Εφαρμογή Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR)

Kostas Papadatos

President, (ISC)² Hellenic Chapter

MSc Infosec, CISSP-ISSMP, CISM, ISO27001 LA, ISO27005 RM, PMP, MBCI , CDPO

HELLENIC

3rd Law Forum on Data Protection & Privacy

22/02/2019

About... (ISC)²

- (ISC)² = *International Information Systems Security Certification Consortium*
- Established in 1989
- Non-profit consortium of information security industry leaders
- Supports security professionals throughout their careers
- Global Standard for information security: (ISC)² CBK®
- Over 100,000 certified professionals; over 160 countries

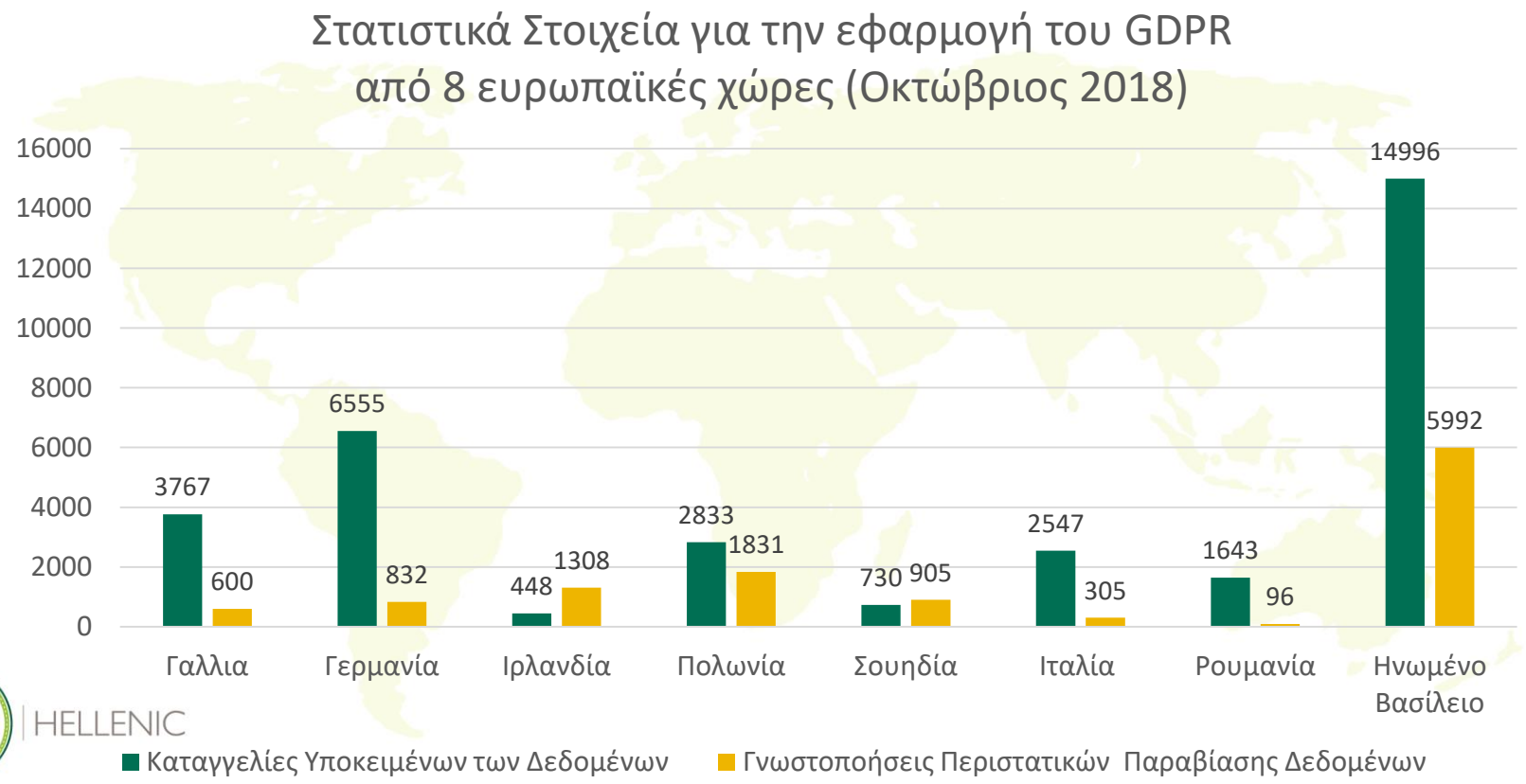
- Official (ISC)2 Chapter (No: 128), 8/7/2014
- Non-Profit Association (No: 30693), 24/6/2015
- Our Mission:
  - *Exchange of ideas and dissemination of knowledge among (ISC)2 members, information security professionals and the public, as well as the promotion (ISC)2 Certifications in the region.*
- Members: **Information Security Professionals** and **(ISC)² credentialed**.

