ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

GDPR

General Data Protection Regulation (EU) 2016/679

AQS
Advanced Quality Services Ltd.
ΣΥΜΒΟΥΛΟΙ ΕΠΙΧΕΙΡΗΣΕΩΝ

Παναγιώτης Σταθόπουλος

IT Manager, με 25ετή εμπειρία στον Σχεδιασμό και Εφαρμογή Συστημάτων Πληροφορικής με έμφαση στην **Ασφάλεια - IT Security** και στην **Προστασία των Δεδομένων**. Υπεύθυνος της Μηχανογραφικής Υποδομής και την οργάνωση των εταιρειών του Ομίλου σε θέματα IT.

Εισηγητής σεμιναρίων για πάνω από 15 χρόνια και άνω των 100 σεμιναρίων σε Ελλάδα και Κύπρο σε θέματα **ISO 27001, IT Security, GDPR κα.**

Πιστοποιημένος DPO Executive (TUV Austria)

https://goo.gl/VmCZeg

AQS
Advanced Quality Services Ltd.
ΣΥΜΒΟΥΛΟΙ ΕΠΙΧΕΙΡΗΣΕΩΝ

Ευάγγελος Μιχαλολιάκος

Σύμβουλος Οργάνωσης της AQS με ιδιαίτερη εμπειρία σε Έργα Business Process Reengineering, εγκατάστασης Συστημάτων Διαχείρισης βάσει των προτύπων ISO 9001, ISO 39001, ISO 29990 κα.

Υπεύθυνος Marketing της AQS

https://goo.gl/iP3YHe

Γιατί χρειάζεται η προστασία δεδομένων 1/2

AQS
Advanced Quality Services Ltd.
ΣΥΜΒΟΥΛΟΙ ΕΠΙΧΕΙΡΗΣΕΩΝ

Γίνεται επεξεργασία των προσωπικών σας δεδομένων ακόμα και χωρίς την ρητή έγκριση σας όταν προβαίνετε σε:

1. Αγορές προϊόντων,
2. Πληρωμές λογαριασμών,
3. Εγγραφή σε ένα e-newsletter,
4. Πλοήγηση, Επικοινωνία, (internet / e-mail), κλπ.

Γιατί χρειάζεται η προστασία δεδομένων 2/2

Αυτά τα προσωπικά δεδομένα τηρούνται και επεξεργάζονται από:

- ✧ Συστήματα πληροφορικής
- ✧ Χειρωνακτικά αρχεία

- ✧ Servers
- ✧ Data bases

- ✧ E-mail messages, digital documents,
- ✧ Videos, κλπ.

Τι είναι προσωπικά δεδομένα;

- **‘Δεδομένα προσωπικού χαρακτήρα’:**
  Κάθε πληροφορία που ταυτοποιεί ή δύναται να ταυτοποιήσει ένα φυσικό πρόσωπο **(‘υποκείμενο των δεδομένων’).**

- **Παραδείγματα:**
  - Το ονοματεπώνυμο, τηλέφωνο, διεύθυνση, κλπ.
  - Η διεύθυνση ηλεκτρονικού ταχυδρομείου (**email**)
  - Η διεύθυνση πρωτοκόλλου διαδικτύου (**IP address**)

Η Ευρωπαϊκή Θέση

"*European Data Protection Authorities take the view that **a company processes personal data** if it uses data to single out a person, **even if it cannot tie a name** to these data*"

Frederick Borgesius (2016, p2)

Νέοι και διευρυμένοι ορισμοί

Ευαίσθητα δεδομένα: Τα δεδομένα που αφορούν

- στη φυλετική ή εθνική **προέλευση**
- στα **πολιτικά** φρονήματα
- στις **θρησκευτικές** ή **φιλοσοφικές** πεποιθήσεις
- στην **υγεία**, στην κοινωνική πρόνοια,
- στη συμμετοχή σε **συνδικαλιστική** οργάνωση, κλπ.

GDPR – EU 2016/679

- Ο νέος κανονισμός Γενικής Προστασίας Δεδομένων (**General Data Protection Regulation)** αντικαθιστά την επίσημη οδηγία 95/46 / ΕΚ από το 1995 και θα τεθεί σε εφαρμογή την **25η Μαΐου 2018** μετά από μια μεταβατική περίοδο δύο ετών (από τον Απρίλη του 2016).

- Δεν απαιτεί καμία **έγκριση** μέσω κοινοβουλίων από τα κράτη-μέλη της Ευρωπαϊκής Ένωσης (ΕΕ).

- Θα **αντικαταστήσει** ένα συνονθύλευμα από 28 διαφορετικά σύνολα εθνικών νόμων

Λόγοι προστασίας δεδομένων σε εταιρείες

- **Κανονιστική** συμμόρφωση
- **Οικονομικές** και άλλες απώλειες
- **Συνεχής** (24 ώρες/7 ημέρες) επιχειρησιακή λειτουργία
- **Παραγωγικότητα** εργαζομένων
- Λήψη **διοικητικών** αποφάσεων

Πρόστιμα από μη συμμόρφωση

- *Η μη συμμόρφωση προς εντολή της εποπτικής αρχής όπως αναφέρεται στο άρθρο 58 παράγραφος 2 επισύρει διοικητικά πρόστιμα έως **20.000.000 EUR** ή **έως το 4 %** του **συνολικού παγκόσμιου** ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι **υψηλότερο**.*

GDPR:

1. Άρθρο 83 - Γενικοί όροι επιβολής διοικητικών προστίμων

2. Άρθρο 84 - Κυρώσεις

ΕΡΩΤΗΜΑΤΑ

- Ερώτηση 1: Ποιός έχει ακόμη **δικαίωμα πρόσβασης** στα προσωπικά δεδομένα;
- Ερώτηση 2: Τηρούνται τα προσωπικά δεδομένα με **ασφάλεια** και **ακρίβεια**;
- Ερώτηση 3: Συλλέγονται τα προσωπικά δεδομένα με τη **συγκατάθεση** των ενδιαφερομένων προσώπων;
- Ερώτηση 4: Πως πρέπει να **προστατευθούν** τα άτομα και οι εταιρείες/οργανισμοί;

ΟΙ 3 ΚΡΙΣΙΜΕΣ ΔΙΑΣΤΑΣΕΙΣ ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ

- IT
- ΝΟΜΙΚΗ
- ΟΡΓΑΝΩΤΙΚΗ

Δικαιώματα Φυσικών Προσώπων

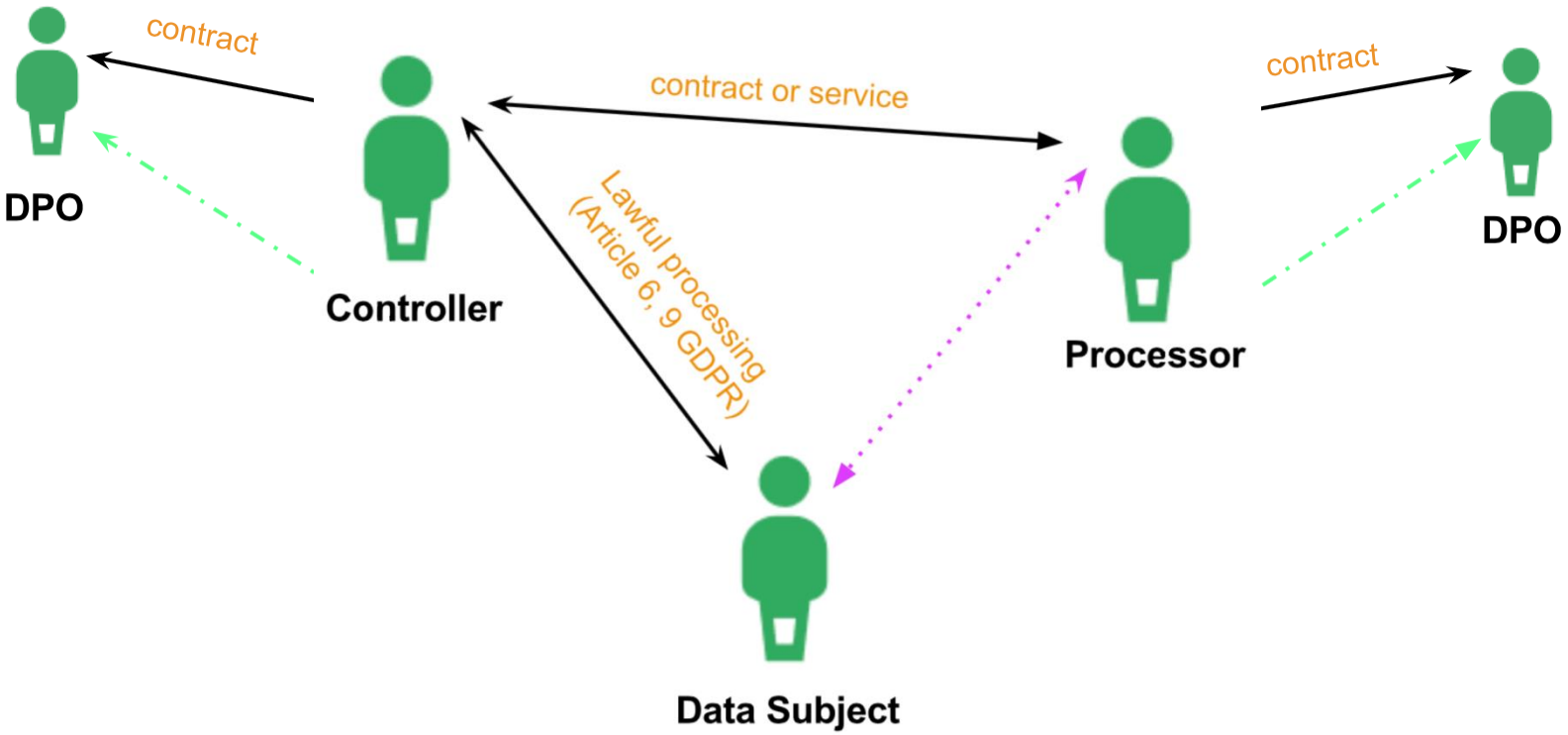
- **Άρθρο 13-14: Ενημέρωση** για τα Προσωπικά Δεδομένα που κατέχουμε & στοιχεία επικοινωνίας
- **Άρθρο 17: Δικαίωμα στην Λήθη / Διαγραφή**
  το υποκείμενο έχει δικαίωμα να ζητήσει την διαγραφή των δεδομένων
- **Άρθρο 20: Δικαίωμα φορητότητας δεδομένων**
  δεδομένα σε κοινώς αναγνωρίσιμο μορφότυπο, και απευθείας διαβίβαση
- **Άρθρο 22: Δικαίωμα εναντίωσης**
  και στη λήψη αποφάσεων με αυτοματοποιημένα μέσα
- **Άρθρο 33: Γνωστοποίηση παραβιάσεων** ασφάλειας, εντός 72 ωρών

