



“1 χρόνος μέχρι την εφαρμογή του ΓΚΠΔ: Η αντίστροφη μέτρηση...”

Ανάλυση κινδύνου και Εκτίμηση Αντικτύπου



HADPP ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΠΡΟΣΤΑΣΙΑΣ
ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ & ΙΔΙΩΤΙΚΟΤΗΤΑΣ

www.dataprotection.gr

Σπύρος Τάσης



1 χρόνος για την εφαρμογή του ΓΚΠΔ

- Το νέο ιδιαίτερα αυστηρό πλαίσιο του Κανονισμού φαίνεται ότι αποτελεί και μία προσπάθεια κανονικοποίησης των οικονομικών/επιχειρηματικών όρων δραστηριοποίησης ιδίως στην ψηφιακή αγορά.
- Οι παραβάσεις ασφαλείας των δεδομένων είναι αναμενόμενες.
- Το ζητούμενο είναι κάθε υπεύθυνος να ενεργήσει σύμφωνα με τα όσα ορίζει ο Κανονισμός ώστε να ελαχιστοποιηθεί ο κίνδυνος.



1 χρόνος για την εφαρμογή του ΓΚΠΔ

Είναι λοιπόν σημαντικό να ξεκινήσουμε με την παραδοχή ότι υπάρχει κίνδυνος για τα προσωπικά δεδομένα που οφείλεται κυρίως σε δύο παράγοντες:

- Οργανωτικό (ανεπαρκείς διαδικασίες και ελλιπής οργάνωση της επίβλεψης τους) και
- Ανθρώπινο (ελλιπής εκπαίδευση του προσωπικού που τα χειρίζεται). Είναι εκπληκτικό το πόσα περιστατικά ασφαλείας οφείλονται στον ανθρώπινο παράγοντα.



1 χρόνος για την εφαρμογή του ΓΚΠΔ



Τι χρειαζόμαστε για μία σωστή Πολιτική Ασφαλείας:

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

Σπύρος Τάσης

1 χρόνος για την εφαρμογή του ΓΚΠΔ

Ανάλυση κινδύνου:

- πιθανές απειλές (τεχνολογικά κενά, ελλείψεις διαδικασίες, ακόμα και ... δυσανεστημένοι 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)

1 χρόνος για την εφαρμογή του ΓΚΠΔ



1 χρόνος για την εφαρμογή του ΓΚΠΔ

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.