(ISC)² CHAPTER HELLENIC

OFFICIAL (ISC)² CHAPTER | HELLENIC

(ISC)² CISSP ISSAP ISSEP ISSMP SSCP CAP CSSLP CCFP HCISPP CCSP

Στατιστικά Στοιχεία σε Ευρωπαϊκό Επίπεδο



HELLENIC

https://www.gdprtoday.org

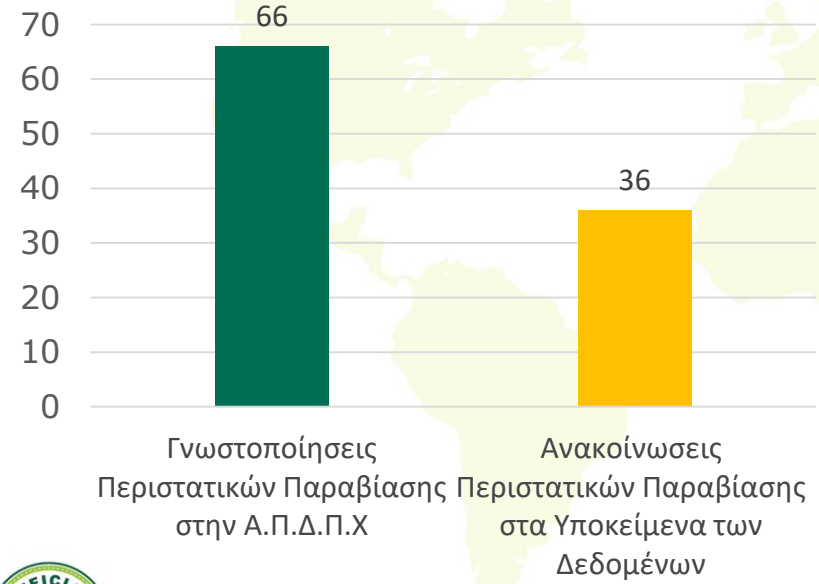
Αποφάσεις Ευρωπαϊκών ΑΠΔΠΧ με βάση τον GDPR

