



EU Cyber Security Policy

Ευρωπαϊκό δίκαιο προστασίας και ασφάλειας δεδομένων στα επόμενα χρόνια

Θοδωρής Κωνσταντακόπουλος

Δικηγόρος M.L.E., LL.M.

Senior Associate,

Μπάλλας, Πελεκάνος & Συνεργάτες Α.Ε.Δ.Ε.



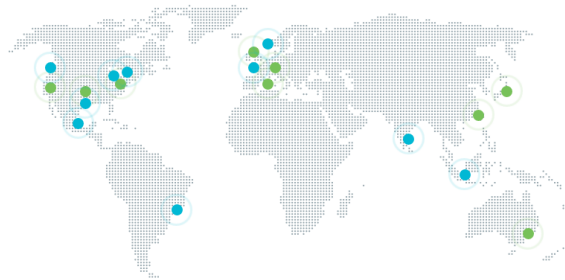
**BALLAS
PELECANOS**
& ASSOCIATES L.P.C.



**Νέες
εμπορικές
τάσεις**
(profiling)

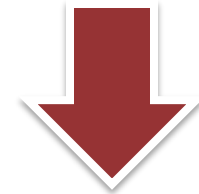


**Νέα μοντέλα
επιχειρηματικής
οργάνωσης**
(international data
transfers)



Τεχνολογική υποδομή +
υπηρεσίες τρίτων (cloud
computing)

Νέες τεχνολογίες και
τεχνολογικές δυνατότητες
(Big Data, IoT)



Ευρωπαϊκή Στρατηγική
στην Ψηφιακή Ενιαία
Αγορά (**Digital Single
Market Strategy**)

Ενίσχυση της
εμπιστοσύνης και της
ασφάλειας των
ψηφιακών υπηρεσιών

Συνθήκες πραγματοποίησης
παραβιάσεων ασφάλειας



“

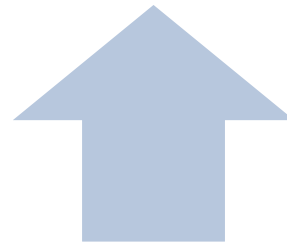
*«κατάλληλα τεχνικά και οργανωτικά
μέτρα ασφάλειας»*



Ανάπτυξη της
επιχειρηματικότητας



Προστασία και
ασφάλεια των
δεδομένων





427 ΕΚ



167 ΕΚ



400 €Κ



65 ΕΚ



ΝΟΜΙΚΟ ΠΛΕΓΜΑ ΥΠΟ ΔΙΑΜΟΡΦΩΣΗ

**Κανονισμός (ΕΕ)
2016/679** – Γενικός
Κανονισμός για την
Προστασία
Δεδομένων (**GDPR**)

Κανονισμός για την
Ιδιωτική Ζωή στις
Ηλεκτρονικές
Επικοινωνίες
(**e-Privacy
Regulation**)

ΟΔΗΓΙΑ 2016/1148
σχετικά με μέτρα για
υψηλό κοινό επίπεδο
ασφάλειας
συστημάτων δικτύου
και πληροφοριών
(**NIS Directive**)



