BUILDING SOLID SUCCESS | bss

Εταιρική Παρουσίαση

ΠΟΛΙΤΙΚΕΣ ΚΑΙ ΔΙΑΔΙΚΑΣΙΕΣ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

ΜΑΪΟΣ 2018

General Data Protection Regulation

Τι είναι ο Κανονισμός Προστασίας Προσωπικών Δεδομένων (GDPR)

Προσωπικά δεδομένα (που οδηγούν σε ΤΑΥΤΟΠΟΙΗΣΗ)

- Ιατρικά – Θρησκευτικά – Πολιτικά κ.ά. **Ευαίσθητα προσωπικά δεδομένα**
- Ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση κ.λ.π. **Αναγνώριση προσώπου**
- Οικονομική κατάσταση
- Εκπαίδευση, προϋπηρεσία
- Ενδιαφέροντα, δραστηριότητες, συνήθειες
- IP Address, e-mail, internet cookies

Παραβίαση προσωπικών δεδομένων

Οποιαδήποτε παραβίαση η οποία οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη αποκάλυψη ή επιτρέπει αθέμιτη πρόσβαση σε προσωπικά δεδομένα τρίτου. Ακόμη και η απώλεια δυνατότητας πρόσβασης θεωρείται παραβίαση.

Παραδείγματα:

- Ελεύθερη φωτογράφηση
- Τηλεφωνικές ενημερώσεις / πληροφορίες
- Μισθοδοσία
- Χρεώσεις / τιμολογήσεις
- IBAN
- Βιομετρικά στοιχεία
- Ιατρικά στοιχεία

Θεμελιώδεις Αρχές του GDPR

- Αρχή της Νομιμότητας της Επεξεργασίας
- Αρχή του Περιορισμού του Σκοπού
- Αρχή της Ελαχιστοποίησης των Δεδομένων
- Αρχή της Ακρίβειας των Δεδομένων
- Αρχή του Περιορισμού της Περιόδου Τήρησης των Δεδομένων
- Αρχή της Ακεραιότητας & της Εμπιστευτικότητας των Δεδομένων
- Αρχή της Λογοδοσίας του Υπεύθυνου Επεξεργασίας

Θεμελιώδεις Αρχές του GDPR - Επεξήγηση

Αρχή της Νομιμότητας της Επεξεργασίας

Η ρητή συγκατάθεση του υποκειμένου των δεδομένων για την επεξεργασία τους.

Απαιτείται έγγραφη και ενυπόγραφη συγκατάθεση των πελατών μας για τη συλλογή και περαιτέρω επεξεργασία των δεδομένων τους.

Θεμελιώδεις Αρχές του GDPR - Επεξήγηση

Αρχή του Περιορισμού του Σκοπού

Τα δεδομένα συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο με τους σκοπούς αυτούς.

Απαιτείται η επιχείρηση να συλλέγει μόνο τα δεδομένα που είναι απαραίτητα για το σκοπό για τον οποίο χρειάζονται.

Θεμελιώδεις Αρχές του GDPR - Επεξήγηση

Αρχή της Ελαχιστοποίησης των Δεδομένων

Τα δεδομένα που συλλέγονται πρέπει να είναι κατάλληλα, συναφή και να περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία.

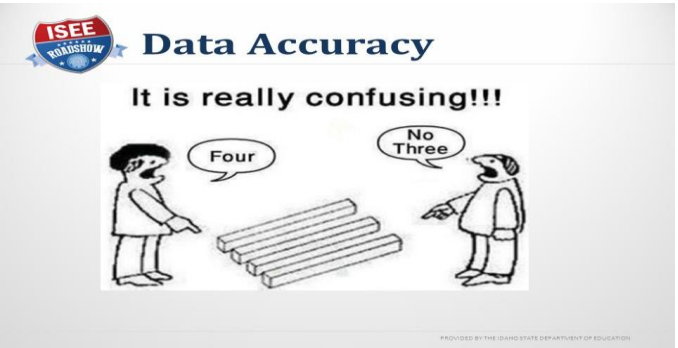
Ζητάμε και συλλέγουμε μόνο όσα δεδομένα μας χρειάζονται για το σκοπό για τον οποίο τα προορίζουμε.