25 Ιουνίου 2018	Επίσημη προειδοποίηση της Γαλλικής Αρχής στην εταιρεία **Teemo & Fidzup**:	•Έλλειψη προηγούμενης συγκατάθεσης για την επεξεργασία δεδομένων •Υπερβολική συλλογή δεδομένων
22 Οκτωβρίου 2018	Επιβολή προστίμου **400.000€** από τη Πορτογαλική Αρχή σε νοσηλευτικό ίδρυμα:	•Παραβίαση της Αρχής της ελαχιστοποίησης των δεδομένων •Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα
23 Οκτωβρίου 2018	Επίσημη προειδοποίηση της Γαλλικής Αρχής στην εταιρεία **SingleSpot**:	• Μη ενδεδειγμένη λήψη συγκατάθεσης για την επεξεργασία δεδομένων θέσης
9 Νοεμβρίου 2018	Επίσημη προειδοποίηση της Γαλλικής Αρχής στην εταιρεία **Vectaury**:	•Παροχή ελλιπούς ενημέρωσης σχετικά με την επεξεργασία δεδομένων •Μη σύννομη λήψη της συγκατάθεσης
22 Νοεμβρίου 2018	Επιβολή προστίμου 20.000€ από την Γερμανική Αρχή του Baden-Württemberg στην ιστοσελίδα **Knuddels.de**:	•Τήρηση Κωδικών Πρόσβασης χρηστών σε μη ασφαλή μορφή (plaintext)
29 Νοεμβρίου 2018:	Επίσημη καταγγελία 7 Ευρωπαϊκών Αρχών σε βάρος της **Google**:	•Παρακολούθηση χρηστών σε μεγάλη κλίμακα •Συλλογή δεδομένων θέσης χωρίς τη σύννομη λήψη συγκατάθεσης χρηστών
21 Ιανουαρίου 2019	Πρόστιμο Γαλλικής Αρχή Προστασίας Δεδομένων (CNIL) στην **Google**:	•Πρόστιμο 50 εκατ. € στην Google για ελλιπή ενημέρωση υποκειμένων και μη λήψη συγκατάθεσης
	Αναμένονται Πρόστιμα από την Αγγλική Αρχή Προστασίας Δεδομένων (ICO) για:	•**British Airways Breach**: 4% του τζίρου θα έφτανε σε **£500 εκ**. •**Marriott International Breach**: 4% του τζίρου θα έφτανε σε **£720 εκ**.

OFFICIAL (ISC)² CHAPTER | HELLENIC

Στοιχεία Παραβιάσεων Α.Π.Δ.Π.Χ

Ενημέρωση ΑΠΔΠΧ: 20 Δεκεμβρίου 2018



Αποφάσεις Α.Π.Δ.Π.Χ για Περιστατικά Παραβίασης

Επίπληξη σε Τράπεζα	για **μη έγκαιρη υποβολή γνωστοποίησης** περιστατικού παραβίασης δεδομένων προσωπικού χαρακτήρα (Απόφαση ΑΡ.69/2018)
Επίπληξη σε Εταιρεία Εμπορίου Αθλητικών Ειδών	για παράβαση των διατάξεων του άρ. 32 του ΓΚΠΔ και, κατά συνέπεια, της **θεμελιώδους αρχής της ασφάλειας των δεδομένων** (Απόφαση ΑΡ. 67/2018)
Επίπληξη σε Τράπεζα	για **μη έγκαιρη υποβολή γνωστοποίησης** περιστατικού παραβίασης δεδομένων προσωπικού χαρακτήρα (Απόφαση ΑΡ.68/2018)

- *Τουλάχιστον άλλα 9 εξετάζονται περαιτέρω.*
- *Για 6 από τα περιστατικά συνεργάζεται με συναρμόδιες αρχές της ΕΕ.*

OFFICIAL (ISC)² CHAPTER | HELLENIC

Συμβουλές Α.Π.Δ.Π.Χ προς Υπεύθυνους και Εκτελούντες την Επεξεργασία

Η Αρχή συνιστά τα ακόλουθα τεχνικά και οργανωτικά μέτρα ασφάλειας:

- **Υλοποίηση δράσεων ευαισθητοποίησης των χρηστών για αποφυγή:**
  - Αποστολής μηνυμάτων ηλεκτρονικού ταχυδρομείου που περιέχουν ΔΠΧ σε λάθος αποδέκτες
  - Εξαπάτησης χρηστών μέσω κακόβουλων μηνυμάτων ηλεκτρονικού ταχυδρομείου και εγκατάστασης κακόβουλου λογισμικού τύπου ransomware ή malware.
- **Υλοποίηση μέτρων προστασίας λογισμικού, όπως:**
  - Έλεγχος κάθε νέας έκδοσης λογισμικού, πριν τη χρήση του
  - Θέσπιση διαδικασίας για την άμεση αντιμετώπιση προβλημάτων που ανακύπτουν κατά τη λειτουργία του λογισμικού
  - Έλεγχος ρυθμίσεων των διακομιστών διαδικτύου, ώστε να μην είναι δυνατή η πρόσβαση σε μη δημόσιες πληροφορίες
  - Άμεση επικαιροποίηση λογισμικού με νέες εκδόσεις ασφάλειας
- **Χρήση λογισμικού κρυπτογράφησης για την αποτροπή της διαρροής ΔΠΧ, λόγω της κλοπής ή της απώλειας ηλεκτρονικών υπολογιστών και μέσων αποθήκευσης.**