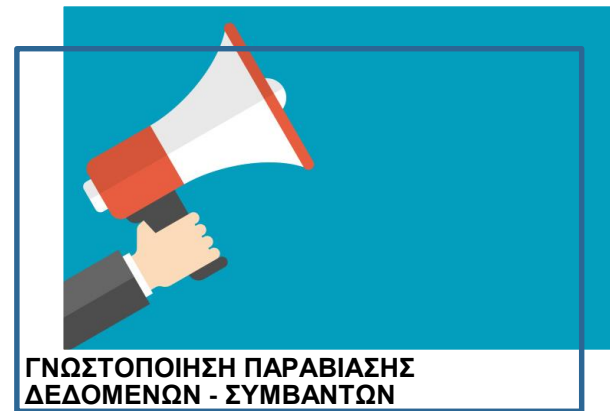
ΝΟΜΙΚΟ ΠΛΕΓΜΑ ΥΠΟ ΔΙΑΜΟΡΦΩΣΗ

	Έναρξη Ισχύος	Ποιους αφορά?	Μέτρα Ασφάλειας
GDPR	25.05.2018	Οριζόντια εφαρμογή	Άρθρα 32, 25
e-Privacy Regulation (πρόταση 10.01.2017)	25.05.2018	• Internet service providers • Mobile network operators • 'over the top' communication service providers πχ. Skype, WhatsApp	Άρθρο 8
NIS Directive	10.05.2018 (προθεσμία ενσωμάτωσης)	• Φορείς εκμετάλλευσης βασικών υπηρεσιών (Ενέργεια, Μεταφορές, Τράπεζες, Υγεία, κλπ.) • Πάροχοι ψηφιακών υπηρεσιών (online marketplaces, online search engines, cloud computing services)	Άρθρα 14, 16



ΝΟΜΙΚΟ ΠΛΕΓΜΑ ΥΠΟ ΔΙΑΜΟΡΦΩΣΗ

2 άξονες συμμόρφωσης:





A.

ΛΗΨΗ ΜΕΤΡΩΝ ΑΣΦΑΛΕΙΑΣ

- ☐ GDPR
- ☐ e-Privacy Regulation
- ☐ NIS Directive

ΛΗΨΗ ΜΕΤΡΩΝ ΑΣΦΑΛΕΙΑΣ - GDPR



«κατάλληλα
τεχνικά και
οργανωτικά
μέτρα»



[N. 2472/1997]

Επιπρόσθετες υποχρεώσεις λήψης μέτρων (κατά περίπτωση)

- **ψευδωνυμοποίηση** και **κρυπτογράφηση** δεδομένων προσωπικού χαρακτήρα
- δυνατότητα διασφάλισης του απορρήτου (**confidentiality**), της ακεραιότητας (**integrity**), της διαθεσιμότητας (**availability**) και της αξιοπιστίας (**resilience**) των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση
- δυνατότητα αποκατάστασης της **διαθεσιμότητας** και της **πρόσβασης** σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος
- διαδικασία για την τακτική δοκιμή (**testing**), εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας

ΛΗΨΗ ΜΕΤΡΩΝ ΑΣΦΑΛΕΙΑΣ - e-Privacy Regulation



Ποιους αφορά?

Internet service providers

Mobile network operators

'over the top'
communication service
providers, πχ. Skype,
WhatsApp

παραπέμπει άμεσα για ζητήματα
ασφάλειας

GDRP



Ποιους αφορά?

Φορείς εκμετάλλευσης βασικών υπηρεσιών

(Ενέργεια, Μεταφορές, Τράπεζες, Υγεία, κλπ.) δηλαδή εταιρείες και οργανισμούς με σημαντικό ρόλο στην κοινωνία και οικονομία

Παρόχους ψηφιακών υπηρεσιών

(online marketplaces, online search engines, cloud computing services)

ΕΞΑΙΡΟΥΝΤΑΙ: πολύ μικρές και μικρές επιχειρήσεις

ΛΗΨΗ ΜΕΤΡΩΝ ΑΣΦΑΛΕΙΑΣ – NIS Directive



Πρόληψη κινδύνων

- «**κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα**» για τη διαχείριση των κινδύνων

Διασφάλιση ασφάλειας

- επίπεδο ασφάλειας ανάλογο προς τον εκάστοτε κίνδυνο «**λαμβάνοντας υπόψη τις πλέον πρόσφατες τεχνικές δυνατότητες**»

Χειρισμός συμβάντων (**incidents**)

- Τα μέτρα θα πρέπει να είναι κατάλληλα για την **αποτροπή και την ελαχιστοποίηση του αντίκτυπου συμβάντων**, με σκοπό τη **διασφάλιση της συνέχειας των υπηρεσιών**.



B.

