HADPP ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ & ΙΔΙΩΤΙΚΟΤΗΤΑΣ

ΓΚΠΔ – GDPR

Η σημασία του Data Protection Impact Assessment

«Πρακτικά και εφαρμοστικά ζητήματα του Κανονισμού GDPR: Η επόμενη μέρα»

ΣΕΒ 7/2/2018

Σπύρος Τάσσης

Δικηγόρος LLM

Προσωπικά Δεδομένα

- Η αντιμετώπιση των ζητημάτων της ιδιωτικότητας θα πρέπει να γίνεται με τρόπο ρεαλιστικό και χωρίς δογματισμό.
- Αναμφισβήτητη η αναγκαιότητα της προστασίας του πυρήνα της ανθρώπινης προσωπικότητας που λέγεται προσωπικά δεδομένα. Σημαντική όμως και η χρήση των δεδομένων αυτών για την προαγωγή της επιχειρηματικής δράσης
- Σε ένα έργο συμμόρφωσης με το GDPR ιδιαίτερο ενδιαφέρον έχει να δούμε το πώς τα δεδομένα διακινούνται, τυγχάνουν επεξεργασίας και διασφαλίζεται η αποτελεσματική προστασία τους.
- Το δικαίωμα συλλογής και επεξεργασίας των προσωπικών δεδομένων εκφέρεται τόσο θετικά (δημιουργία αρχείου) όσο και αρνητικά (διαφύλαξη και έλεγχος πρόσβασης).
- Ο Νομοθέτης αναγνωρίζει ότι τα δεδομένα αυτά είναι δυνατό να επηρεάσουν κατά τρόπο μη-αναλογικό τη συμπεριφορά και τις αποφάσεις ενός ανθρώπου καθώς επίσης την πραγματική και νομική του κατάσταση και συνεπώς κρίθηκε ότι η απόκτηση, επεξεργασία και πρόσβαση σε τέτοιου είδους δεδομένα θα πρέπει να γίνεται σε σαφή και αυστηρά πλαίσια.

Πολιτική Ασφαλείας

- Ενημέρωση (awareness)
- Καταγραφή των προσωπικών δεδομένων (data inventory – data mapping) και των μηχανισμών διακίνησης τους (data transfer)
- Ανάλυση κινδύνου και εκτίμηση αντικτύπου
- Σαφής καταγραφή των διαδικασιών και αρμοδιοτήτων (Εσωτερική Πολιτική Προστασίας Δεδομένων)
- Όχι εφησυχασμός.

Εκτίμηση Αντικτύπου

Άρθρο 35 - κατηγορίες επεξεργασίας που (ιδίως) απαιτούν Εκτίμηση Αντικτύπου

- **συστηματική και εκτενής αξιολόγηση προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ,**

- **μεγάλης κλίμακας επεξεργασία των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1 (ευαίσθητα) ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10**

- **συστηματική παρακολούθηση δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.**

Ανάλυση κινδύνου – Διενέργεια DPIA

Ως «κίνδυνος» νοείται μια υπόθεση εργασίας που περιγράφει ένα συμβάν και τις επιπτώσεις του, που έχουν εκτιμηθεί με όρους σοβαρότητας και πιθανότητας επέλευσης.

Ως «διαχείριση κινδύνου» μπορούν να νοηθούν οι συντονισμένες δραστηριότητες για την καθοδήγηση και τον έλεγχο ενός οργανισμού ως προς τον κίνδυνο.

Σπύρος Τάσσης

Ανάλυση Κινδύνου - Εκτίμηση Αντικτύπου

Ανάλυση κινδύνου:

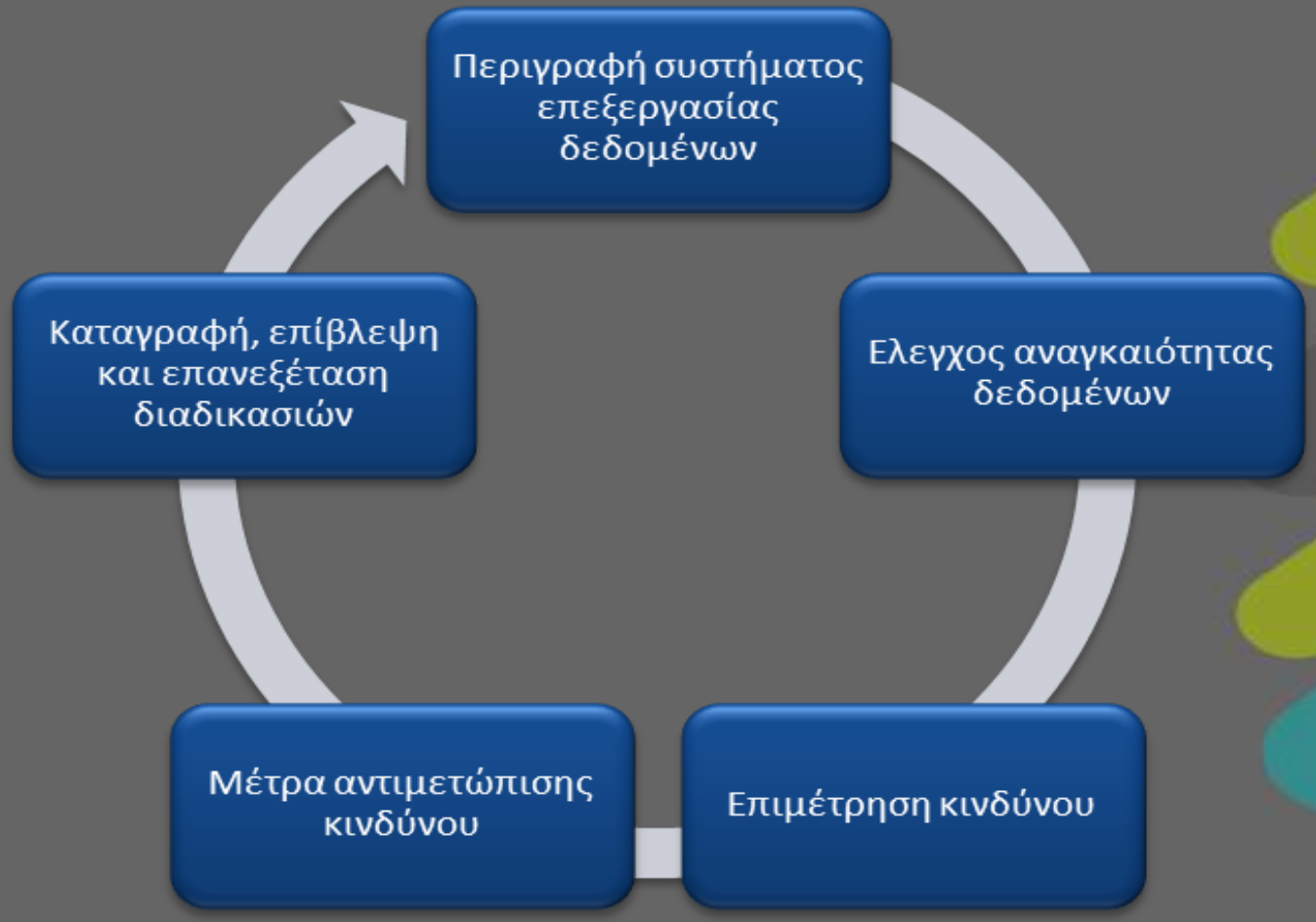
- **πιθανές απειλές (τεχνολογικά κενά, ελλιπείς διαδικασίες, ακόμα και … δυσαρεστημένοι υπάλληλοι)**
- **κατηγοριοποίηση των δεδομένων ανάλογα με την κρισιμότητα τους**
- **αποτελεσματικές διαδικασίες μείωσης του αντικτύπου (DPIA)**

Δραστηριότητες επεξεργασίας:

- **Υψηλού κινδύνου (DPIA, διαβούλευση, γνωστοποιήσεις άρθρου 33)**
- **Κινδύνου (DPIA, γνωστοποιήσεις)**
- **Χαμηλού κινδύνου (προαιρετικό DPIA, χωρίς υποχρέωση γνωστοποιήσεων)**

Σπύρος Τάσσης

Ανάλυση Κινδύνου



Ανάλυση κινδύνου – Διενέργεια DPIA

Νοσοκομείο που επεξεργάζεται τα γενετικά δεδομένα και τα δεδομένα υγείας των ασθενών του (πληροφοριακό σύστημα του νοσοκομείου):

- Ευαίσθητα δεδομένα ή δεδομένα εξαιρετικά προσωπικού χαρακτήρα.