Πράξεις Επεξεργασίας που απαιτούν διενέργεια Μελέτης Εκτίμησης Αντικτύπου (DPIA)

- Η Α.Π.Δ.Π.Χ δημοσίευσε λίστα με τις πράξεις επεξεργασίας για τις οποίες κρίνει απαραίτητη τη διενέργεια Μελέτης Εκτίμησης Αντικτύπου (DPIA), ***ΑΠΟΦΑΣΗ 65/2018.***

- Ομαδοποίηση Κριτηρίων με Βάση:
  - Το είδος και σκοπούς επεξεργασίας
  - Το είδος δεδομένων και/ή τις κατηγορίες υποκειμένων
    - ***Εξαίρεση αρχείων καταγραφής για λόγους ασφάλειας εφόσον η επεξεργασία περιορίζεται στα απολύτως απαραίτητα δεδομένα και είναι ειδικά τεκμηριωμένη.***
    - ***Χαρακτηριστικό παράδειγμα που εμπίπτει στην υποχρέωση διενέργειας DPIA, αποτελεί η χρήση συστημάτων Data Loss Prevention (DLP).***
  - Πρόσθετα χαρακτηριστικά και/ή Χρησιμοποιούμενα μέσα επεξεργασίας

Οδηγίες Ασφάλειας Ευρωπαϊκών Αρχών

- Πολλές Αρχές Προστασίας, εκδίδουν οδηγίες ασφάλειας σχετικά με την εφαρμογή του GDPR.
- Δύο από τις Αρχές με το πλουσιότερο έργο:
  - Γαλλίας (CNIL)
  - Ηνωμένου Βασιλείου (ICO).

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

- Οδηγία για τη Διενέργεια Μελέτης Εκτίμησης Αντικτύπου (DPIA)
- Ανάπτυξη λογισμικού για τη διενέργεια Μελέτης Εκτίμησης Αντικτύπου (DPIA)
- Οδηγία σχετικά με τη χρήση της τεχνολογίας Blockchain στο πλαίσιο του GDPR
- Οδηγία σχετικά με την ασφάλεια των δεδομένων προσωπικού χαρακτήρα (SECURITY OF PERSONAL DATA)
- …

ico. Information Commissioner's Office

- Οδηγός Συμμόρφωσης με τις απαιτήσεις του GDPR (see Security section)
  - Οδηγός για την ασφάλεια των δεδομένων προσωπικού χαρακτήρα
  - Οδηγός σχετικά με τη χρήση κρυπτογράφησης στο πλαίσιο του GDPR
  - Οδηγός σχετικά με τη χρήση κωδικών πρόσβασης σε online υπηρεσίες
- …

OFFICIAL (ISC)² CHAPTER | HELLENIC

Οδηγίες Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, στο πλαίσιο της άσκησης των καθηκόντων του για τη διασφάλιση της συνεκτικής εφαρμογής του GDPR, έχει καταρτίσει τις κάτωθι κατευθυντήριες γραμμές:

- Guidelines 1/2018 on certification and identifying certification criteria
- Guidelines 2/2018 on derogations of Article 49
- Guidelines 3/2018 on the territorial scope of the GDPR
- Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the GDPR

OFFICIAL (ISC)² CHAPTER | HELLENIC

edpb European Data Protection Board

Ευχαριστώ!

OFFICIAL (ISC)² CHAPTER | HELLENIC