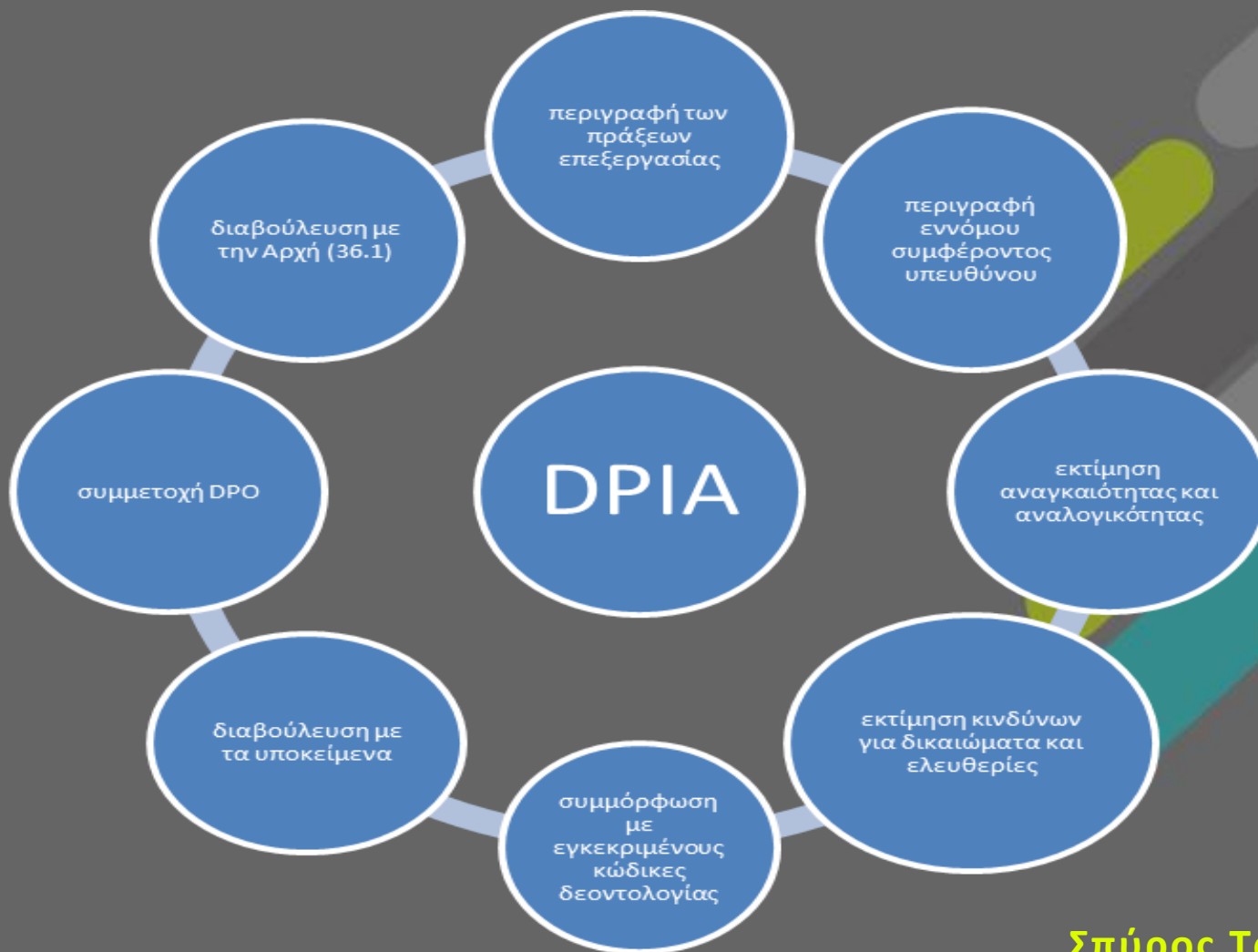


1 χρόνος για την εφαρμογή του ΓΚΠΔ

- Αρχή της συνεκτικότητας
- Ελεύθερη ροή δεδομένων στην ΕΕ και ενιαίοι κανόνες
- Υπεύθυνος προστασίας δεδομένων (DPO)
- Κοινοί Υπεύθυνοι Επεξεργασίας

Σπύρος Τάσης

1 χρόνος για την εφαρμογή του ΓΚΠΔ



1 χρόνος για την εφαρμογή του ΓΚΠΔ

- 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.*



1 χρόνος για την εφαρμογή του ΓΚΠΔ

ΣΥΜΠΕΡΑΣΜΑ

(Γενικές αρχές για την αποφυγή συνεπειών)

- Υιοθέτηση μίας αντιμετώπισης των προσωπικών δεδομένων με άξονα την ύπαρξη κινδύνων στην ασφάλεια τους (Risk-based approach). Οι κυρώσεις θα είναι ανάλογες του κινδύνου.
- Ελαχιστοποίηση προσωπικών δεδομένων (the less the merrier)
- Επαρκείς τεχνολογικές λύσεις για μέγιστη προστασία (ψευδωνυμοποίηση – ανωνυμοποίηση)
- Στόχος η προστασία ήδη από το σχεδιασμό ή εξ' ορισμού (Privacy by Design – Privacy by Default)
- Κάντε την συμμόρφωση σας με τον Κανονισμό επιλογή πρώτης προτεραιότητας για τους επόμενους μήνες

Σπύρος Τάσης



1 χρόνος για την εφαρμογή του ΓΚΠΔ

Ευχαριστώ

Σπύρος Τάσης



HADPP

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΠΡΟΣΤΑΣΙΑΣ
ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ & ΙΔΙΩΤΙΚΟΤΗΤΑΣ

www.dataprotection.gr