GDPR
Εισαγωγική Παρουσίαση

«ΣΥΝΔΕΣΜΟΣ ΠΕΤΡΕΛΑΙΟΕΙΔΩΝ ΗΡΑΚΛΕΙΟΥ»

07/05/2018

Μανούσος Κλειδής

Senior Business Consultant

Φώτης Ρωμούδης

Senior IT Consultant

Τι είναι το GDPR (1)

Η ΕΕ για να αντιμετωπίσει τις δυσκολίες που ανακύπτουν από την αυξανόμενη μετακίνηση δεδομένων σε **Διεθνές Επίπεδο** δημιούργησε ένα νέο καθεστώς προστασίας δεδομένων - το GDPR

Το GDPR αποβλέπει στο να **εναρμονίσει το νομοθετικό καθεστώς προστασίας δεδομένων σε όλη την ΕΕ**, χωρίς προηγούμενη εθνική πράξη ενσωμάτωσης

Το **GDPR** έχει σχεδιαστεί για να αντιμετωπίσει τεχνολογικές και κοινωνικές αλλαγές που έλαβαν χώρα **τα τελευταία 20 χρόνια**, υιοθετώντας μια τεχνολογικά ουδέτερη προσέγγιση στον Κανονισμό

Τι είναι το GDPR (2)

Ο Νέος Ευρωπαϊκός Κανονισμός **2016/679** έχει τεθεί σε ισχύ στις 4 Μαΐου 2016 και θα εφαρμοστεί **ΥΠΟΧΡΕΩΤΙΚΑ** από τις **25 Μαΐου 2018**.

Ο Κανονισμός είναι ένα αναγκαίο βήμα για την ενδυνάμωση των θεμελιωδών δικαιωμάτων των πολιτών στην **ψηφιακή εποχή** και τη διευκόλυνση των επιχειρήσεων, απλοποιώντας του κανόνες για τις εταιρείες στην **Ελεύθερη Ψηφιακή Αγορά.**

Ο εν λόγω Κανονισμός δεν απαιτεί προηγουμένως συγκεκριμένη νομοθετική πράξη του Κράτους Μέλους προκειμένου να εφαρμοστεί.

Ασφάλεια Προσωπικών Δεδομένων

- Τι είναι τα δεδομένα; (data)

Τα δεδομένα είναι ένα σύνολο από σύμβολα τα οποία έχουν καταγραφεί.

- Τι είναι η πληροφορία; (information)

Πληροφορία ονομάζεται το σύνολο των δεδομένων τα οποία συνδέονται από την έννοια τους.

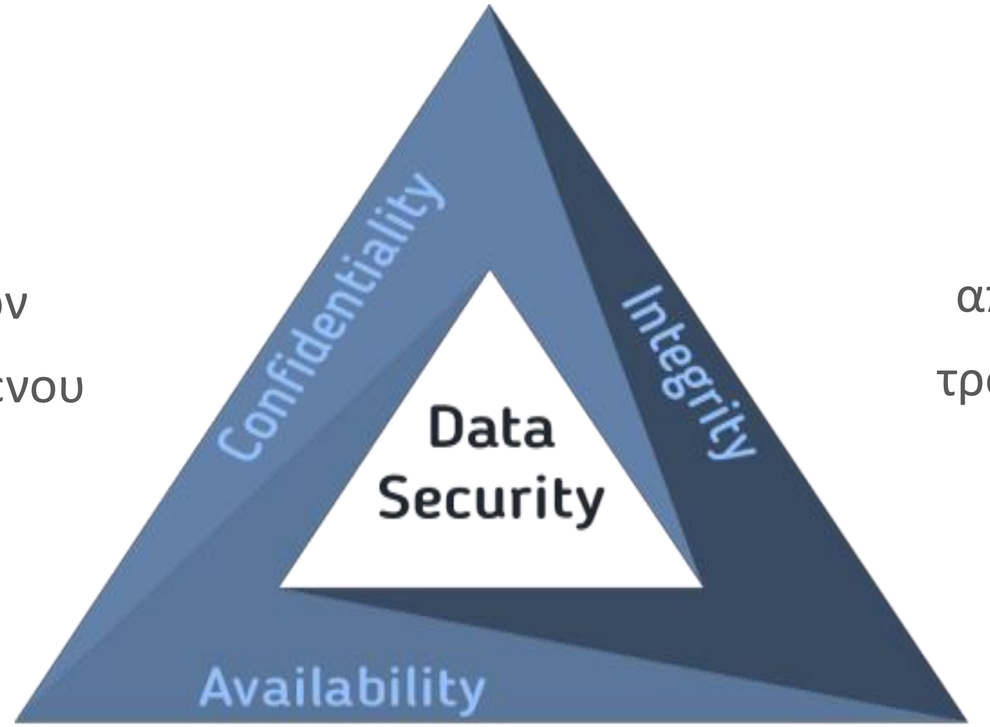
- Τι είναι τα προσωπικά δεδομένα;

Κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»). Δεδομένα όπως διευθύνσεις διαδικτυακού πρωτοκόλλου (IP), αναγνωριστικά cookies ή άλλα αναγνωριστικά στοιχεία όπως ετικέτες αναγνώρισης μέσω ραδιοσυχνοτήτων μπορούν να χρησιμοποιηθούν για την ταυτοποίηση φυσικών προσώπων.

CIA

Εμπιστευτικότητα (confidentiality)

Εμπιστευτικότητα είναι η αποκάλυψη πληροφοριών χωρίς την άδεια του υποκειμένου



Ακεραιότητα (integrity)

Ακεραιότητα ονομάζεται η αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας

Διαθεσιμότητα (availability)

Διαθεσιμότητα δεδομένων ονομάζεται η αποφυγή της καθυστέρησης ενός εξουσιοδοτημένου υποκειμένου να αποκτήσει πρόσβαση σε πληροφορίες ή υπολογιστικούς πόρους

ΟΡΙΣΜΟΣ
Τι είναι η ασφάλεια προσωπικών δεδομένων ?
(Information Security)

Ασφάλεια προσωπικών δεδομένων
είναι η προστασία
της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας

Η απώλεια έστω και μιας από τις αρχές
της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας
αποτελεί παραβίαση
της ασφάλειας προσωπικών δεδομένων

Ποια δεδομένα πρέπει να προστατεύονται (1/2)

Τα δεδομένα προσωπικού χαρακτήρα **κάθε εν ζωή φυσικού προσώπου** (υποκείμενο δεδομένων), δηλαδή κάθε πληροφορία που αφορά ταυτοποιημένο φυσικό πρόσωπο ή κάθε πληροφορία που μπορεί **άμεσα ή έμμεσα να ταυτοποιήσει** ένα φυσικό πρόσωπο, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης ή σε στοιχεία που αφορούν τη σωματική, ψυχολογική, οικονομική ή κοινωνική κατάσταση του εν λόγω φυσικού προσώπου (προφίλ)

Ποια δεδομένα πρέπει να προστατεύονται (2/2)

Άρα **δεν αφορά** τα δεδομένα των **νομικών προσώπων** (εταιρειών κ.λπ).

Αφορά όμως τα δεδομένα μιας **ατομικής επιχείρησης** ή μιας Μονοπρόσωπης εταιρίας ή μιας που νομικά αντιμετωπίζεται ως φυσικό πρόσωπο (πχ ατομική επιχείρηση ΠΡΟΜΗΘΕΙΑΣ ΑΝΤΑΛΛΑΚΤΙΚΩΝ)

