COSMOS BUSINESS SYSTEMS AEBE

TURN Key SOLUTIONS

30 YEARS Your IT Business Partner

GDPR/ISO27001

GDPR & SECURITY CONSULTING SERVICES

By

Cosmos Business Systems

Τι είναι το GDPR ;

Ο Ευρωπαϊκός Κανονισμός 2016/679 (General Data Protection Regulation, GDPR) ψηφίστηκε στις 27.04.2016 και τίθεται σε υποχρεωτική εφαρμογή για όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης στις 25.05.2018, διαμορφώνοντας ένα ενιαίο νομικό πλαίσιο. Ο νέος κανονισμός αυξάνει τις υποχρεώσεις των επιχειρήσεων, ενώ το μέγεθος των προβλεπόμενων προστίμων είναι μεγάλο.

Το αντικείμενο του Γενικού Κανονισμού η διαμόρφωση νομικού πλαισίου για την επεξεργασία προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση, με μία σειρά περιορισμών και νέων υποχρεώσεων στις επιχειρήσεις σχετικά με:

- την επεξεργασία των προσωπικών δεδομένων, από τη συλλογή έως και την καταστροφή τους
- τη δυνατότητα μεταφοράς τους σε άλλες χώρες
- την προστασία των δικαιωμάτων των φυσικών προσώπων
- την ασφάλεια (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα) των προσωπικών δεδομένων και
- τις ενέργειες γνωστοποίησης που οφείλει να κάνει η επιχείρηση σε περίπτωση παραβίασης.

Σε περίπτωση παράβασης προβλέπονται σημαντικά αυξημένα πρόστιμα, που ανάλογα με το είδος και το μέγεθός της, φθάνουν έως τα 20 εκατομμύρια ευρώ ή το 4% του παγκόσμιου ετήσιου κύκλου εργασιών.

Το πλεονέκτημα μας βασίζεται στην ικανή τεχνική ομάδα και στην διαδικασία παρακολούθησης των σχετικών υποδομών πελατών μας.

Τι προσφέρουμε;

- ISO27001 driven GDPR compliance
- ISO27001 Consulting Services (Εκπαίδευση, εργαλεία, διαδικασίες)
- Regulatory compliance & Νομικές Υπηρεσίες
- Internal Audits και Vulnerability Assessments
- Performance Monitoring και KPIs (NMS outsourced & on-premise)

Διαδικασία Ελέγχου και Εφαρμογής GDPR και ISO27001

- Καταγραφή των δεδομένων που υπάρχουν αποθηκευμένα στην υποδομή
- Ενδελεχής έρευνα και καταγραφή διαδικασιών και διεργασιών στις οποίες θα εφαρμοστούν τα πρότυπα και οι κανονισμοί. Πραγματοποίηση GAP Analysis (σελ. 8)
- Επιλογή των κατάλληλων Controls και διαδικασιών από το ISO27001 προς εφαρμογή
- Προτάσεις για λογισμικό και υπηρεσίες που θα βελτιώσουν το GDPR Compliance.
- Μελέτη Ρίσκων και DPIA
- Εγκατάσταση & παραμετροποίηση λογισμικού για την κάλυψη του προτύπου
- Εκπαίδευση σε κάθε στάδιο σχεδιασμού κ υλοποίησης

AUDIT

Βασικοί Έλεγχοι πρόσβασης & Διαφάνειας

- Καταγραφή εταιρικών διαδικασιών σε σχέση με σχετικά πρότυπα προστασίας δεδομένων
- Καταγραφή δεδομένων και τρόπου επεξεργασίας τους
- Ανασκόπηση υφιστάμενων εσωτερικών & εξωτερικών δυνατοτήτων για Reporting προσωπικών δεδομένων
- Εσωτερικός έλεγχος για την επίγνωση των κανόνων σχετικά με την προστασία προσωπικών δεδομένων

ΣΧΕΔΙΑΣΜΟΣ

Σχεδιασμός μοντέλου και βημάτων υλοποίησης

- Σχεδιασμός πολιτικών προστασίας δεδομένων και περιγραφή ιδανικών διαδικασιών επεξεργασίας τους
- Εσωτερική Εκπαίδευση και επικοινωνία των νέων κανόνων
- Σχεδιασμός εσωτερικής αναφοράς προς την διοίκηση καθώς κ προς ρυθμιστικούς φορείς