Βασικοί ρόλοι

1. **Υπεύθυνος Επεξεργασίας (Data Controller):** Οποιοσδήποτε καθορίζει τον σκοπό και τον τρόπο της επεξεργασίας.

2. **Εκτελών την Επεξεργασία (Data Processor)**: Οποιοσδήποτε επεξεργάζεται δεδομένα για λογαριασμό του υπεύθυνου επεξεργασίας.

3. **Υπεύθυνος Προστασίας Δεδομένων (Data Protection Officer):** Οποιοσδήποτε συμμετέχει, δεόντως και εγκαίρως, σε όλα τα ζητήματα τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα.


contract
DPO
Controller
contract or service
Lawful processing
(Article 6, 9 GDPR)
Processor
contract
DPO
Data Subject

Υπεύθυνος Προστασίας Δεδομένων

- Σε **κάθε δημόσιο** φορέα
- και σε κάθε **ιδιωτικό** φορέα υπό **προϋποθέσεις**

ορίζεται ένα **πρόσωπο** ως ΥΠΔ - DPO.

Μια **Εσωτερική Αρχή Προστασίας Δεδομένων** που διασφαλίζει ότι ο οργανισμός τηρεί τις διατάξεις του Κανονισμού και συνεργάζεται με την Εθνική Αρχή Προστασίας για την τήρηση των διατάξεων.

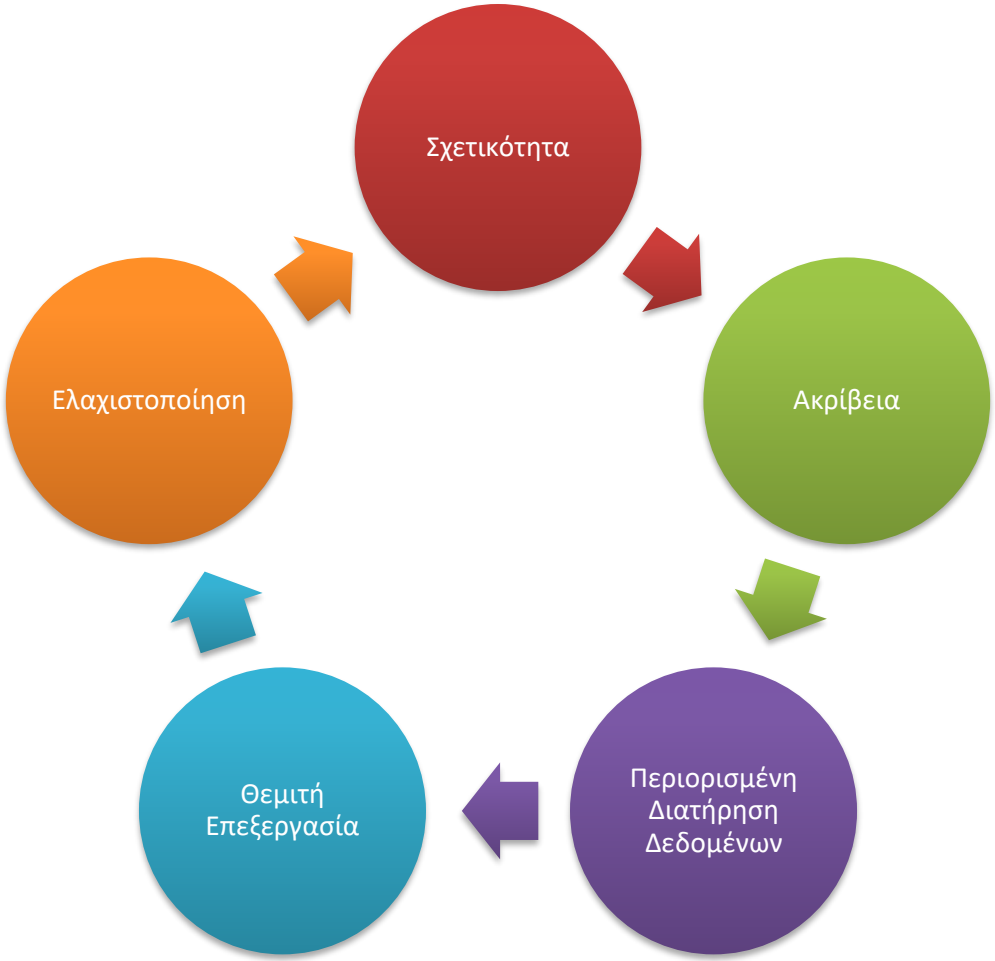
Πώς πρέπει να λειτουργεί η προστασία δεδομένων

- Θα πρέπει να υπάρχουν **όρια** στο τι στοιχεία συλλέγονται και νοούνται ως προσωπικά δεδομένα.

- Οι προσωπικές πληροφορίες θα πρέπει να λαμβάνονται με **νόμιμα** και **θεμιτά** μέσα, με τη **συγκατάθεση** του ατόμου (υποκείμενο των δεδομένων).

- Οι προσωπικές πληροφορίες πρέπει να είναι **σωστές**, σχετικές με τους σκοπούς για τους οποίους χρησιμοποιούνται, **ακριβή**, **πλήρη** και **ενημερωμένες**, κ.λπ.

Ενάρετος κύκλος



AQS
Advanced Quality Services Ltd.
ΣΥΜΒΟΥΛΟΙ ΕΠΙΧΕΙΡΗΣΕΩΝ

Αρχές ποιότητας των δεδομένων

- **Νόμιμη** Επεξεργασία (Lawful Processing)
- Προσδιορισμός του **Σκοπού** (Purpose Specification)
- **Ελαχιστοποίησης** Δεδομένων (Data Minimization)
- **Σχετικότητα** Δεδομένων (Data Relevancy)
- **Ακρίβεια** Δεδομένων (Data Accuracy)
- Περιορισμένη **Διατήρηση** (Limited Data Retention)
- **Θεμιτή** Επεξεργασία (Fair Processing)
- **Λογοδοσία** (Accountability)

Προστασία των δεδομένων...

- **Από το σχεδιασμό**: Σχεδιασμός οργανωτικών, τεχνικών διοικητικών μέτρων σχεδιασμένα για την εξυπηρέτηση των αρχών προστασίας δεδομένων.
  - Ψευδωνυμοποίηση
  - Privacy Controls & Dashboards

- **Εξ'ορισμού:** Κάθε πράξη επεξεργασίας, κάθε ρύθμιση, κάθε εργαλείο, εξ'ορισμού εξυπηρετούν την ιδιωτικότητα
  - Ρυθμίσεις
  - Εύκολη πρόσβαση και ενημέρωση επί των ρυθμίσεων

Άρθρο 25 EU GDPR

Προστασία σε όλη την εταιρεία

- Η προστασία των προσωπικών δεδομένων ενσωματώνεται σε **όλες τις πτυχές** ενός οργανισμού:
  - Εταιρικά Στοιχεία / Αρχεία / Υποδομές
  - HR (Πρόσληψη / απομάκρυνση προσωπικού)
  - Εταιρική ιστοσελίδα (Policies),
  - Digital Marketing (Analytics, Remarketing, Social media)
  - Ανάπτυξη προϊόντων *(PbD & PbD)*

Αρχές ποιότητας των δεδομένων

Πώς υλοποιούνται;

- ✓ Με σχέδια,
- ✓ πολιτικές,
- ✓ οργάνωση,
- ✓ ανθρώπους,
- ✓ τεχνολογία και εργαλεία