Παραδείγματα

Στοιχεία Φυσικού Προσώπου: Όνομα, Επώνυμο, Διεύθυνση σπιτιού, Διεύθυνση εργασίας, Αριθμός τηλεφώνου, Διεύθυνση ηλεκτρονικού ταχυδρομείου, Αριθμός διαβατηρίου, Αριθμός Δελτίου Ταυτότητας, Αριθμός κοινωνικής ασφάλισης, Άδεια οδήγησης, Γενετικές πληροφορίες, Ιατρικές πληροφορίες, Πολιτιστική ταυτότητα, αναρτήσεις σε ιστότοπους κοινωνικής δικτύωσης

Χρηματο-οικονομικά Στοιχεία: Στοιχεία τραπεζών / αριθμοί λογαριασμού, Αριθμός φορολογικού αρχείου, Αριθμοί πιστωτικών / χρεωστικών καρτών

Ηλεκτρονικά Μέσα: Διεύθυνση IP (περιοχή της ΕΕ), Θέση / δεδομένα GPS, Cookies, ιστορικό αναζητήσεων, συλλογή στοιχείων για συμπεριφορική διαφήμιση

Φωτογραφικό υλικό ή βιντεοσκόπηση.

Πρέπει να εφαρμόσει η εταιρεία μου το GDPR

Αν ο Οργανισμός μας επεξεργάζεται ή έχει υπό τον έλεγχό του προσωπικά δεδομένα π.χ.

1. Πελάτες
2. εργαζομένων
3. εξωτερικών συνεργατών – συνεργεία

η απάντηση είναι **«Ναι»**

Τι είναι επεξεργασία

«Κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή»

Ποιος μας εποπτεύει

Ο GDPR επιφέρει σημαντικές αλλαγές στη νομοθεσία της Ευρωπαϊκής Ένωσης για την προστασία δεδομένων σε συνεργασία με τις **υφιστάμενες εθνικές αρχές**.

Στην Ελλάδα η εθνική αρχή είναι η :

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)

Κηφισίας 1-3, Τ.Κ. 115 23, Αθήνα
Tel:+30 210 6475600 - Fax: +30 210 6475628
email: contact@dpa.gr
www.dpa.gr

Τα βασικά Δικαιώματα των Πολιτών (1/2)

Σύμφωνα με την ΑΠΔΠΧ έχουμε την υποχρέωση να διασφαλίζουμε:

Το Δικαίωμα ενημέρωσης και πρόσβασης στα δεδομένα
Δηλαδή περισσότερη και σαφέστερη ενημέρωση κατά τη συλλογή των δεδομένων για την επεξεργασία τους και για το δικαίωμα πρόσβασης σε αυτά.

Το Δικαίωμα διόρθωσης
Το δικαίωμα να μπορούν να απαιτήσουν οι πολίτες από τον υπεύθυνο επεξεργασίας τη διόρθωση ανακριβών δεδομένων καθώς και τη συμπλήρωση ελλιπών δεδομένων που τους αφορούν.

Το Δικαίωμα περιορισμού της επεξεργασίας
Ο πολίτης δικαιούται να ζητά από τον υπεύθυνο επεξεργασίας τον περιορισμό της επεξεργασίας των δεδομένων του υπό συγκεκριμένες προϋποθέσεις.

Τα βασικά Δικαιώματα των Πολιτών (2/2)

Το Δικαίωμα εναντίωσης στην επεξεργασία

Ο πολίτης έχει το δικαίωμα να αντιταχθεί στην επεξεργασία των δεδομένων του υπό συγκεκριμένες προϋποθέσεις και ιδίως όταν πρόκειται για κατάρτιση «προφίλ» ή για σκοπούς απευθείας εμπορικής προώθησης.

Το Δικαίωμα στη «λήθη»

Ο πολίτης όταν δεν επιθυμεί πλέον την επεξεργασία και διατήρηση προσωπικών του δεδομένων, έχει το δικαίωμα να ζητήσει τη διαγραφή τους, υπό την προϋπόθεση ότι τα δεδομένα του δεν τηρούνται για κάποιο συγκεκριμένο νόμιμο και δηλωμένο σκοπό.