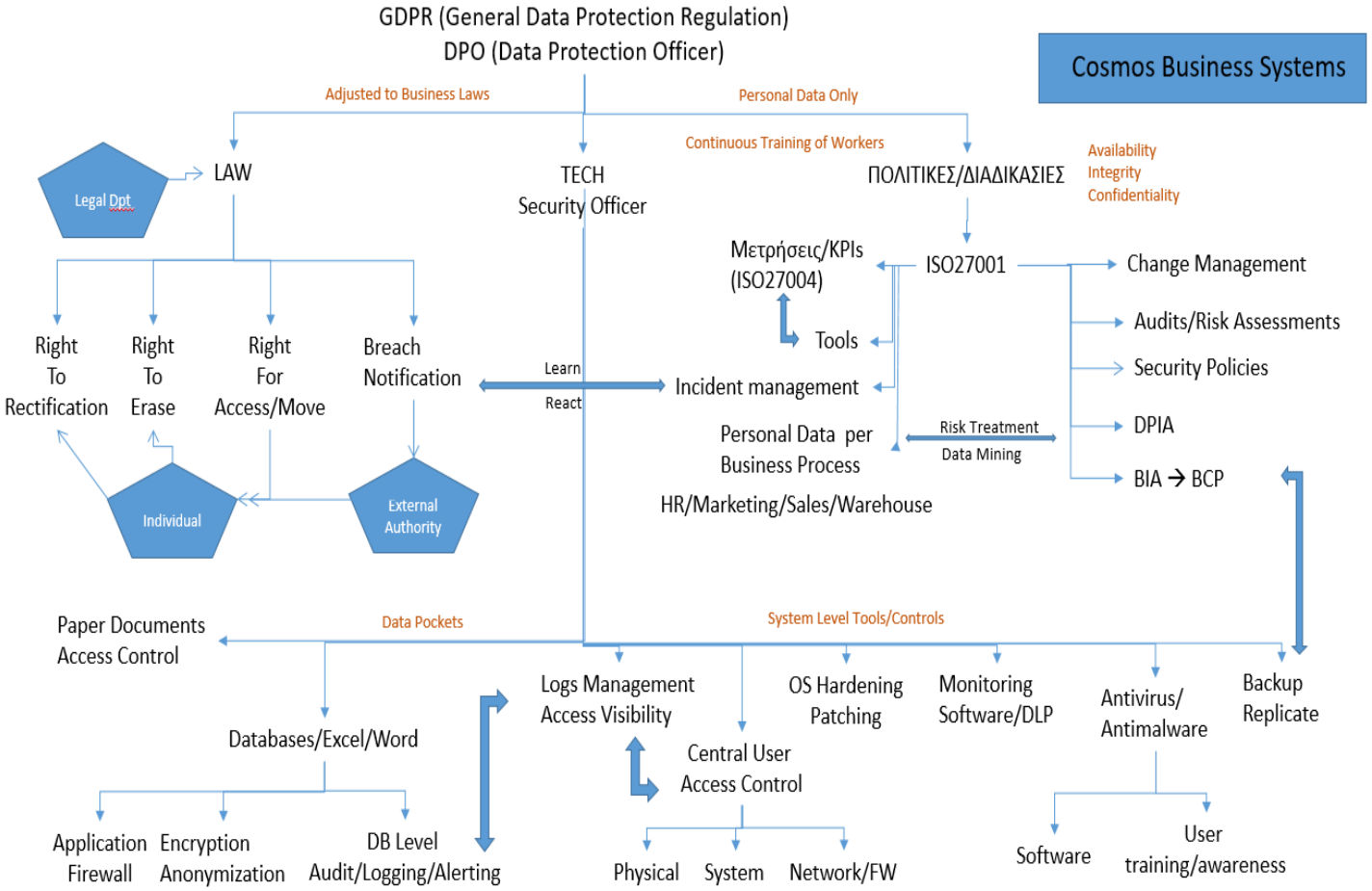
ΥΛΟΠΟΙΗΣΗ

Εφαρμογή & υποστήριξη διαδικασιών

- Εφαρμογή λειτουργικού μοντέλου για προστασία δεδομένων
- Περαιτέρω εταιρική εκπαίδευση σχετικά με την προστασία δεδομένων

ΠΕΡΙΓΡΑΦΗ ΥΠΗΡΕΣΙΩΝ
ISO 27001/ GDPR CONSULTING

Σχέδιο Δράσης – Ενοποίηση GDPR και ISO27001



Βήματα προετοιμασίας για GDPR

1. Ενημέρωση

Ενημέρωση των βασικών στελεχών σχετικά με τις νομοθετικές αλλαγές του ευρωπαϊκού κανονισμού.