- Δεδομένα που αφορούν ευάλωτα υποκείμενα δεδομένων.

- Δεδομένα μεγάλης κλίμακας επεξεργασίας.

Αν ο υπεύθυνος επεξεργασίας θεωρεί ότι μια πράξη επεξεργασίας που ενδεχομένως αντιστοιχεί στις ανωτέρω αναφερόμενες περιπτώσεις εξακολουθεί να μην «ενδέχεται να επιφέρει υψηλό κίνδυνο» θα πρέπει να δικαιολογεί και να τεκμηριώνει τους λόγους μη διενέργειας DPIA και να περιλαμβάνει/καταγράφει τις απόψεις του υπεύθυνου προστασίας δεδομένων.

Σπύρος Τάσσης

Εκτίμηση Αντικτύπου

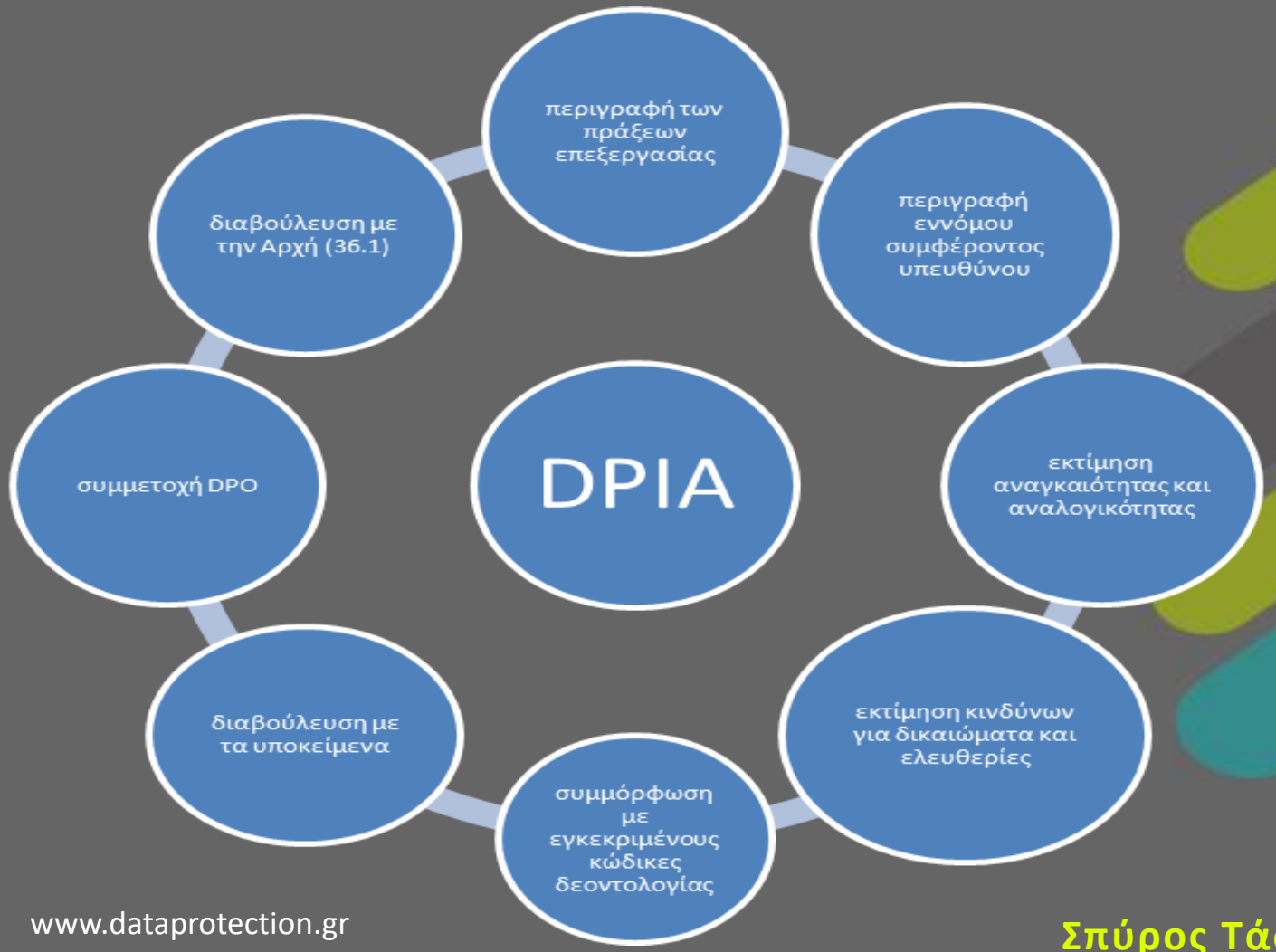
1. Η DPIA είναι μια διαδικασία που έχει σχεδιαστεί για να βοηθήσει τους οργανισμούς να εντοπίζουν, να αξιολογούν και να μετριάζουν (ή να ελαχιστοποιούν) τους κινδύνους από την επεξεργασία των δεδομένων.