Το Δικαίωμα στη φορητότητα των δεδομένων

Ο πολίτης δικαιούται να λάβει ή να ζητήσει τη μεταφορά των δεδομένων του, σε «μηχαναγνώσιμη» μορφή, από έναν υπεύθυνο επεξεργασίας σε άλλον υπό συγκεκριμένες προϋποθέσεις, εφόσον το επιθυμεί.

Εδαφική Εφαρμογή

Το GDPR
εφαρμόζεται σε εντός και εκτός ΕΕ οργανισμούς αν αυτοί:
(i) προσφέρουν αγαθά ή υπηρεσίες σε πολίτες της ΕΕ ή
(ii) επιβλέπουν τη συμπεριφορά των πολίτων της ΕΕ

Πολλοί οργανισμοί που δεν υπόκεινται στην
ήδη υφιστάμενη
για την προστασία δεδομένων νομοθεσία της ΕΕ,

θα υπόκεινται στο GDPR
(πχ ιδιαιτέρως οι διαδικτυακές επιχειρήσεις)

Ποιοι συμμετέχουν στην επεξεργασία

Υπεύθυνος επεξεργασίας»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα

«**Εκτελών την επεξεργασία**»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας

«**Αποδέκτης**»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, στα οποία κοινοποιούνται τα δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για τρίτον είτε όχι

Τι πρέπει να κάνουμε (1/2)

- Θα πρέπει να γνωρίζουμε **αναλυτικά τα δεδομένα** μας, τι περιλαμβάνουν, που αποθηκεύονται και πως/ποιοι τα διαχειρίζονται

- Πρέπει να αποκτήσουμε **σαφή και ακριβή συγκατάθεση** κατά την επεξεργασία των προσωπικών δεδομένων

- Θα πρέπει να είμαστε σε θέση **να «διαγράψουμε»** όλα τα δεδομένα όταν ζητηθεί από το υποκείμενο των δεδομένων

- Θα πρέπει να μπορούμε **να περιορίσουμε την πρόσβαση** στα δεδομένα μας, όταν πραγματοποιείται επεξεργασία τους

Τι πρέπει να κάνουμε (2/2)

- Θα πρέπει να μπορούμε να εκτελέσουμε **«εκτιμήσεις αντικτύπου»** σχετικά με την προστασία των προσωπικών δεδομένων.

- Σε περίπτωση παραβίασης θα πρέπει να είμαστε σε θέση να αναφέρουμε την παραβίαση δεδομένων **εντός 72 ωρών με δομημένο τρόπο.**

- Απαιτείται **συνεχής** παρακολούθηση των κινδύνων προστασίας σε **ολόκληρο** τον οργανισμό μας.

- Τέλος, θα πρέπει να αξιοποιήσουμε θετικά τον ρόλο του **Υπεύθυνου Προστασίας Δεδομένων (DPO)**

Συνέπειες Παραβίασης - Ποινές

Οι συνέπειες παραβίασης
για την προστασία δεδομένων
αυξάνονται σημαντικά υπό το GDPR,
το οποίο θέτει ένα **μέγιστο πρόστιμο** για μονομερή παραβίαση
έως **€20 εκ.**,
ή το 4% των ετήσιων παγκόσμιων εισοδημάτων

Προειδοποίηση

Επίπληξη

Αναστολή της
επεξεργασίας δεδομένων

Πρόστιμο

Έννομη Προστασία - Καταγγελία

Άρθρο 77 Δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή

«…*καταγγελία σε εποπτική αρχή, ιδίως στο κράτος μέλος στο οποίο έχει* ***τη συνήθη διαμονή του*** *ή τον τόπο εργασίας του ή τον τόπο της εικαζόμενης παράβασης, εάν το υποκείμενο των δεδομένων θεωρεί ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορά παραβαίνει τον παρόντα κανονισμό*.»