2. Αρχείο των δραστηριοτήτων επεξεργασίας

Τεκμηρίωση των διαδικασιών επεξεργασίας καθώς και το είδος των προσωπικών δεδομένων σε έντυπη και ηλεκτρονική μορφή.

3. Πολιτική Προστασίας Προσωπικών Δεδομένων

Έλεγχος και επανασχεδιασμός της δημοσιευμένης πολιτικής προστασίας προσωπικών δεδομένων.

4. Δικαιώματα των υποκειμένων

Έλεγχος των διαδικασιών ώστε να καλύπτουν τα δικαιώματα των υποκειμένων όπως διαγραφή, τροποποίηση κ.λπ.

5. Συμβάσεις με εκτελούντες την επεξεργασία

Έλεγχος και τροποποίηση των συμβάσεων με εκτελούντες την επεξεργασία ώστε να καλύπτει τα απαραίτητα άρθρα του κανονισμού.

6. Συγκατάθεση των υποκειμένων

Επανασχεδιασμός του τρόπου λήψης συναίνεσης και ανανέωση των υφιστάμενων συναινέσεων που δεν καλύπτουν το GDPR.

7. Παραβίαση Ασφάλειας Προσωπικών δεδομένων

Σχεδιασμός και υλοποίηση συστήματος διαχείρισης απειλών 24x7x365 και ανάπτυξη της διαδικασίας αναφοράς συμβάντος παραβίασης προς την αρμόδια αρχή και τα υποκείμενα.

8. Υπεύθυνος Προστασίας Δεδομένων (Data Protection Officer)

Ανάθεση σε φυσικό πρόσωπο της ιδιότητας του DPO και τοποθέτηση του ρόλου του στο σχετικό εταιρικό οργανόγραμμα.

9. Διεθνής Παρουσία Εταιρίας

Σε περίπτωση διεθνής παρουσίας σε άλλη χώρα της EU θα πρέπει να οριστεί ο κύρια υπεύθυνος για την παρακολούθηση του GDPR κανονισμού.

GDPR Compliance
Initial Audit & Evaluation Steps

- **Φάση Εκπαίδευσης & παρουσίασης ερωτηματολογίων**

Βασική εκπαίδευση στον κανονισμό GDPR μέσω γενικής περιγραφής κ ανάλυσης των ερωτημάτων, παρουσία των BU Managers ανά Business Service (Sales, Marketing, HR, Technical, Warehouse, Developers /LAB, κλπ.)

- **Φάση γενικής κατανόησης των εταιρικών διαδικασιών**

  - ❖ Συνεντεύξεις με BU Managers ανά Business process και συλλογή στοιχείων σχετικά με τις εταιρικές διεργασίες & ρόλους. Επιπλέον ανάλυση όπου υπάρχει συσχέτιση με προσωπικά δεδομένα.
  - ❖ Από κοινού συμπλήρωση πινάκων για το είδος των δεδομένων, την σημασία τους κ την επεξεργασία τους (Data Inventory) βάση λίστας παραδειγμάτων Personal Data.
  - ❖ Καταγραφή της δικτυακής τοπολογίας, DMZ & network devices, ασύρματα δίκτυα, firewalls κλπ.
  - ❖ Καταγραφή των διαδικασιών πρόσβασης στα συστήματα και δίκτυα (Active Directory, SSO, κλπ.)
  - ❖ Καταγραφή συστημάτων ελέγχου φυσικής πρόσβασης στον χώρο (κάρτες, video, Access Control, καλωδιώσεις, κλπ.)