2. Μια DPIA είναι άμεση συνέπεια της αρχής της λογοδοσίας του GDPR. Ένας οργανισμός είναι υπόλογος για την απόδειξη ότι έχει λάβει όλα τα απαραίτητα μέτρα για να εξασφαλίσει τη συμμόρφωση με το GDPR (WP29).

3. Μια DPIA είναι το τέλειο εργαλείο για τον προσδιορισμό των επιπτώσεων σε σχέση με εκείνες τις δραστηριότητες επεξεργασίας δεδομένων που θα μπορούσαν να συνιστούν υψηλό κίνδυνο παραβίασης των δικαιωμάτων και ελευθεριών όλων των εμπλεκόμενων ατόμων.

4. Μια DPIA είναι μία πολύ καλή αφορμή για νοικοκύρεμα των δεδομένων, μείωση του κόστους αποθήκευσης και κατανόηση των πραγματικά σημαντικών δεδομένων για την επιχειρηματική δράση κάθε εταιρείας

Εκτίμηση Αντικτύπου



www.dataprotection.gr

Σπύρος Τάσσης

Φάσεις Εκτίμησης Αντικτύπου

1. Αναγνωρίστε την ανάγκη για την DPIA (εάν οι κίνδυνοι της επεξεργασίας απαιτούν μια DPIA). Εν αμφιβολία πραγματοποιήστε τη…

2. Σχηματοποιήστε τη ροή των δεδομένων (data flows), πώς συλλέγονται, αποθηκεύονται, χρησιμοποιούνται και διαγράφονται οι πληροφορίες στο πλαίσιο της επεξεργασίας.

3. Καταγράψτε το εύρος των απειλών και τις πιθανές επιπτώσεις τους στα δικαιώματα και τις ελευθερίες των υποκειμένων.

4. Προσδιορίστε και αξιολογήστε τις πιθανότητες κινδύνου και ορίστε μία σαφή διαδικασία αντιμετώπισης και περιορισμού της επίπτωσης στα υποκείμενα και την εταιρεία.

5. Τμηματοποιήστε την DPIA κατά τρόπο ώστε να καλύπτει κάθε κατηγορία και διαδικασία επεξεργασίας και να μπορούν να αποσπαστούν τα τμήματα της για ενημέρωση των κατάλληλων δομών.

6. Εφαρμόστε τα αποτελέσματα της DPIA στο έργο συμμόρφωσης και υιοθετήστε μια τακτική ετήσια και τυχόν έκτακτες διαδικασίες ανανέωσης της.

Γενικές Αρχές μίας ορθής DPIA

- **Σε ποια χρονική στιγμή θα πρέπει να πραγματοποιηθεί μια DPIA;** ***Πριν από την επεξεργασία.***
- **Ποιος είναι υποχρεωμένος να εκτελέσει την DPIA;** ***Ο υπεύθυνος επεξεργασίας, σε συνεργασία με τον DPO και τον εκτελούντα την επεξεργασία***
- **Ποια είναι η μεθοδολογία για την πραγματοποίηση μιας DPIA;** ***Διαφορετικές μεθοδολογίες αλλά κοινά κριτήρια.***
- **Πρέπει να δημοσιεύεται η Εκτίμηση Αντικτύπου;** ***Προτείνεται να δημοσιεύεται έστω και εν μέρει. Σε κάθε περίπτωση αν προηγήθηκε διαβούλευση με την Αρχή θα πρέπει να κοινοποιείται σε αυτή.***

Ευχαριστώ

Σπύρος Τάσσης

HADPP ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ & ΙΔΙΩΤΙΚΟΤΗΤΑΣ

www.dataprotection.gr
Info@dataprotection.gr