GDPR
Από τη Θεωρία στην Πράξη
Μύθοι και Πραγματικότητα

Κώστας Παπαχριστοφής (MSc, MBA)

Certified DPO (TUV Austria)
InterLei, Educational ICT Consultant/Instructor
Security Expert

Θεωρητικά είναι δυο ....

συμπληρωματικές έννοιες

PRIVACY

τα ΔΠΧ συλλέγονται, επεξεργάζονται, προστατεύονται και καταστρέφονται νόμιμα

SECURITY

προστασία για όλους τους τύπους πληροφορίας

Δυο υποέργα που πρέπει να τρέχουν παράλληλα !

interLei

Στην πραγματικότητα....

δεν υπάρχει Privacy χωρίς Security

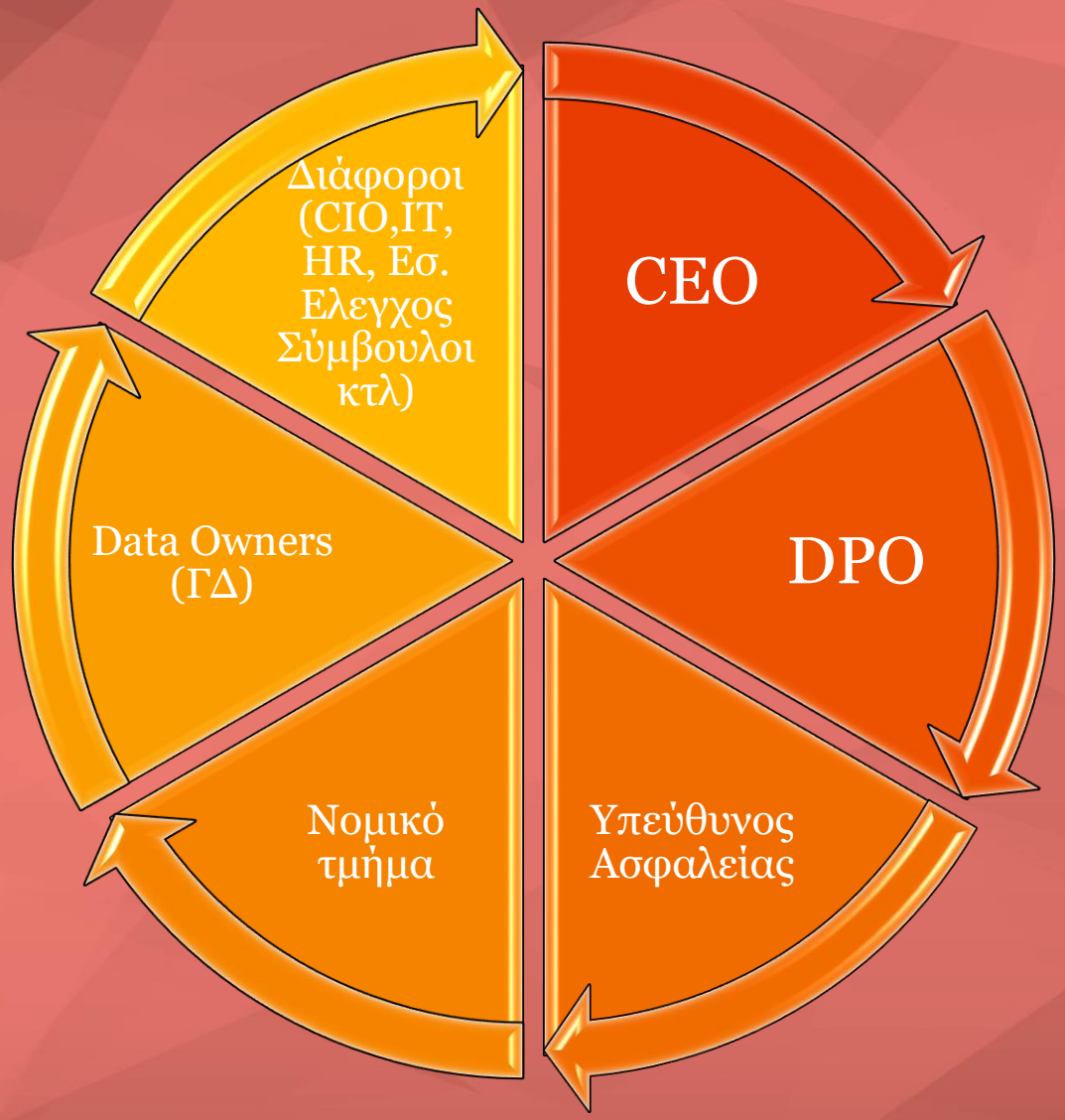
Υπεύθυνος Ασφάλειας

ΤΕΧΝΙΚΑ ΜΕΤΡΑ

DPO

interLei

Η συμμόρφωση απαιτεί Ομάδα (έργου)



interLei

Οργανωτικά μέτρα

PRIVACY

Ρόλοι και τα καθήκοντα που εμπλέκονται άμεσα στο GDPR & υποστηρικτικές ομάδες.

Δημιουργία πολιτικών για τήρηση και προστασία των ΔΠΧ (Subject Requests, Retention, Data Breach, third party Policies)

Δημιουργία ή τροποποίηση υφιστάμενων privacy notices (newsletter, online, cookies κα).

Προαιρετικές πιστοποιήσεις (προσωπικού και εταιρείας)

SECURITY

Δημιουργία πολιτικών ασφάλειας GDPR

Δημιουργία πολιτικών ασφαλείας οργανισμού

Σχέδια ανάκαμψης από καταστροφή (Business Continuity, Disaster Recovery Plans)

Έλεγχοι παρείσδυσης (Penetration tests)

interLei

Προστασία δεδομένων από το σχεδιασμό και εξ ορισμού

Privacy by Design