Δηλαδή Ένα **Σύστημα Προστασίας Δεδομένων**

Σύστημα Προστασίας Δεδομένων

AQS

Advanced Quality Services Ltd.
ΣΥΜΒΟΥΛΟΙ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΒΗΜΑΤΑ ΣΥΜΜΟΡΦΩΣΗΣ (1/2)

ΕΚΠΑΙΔΕΥΣΗ

1. AUDIT ΥΠΟΔΟΜΩΝ

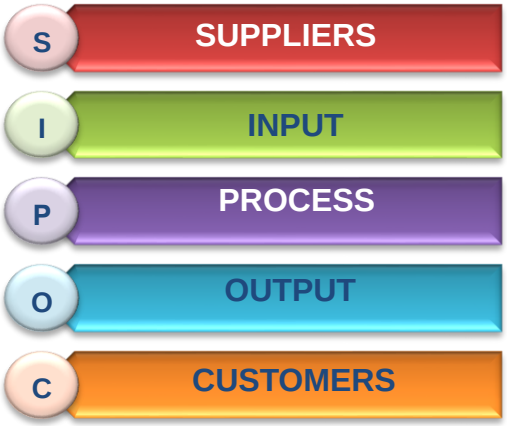
2. AUDIT ΔΙΑΔΙΚΑΣΙΩΝ

3. ΔΙΕΡΓΑΣΙΕΣ SIPOC

4. ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

ΣΗΜΕΙΑ ΕΛΕΓΧΟΥ	ΝΑΙ	ΜΕΡΙΚΩΣ	ΟΧΙ	ΠΑΡΑΤΗΡΗΣΕΙΣ
5. ΑΣΦΑΛΕΙΑ ΕΦΑΡΜΟΓΩΝ – ΓΕΝΙΚΑ				
Υπάρχουν επικυρωμένες πολιτικές και διαδικασίες πληροφορικής (Ανάπτυξη και λειτουργία συστημάτων, ασφάλεια δικτύου κλπ)			×	
Με ποια διαδικασία εργάζονται στον χώρο του υπολογιστή (computer room) τα συνεργεία καθαρισμού, ηλεκτρολόγοι, ψυκτικοί κλπ;	x			
Υπάρχει εγχειρίδιο (manual) διαδικασιών ασφάλειας πληροφορικής;			x	
Κάθε πότε διεξάγονται έλεγχοι πληροφορικής (IT Auditing) και από ποια ομάδα;		x		
Έχει πιστοποιηθεί η Πληροφορική από κάποιον Οργανισμό σε κάποια λειτουργία της (πχ. ISO 27001 για ασφάλεια κλπ);			x	
Υπάρχει οργάνωση ασφάλειας πληροφορικής (υπεύθυνος, ομάδα, διαδικασίας, λειτουργίας κλπ);	x			
Υπάρχει μητρώο πληροφορικής περιουσίας (εξοπλισμού, λειτουργικού συστήματος και βάσης δεδομένων, λογισμικού εφαρμογών, δεδομένων, εντύπων, υλικών, αδειών χρήσης, τεκμηρίωσης)	x			
Σχέδιο επαναφοράς πληροφορικής Back up / Recovery διαδικασίες Αποθήκευση back up τοπικά (vault) Αποθήκευση back up εκτός (offsite) Data Center Backup (Hot, Warm) IT Disaster recovery plan Δοκιμές σχεδίου	x x x x		x x	

Υποκείμενα ΠΔ	Κατηγορίες ΠΔ	Σκοπός συλλογής	Αποδέκτες	Γνωστοποίηση σε	Σημείο Αρχειοθέτησης	Χρόνος Διατήρησης	Υψηλός (Υ) / Χαμηλός (Χ) Κίνδυνος *
Admin Πελάτη	Ονοματεπώνυμο, τηλέφωνο, email	Διεκπεραίωση εργασιών υποστήριξης email	CTO	Συνεργάτη, Μεταπωλητή	Εφαρμογή XERO, Email εταιρείας, ηλεκτρ. ατζέντα, file server εταιρείας, σύστημα ticketing	Επ' αόριστον	X
Admin Συνεργάτη	Ονοματεπώνυμο, τηλέφωνο, email	Διεκπεραίωση εργασιών υποστήριξης email	CTO	Συνεργάτη, Μεταπωλητή	Εφαρμογή XERO, Email εταιρείας, ηλεκτρ. ατζέντα, file server εταιρείας, σύστημα ticketing	Επ' αόριστον	X
Χρήστης Εφαρμογής	IP address, user name	Διεκπεραίωση εργασιών παρακολούθησης	CTO	Συνεργάτη	Email εταιρείας, File server εταιρείας	Μέχρι την λήξη της εργασίας	X
Εργαζόμενοι	Ονοματεπώνυμο, Διεύθυνση, τηλέφωνο, email, φορολογικά στοιχεία, Αρ. Αστυνομικής Ταυτότητας / Διαβατηρίου	Εκτέλεση Εργασιών, Εκπλήρωση υποχρεώσεων εταιρείας έναντι του Νόμου		Εξωτερικός Πάροχος Λογιστ. Υπηρεσιών	Email εταιρείας, file server, φυσικός φάκελος	Μέχρι τη λύση της εταιρείας ή όπως προβλέπει ο Νόμος	X



ΒΗΜΑΤΑ ΣΥΜΜΟΡΦΩΣΗΣ (2/2)

5. ΣΧΕΔΙΑΣΜΟΣ ΡΟΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

6. RISK ASSESSMENT

7. ΤΕΧΝΙΚΗ ΚΑΙ ΝΟΜΙΚΗ ΕΠΕΞΕΡΓΑΣΙΑ

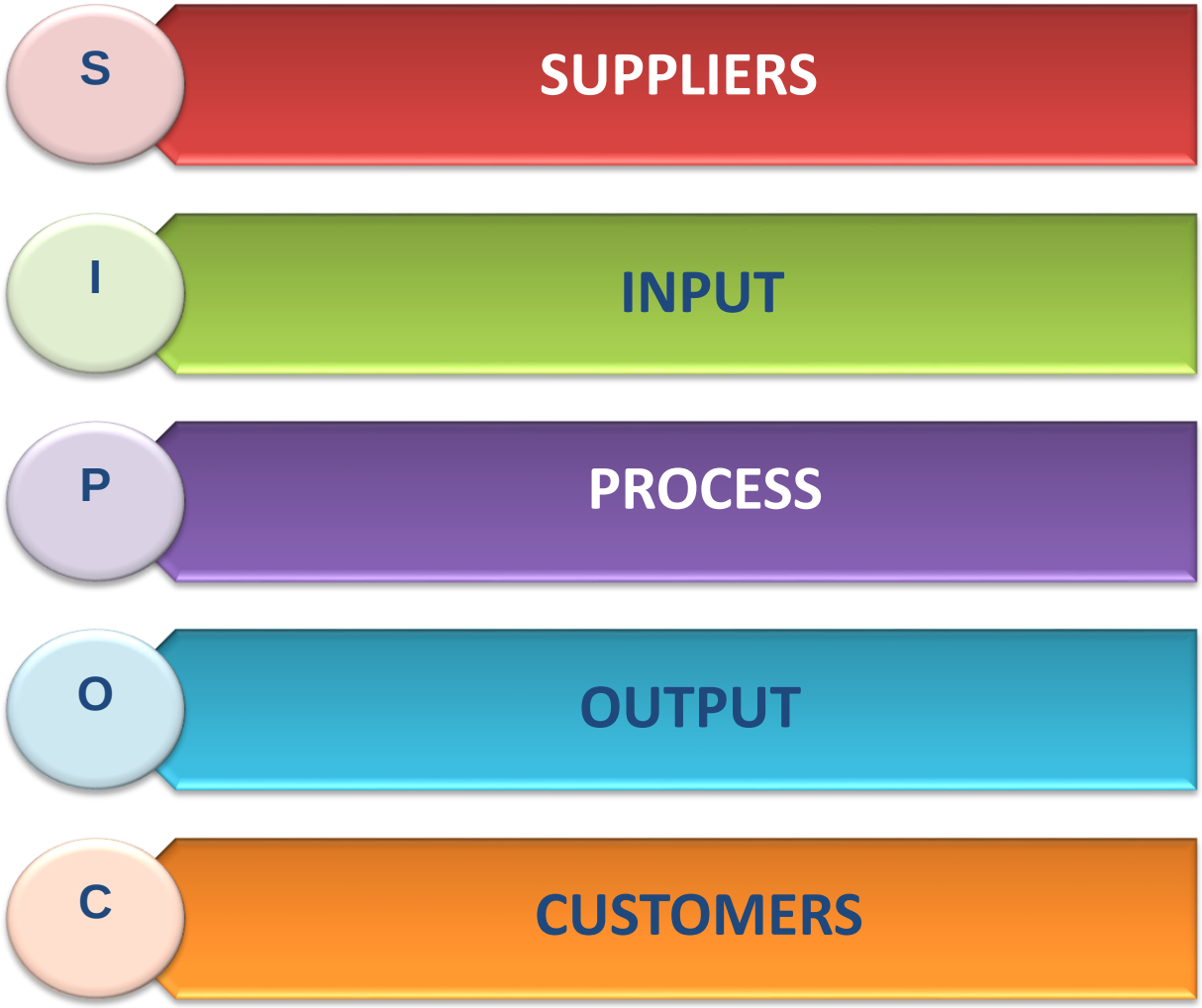
8. ΣΧΕΔΙΑΣΜΟΣ ΠΟΛΙΤΙΚΩΝ, ΔΙΑΔΙΚΑΣΙΩΝ & ΜΕΤΡΩΝ ΕΛΕΓΧΟΥ ΚΑΙ ΑΠΟΤΡΟΠΗΣ

9. AUDIT ΕΦΑΡΜΟΓΗΣ

-Σχεδιασμός Πολιτικών & Διαδικασιών
-Πρόταση τεχνικών λύσεων
-Νομικές συμβουλές κάλυψης απαιτήσεων