Θεμελιώδεις Αρχές του GDPR - Επεξήγηση

Αρχή της Ακρίβειας των Δεδομένων

Τα δεδομένα που συλλέγονται πρέπει να είναι ακριβή και, όταν είναι αναγκαίο, να επικαιροποιούνται.

Πρέπει να λαμβάνουμε όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων που είναι ανακριβή σε σχέση με το σκοπό επεξεργασίας τους.



Θεμελιώδεις Αρχές του GDPR- Επεξήγηση

Αρχή του Περιορισμού της Περιόδου Τήρησης των Δεδομένων

Τα δεδομένα που συλλέγονται πρέπει να είναι ή/και να διατηρούνται μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας.

Δεν συνεχίζουμε να τηρούμε δεδομένα όταν έχει παρέλθει το απαιτούμενο διάστημα για το σκοπό της επεξεργασίας τους.

ΕΞΑΙΡΕΣΗ: - Αρχειοθέτηση για δημόσιο συμφέρον Επιστημονική ή Ιστορική Έρευνα Νομοθεσία

Θεμελιώδεις Αρχές του GDPR - Επεξήγηση

Αρχή της Ακεραιότητας & Εμπιστευτικότητας των Δεδομένων

Τα δεδομένα υποβάλλονται σε επεξεργασία με τρόπο που εγγυάται την ασφάλειά τους.

Λαμβάνουμε όλα τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία των δεδομένων από μη εξουσιοδοτημένο χρήστη, από παράνομη επεξεργασία, τυχαία απώλεια, καταστροφή ή φθορά κλπ.

Θεμελιώδεις Αρχές του GDPR - Επεξήγηση

Αρχή της Λογοδοσίας του Υπεύθυνου Επεξεργασίας

Ο Υπεύθυνος Επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με τις επιταγές του Κανονισμού.

Δεν αρκεί να είμαστε σύννομοι, πρέπει να μπορούμε και να το αποδείξουμε.

BUILDING SOLID SUCCESS | bss

Ποιες είναι οι πολιτικές;

- Ασφάλεια Επικοινωνιών και Δικτύων (Communications and Network Security)
- Πρόσβαση Χρηστών (User Access)
- Αποδεκτή Χρήση Πληροφοριακών Συστημάτων (Acceptable Use)
- Χρήση Κρυπτογραφίας (Encryption)
- Παρακολούθηση Ασφάλειας Συστημάτων (Security Monitoring)
- Τεχνικοί Έλεγχοι Ασφάλειας (Security Testing)

Ποιες είναι οι πολιτικές;

- Διαβάθμιση & Προστασία Πληροφοριακών Πόρων (Asset Classification & Protection)
- Διαχείριση Ανθρώπινου Δυναμικού (Personnel Security)
- Ασφάλεια Διαδικτύου και Ηλεκτρονικής Αλληλογραφίας (Internet & e-mail security)
- Προστασία από Κακόβουλο Λογισμικό
- Πρόσβαση Συνεργατών (Third Party Connectivity), Φορητά Υπολογιστικά Συστήματα & Τηλε-εργασία (Mobile Computing and Teleworking)…

Ποιες είναι οι διαδικασίες;

- Λεπτομερή βήματα για χρήστες, διαχειριστές, εξωτερικοί συνεργάτες κ.λ.π. σε θέματα σχετικά με την ασφάλεια.
- Μία διαδικασία πρέπει να περιλαμβάνει:
  - Εύρος Εφαρμογής και Στόχους
  - Γεγονότα που εκκινούν τη διαδικασία events)
  - Συσχέτιση με Πολιτικές Ασφάλειας
  - Αλληλεπίδραση με άλλες διαδικασίες ή πολιτικές
  - Ρόλοι και Αρμοδιότητες εμπλεκομένων
  - Πόροι που απαιτούνται
  - Αναλυτική Περιγραφή Διαδικασίας (διαγράμματα ροής για περίπλοκα θέματα,
  - Σχετικά έντυπα και φόρμες (για την εφαρμογή της διαδικασίας)
  - Δείκτες μέτρησης αποτελεσματικότητας της διαδικασίας
  - Πρότυπα & Οδηγίες ΣΔΑΠ που σχετίζονται με τη συγκεκριμένη διαδικασία