Η αρχή μας συμβουλεύει (1/3)

ΕΝΗΜΕΡΩΣΗ – ΕΤΟΙΜΟΤΗΤΑ : Ενημερώστε το ανθρώπινο δυναμικό του οργανισμού σας για τις επερχόμενες μεταβολές, υπογραμμίζοντας τις σημαντικές επιπτώσεις σε περίπτωση παραβιάσεων. Αξιολογήστε τους πιθανούς κινδύνους για τα προσωπικά δεδομένα που συλλέγετε και επεξεργάζεστε. Διαμορφώστε στρατηγική αντιμετώπισης των πιθανών κινδύνων με τεχνικά και οργανωτικά μέτρα.

ΚΑΤΑΓΡΑΦΗ: Οφείλετε να τηρείτε ειδικά αρχεία επεξεργασιών;
Αν ναι, καταγράψτε ενδελεχώς τα δεδομένα που τηρείτε και μεταβιβάζετε, τις επεξεργασίες στις οποίες προβαίνετε, τον σκοπό τους και τη νομική βάση.

ΕΛΕΓΧΟΣ ΤΗΡΗΣΗΣ ΤΗΣ ΣΥΜΜΟΡΦΩΣΗΣ: Εξετάζετε συνεχώς αν κατά την επεξεργασία των δεδομένων τηρούνται οι αρχές που διέπουν τη νόμιμη επεξεργασία των δεδομένων και αν γίνονται σεβαστά τα δικαιώματα των υποκειμένων.

Η αρχή μας συμβουλεύει (2/3)

ΕΛΕΓΧΟΣ ΣΥΓΚΑΤΑΘΕΣΗΣ: Εξετάστε τις μεθόδους για εξασφάλιση συγκατάθεσης για κάθε επιδιωκόμενο σκοπό επεξεργασίας.

ΑΝΑΘΕΩΡΗΣΗ ΠΟΛΙΤΙΚΩΝ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΔΙΑΔΙΚΑΣΙΩΝ: Επικαιροποιήστε τις διαδικασίες για τον χειρισμό των αιτημάτων και την ικανοποίηση των δικαιωμάτων των πολιτών, ιδίως ως προς τη διαγραφή δεδομένων (δικαίωμα στη λήθη) ή την παροχή τους σε αναγνώσιμο ηλεκτρονικό μορφότυπο (φορητότητα δεδομένων).

ΕΚΤΙΜΗΣΗ ΕΠΙΠΤΩΣΕΩΝ: Θα πρέπει να είστε σε θέση να εκτιμήσετε τις πιθανότητες επέλευσης κινδύνων και τις συνέπειες στα προσωπικά δεδομένα.

Η αρχή μας συμβουλεύει (3/3)

ΥΠΕΥΘΥΝΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ: Ανάλογα με τη δραστηριότητα που ασκείτε, εξετάστε αν χρειάζεται να ορίσετε «υπεύθυνο προστασίας δεδομένων»

ΠΑΡΑΒΙΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ: Υιοθετήστε μεθόδους για την ανίχνευση, την καταγραφή και τη διερεύνηση περιστατικών παραβιάσεων. Διαθέτετε διαδικασία για τις γνωστοποιήσεις παραβιάσεων προς την Αρχή και τα υποκείμενα;

ΔΡΑΣΤΗΡΙΟΤΗΤΑ ΣΕ ΠΕΡΙΣΣΟΤΕΡΑ ΚΡΑΤΗ ΜΕΛΗ: Στην περίπτωση αυτή πρέπει να προτείνετε το κράτος της κύριας εγκατάστασής σας

ΔΙΑΒΙΒΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ ΕΚΤΟΣ ΕΕ: Αν διαβιβάζετε δεδομένα και σε τρίτες χώρες, επιλέξτε κάποιο μηχανισμό διαβίβασης, όπως πιστοποιήσεις στο Privacy Shield (για τις ΗΠΑ)