-Audit Checklists
-Διορθωτικές ενέργειες
-Επιβεβαίωση συμμόρφωσης

ΑΝΙΧΝΕΥΣΗ ΔΕΔΟΜΕΝΩΝ – ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΔΙΕΡΓΑΣΙΩΝ



ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ ΓΙΑ ΠΡΟΩΘΗΣΗ SIPOC (ενδεικτικά)

AQS
Advanced Quality Services Ltd.
ΣΥΜΒΟΥΛΟΙ ΕΠΙΧΕΙΡΗΣΕΩΝ

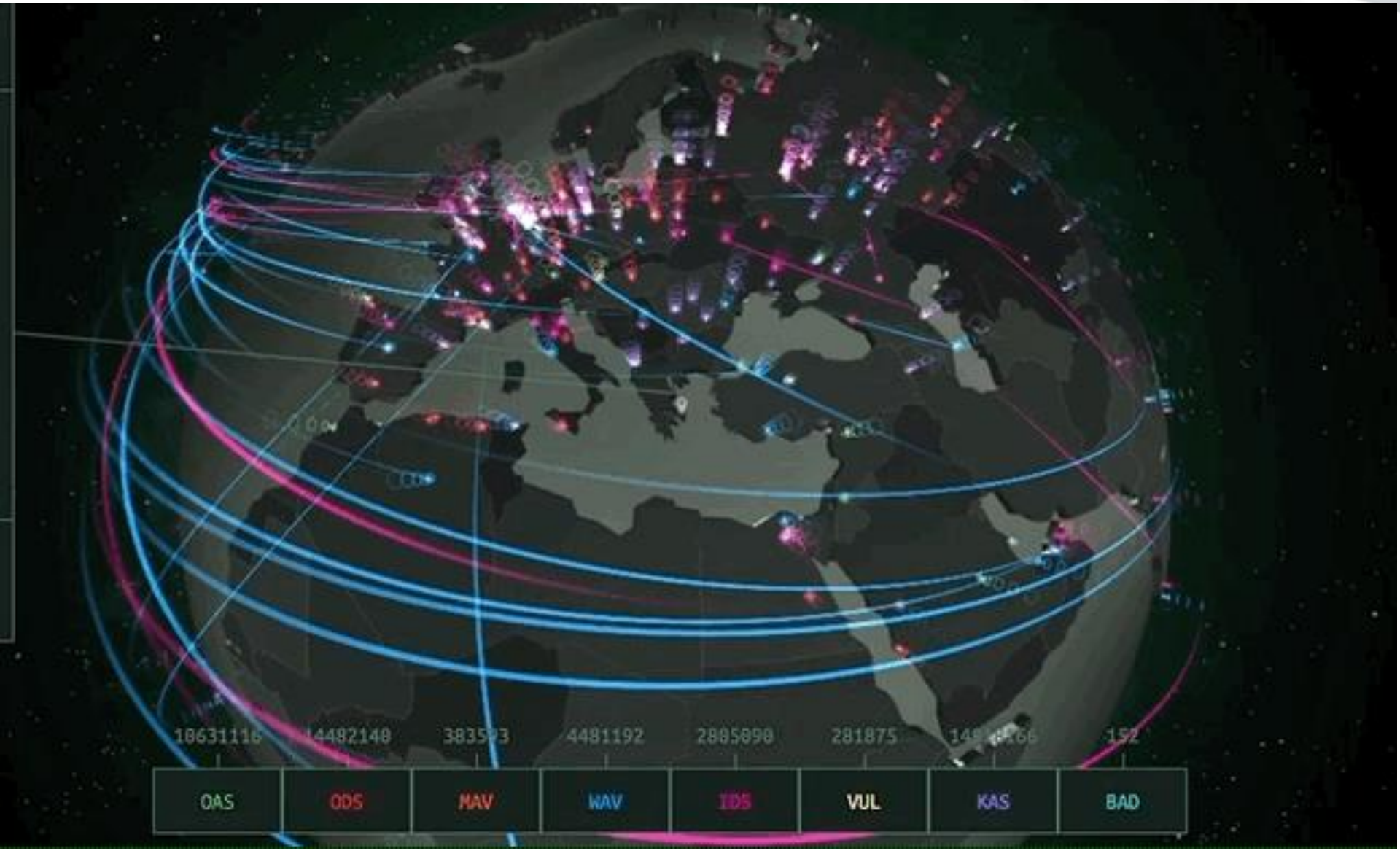
ΠΡΟΜΗΘΕΥΤΕΣ **S**	INPUT **I**	ΔΙΕΡΓΑΣΙΑ (PROCESS) **P**	OUTPUT **O**	ΠΕΛΑΤΕΣ (CUSTOMERS) **C**	ΠΑΡΑΤΗΡΗΣΕΙΣ
		Επιλογή Κατηγοριών Υπεύθυνος Marketing			
Υπεύθυνος Marketing	Κατηγορίες Πελατών	**Δημιουργία λίστας** Στέλεχος Marketing	Λίστα με: • Emails • Ονοματεπώνυμο • Ημερ. Γέννησης • Περιοχή	Υπεύθυνος Αποστολής Newsletter	Οι λίστες μεταφέρονται στην πλατφόρμα αποστολής Ψ
		Ετοιμασία newsletter Υπεύθυνος Marketing			
		Αποστολή ΧΨ			

SIPOC (ενδεικτικά)

AQS
Advanced Quality Services Ltd.
ΣΥΜΒΟΥΛΟΙ ΕΠΙΧΕΙΡΗΣΕΩΝ

Ημερομηνία:		25/4/2017				
Α/Α	**ΠΡΟΜΗΘΕΥΤΕΣ** **S**	**PERSONNAL DATA INPUT** **I**	**ΔΙΕΡΓΑΣΙΑ SIPOC** **P**	**OUTPUT** **O**	**ΠΕΛΑΤΕΣ** **C**	**ΠΑΡΑΤΗΡΗΣΕΙΣ**
1	1. ΠΕΛΑΤΕΣ / ΣΥΝΕΡΓΑΤΕΣ 2. ΜΕΤΟΧΟΙ 3. ΙΣΤΟΣΕΛΙΔΕΣ ΜΕ ΛΙΣΤΕΣ	1. ΣΥΣΤΑΣΕΙΣ ΠΕΛΑΤΩΝ / 2. ΣΥΝΕΡΓΑΤΩΝ 3. COLD CALLS 4. ΕΠΑΦΕΣ LINKED IN 5. ΠΡΟΣΩΠΙΚΕΣ ΕΠΑΦΕΣ 6. ΔΗΜΟΣΙΕΥΜΕΝΕΣ	**ΕΥΡΕΣΗ ΛΙΣΤΩΝ ΠΑΡΑΛΗΠΤΩΝ NEWSLETTER** ***ΥΠΕΥΘ. ΑΝΑΠΤ. ΠΩΛΗΣΕΩΝ / MARKETING*** **ΛΙΣΤΕΣ ΠΑΡΑΛΗΠΤΩΝ**	ΛΙΣΤΕΣ ΜΕ EMAILS ΠΡΟΣ ΑΠΟΣΤΟΛΗ	ΥΠΕΥΘΥΝΟΣ ΑΝΑΠΤ. ΠΩΛΗΣΕΩΝ / MARKETING	Οι λίστες διατηρούνται στην εφαρμογή Sendy και περιέχουν εταιρικά και προσωπικά emails. Η λίστα αυτή είναι απαλλαγμένη από τα emails που έχουν διαγραφεί μετά από εντολή των κατόχων.
2	1. ΥΠΕΥΘΥΝΟΣ ΑΝΑΠΤ. ΠΩΛΗΣΕΩΝ / MARKETING 2. ΕΦΑΡΜΟΓΗ NEWSLETTER (SENDY)	ΛΙΣΤΕΣ ΜΕ EMAILS ΠΡΟΣ ΑΠΟΣΤΟΛΗ	**ΦΟΡΤΩΣΗ ΣΕ ΕΦΑΡΜΟΓΗ / ΑΠΟΣΤΟΛΗ EMAILS** ***ΥΠΕΥΘ. ΑΝΑΠΤ. ΠΩΛΗΣΕΩΝ / MARKETING***	1. ΑΠΕΣΤΑΛΜΕΝΕΣ ΛΙΣΤΕΣ 2. REPORT ΑΠΟΣΤΟΛΩΝ	ΥΠΕΥΘΥΝΟΣ ΑΝΑΠΤ. ΠΩΛΗΣΕΩΝ / MARKETING	
3	1. ΥΠΕΥΘΥΝΟΣ ΑΝΑΠΤ. ΠΩΛΗΣΕΩΝ / MARKETING 2. ΕΦΑΡΜΟΓΗ NEWSLETTER (SENDY)	1. ΑΠΕΣΤΑΛΜΕΝΕΣ ΛΙΣΤΕΣ 2. REPORT ΑΠΟΣΤΟΛΩΝ	**FOLLOW UP ΣΕ ΠΑΡΑΛΗΠΤΕΣ / ΚΑΤΑΓΡΑΦΗ ΣΤΟΙΧΕΙΩΝ ΕΠΙΚΟΙΝΩΝΙΑΣ** ***ΥΠΕΥΘ. ΥΠΕΥΘΥΝΟΣ ΠΩΛΗΣΕΩΝ / MARKETING***	ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ ΑΠΟΔΕΚΤΩΝ NEWSLETTER	ΥΠΕΥΘΥΝΟΣ ΑΝΑΠΤ. ΠΩΛΗΣΕΩΝ / MARKETING	Τα στοιχεία που καταγράφονται είναι ονοματεπώνυμο, εταιρικό τηλέφωνο, εταιρικό email, σημειώσεις επικοινωνίας.
4	ΕΝΔΙΑΦΕΡΟΜΕΝΟΙ ΠΕΛΑΤΕΣ	1. ΟΝΟΜΑΤΕΠΩ-ΝΥΜΟ 2. EMAIL 3. ΤΗΛΕΦΩΝΟ 4. ΕΤΑΙΡΕΙΑ	**ΣΥΜΠΛΗΡΩΣΗ & ΑΠΟΣΤΟΛΗ ΦΟΡΜΑΣ PRE-SALES** **ΦΟΡΜΑ PRE-SALES**	ΣΥΜΠΛΗΡΩΜΕΝΕΣ ΦΟΡΜΕΣ PRE-SALES	ΥΠΕΥΘΥΝΟΣ ΑΝΑΠΤ. ΠΩΛΗΣΕΩΝ / MARKETING	Η φόρμα αποστέλλεται ως email στο sales@sophimail.com Στη Φόρμα δεν υπάρχει ενημέρωση για χρήση των στοιχείων.

