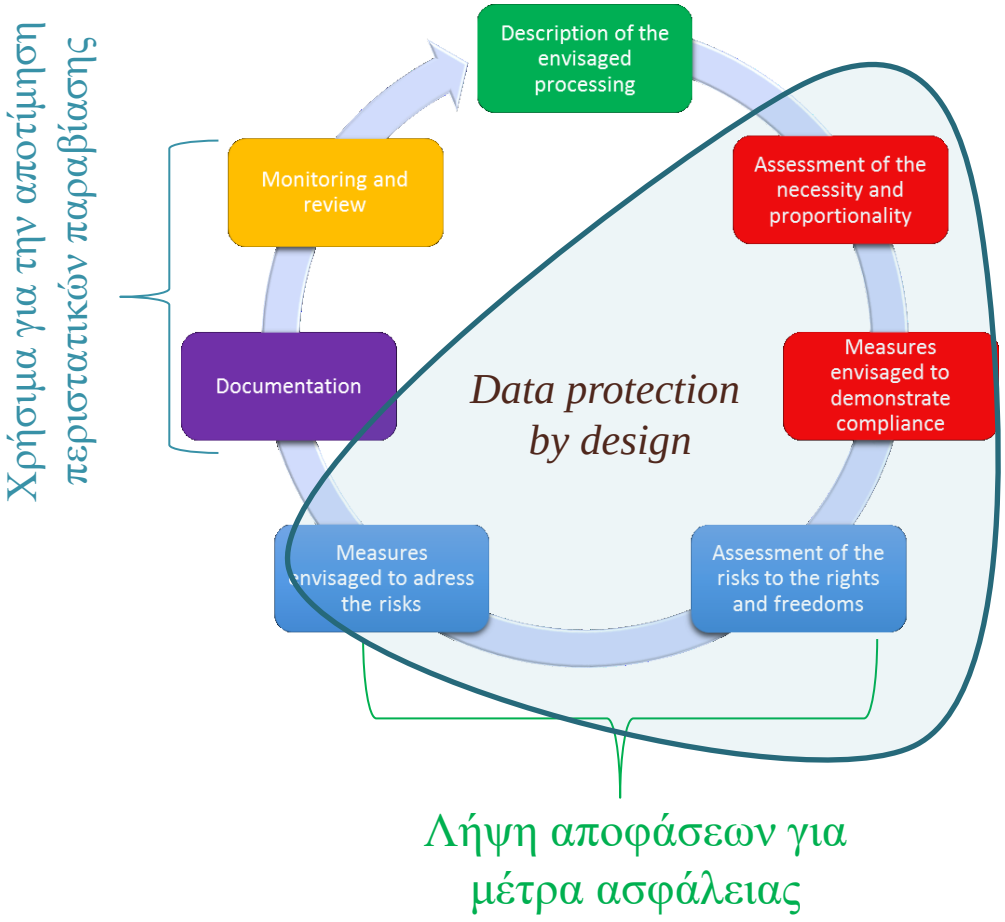
Πηγή **CNIL.**

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

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.

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

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
  - Προετοιμασία εν όψει της 25/5/2018, διαρκής εφαρμογή στη συνέχεια
- Μία πρώτη αποτίμηση σημαντικών «ελλείψεων», με εύρεση τρόπων αντιμετώπισής τους, είναι σημαντικό να γίνει έγκαιρα, γιατί θα διευκολύνει τα επόμενα βήματα

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

2 Καταγραφή επεξεργασιών

- **Αναγνώριση των δραστηριοτήτων**
  - **Προσοχή: Πολλές μπορεί να μην είναι άμεσα εμφανείς!**
  - Αρχείο εγγράφων, αρχείο προσωπικού, αρχείο πελατών , 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

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Έλεγχος τήρησης συμμόρφωσης

- **Για κάθε έναν από τους σκοπούς επεξεργασίας:**
  - Είναι ο σκοπός σαφής;
  - 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