ΓΝΩΣΤΟΠΟΙΗΣΗ ΠΑΡΑΒΙΑΣΗΣ ΔΕΔΟΜΕΝΩΝ + ΣΥΜΒΑΝΤΩΝ

- ☐ GDPR
- ☐ NIS Directive

ΓΝΩΣΤΟΠΟΙΗΣΗ ΠΑΡΑΒΙΑΣΗΣ - GDPR



«παραβίαση δεδομένων προσωπικού χαρακτήρα»

παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγησης ή πρόσβασης δεδομένων προσωπικού χαρακτήρα

Ενδέχεται να προκαλέσει κίνδυνο (risk)?

ΟΧΙ

Δεν υπάρχει υποχρέωση γνωστοποίησης, αλλά θα πρέπει η παραβίαση να τηρηθεί σε αρχείο

ΝΑΙ

Ο υπεύθυνος επεξεργασίας γνωστοποιεί αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος την παραβίαση στην εποπτική αρχή

Ενδέχεται να προκαλέσει υψηλό κίνδυνο (high risk)?

ΟΧΙ

Δεν υπάρχει άλλη υποχρέωση

ΝΑΙ

Ο υπεύθυνος επεξεργασίας πρέπει να ανακοινώσει «αμελλητί» την παραβίαση στο υποκείμενο των δεδομένων

ΓΝΩΣΤΟΠΟΙΗΣΗ ΣΥΜΒΑΝΤΟΣ – NIS Directive



«**συμβάν**»: κάθε γεγονός που έχει στη πραγματικότητα μια δυσμενή επίπτωση στην ασφάλεια συστημάτων δικτύου και πληροφοριών

ΦΟΡΕΙΣ ΕΚΜΕΤΑΛΛΕΥΣΗΣ ΒΑΣΙΚΩΝ ΥΠΗΡΕΣΙΩΝ

συμβάντα με **σοβαρό αντίκτυπο** (significant impact) στη συνέχεια των βασικών υπηρεσιών που παρέχουν

Κριτήρια:

- (α) ο αριθμός των χρηστών που επηρεάζονται από τη διατάραξη της βασικής υπηρεσίας·
- (β) η διάρκεια του συμβάντος·
- (γ) το γεωγραφικό εύρος της περιοχής που επηρεάζεται από το συμβάν.

ΠΑΡΟΧΟΙ ΨΗΦΙΑΚΩΝ ΥΠΗΡΕΣΙΩΝ

συμβάντα με **σημαντικό αντίκτυπο** (substantial impact) στην παροχή της υπηρεσίας που προσφέρουν εντός της Ένωσης

Κριτήρια:

- (α) ο αριθμός των χρηστών που επηρεάζονται·
- (β) η διάρκεια του συμβάντος·
- (γ) το γεωγραφικό εύρος της περιοχής που επηρεάζεται·
- (δ) η έκταση της διατάραξης της λειτουργίας της υπηρεσίας·
- (ε) η έκταση του αντίκτυπου στις οικονομικές και κοινωνικές δραστηριότητες.

στην **αρμόδια αρχή** ή στην **CSIRT** (Computer Security Incident Response Team)

ΠΑΡΑΤΗΡΗΣΕΙΣ ΠΡΟΣ ΣΥΖΗΤΗΣΗ

Απόδειξη Συμμόρφωσης

Η τήρηση εγκεκριμένου
κώδικα δεοντολογίας ή
εγκεκριμένου
μηχανισμού
πιστοποίησης δύναται
να χρησιμοποιηθεί ως
στοιχείο για την απόδειξη
της συμμόρφωσης με τις
απαιτήσεις ασφάλειας



Οι εκτελούντες
την επεξεργασία
συχνά δε
γνωρίζουν τι
δεδομένα
επεξεργάζονται

Γνωστοποιήσεις
σε περισσότερες
Αρχές



Ευχαριστώ!

Θοδωρής Κωνσταντακόπουλος

Δικηγόρος M.L.E., LL.M.

Senior Associate,

Μπάλλας, Πελεκάνος & Συνεργάτες Α.Ε.Δ.Ε.



**BALLAS
PELECANOS**
& ASSOCIATES L.P.C.