Τεχνολογικοί Κίνδυνοι



https://cybermap.kaspersky.com/

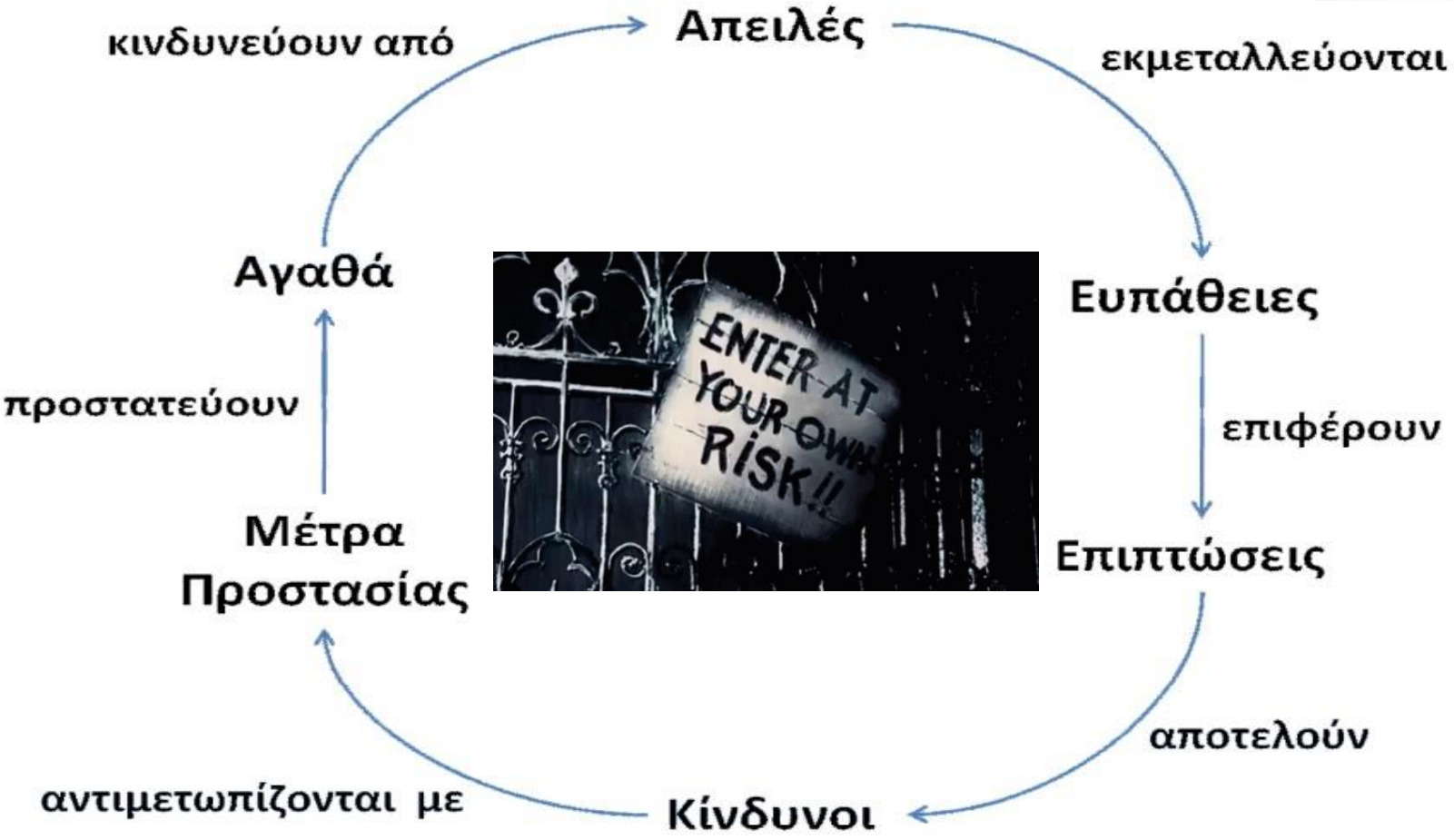
Κίνδυνοι προστασίας ΠΔ

- ΠΔ που συλλέγονται και αποθηκεύονται χωρίς λόγο
- ΠΔ που δεν διαχειρίζονται σωστά
- Μη καθορισμένη περίοδος διατήρησης των ΠΔ
- Μη αποτελεσματικοί έλεγχοι προστασίας δεδομένων

- Νέοι μηχανισμοί συλλογής δεδομένων
- Νέοι τρόποι επιτήρησης

Τελευταία Περιστατικά

Ανάλυση Κινδύνου



Εκτίμηση Επικινδυνότητας

ΠΙΘΑΝΟΤΗΤΑ ΝΑ ΣΥΜΒΕΙ	ΕΠΙΠΤΩΣΗ				
	ΑΜΕΛΗΤΕΑ (χειρισμός χωρίς επιπτώσεις)	**ΜΙΚΡΗ** (π.χ. περιορισμένη επίπτωση στο Σύστημα, μικρή καθυστέρηση σε επιχειρησιακές λειτουργίες)	**ΜΕΣΑΙΑ** (π.χ. πιθανό να καταλήξει σε μη συμμορφώσεις ή σε απώλεια πληροφοριών, αναστρέψιμη επίπτωση στο όνομα της εταιρείας)	**ΣΟΒΑΡΗ** (π.χ. σημαντικά προβλήματα στο Σύστημα όπως παράπονα, νομικές ενέργειες, πρόστιμα, επιπτώσεις στο όνομα της εταιρείας, σημαντική απώλεια εσόδων)	**ΚΑΤΑΣΤΡΟΦΙΚΗ** (π.χ. απώλεια σημαντικών πελατών, απώλεια πιστοποιητικού, υψηλότατα πρόστιμα, πολύ σημαντική απώλεια εσόδων, διακοπή λειτουργίας εταιρείας)
ΠΟΛΥ ΜΕΓΑΛΗ ΠΙΘΑΝΟΤΗΤΑ (~90%)	ΜΕΣΑΙΑ	ΥΨΗΛΗ	ΥΨΗΛΗ	ΠΟΛΥ ΥΨΗΛΗ	ΠΟΛΥ ΥΨΗΛΗ
ΑΥΞΗΜΕΝΗ ΠΙΘΑΝΟΤΗΤΑ (~70%)	ΜΕΣΑΙΑ	ΜΕΣΑΙΑ	ΥΨΗΛΗ	ΥΨΗΛΗ	ΠΟΛΥ ΥΨΗΛΗ
ΜΕΤΡΙΑ ΠΙΘΑΝΟΤΗΤΑ (~50%)	ΧΑΜΗΛΗ	ΜΕΣΑΙΑ	ΜΕΣΑΙΑ	ΥΨΗΛΗ	ΥΨΗΛΗ
ΜΙΚΡΗ ΠΙΘΑΝΟΤΗΤΑ (~30%)	ΧΑΜΗΛΗ	ΜΕΣΑΙΑ	ΜΕΣΑΙΑ	ΜΕΣΑΙΑ	ΥΨΗΛΗ
ΑΠΙΘΑΝΟ (~10%)	ΧΑΜΗΛΗ	ΧΑΜΗΛΗ	ΧΑΜΗΛΗ	ΜΕΣΑΙΑ	ΜΕΣΑΙΑ