Τεχνικά και Οργανωτικά μέτρα (ψευδωνυμοποιηση)	Αρχές προστασίας (Ελαχιστοποίηση)	Κρυπτογράφηση	Αναγνώριση και αντιμετώπιση παραβίασης

Privacy by Default

Συλλογή των απαραίτητων δεδομένων (Σκοπός)	Βαθμός Επεξεργασίας (για το σκοπό που συλλέχθηκαν)	Χρόνος τήρησης των δεδομένων	Περιορισμός πρόσβασης στα δεδομένα

interLei

Εκτίμηση Αντίκτυπου (DPIA)

- Διενέργεια PIA όταν:
  - Ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων (πριν από την επεξεργασία)
  - Έχουμε συστηματική και εκτενή αξιολόγηση προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ
  - Μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων
  - Συστηματική παρακολούθηση δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα
- Σήμερα ξέρουμε ότι θέλουμε στα παρακάτω:
  - Marketing
  - Ανθρώπινο Δυναμικό
  - Πληροφορική (IT)
  - Logistics

interLei

Παραδείγματα ενημέρωσης ΑΠΔΠΧ και ΥΔ (εντός 72 ωρών)

Παράδειγμα	ΑΠΔΠΧ	ΥΔ	Σχόλια
Απώλεια ή κλοπή USB /laptop/tablet/mobile με ΔΠΧ	ΝΑΙ	ΝΑΙ*	Αν ήταν κρυπτογραφημένα δεν θα χρειαζόταν
Virus/Ransomware χωρίς backup	ΝΑΙ	ΝΑΙ	Αν υπήρχε backup τότε δεν θα υπήρχε ενημέρωση προς ΥΔ. Γκρίζα ζώνη για την ΑΠΔΠΧ
Cyber ή DoS attack στο e-shop ή website (ΔΠΧ)	ΝΑΙ	ΝΑΙ/ΌΧΙ	Στο DoS ΌΧΙ (ΥΔ)
Direct mail marketing με παραλήπτες στο To/Cc αντί Bcc	ΝΑΙ	ΝΑΙ/ΟΧΙ	Ναι αν το περιεχόμενο είχε προσωπικές προτιμήσεις ή ιδιαίτερες πωλήσεις σε λίστα πελατών. Όχι αν αφορούσε μόνο email addresses