- **Εργασίες πελάτη (σε συνεργασία όπου απαιτείται με την CBS)**

  - ➢ Σε βάθος συμπλήρωση του αρχικού ερωτηματολογίου Audit και αναλυτική περιγραφή των διαδικασιών ανά Business Unit & Service
  - ➢ Συμπλήρωση του ερωτηματολογίου Gap1 (Procedures & General + Software used)
  - ➢ Συμπλήρωση του ερωτηματολογίου Gap2 (MS Systems)
  - ➢ Συμπλήρωση του ερωτηματολογίου Data Mining ανά Business Process & Service (Bus & web sites/portals)

- Καταγραφή κ αναλυτική περιγραφή διαδικασίας τυχόν μεταφοράς δεδομένων από και προς τρίτα συστήματα
- Ενημέρωση προς την Cosmos των πολιτικών ασφάλειας καθώς κ των οδηγιών εργασίας που αφορούν γενικές διαδικασίες CIA (Continuity, Integrity, Availability) όπως backup procedures, Redundancy, laptop/mobile disposal κλπ.

- **Παραδοτέα**

- ✓ Πίνακας καταγραφής γενικών ευπαθειών, πιθανός κίνδυνος κ τρόπος επίλυσης/κάλυψης βάση της μεθοδολογίας των παραπάνω φάσεων.
- ✓ Συνοπτική μελέτη τοπολογίας κ τρωτότητας δικτύου LAN & WAN σε σχέση με τον διαχωρισμό κ την κατάτμηση του.
- ✓ Αναφορά κινδύνων κ προτάσεις ανασχεδιασμού σχετικά με την σύνδεση με εξωτερικά δίκτυα καθώς κ προστασία των σχετικών web portals.
- ✓ Τα παραπάνω ερωτηματολόγια επεξεργασμένα κ σε συσχέτιση με το σύνολο των επιπλέον καταγραφών και ευπαθειών.

- **Προτεινόμενα προϊόντα ανά κατηγορία**

1) ManageEngine Servicedesk, Quest K1000 καλύπτουν τα παρακάτω:
   - Asset management & CMDB
   - Incident Management
   - Configuration & Change Management
   - Reporting
2) PRTG , Solarwinds NPM/APM, ManageEngine Application manager
   - Γενική παρακολούθηση υποδομής (NMS), Network & Application Mapping
   - Παρακολούθηση εφαρμογών (Databases, Mail Servers, κλπ.)
   - Alerting & Reporting
3) ManageEngine Event Analyzer, Solarwinds Log Manager καλύπτουν SIEM services:
   - Log & Event correlation
   - Windows Events & Threats
   - File & Database Access
   - Alerting & Reporting
4) ManageEngine ADManager & AD Audit, Quest File Explorer καλύπτουν τα :
   - User access
   - Active Directory Alerting & Audit
   - File Access Auditing
   - Reporting
5) Εξειδικευμένες λύσεις Data Classification & Data Loss Prevention (DLP) μέσω συνεργατών
6) Κλασικές λύσεις Veritas Backup Exec, Antivirus Symantec SEP, Cisco Wireless Controller & ISA Authenticator όπως ήδη προσφέρονται από το εταιρικό portfolio

Τι είναι Gap Analysis;

Η Cosmos Business Systems προχωρά σε υλοποίηση GAP Analysis με βάση την υπάρχουσα βάση των IT Assets καθώς κ με σειρά συνεντεύξεων με τα σχετικά τμήματα πληροφορικής του πελάτη.

Ακολουθεί ως παραδοτέο και το σχετικό πλάνο ενεργειών το οποίο θα παραδοθείς τον πελάτη αναλυτικά
Η όλη διαδικασία βασίζεται κυρίως στο πρότυπο ISO27001 με γνώμονα κ τον Ευρωπαϊκό κανονισμό GDPR 2016/679.

α. Καταγραφή IT υποδομής

Κατά την διαδικασία καταγραφής της υποδομής θα δοθούν από το IT όλα τα απαραίτητα τεχνικά στοιχεία που την αποτελούν, ώστε να γίνει κατανοητό στον σύμβουλο το μέγεθος κ η πολυπλοκότητα της.