Συνήθη Ευρήματα σε Οργανισμούς

1. Website:

- Μη ενημέρωση επισκέπτη
- Παντελής έλλειψη όρων χρήσης
- Δεν αναφέρονται τα cookies που χρησιμοποιούνται

2. Πολιτική Προστασίας Προσωπικών Δεδομένων (Data Privacy Policy)

- Αναφέρεται στο υπάρχον κανονιστικό πλαίσιο (Not GDPR Compliant)
- Έλλειψη των απαραίτητων στοιχείων στελέχους για επικοινωνία
- Εάν υπάρχει, είναι πολύ περίπλοκη (legal terms) και όχι εύκολα κατανοητή

Συνήθη Ευρήματα σε Οργανισμούς

AQS
Advanced Quality Services Ltd.
ΣΥΜΒΟΥΛΟΙ ΕΠΙΧΕΙΡΗΣΕΩΝ

3. Τεχνικές Κρυπτογράφησης (Encryption)

- Δεν χρησιμοποιείται στον ιστότοπο (SSL Certificate on Website) για επικοινωνίες
- Μη χρήση κρυπτογράφησης σε προσωπικά δεδομένα που είναι αποθηκευμένα σε βάσεις δεδομένων
- Εάν υπάρχει, δεν έχει γίνει ανάλυση κινδύνων για απώλεια κλειδιών, κλπ.

4. Πολιτικές Προστασίας Δεδομένων και Ασφάλειας Πληροφορικής

- Έλλειψη των απαραίτητων πολιτικών (βλ. ενότητα 5)
- Μη τεκμηρίωση όποιων πολιτικών υπάρχουν
- Μη εκπαίδευση όλου του κρίσιμου προσωπικού σε θέματα ασφάλειας δεδομένων

Συνήθη Ευρήματα σε Οργανισμούς

AQS
Advanced Quality Services Ltd.
ΣΥΜΒΟΥΛΟΙ ΕΠΙΧΕΙΡΗΣΕΩΝ

5. Ανάπτυξη και Λειτουργία Εφαρμογών (Συστημάτων) Πληροφορικής

- Μη εξουσιοδοτημένη ανάπτυξη εφαρμογής
- Μη τεκμηριωμένες διαδικασίες αλλαγής εφαρμογών
- Ανάπτυξη και συντήρηση εφαρμογών με βάση την εμπειρία και όχι ένα πρότυπο
- Δοκιμές εφαρμογών με πραγματικά προσωπικά δεδομένα
- Μη αποτελεσματική διαχείριση των μη δομημένων δεδομένων (word documents, emails, κλπ.).
- Μη αποτελεσματική παρακολούθηση των συμβάντων και γεγονότων ασφάλειας πληροφοριών και παραβίασης δεδομένων στα δεδομένα της εταιρείας

Συνήθη Ευρήματα σε Οργανισμούς

6. Εσωτερικά Μέτρα Προστασίας Δεδομένων

- Μη αποτελεσματική εφαρμογή μέτρων πρόληψης κλοπής δεδομένων που έχουν αποθηκευθεί σε εξοπλισμό (servers), προσωπικούς υπολογιστές (laptops), μέσα (digital media) και συσκευές (mobile and smart devices).
- Μη αποτελεσματική εφαρμογή μέτρων πρόληψης μεταφοράς δεδομένων
- Μη αποτελεσματική εφαρμογή μέτρων καταστροφής δεδομένων που έχουν αποθηκευθεί

Συνήθη Ευρήματα σε Οργανισμούς

7. Κίνδυνοι Διαχείρισης και Επεξεργασίας Δεδομένων από Τρίτους

- Μη αποτελεσματικός έλεγχος (due diligence) και αξιολόγηση (evaluation) των οργανωτικών και τεχνικών μέτρων προστασίας δεδομένων της εταιρείας ‘ΒΗΤΑ’ (Processor) από την εταιρεία ‘ΑΛΦΑ’ (controller).
- Μη ολοκληρωμένη τεκμηρίωση της επεξεργασίας δεδομένων της εταιρείας ‘ΑΛΦΑ’ (controller) (συμμόρφωση με EU GDPR) από την εταιρεία ‘ΒΗΤΑ’ (Processor).
- Μη αποτελεσματική παρακολούθηση του προσωπικού που διαχειρίζεται δεδομένα της εταιρείας ‘ΑΛΦΑ’ (controller) μέσω Cloud από την εταιρεία ‘ΒΗΤΑ’ (Processor)

8. Φυσική Ασφάλεια

AQS
Advanced Quality Services Ltd.
ΣΥΜΒΟΥΛΟΙ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ

1. Αρχιτεκτονική συστημάτων IT

Διάκριση συστημάτων προς αποφυγή διασποράς κινδύνου

- Email server
- File server
- e-shop
- website

Ιδιωτική υποδομή - για αποκλειστικό έλεγχο

Virtualization - για υψηλή διαθεσιμότητα και βέλτιστη αξιοποίηση πόρων

- on premises ή στο cloud
- σε φυσικούς ή virtual servers

2. Δίκτυα IT

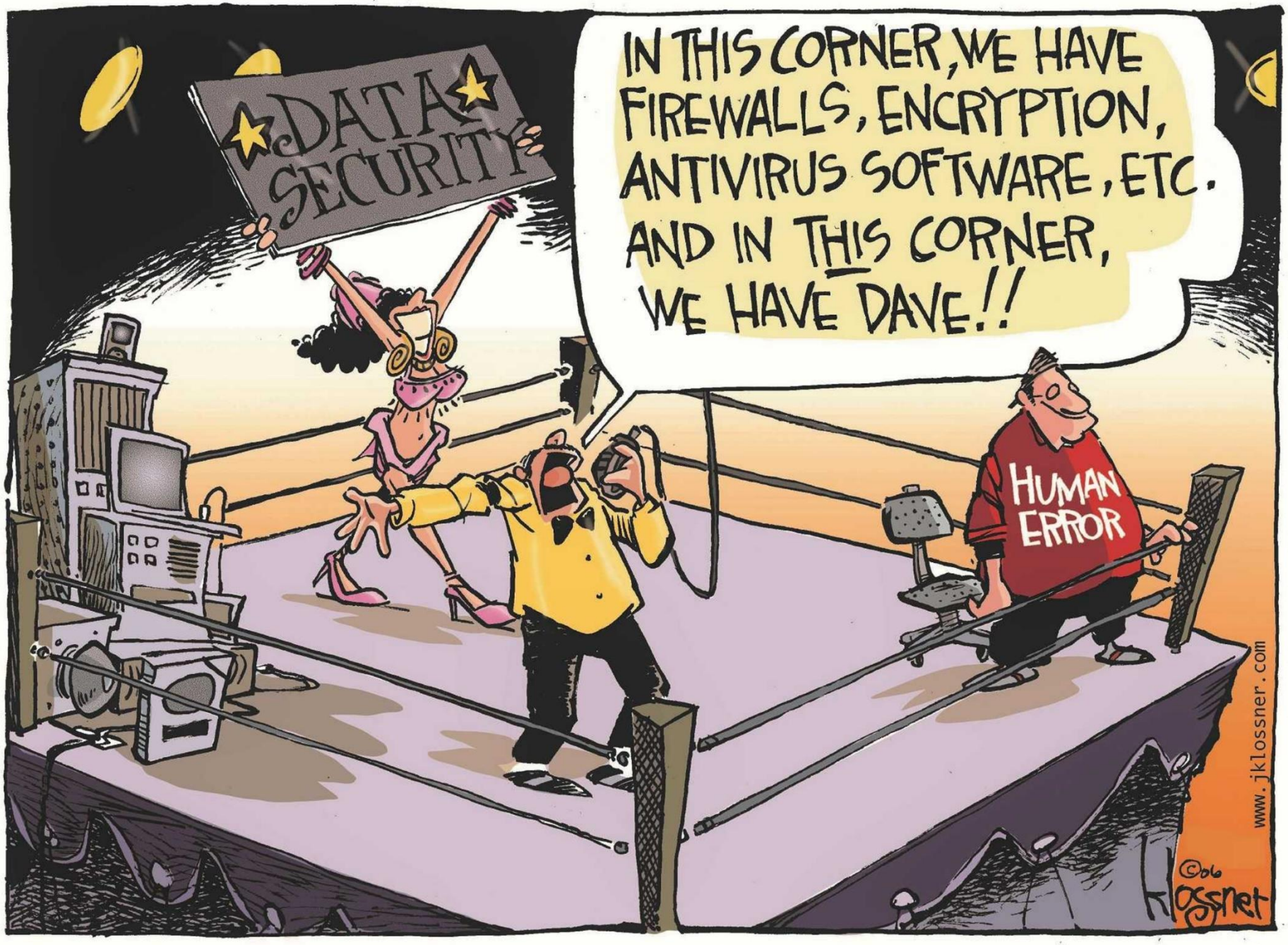
- **Firewall** και Πολιτικές Ασφαλείας
- **IPS** / IDS – για αποτροπή επιθέσεων
- **VPN** - για ασφαλή απομακρυσμένη πρόσβαση στο εταιρικό δίκτυο
- **SPF**/DKIM/DMARK - για προστασία του email domain

3. Εφαρμογές και Δεδομένα

- **Κρυπτογράφηση** με pass-phrase και SSL Certificate - για Εμπιστευτικότητα !
- **Αντίγραφο Ασφαλείας**, Δοκιμή **Επαναφοράς** και **Φορητότητας** !!
- **Τακτικές Ενημερώσεις** λογισμικού, Ειδικά τις ενημερώσεις ασφαλείας !!!