Τα βήματα για την συμμόρφωση

- Μεθοδολογία Υλοποίησης Συμμόρφωσης
- Action Plan Έργου Συμμόρφωσης
- Ροές (Data Mapping) Προσωπικών Δεδομένων
- Καταγραφή Κινδύνων
- Σύνταξη Μητρώου
- Αναθεώρηση Συμβάσεων
- Αξιολόγηση Επιπτώσεων και Εκτίμηση Επικινδυνότητας
- Εφαρμογή Σχεδίων Προστασίας - Πολιτικές και Διαδικασίες
- Σύνδεση GDPR με ISO 27001
- Μέτρηση Δεικτών και Βελτίωση του Συστήματος
- Audit Εφαρμογής

Data Protection Officer (1/2)

Σύμφωνα με τον Κανονισμό, ο DPO αναλαμβάνει:

Να εκπροσωπήσει τον Υπεύθυνο Επεξεργασίας ή τον Εκτελούντα την Επεξεργασία (ανάλογα με το ποιος τον ορίζει) έναντι των αρχών

Να συμβουλεύσει τη Διοίκηση σε θέματα προστασίας προσωπικών δεδομένων

Να εισηγηθεί απευθείας στη Διοίκηση τις κατάλληλες πολιτικές προστασίας των δεδομένων θεωρώντας τα ως πολύτιμο περιουσιακό στοιχείο του Οργανισμού

Δεξιότητες και Εκπαίδευση

Ο DPO πρέπει να έχει εξειδικευμένη γνώση του νομικού πλαισίου προστασίας Δεδομένων Προσωπικού Χαρακτήρα σε εθνικό και ευρωπαϊκό επίπεδο

Να έχει βασική γνώση στοιχείων Ασφάλειας Πληροφοριών και Πληροφοριακών Συστημάτων, ώστε να μπορεί να κατανοήσει, να σχεδιάσει και να εποπτεύσει την εφαρμογή ενός προγράμματος προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Data Protection Officer (1/2)

Ο DPO έχει μεγάλο βαθμό ανεξαρτησίας:
Δεσμεύεται από εμπιστευτικότητα
Άμεση πρόσβαση στη Διοίκηση (π.χ. αναφέρεται, στον Πρόεδρο του Διοικητικού Συμβουλίου κλπ)

Το Υποκείμενο των Δεδομένων έχει ξεκάθαρη πρόσβαση στον DPO

Δεν πρέπει να υπάρχει σύγκρουση συμφερόντων λόγω πρόσθετων αρμοδιοτήτων ή καθηκόντων

Αποτελεί τον κύριο συνομιλητή της Διοίκησης για τα θέματα προστασίας δεδομένων και εξασφαλίζει την υποστήριξή της και τον απαιτούμενο προϋπολογισμό για την εφαρμογή του Προγράμματος Προστασίας Δεδομένων

.

Η διαδικασία της συμμόρφωσης (1/4)

Προετοιμασία – Αποτύπωση υφιστάμενης κατάστασης
(προσδιορίζουμε τα σημεία που ο οργανισμός καλύπτει ήδη τις απαιτήσεις και τα σημεία που χρειάζονται πρόσθετοι μηχανισμοί ελέγχου)

Προβαίνουμε σε:

- Καταγραφή υπευθύνων ανά τμήμα
- Καταγραφή διαθέσιμων πόρων
- Καταγραφή και χαρτογράφηση των Δεδομένων Προσωπικού Χαρακτήρα
- Χαρτογράφηση του εγκατεστημένου πληροφοριακού συστήματος
- Καταγραφή Τεκμηρίωσης

Η διαδικασία της συμμόρφωσης (2/4)

Ανάπτυξη πολιτικών, διαδικασιών & δημιουργία πρότυπων συμβάσεων

- Πολιτικές συλλογής και επεξεργασίας δεδομένων
- Πολιτικές ασφάλειας, Σχέδιο ασφάλειας, Σχέδιο ανάκαμψης και καταστροφών
- Μηχανισμός εντοπισμού παραβιάσεων
- Σχέδιο διαχείρισης των συμβάντων
- Αρχείο καταγραφής ενεργειών
- Προσαρμογή των συμβάσεων του οργανισμού &