Ενημέρωση – Ενημέρωση - Ενημέρωση

interLei

Incident Response Plan

Μηχανισμός αντιμετώπισης περιστατικών παραβίασης ΔΠΧ (Άρθρα 33,34,12)

- Σύσταση ομάδας διαχείρισης παραβιάσεων
- Διαδικασίες
- Κατανόηση τρόπων παραβίασης δεδομένων και ενημέρωσης (εσωτερικά και ΑΠΔΠΧ, ΥΔ)
- Εκπαίδευση ομάδας & προσωπικού

interLei

ΤΕΧΝΙΚΑ ΜΕΤΡΑ

Περιμετρική Ασφάλεια
Firewall, IPS, VPNs, Web Security

Email security
Antivirus, Antimalware, Antispam, DLP

Backup
Advanced Backup, Archiving and recovery με (κρυπτογράφηση)

Endpoint protection
MDM/EMM,
Κρυπτογράφηση Συσκευών
VPNs
Personal Firewall, Antivirus

PC/Server security
DLP, Personal Firewall, Antivirus
Digital Right Management, OS Management, URL/Content Filtering

Monitoring
Security Monitoring / SIEM
DLP

interLei

Οι περισσότερες παραβιάσεις της ιδιωτικής ζωής παραμένουν άγνωστες, αυτό που αναφέρεται στον υπεύθυνο προστασίας προσωπικών δεδομένων μπορεί να είναι μόνο η κορυφή του παγόβουνου

interLei

ΜΥΘΟΣ

Συγκατάθεση για όλα

Εύκολο να λάβεις/διαχειριστείς συγκαταθέσεις

Δεν επικοινωνούμε χωρίς συγκατάθεση

Περίοδος χάριτος

GDRP αφορά μόνο την ιδιωτικότητα (privacy)

ΠΡΑΓΜΑΤΙΚΟΤΗΤΑ

Αν το επιτρέπει η Νομοθεσία, η Σύμβαση, λόγοι Δημοσίου συμφέροντος δεν απαιτείται Συγκατάθεση

Πολλά κανάλια επικοινωνίας - websites, eshops, φυσικό κατάστημα, mobile app, SMS, Viber, Social Media, διαγωνισμοί, έλλειψη κινήτρου - Κεντρικοποίηση

Μπορεί για το Σκοπό εκπλήρωσης υπηρεσίας, αν έγινε εφαρμογή opt-out κ.α

Εξαρτάται. Ποιος δεν θα επιβάλλει ποινή από την πρώτη μέρα σε μια μεγάλη διαρροή προσωπικών δεδομένων ?

Πολλά τεχνικά μέτρα και ειδικά Κρυπτογράφηση, Ψευδωνυμοποίηση και Ανωνυμοποίηση.
Ενημέρωση (Security and Privacy Awareness)

interLei

Ολιστική Προσέγγιση

Οργάνωση Ομάδας έργου

- Ρόλοι & Αρμοδιότητες

Προετοιμασία

- Kick-off
- Ενημέρωση ομάδας
- Ενημέρωση Data Owners

Διάγνωση

- Data Flow Mapping
- Gap Analysis
- IT and Security
- Μέθοδοι Συγκατάθεσης
- Κείμενα συγκατάθεσης

Πλάνο Συμμόρφωσης

- Πολιτικές GDPR
- Ενέργειες συμμόρφωσης
- Εκπαίδευση Προσωπικού
- Ongoing Compliance / monitoring and Consulting

Ασφαλιστική Κάλυψη

Δεν είναι το πρόστιμο το μεγαλύτερο πλήγμα αλλά η Φήμη, η Εμπιστοσύνη, η Αξιοπιστία και πως θα το εκμεταλλευτούν Ανταγωνιστές και Συνεργάτες

interLei

THANK YOU

WANT TO KNOW MORE ?

We will be happy to meet you on our **Booth**

GDPR – the countdown to 25 May 2018 continues

info@interlei.gr

www.interlei.gr

https://www.linkedin.com/company/interlei---international-learning-institute

www.facebook.com/interlei.gr/

interLei