Ποιο συγκεκριμένα θα ζητηθούν τα παρακάτω CI assets που επεξεργάζονται τα ΠΔ:

- Λίστα των υπολογιστών με λειτουργικό σύστημα κ εφαρμογές προστασίας
- Λίστα των servers με λειτουργικό σύστημα, εφαρμογές κ ρόλο στην επιχειρηματική λειτουργικότητα.
- Χάρτης δικτύου (topology map) του συνόλου της υποδομής
- Περίληψη των ειδικών εφαρμογές που καλύπτουν της επιχειρηματικές ανάγκες (ERP/CRM, portal κλπ.)

Παρόλο που θα εξεταστεί το σύνολο της IT υποδομής έμφαση κ εξειδίκευση θα δοθεί στα σημεία που γίνεται επεξεργασία ΠΔ (συλλογή, αποθήκευση, μεταβίβαση) καθώς η συγκεκριμένη μελέτη αφορά τον GDPR Ευρωπαϊκό κανονισμό.

β. Αξιολόγηση της IT υποδομής σε σχέση με την Ασφάλεια δεδομένων

Πέρα από την συλλογή κ αξιολόγηση των IT Assets (από τις παραπάνω λίστες κ καταγραφές) θα πρέπει να αξιολογηθεί η ασφάλεια της IT υποδομής ως σύνολο κ με βάση τις διεργασίες που εκπληρώνει στα ΠΔ.
Έτσι θα αποτυπωθούν πολύ καλύτερα οι πιθανές ευπάθειες ώστε να γίνουν κ οι ανάλογες προτάσεις.

Η αξιολόγηση αυτή θα βασιστεί σε συνεντεύξεις του συμβούλου με την υπεύθυνη ομάδα πληροφορικής στις οποίες θα γίνει ανασκόπηση των λιστών υλικού κ λογισμικού.
Επίσης, Θα αξιολογηθεί η δικτυακή λειτουργία βάση της ροής των ΠΔ και, όπου είναι δυνατό, θα ζητηθούν πληροφορίες κ για εφαρμογές τρίτων κατασκευαστών.
Θα γίνει επισκόπηση των διαδικασιών ασφάλειας και θα υπάρχει η σχετική μεταφορά τεχνογνωσίας όπου είναι εφικτό.

Οι ενότητες που θα εξεταστούν αφορούν:

- Πολιτικές IT Ασφάλειας
- Διαχείριση υλικού και μέσων πληροφορικής
- Ασφάλεια βάσεων Δεδομένων
- IT Access Control & Authentication
- Φυσική Ασφάλεια (σε χώρους IT υποδομής)
- IT Technical Procedures & Support
- Responsibilities & Job tasks
- EndPoint Security
- Network Security
- Application Access & Control
- Cloud Operations

Στο τέλος της αξιολόγησης κ στα πλαίσια του IT Security GAP Analysis θα δοθούν και οι σχετικές συστάσεις για διορθώσεις σε επίπεδο τεχνολογίας (και όχι συγκεκριμένου προϊόντος ή εφαρμογή του σχεδιασμού και υλοποίησης του). Τυχόν υλοποίηση των βελτιώσεων ή/και προμήθεια επιπλέον λογισμικού/υλικού αφορά την επόμενη φάση κ είναι εκτός του πλαισίου του GAP Analysis.

STRATEGIC COMMITMENT ON SECURITY SERVICES

Το πλεονέκτημα μας βασίζεται στην ικανή τεχνική ομάδα και στην διαδικασία παρακολούθησης των σχετικών υποδομών πελατών μας.

- Για την Cosmos η βασική ιδέα βρίσκεται στην ενοποίηση διαδικασιών ISO27001 και νομοθεσίας GDPR ώστε να σχεδιαστεί ένα αποτέλεσμα που θα καλύπτει ολοκληρωμένα την ασφάλεια πληροφοριακών συστημάτων.

- Η εξειδικευμένη τεχνική ομάδα μας παρακολουθεί τις εξελίξεις στον τομέα και συνδυάζει τις διαθέσιμες επιλογές για το καλύτερο αποτέλεσμα στην προστασία προσωπικών δεδομένων.

Καλέστε μας για οποιαδήποτε πληροφορία ή παρουσίαση στον χώρο σας:

κ. Άρης Χατζηπαπάς
Security & Compliance Officer, ISO27001 Lead Auditor
hatjipapasa@cbs.gr

Τηλ. +30 210 6492800 Fax: +30 210 6464069 www.cbs.gr