Ασφάλεια Πληροφοριών & Είδη Παραβιάσεων

«Εμπιστευτικότητας (Confidentiality)»
Μη εξουσιοδοτημένη πρόσβαση ή τυχαία αποκάλυψη προσωπικών δεδομένων.

«Διαθεσιμότητας (Availability)»
Τυχαία ή μη εξουσιοδοτημένη πρόσβαση που οδηγεί σε απώλεια ή καταστροφή προσωπικώνδεδομένων.

«Ακεραιότητας (Integrity)»
Μη εξουσιοδοτημένη ή τυχαία αλλαγή των δεδομένων προσωπικού χαρακτήρα.

Τα 6 W's διαδικασιών

Παράδειγμα: Παρακολούθηση Ασφάλειας Συστήματος

WHO	➢	Ο διαχειριστής του συστήματος
WHAT	➢	Εξετάζει περιστατικά ασφαλείας για το σύστημα που επιβλέπει
…HOW	➢	Εξετάζοντας κάθε περιστατικό ξεχωριστά
WHEN	➢	Καθημερινά
WHERE	➢	Και συμπληρώνει τα σχετικά έγγραφα
WHY	➢	Για μελλοντική χρήση (και για έλεγχο συμμόρφωσης)

Βασικές Αρχές Ασφάλειας Πληροφοριών

① Η ανάγκη για την Ασφάλεια Πληροφοριών

② Βασικές Αρχές Ασφάλειας Πληροφοριών

③ Ασφάλεια Πληροφοριών & GDPR

④ Αξιολόγηση Κινδύνων Ασφάλειας Πληροφοριών (Risk Assessment)

⑤ Απαιτούμενα Οργανωτικά Μέτρα Ασφάλειας

⑥ Απαιτούμενα Τεχνικά Μέτρα Ασφάλειας

⑦ Συμμόρφωση με πρότυπα και βέλτιστες πρακτικές ασφάλειας

⑧ Ανάπτυξη Πλάνου Συνέχισης Επιχειρηματικών Λειτουργιών (BCP/DRP)

Ενδεικτική Διαδικασία: Διαχείριση Περιστατικών Ασφαλείας

Βασικές Αρχές | Πολιτικές | Διαδικασίες | Οδηγίες | Αρχεία

Sample Security Incident Response

Help Desk
System Admins
IT Manager
Security Officer
IR Team
• Audit, Legal, PR
Security Forum
CEO
Board of Directors

Preparation
- Policies
- Roles
- Responsibilities
- Escalation Procedure
- Tools...

Detection & Identification
- Monitoring
- Determine type & impact
- Capture Records ...

Eradication
- Kill attacker active sessions
- Delete fake files
- Eliminate backdoors
- Apply patches
- Correct improper settings ...

Corrective Actions
- Areas of improvement
- Executive summary

Security Incident

Containment
- Conduct impact assessment
- Protecting sensitive information
- Building image of compromised system

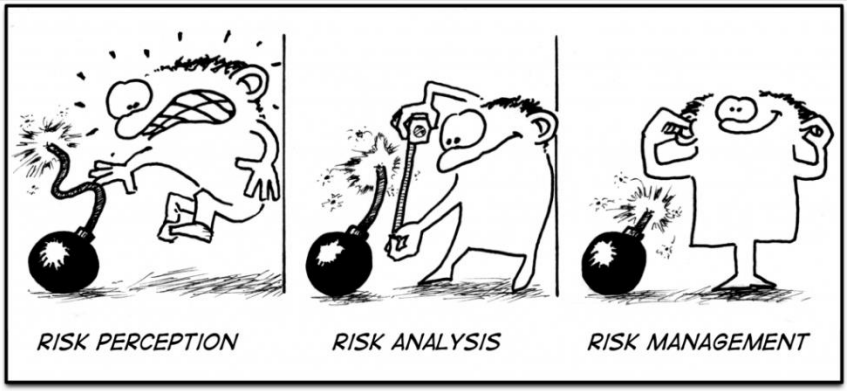
Recovery
- Damage assessment
- Re-install damaged files
- Bring up service
- Verify successful operation ...