4. Χρήστες

- Πολύπλοκα **Passwords** και ταυτοποίηση χρήστη (**2-factor** authentication)
- **Διαβαθμισμένη** Πρόσβαση - βάσει ρόλου
- Πλήρης **κρυπτογράφηση** - επικοινωνίες, δεδομένα, συσκευές
- **DLP** και … εκπαίδευση !


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©06
Klossner

5. Πολιτικές Προστασίας Δεδομένων και Ασφάλειας Πληροφορικής

- Πολιτική Διαβάθμισης Πληροφοριών
- Πολιτική Διαχείρισης Δικτύου και Διαδικτύου
- Πολιτική Διαχείρισης Ασφάλειας Ηλεκτρονικού Ταχυδρομείου
- Πολιτική Αντιγραφής
- Πολιτική Διαχείρισης Κωδικών Ασφάλειας
- Πολιτική Φυσικής και Τεχνικής Ασφάλειας Πληροφορικής
- Πολιτική Διαχείρισης Περιστατικών Ασφάλειας
- Πολιτική Παρακολούθησης Συμβάσεων με Εξωτερικούς Συνεργάτες
- Πολιτική Απόσυρσης Πληροφοριακών Αγαθών

6. Παρακολούθηση – Αντιμετώπιση απειλής

- **Real-time** Παρακολούθηση και τακτικές αναφορές (SIEM tools)
- Αντιμετώπιση της απειλής βάσει **πλάνου**
- **Γνωστοποίηση** κατά τις απαιτήσεις του GDPR – 72 ώρες (Άρθρο 33)

7. Επιχειρησιακή Συνέχεια - DR plan

- **Virtualization** - για υψηλή διαθεσιμότητα και μείωση κόστους
- **Scalability** & **Capacity** planning - για βέλτιστη αξιοποίηση πόρων & Οικονομία
- Κατάρτιση **DR plan** και δοκιμές – Keep your business running!

Συμπέρασμα

AQS

Advanced Quality Services Ltd.
ΣΥΜΒΟΥΛΟΙ ΕΠΙΧΕΙΡΗΣΕΩΝ

Συμπέρασμα

- Η **σύγκλιση των τεχνολογιών πληροφορικής και επικοινωνιών**,
- η αποκέντρωση της επεξεργασίας δεδομένων σε μεγάλα κέντρα δεδομένων με βάση την τεχνολογία **cloud**,
- η **διείσδυση** της επεξεργασίας και της δικτύωσης στο σύνολο σχεδόν της ανθρώπινης δραστηριότητας και ζωής

αλλάζουν ριζικά το περιβάλλον εκμετάλλευσης και χρήσης των εταιρικών πληροφοριών και των **προσωπικών δεδομένων**,

αλλά και εγείρουν και άλλα ζητήματα σε σχέση με την ασφάλεια, ακεραιότητα και προστασία των.

Η αξία των προσωπικών δεδομένων

- Πολλοί θεωρούν ότι τα **προσωπικά δεδομένα** είναι το πιο καυτό **εμπόρευμα** στην αγορά στη σημερινή κοινωνία δικτύου.

- Μαζικές τάσεις, όπως τα μεγάλα δεδομένα (**Big Data**), οι έξυπνες πόλεις, το Internet of Things και η ταχεία ανάπτυξη της **κινητής τηλεφωνίας** οδήγησαν στη χρήση των προσωπικών δεδομένων για να αποκτήσουν, οι εταιρείες που τα συλλέγουν, γνώσεις και **ανταγωνιστικό πλεονέκτημα**.

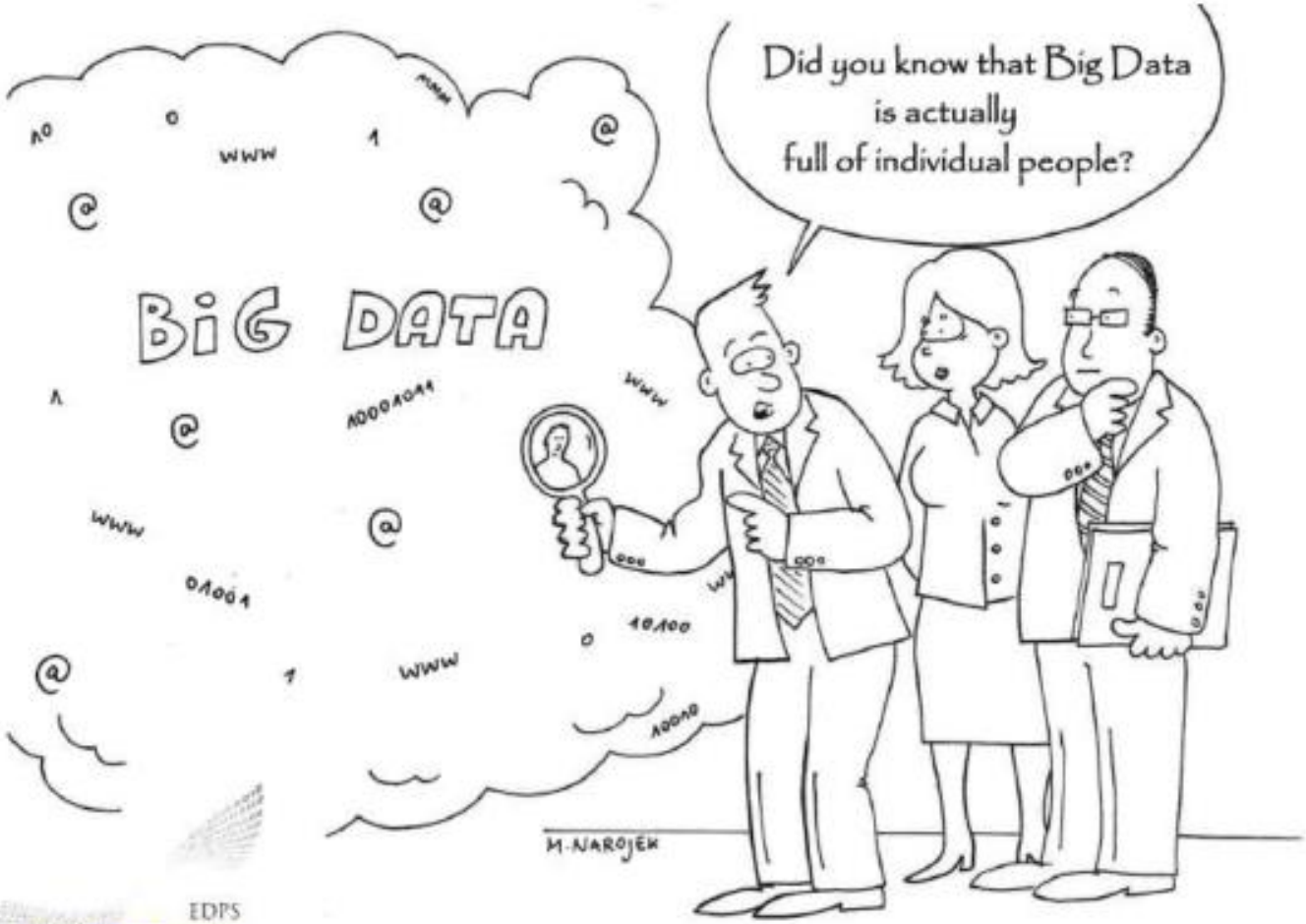
- Το **Σύστημα,** και τα **μέτρα** που περιέχονται σε αυτό, αποτελούν την βάση για να βελτιώσετε αποτελεσματικά την προστασία των ΠΔ της εταιρείας σας.

Κρίσιμοι Παράγοντες Επιτυχίας Προστασίας Δεδομένων

Αυτά (σύστημα, μέτρα, σχέδια, πολιτικές και πρακτικές), συνοψίζονται, με βάση το Μοντέλο Διακυβέρνησης Προστασίας Προσωπικών Δεδομένων σε **4 Πυλώνες**

- **Οργάνωση**
- **Μέτρα**
- **Άνθρωποι**
- **Τεχνολογία**

που πρέπει να δώσετε ιδιαίτερη έμφαση για να έχετε τα καλύτερη προστασία προσωπικών δεδομένων που συλλέγεται και διατηρείτε στην εταιρεία σας.



EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

Data Protection Day • 28 January 2016

Don’t throw out the baby…

- Συμμόρφωση με τον GDPR.
- Συμμόρφωση με τις επιταγές της ηθικής.
- Ανταγωνιστικό πλεονέκτημα.
- Άντληση (εμπορικής αξίας).

Όμιλος AQS

AQS

Advanced Quality Services Ltd.
ΣΥΜΒΟΥΛΟΙ ΕΠΙΧΕΙΡΗΣΕΩΝ

Abpm

Advanced Business Process Management

iBcl

Innovative Business
Consulting & Learning

TQM
Training

APPLIED
PROFESSIONAL
TRAINING

ΣΥΝΤΟΜΗ ΠΑΡΟΥΣΙΑΣΗ AQS

- Η εταιρεία Advanced Quality Services Ltd. ιδρύθηκε το **Νοέμβριο του 1993**.
- Είναι στελεχωμένη με δυναμικό συμβούλων υψηλής τεχνογνωσίας, που διαθέτει μακρόχρονη εμπειρία σε διευθυντικές θέσεις διεθνών και ελληνικών επιχειρήσεων.
- Έχει αποκτήσει σημαντική συμβουλευτική εμπειρία πραγματοποιώντας περισσότερα από **800 οργανωτικά Έργα** σε επιχειρήσεις και οργανισμούς του **Ιδιωτικού** και του ευρύτερου **Δημοσίου** Τομέα.
- Έχει επίσης πολύχρονη εκπαιδευτική εμπειρία παρέχοντας υψηλού επιπέδου εκπαίδευση σε πάνω από **20.000** μεσαία και υψηλόβαθμα **στελέχη επιχειρήσεων**.

ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

Η AQS δραστηριοποιείται σε δύο περιοχές:

- Συμβουλευτικές Υπηρεσίες Οργάνωσης
- Υπηρεσίες Εκπαίδευσης & Ανάπτυξης

ΣΥΜΒΟΥΛΕΥΤΙΚΕΣ ΥΠΗΡΕΣΙΕΣ

- Επιχειρησιακός Σχεδιασμός (Business Planning) κάνοντας χρήση της καταξιωμένης μεθοδολογίας Balanced Scorecard & Strategy Maps.
- Ανασχεδιασμός (Reengineering) - Συστήματα Ποιότητας – Αποδοτικότητας.
- Σχεδιασμός και Ανάπτυξη Συστημάτων Διαχείρισης σύμφωνα με τα Πρότυπα ISO 9001, ISO 14001, ISO 22000 (HACCP), ΕΛΟΤ 1429, OHSAS 18001, ISO 13485, ISO 20121, ISO 20000, ISO 39001, ISO 17025, ISO 17020, ISO 17065, ISO 15189, ISO 50001 κ.α.
- Σχεδιασμός και Ανάπτυξη Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών - ISO 27001, Ασφάλειας Προσωπικών Δεδομένων - GDPR Compliance, Υπηρεσίες DPO κ.α.
- Σχεδιασμός και Υλοποίηση Συστημάτων Διαχείρισης & Βελτίωσης της εφοδιαστικής αλυσίδας.

Η ΕΜΠΕΙΡΙΑ ΤΗΣ ΕΤΑΙΡΕΙΑΣ ΜΑΣ ΣΤΑ ΕΡΓΑ GDPR

AQS
Advanced Quality Services Ltd.
ΣΥΜΒΟΥΛΟΙ ΕΠΙΧΕΙΡΗΣΕΩΝ

Η **AQS** είναι **πρωτοπόρος** εταιρεία στην Υποστήριξη Οργανισμών για τη συμμόρφωσή τους με τον GDPR και έχει εκπαιδεύσει πληθώρα στελεχών στο αντικείμενο αυτό (ενδεικτικά αναφέρονται οι Οργανισμοί:

ΟΤΕ ΑΕ, ΤΡΑΠΕΖΑ ΤΗΣ ΕΛΛΑΔΟΣ Α.Ε, FOURLIS A.E., ΦΑΡΜΑΣΕΡΒΛΙΛΛΥ ΑΕΒΕ, ΑΒ ΒΑΣΙΛΟΠΟΥΛΟΣ, FCABANK, ΕΥΡΩΠΑΪΚΗ ΠΙΣΤΗ Α.Ε.Γ.Α., GM HELLAS SA, ΜΕΓΑ ΑΕ, ACTIONAID ΕΛΛΑΣ, MARINE TRUST Ltd, AEGEAN BALTIC BANK, ΚΡΕΤΑΦΑΡΜ ΑΒΕΕ, ΕΤΑΙΡΕΙΑ ΑΚΙΝΗΤΩΝ ΔΗΜΟΣΙΟΥ ΑΕ, ΑΧΑ ΑΣΦΑΛΙΣΤΙΚΗ, ΕΘΝΙΚΟ ΚΤΗΜΑΤΟΛΟΓΙΟ & ΧΑΡΤΟΓΡΑΦΗΣΗ ΑΕ, SUPERFAST FERRIES SA κα.)

ενώ έχει υλοποιήσει και αντίστοιχα συμβουλευτικά Έργα.

Επιπλέον, έχει υλοποιήσει σημαντικά Έργα Compliance Management αυστηρότατων απαιτήσεων, καθώς και εφαρμογές παρεμφερών συστημάτων, όπως το **ISO 27001** (Πρότυπο για την Ασφάλεια Πληροφοριών).

Η ΟΜΑΔΑ ΜΑΣ

Επικεφαλής του αντίστοιχου Business Unit της AQS (και των Ομάδων Έργου) είναι ο **Ιωάννης Κυριαζόγλου**, με 42 έτη εμπειρία και διεθνή δραστηριότητα σε έργα Πληροφορικής σε Ηνωμένες Πολιτείες, Καναδά και Μέση Ανατολή, ενώ διαθέτει πλούσιο συγγραφικό Έργο.

https://goo.gl/qERUw7

HALCOR
ΕΛΛΗΝΙΚΑ ΠΕΤΡΕΛΑΙΑ
JANSSEN-CILAG
BINGO
Tottis QUALITY
TOSOH
BIOTEP
ALUMIL
Building excellence every day
ThyssenKrupp Marine Systems
The Chemistry of Innovation
EUROPA
ALUMINUM SYSTEMS
APIVITA
ΜΟΤΟΡ ΟΤΑ (ΕΛΛΑΣ)
ΔΙΥΛΙΣΤΗΡΙΑ ΚΟΡΙΝΘΟΥ Α.Ε.
mitsubishi
Calda ENERGY
polyeco
waste management
BiC
FAMAR
HEALTH CARE SERVICES
CABLEL®
Holiday Inn
HOTELS - RESORTS
Gerolymatos
ΟΜΙΛΟΣ ΕΤΑΙΡΕΙΩΝ
ST. JUDE MEDICAL
MORE CONTROL. LESS RISK.
friesland foods
ΟΜΙΛΟΣ ΕΠΙΧΕΙΡΗΣΕΩΝ ΣΑΡΑΚΑΚΗ
AKTOR
Eurobank EFG
cybarco
GENESIS pharma
kosmocar
Mercedes-Benz
MINOAN LINES
RILKEN
ΠΕΡΙΦΕΡΕΙΑ ΒΟΡΕΙΟΥ ΑΙΓΑΙΟΥ
elounda bay palace
Enel Green Power
Ι. ΛΑΔΑΚΗΣ Α.Ε.
ΤΣΜΕΔΕ
Δήμος Αμαρουσίου
HELLENIC SHIPYARDS S.A.
SKARAMANGA YARD
ICAP
GROUP
ΠΕΡΙΦΕΡΕΙΑ ΗΠΕΙΡΟΥ
HELLENIC REPUBLIC REGION OF EPIRUS
ΕΥΔΑΠ
ΕΛΤΑ
ΚΤΗΜΑΤΟΛΟΓΙΟ Α.Ε.
Pharmathen
ΔΗΜΟΣ ΑΘΗΝΑΙΩΝ
NEOPLAN
ΕΒΡΟ ΦΑΡΜΑ
ΣΥ.ΦΑ ΘΕΣΣΑΛΟΝΙΚΗΣ
ΟΜΙΛΟΣ ΕΠΙΧΕΙΡΗΣΕΩΝ
aldemar
HOTELS & SPA
YALCO
ΣΩΚΡΑΤΗΣ Α. ΚΩΝΣΤΑΝΤΙΝΟΥ & ΥΙΟΣ Α.Ε.
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΕΣΩΤΕΡΙΚΩΝ

AQS
Advanced Quality Services Ltd.
ΣΥΜΒΟΥΛΟΙ ΕΠΙΧΕΙΡΗΣΕΩΝ

Μπορούμε να βοηθήσουμε

- TRAINING (Ανοικτά Σεμινάρια & Ενδοεπιχειρησιακά)
- AUDIT (Έλεγχος, Διάγνωση και Ανάλυση)
- GDPR (Ολοκληρωμένο Σύστημα Συμμόρφωσης)
- DPO (Υπηρεσίες και Πιστοποίηση)

Article 83
General conditions for imposing administrative fines

Crossreferencing of articles within the GDPR, created by Institute of Management for Information Systems, 2016