Έλεγχος συγκατάθεσης

- **Αν η νομική βάση για την επεξεργασία προσωπικών δεδομένων είναι η συγκατάθεση**, ο υπεύθυνος επεξεργασίας πρέπει **να μπορεί να αποδείξει** ότι έχει λάβει τη συγκατάθεση των προσώπων
- Είναι η συγκατάθεση ελεύθερη;
- Είναι συγκεκριμένη και ρητή, για σαφώς προσδιορισμένο σκοπό;
- Έχει προέλθει με δήλωση / με σαφή θετική ενέργεια;
  - Π.χ. συμπλήρωση ενός τετραγωνιδίου κατά την επίσκεψη σε διαδικτυακή ιστοσελίδα, επιλογή επιθυμητών τεχνικών ρυθμίσεων για υπηρεσίες της κοινωνίας της πληροφορίας
  - Η σιωπή, τα προ-συμπληρωμένα τετραγωνίδια ή η αδράνεια δεν πρέπει να εκλαμβάνονται ως συγκατάθεση.
- Για ανήλικους, εφόσον η επεξεργασία αφορά υπηρεσίας της κοινωνίας της πληροφορίας, η συγκατάθεση θεωρείται «έγκυρη» όταν το παιδί είναι τουλάχιστον 16 ετών (*)
  - Διαφορετικά, η συγκατάθεση πρέπει να δίνεται από το πρόσωπο που έχει τη γονική μέριμνα
  - Ο υπεύθυνος επεξεργασίας πρέπει να βρει την κατάλληλη μέθοδο

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

5 Αναθεώρηση πολιτικών προστασίας δεδομένων και διαδικασιών

- Η υποχρέωση ενημέρωσης «διευρύνεται»
  - Αλλαγή πολιτικής προστασίας δεδομένων και ενημερωτικών εντύπων
- Σε σχέση με το νυν νομικό πλαίσιο, προστίθεται – μεταξύ άλλων – η υποχρέωση ενημέρωσης για:
  - τη νομική βάση για την επεξεργασία (που «δυσκολεύει» την ενημέρωση, καθώς προϋποθέτει νομική ανάλυση)
  - το χρονικό διάστημα επεξεργασίας/αποθήκευσης.
  - Την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της δημιουργίας προφίλ, με πληροφορίες σχετικά με τη λογική που ακολουθείται και ενδεχόμενες συνέπειες
- Υποχρέωση ενημέρωσης ακόμα και όταν τα δεδομένα συλλέγονται από άλλες πηγές
  - Με χρονικά όρια εντός των οποίων αυτή πρέπει να γίνει
- Τα στοιχεία του υπεύθυνου προστασίας δεδομένων – όταν υπάρχει - πρέπει επίσης να δημοσιοποιούνται
- Αλλαγή/επικαιροποίηση διαδικασιών για την ικανοποίηση των αιτημάτων των υποκειμένων των δεδομένων, λόγω (και) των νέων δικαιωμάτων (όταν αυτά έχουν εφαρμογή)
  - Δικαίωμα στη λήθη - Δικαίωμα στη φορητότητα

Ενισχυμένη αρχή της Διαφάνειας

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

Εκτίμηση αντικτύπου

- Υπάρχει υποχρέωση εκπόνησης εκτίμησης αντικτύπου ως προς την προστασία δεδομένων (DPIA);
  - Έλεγχος ως προς το αν το είδος της επεξεργασίας καθιστά υποχρεωτική την εκτίμηση αντικτύπου
  - Η Αρχή οφείλει να εκδώσει κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται υποχρεωτικά στην απαίτηση για DPIA
  - DPIA μπορεί να γίνει ακόμα και πριν τις 25/5/2018 - είναι μια ορθή πρακτική και μπορεί να αποκαλύψει «ατέλειες»
- Πρέπει να γίνεται με συστηματικό τρόπο, λαμβάνοντας υπόψη τις πιθανότητες επέλευσης κινδύνων και τις συνέπειες στα προσωπικά δεδομένα
  - Ποιος θα **πραγματοποιήσει** την DPIA;
  - Ποιοι **εργαζόμενοι**/τμήματα πρέπει να εμπλακούν;
  - Ποιος θα **αξιολογήσει** τα αποτελέσματα της DPIA;
- DPIA και για το Δημόσιο Τομέα
- Σε κάθε περίπτωση, αν μετά την εφαρμογή των μέτρων παραμένει υψηλός κίνδυνος για την προστασία δεδομένων, προβλέπεται διαβούλευση με την Αρχή.

7 Υπεύθυνος Προστασίας Δεδομένων

- Υπάρχει υποχρέωση ορισμού Υπεύθυνου Προστασίας Δεδομένων (DPO);
  - Ακόμα και χωρίς ρητή υποχρέωση μπορεί να ορισθεί
- Τα στοιχεία του γνωστοποιούνται στην εποπτική Αρχή
- Ο ρόλος του είναι **συμβουλευτικός**, όχι αποφασιστικός.
  - Οι τελικές αποφάσεις λαμβάνονται από τη Διοίκηση.
  - Ωστόσο, ο DPO πρέπει να αξιοποιείται ουσιαστικά από τον φορέα
    - Πρέπει να διασφαλίζεται ότι συμμετέχει δεόντως και εγκαίρως σε όλα τα ζητήματα τα οποία σχετίζονται με την προστασία προσωπικών δεδομένων
- Δύο ή περισσότεροι φορείς μπορούν να έχουν κοινό DPO
  - Αλλά πρέπει να μπορεί εύκολα κάποιος να απευθυνθεί στο DPO για κάθε φορέα.