Συνοπτικός Οδηγός Ασφάλειας & GDPR (1/2)

Άρθρα Κανονισμού/Απαιτήσεις	Προτεινόμενες Ενέργειες
Security of processing Άρθρο 32	• Εφαρμογή ενός ολοκληρωμένου Πλαισίου Διαχείρισης Κινδύνου (Risk Assessment Framework) • Υλοποίηση Οργανωτικών μέτρων ασφαλείας • Υλοποίηση Τεχνικών μέτρων ασφαλείας • Υλοποίηση Πλάνου Συνέχισης Λειτουργιών & Ανάκαμψης από Καταστροφή • Παρακολούθηση συμμόρφωσης & έλεγχος αποτελεσματικότητας τεχνικών & οργανωτικών μέτρων • Πιστοποίηση με εγκεκριμένο σχήμα αποδεικνύει συμμόρφωση
Data protection by design & by default Άρθρο 25	• Εφαρμογή των αρχών Privacy by Design & Privacy by Default με την ανάπτυξη κατάλληλων πολιτικών, διαδικασιών και εξειδικευμένων τεχνολογιών • Περιορισμός συλλογής δ.π.χ. (if you don't need it, don't keep it) • Αυστηρός έλεγχος πρόσβασης σε δ.π.χ. (need to know) • Αξιολόγηση συμμόρφωσης προμηθευτών • Πιστοποίηση με εγκεκριμένο σχήμα (οργανισμού ή/και προμηθευτών) αποδεικνύει συμμόρφωση
Breach notification Άρθρο 33, 34	• Ελαχιστοποίηση, περιορισμός πρόσβασης και κρυπτογράφηση δ.π.χ. • Ανάπτυξη οργανωτικών μέτρων ασφαλείας και υλοποίηση εξειδικευμένων τεχνολογικών μέτρων που μπορούν να αυτοματοποιήσουν τις εσωτερικές διαδικασίες • Διαρκής έλεγχος, έγκαιρος εντοπισμός, και διαχείριση περιστατικών ασφαλείας • Γνωστοποίηση περιστατικών στην Εποπτική Αρχή εντός 72 ωρών • Έγκαιρη γνωστοποίηση περιστατικών στα Υποκείμενα

Συνοπτικός Οδηγός Ασφάλειας & GDPR (2/2)

Άρθρα Κανονισμού/Απαιτήσεις	Προτεινόμενες Ενέργειες
Data protection impact assessment Άρθρο 35	• Ανάπτυξη Καταλόγου Διαβαθμισμένων Εταιρικών Πληροφοριακών Πόρων (Classified Data Inventory) όπου συμπεριλαμβάνονται τα δ.π.χ. • Εφαρμοφή ειδικευμένων μεθοδολογιών, πολιτικών και διαδικασιών για τη διεξαγωγή DPIAs ή ενσωμάτωση DPIA στο υφιστάμενο Πλαίσιο Διαχείρισης Εταιρικού Κινδύνου (Enterprise Risk Management Framework)
Data Protection Officer Άρθρο 37, 38, 39	• Καθορισμός Οργανωτικού πλαισίου Διαχείρισης Προσωπικών Δεδομένων • Καθορισμός ρόλου και αρμοδιοτήτων DPO
Compliance Άρθρο 5 (2), 24 (1), 28 (5), 30 (2), 32 (1), 32 (5), 83 (2)	• Παρακολούθηση συμμόρφωσης (συμπεριλαμβάνει τεχνικά & οργανωτικά μέτρα) με την ανάπτυξη κατάλληλων πολιτικών, διαδικασιών και εξειδικευμένων τεχνολογιών • Πιστοποίηση με εγκεκριμένο σχήμα (οργανισμού ή/και προμηθευτών) αποδεικνύει συμμόρφωση
Supplier Security Άρθρο 28, 25, 33 (2)	• Συνεχής αξιολόγηση συμμόρφωσης Εκτελούντος την Επεξεργασία & Προμηθευτών • Πιστοποίηση Εκτελούντος την Επεξεργασία & Προμηθευτών με εγκεκριμένο σχήμα αποδεικνύει συμμόρφωση
Records Management Άρθρο 30	• Ανάπτυξη Καταλόγου Διαβαθμισμένων Εταιρικών Πληροφοριακών Πόρων (Classified Data Inventory) όπου συμπεριλαμβάνονται τα δ.π.χ. • Τεκμηρίωση τεχνικών και οργανωτικών μέτρων ασφαλείας



Risk Assessment & DPO

- Γιατί πρέπει να γνωρίζω το Risk Assessment;
  - Είναι ο ακρογωνιαίος λίθος της Ασφάλειας Πληροφοριών
  - Η επιλογή των Τεχνικών & Οργανωτικών Μέτρων πρέπει να βασίζεται στα αποτελέσματά του
  - Ο DPO πρέπει να μπορεί να ερμηνεύει και να εκφέρει άποψη στα αποτελέσματά του
  - Μπορεί να απαιτηθεί η ενεργή συμμετοχή του DPO κατά τη διεξαγωγή του
  - Είναι σημαντικό εργαλείο για τον έλεγχο συμμόρφωσης του οργανισμού
- Ποιος εκτελεί το Risk Assessment;
  - Συνήθως η Διεύθυνση Ασφάλειας Πληροφοριών (CISO, ISO…)
  - Σε μερικές περιπτώσεις Διευθύνσεις Συμμόρφωσης ή/και Διαχείρισης Κινδύνου
- Ποια είναι η σχέση του Risk Assessment με το DPI;
  - Το DPIA είναι ουσιαστικά μία μεθοδολογία Risk Assessment (υποσύνολο) με κοινές αρχές και αρκετούς στόχους
  - Πολλές από τις δράσεις που απαιτούνται για το DPIA (π.χ. Καταγραφή Πόρων & Information Flow) εκπονούνται ήδη για το Risk Assessment
  - Πολλοί οργανισμοί ίσως αποφασίσουν να ενσωματώσουν το DPIA στο ευρύτερο Εταιρικό Πλαίσιο Διαχείρισης Κινδύνων (Enterprise Risk Assessment Framework)

Οργανωτικά Μέτρα Ασφάλειας

Οργανωτική Δομή Ασφάλειας Πληροφοριών

Βέλτιστες Πρακτικές Ανάπτυξης & Διαχείρισης Εγγράφων

Τεκμηρίωση ΣΔΑΠ (Εγχειρίδιο Ασφάλειας)