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

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
  - Σωστά εφαρμοζόμενες τεχνικές κρυπτογράφησης ή/και ανωνυμοποίησης/ψευδωνυμοποίησης
  - Μία ορθά εκπονηθείσα DPIA αναμένεται να συμβάλλει σε μεγάλο βαθμό στην ελαχιστοποίηση των κινδύνων

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
  - Σωστά εφαρμοζόμενες τεχνικές κρυπτογράφησης ή/και ανωνυμοποίησης/ψευδωνυμοποίησης
  - Μία ορθά εκπονηθείσα DPIA αναμένεται να συμβάλλει σε μεγάλο βαθμό στην ελαχιστοποίηση των κινδύνων

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

9 Δραστηριότητα σε περισσότερα Κράτη-Μέλη

- Εάν ο φορέας δραστηριοποιείται σε περισσότερα από ένα Κράτη-Μέλη, θα πρέπει να οριστεί το Κράτος της κύριας εγκατάστασης.
  - Η Αρχή αυτού του Κράτους-Μέλους είναι η επικεφαλής εποπτική Αρχή, με την οποία «συνομιλεί» ο φορέας
- Διερεύνηση:
  - Ποιος ο τόπος εγκατάστασης (έδρα);
    - Υπάρχουν άλλες εγκαταστάσεις εντός Ε.Ε.;
  - Ποιος ο τόπος που λαμβάνονται οι βασικές αποφάσεις για την επεξεργασία;
    - Είναι η έδρα;
    - Μήπως οι αποφάσεις λαμβάνονται και τίθενται σε εφαρμογή σε άλλη εγκατάσταση;
  - Υπάρχουν από κοινού υπεύθυνοι;

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

10 Διαβιβάσεις δεδομένων εκτός ΕΕ

- Θα πρέπει να συντρέχει κάποια εκ των προϋποθέσεων νόμιμης διαβίβασης (μηχανισμός διαβίβασης) – όπως ισχύει και τώρα
  - Δεσμευτικοί Εταιρικοί Κανόνες (BCRs)
  - Πρότυπες Συμβατικές Ρήτρες (SCCs)
  - Απόφαση επάρκειας
  - Προσχώρηση στην «ασπίδα ασφαλείας» (Privacy Shield) για τις Η.Π.Α.
  - ….
- Αξιολόγηση και επιλογή του κατάλληλου μηχανισμού διαβίβασης.
- «Διευρύνεται» η υποχρέωση ενημέρωσης στα πρόσωπα των οποίων τα δεδομένα διαβιβάζονται

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Υλοποίηση των βημάτων

Επιχειρησιακά / Διαχειριστικά

Τεχνικά

1. Ενημέρωση - Ετοιμότητα
2. Καταγραφή επεξεργασιών
3. Έλεγχος συμμόρφωσης
4. Έλεγχος συγκατάθεσης
5. Αναθεώρηση πολιτικών
6. Εκτίμηση επιπτώσεων
7. Υπεύθυνος προστασίας δεδομένων
8. Παραβιάσεις δεδομένων
9. Δραστηριότητα σε πολλά ΚΜ
10. Διαβιβάσεις

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Συμμόρφωση Πληροφοριακών Συστημάτων Εκπαιδευτικών Ιδρυμάτων

- Στάδιο Α.1: Καταγραφή και Αξιολόγηση Υφιστάμενης Κατάστασης
- Στάδιο Α.2: Ορισμός του/της Υπεύθυνου/ης Προστασίας Δεδομένων
- Στάδιο Α.3: Εκτίμηση Αντικτύπου Ιδιωτικότητας και Κατάρτιση Σχεδίου Συμμόρφωσης
- Στάδιο Α.4: Εφαρμογή και παρακολούθηση του Σχεδίου Συμμόρφωσης