Πρόγραμμα Εκπαίδευσης & Επιμόρφωσης στην Ασφάλεια Πληροφοριών

Πρόγραμμα Ελέγχου Συμμόρφωσης

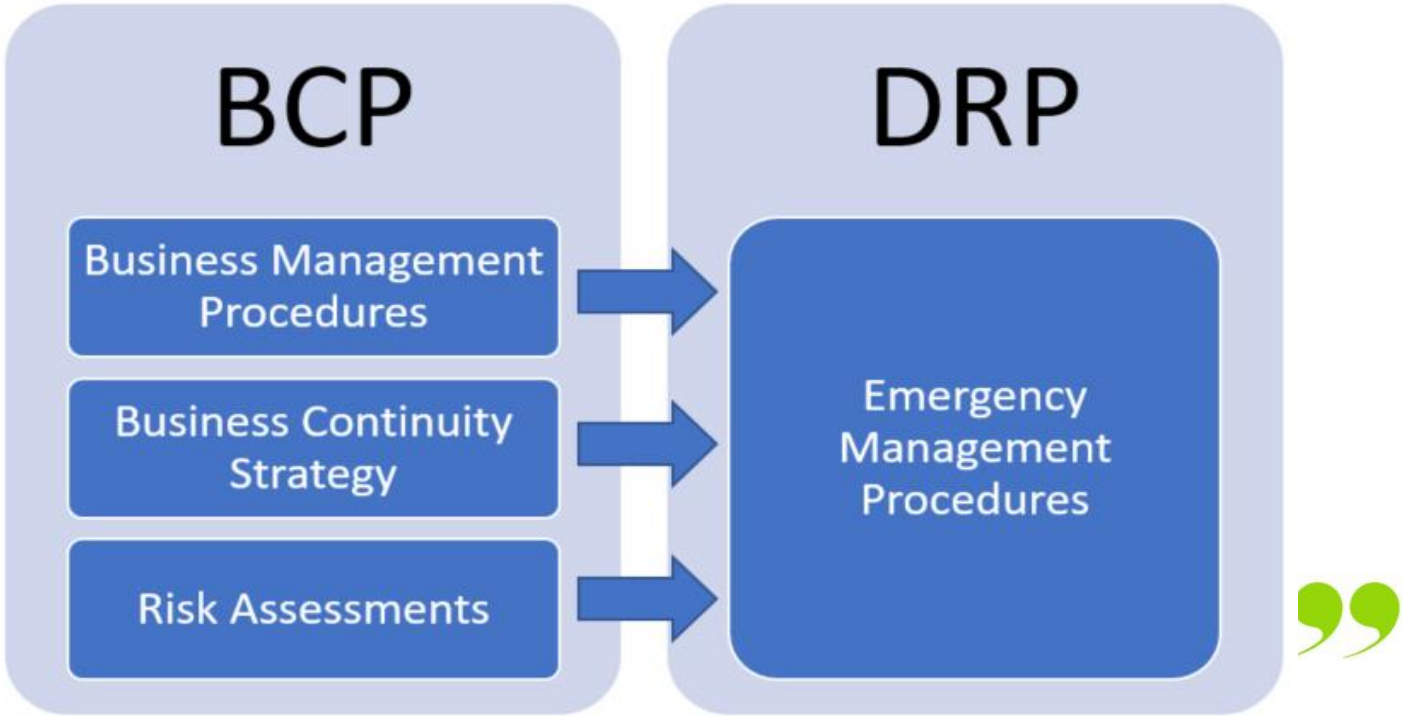
Αρχεία

- Κατά τη διάρκεια δημιουργίας και ανάπτυξης μιας διαδικασίας, ενός τεχνικού προτύπου και άλλων διεργασιών ελέγχου, πρέπει να δημιουργείται μια λίστα από απαιτούμενα αρχεία που αποδεικνύουν τη συμμόρφωση και να καθορίζεται ο τρόπος διαχείρισής τους.

- Ειδικά κατά τη σύνταξη διαδικασιών, πρέπει να δημιουργούνται φόρμες και άλλα μέσα που έχουν επιλεγεί για τη συλλογή και τη διατήρηση αρχείων.

Πλάνο Συνέχισης Επιχειρηματικών Λειτουργιών (BCP/DRP)

- Βασικές Αρχές Συνέχισης Επιχειρηματικών Λειτουργιών
- Διαδικασία Συνέχισης Επιχειρηματικών Λειτουργιών



Τα Βήματα της Διαδικασίας Επιχειρησιακής Συνέχειας

BUILDING SOLID SUCCESS | bss

start now!

Ας ξεκινήσουμε!

Ερωτήσεις;;;

BUILDING SOLID SUCCESS | bss

μικροῦ δ' ἀγῶνος οὐ μέγα ἔρχεται κλέος

Σας ευχαριστώ πολύ.

Λ. ΒΟΥΛΙΑΓΜΕΝΗΣ 51 & ΣΑΚΗ ΚΑΡΑΓΙΩΡΓΑ 104, 166 75 ΓΛΥΦΑΔΑ, **www.bssplus.gr**