Στάδιο Α.1: Καταγραφή και Αξιολόγηση Υφιστάμενης Κατάστασης

- Καταγραφή σκοπών επεξεργασίας/δεδομένων/αρχείων/ροών δεδομένων
- Αξιολόγηση του επιπέδου συμμόρφωσης προς τις ισχύουσες νομικές απαιτήσεις
- Εξέταση και εκτίμηση των νομικών βάσεων της επεξεργασίας κάθε ομάδας δεδομένων.
- Νομικός έλεγχος των ισχυουσών πολιτικών προστασίας δεδομένων/απορρήτου, των συμβάσεων με προμηθευτές και συνεργάτες που έχουν πρόσβαση στα πληροφοριακά συστήματα του Ιδρύματος, των εντύπων συγκατάθεσης, των γνωστοποιήσεων στην ΑΠΔΠΧ (εάν υφίστανται), των μεθόδων και διαδικασιών διαβίβασης δεδομένων σε τρίτους φορείς και του επιπέδου ενημερότητας του προσωπικού του Ιδρύματος.
- Αποτύπωση και νομική αξιολόγηση της υπάρχουσας κατάστασης.

Στάδιο Α.2: Ορισμός του/της Υπεύθυνου/ης Προστασίας Δεδομένων

- Ο ορισμός του Υπεύθυνου Προστασίας Δεδομένων μπορεί να πραγματοποιηθεί σε οποιοδήποτε στάδιο της διαδικασίας. Όμως, τα οφέλη της έγκαιρης επιλογής του είναι σημαντικά, καθώς εφόσον θα έχει τη δυνατότητα να συμμετάσχει στις δράσεις προσαρμογής στον ΓΚΠΔ, θα αποκτήσει σημαντική εμπειρία και γνώση.

Στάδιο Α.3: Εκτίμηση Αντικτύπου Ιδιωτικότητας και Κατάρτιση Σχεδίου Συμμόρφωσης (1/2)

- Υλοποίηση Εκτίμησης Αντικτύπου Ιδιωτικότητας και εντοπισμός αδυναμιών στην ασφάλεια των πληροφοριακών συστημάτων, που δύναται να επηρεάσουν την προστασία προσωπικών δεδομένων
- Διαβούλευση με τα υποκείμενα των δεδομένων ή εκπροσώπων τους, όπου αυτή ενδείκνυται
- Κατάρτιση Σχεδίου Συμμόρφωσης στο οποίο θα περιλαμβάνονται:
  - Σχεδιασμός νέων ή προσαρμογή υφιστάμενων πολιτικών και διαδικασιών προστασίας προσωπικών δεδομένων.
  - Ενσωμάτωση διαδικασιών «ελαχιστοποίησης» της επεξεργασίας.
  - Σχεδιασμός ορθής νομικής διατύπωσης σε έντυπα ενημέρωσης, γνωστοποίησης και συγκατάθεσης.

Στάδιο Α.3: Εκτίμηση Αντικτύπου Ιδιωτικότητας και Κατάρτιση Σχεδίου Συμμόρφωσης (2/2)

- Κατάρτιση Σχεδίου Συμμόρφωσης στο οποίο θα περιλαμβάνονται (συνέχεια):
  - Θέσπιση διαδικασιών διαχείρισης αιτημάτων για την ενάσκηση των δικαιωμάτων των υποκειμένων των δεδομένων.
  - Σύνταξη ή τροποποίηση συμβάσεων με εργαζόμενους, προμηθευτές και συνεργάτες.
  - Σχεδιασμός διαδικασιών καταγραφής παραβιάσεων και αναφοράς τους στην Εποπτική Αρχή και στα υποκείμενα των δεδομένων.
  - Σχεδιασμός πολιτικής προστασίας των προσωπικών δεδομένων των εργαζομένων.
  - Διατύπωση συστάσεων για τον περιορισμό της επικινδυνότητας (risk mitigation) των πληροφοριακών συστημάτων που διαχειρίζονται προσωπικά δεδομένα.

Στάδιο Α.4: Εφαρμογή και παρακολούθηση του Σχεδίου Συμμόρφωσης

- Για την εφαρμογή του Σχεδίου Συμμόρφωσης στον ΓΚΠΔ είναι αναγκαία η αποτύπωση των απαιτούμενων ενεργειών και η παρακολούθηση της υλοποίησής τους. Η παρακολούθηση της εφαρμογής αποτελεί μέρος των υποχρεώσεων του/της DPO.
- Ως πρώτο βήμα στη διαδικασία της εφαρμογής του σχεδίου συμμόρφωσης, το Ίδρυμα απαιτείται να εφαρμόσει δράσεις επιμόρφωσης και ενημερότητας στα θέματα του ΓΚΠΔ.