- **Τεχνικά μέτρα**, που θα πρέπει να ληφθούν για την συμμόρφωση με τις απαιτήσεις του Κανονισμού, καθώς και πιθανές συστάσεις για μέτρα, τα οποία ναι μεν, δεν είναι απαραίτητα για την συμμόρφωση προς τον Κανονισμό, αλλά θα μπορούσαν να συμβάλλουν στην εύρυθμη λειτουργία του.

Η διαδικασία της συμμόρφωσης (3/4)

Εκπαίδευση πριν την συμμόρφωση

Ενημέρωση & εκπαίδευση προς όλους τους εργαζομένους για να καταλάβουν τα κρίσιμα σημεία του κανονισμού και να συμβάλλουν με προτάσεις, παρατηρήσεις και ιδέες για την συμμόρφωση

Εκπαίδευση μετά την συμμόρφωση

Ενημέρωση & εκπαίδευση προς όλους τους εργαζομένους για το σύστημα, για τις διαδικασίες εφαρμογής ανά τμήμα/ διεύθυνση, για τις αναθεωρημένες συμβάσεις, για την διαδικασία ειδοποίησης σε περίπτωση απώλειας προσωπικών δεδομένων

Η διαδικασία της συμμόρφωσης (4/4)

Εσωτερική αξιολόγηση & επιθεώρηση συμμόρφωσης GDPR
Η επιθεώρηση και αξιολόγηση συμμόρφωσης στο GDPR για την καλύτερη διασφάλιση και υιοθέτηση των βέλτιστων πρακτικών αρχικά είναι εσωτερική (από τον DPO και την ομάδα του)

Εξωτερική αξιολόγηση & επιθεώρηση συμμόρφωσης GDPR
Η επιθεώρηση και αξιολόγηση συμμόρφωσης όλου του συστήματος από εξωτερικούς Πιστοποιημένους επιθεωρητές (νομική, οργανωτική & τεχνική) ώστε η εταιρεία να πιστοποιηθεί με το **GDPR SEAL**

Βασικοί Κανόνες Ασφαλείας

- PASSWORDS
- ANTI - VIRUS
- UPDATES
- ATTACHMENTS
- BACKUP

Social impact

Let me in: «Άσε το κακό να μπεί»

Το 84% των χρηστών του Google δήλωσε ότι του άρεσε αυτή η ταινία

Κωδικοί Ασφαλείας (Passwords)

SplashData 2017 Top 20 worst passwords

1	123456 (top 2016 list)		11	admin (up 4)
2	password (top 2016 list)		12	welcome (unchanged)
3	12345678 (up 1)		13	monkey (new)
4	qwerty (up 2)		14	login (down 3)
5	12345 (down 2)		15	abc123 (down 1)
6	123456789 (new)		16	starwars (new)
7	letmein (new)		17	23123 (new)
8	1234567 (Unchanged)		18	dragon (up 1)
9	football (down 4)		19	passw0rd (down 1)
10	iloveyou (new)		20	master (up 1)

Κωδικοί Ασφαλείας (Passwords)

- Ισχυροί Κωδικοί
- Διαφορετικοί Κωδικοί ανά Εφαρμογή
- Αλλαγή Κωδικού ανά 2 Μήνες

Εγκατάσταση αντιϊκού προγράμματος (Anti-virus)

- Τακτικός έλεγχος αρχείων
- Τακτική ενημέρωση του προγράμματος
- Κρυπτογράφηση αρχείων

Ενημερώσεις Προγραμμάτων

- Έλεγχος συμβατότητας με τις κρίσιμες εφαρμογές
- Αυτόματη ενημέρωση προγραμμάτων
- Εγκατάσταση νέων εκδόσεων λειτουργικών συστημάτων

Αποφυγή εκτέλεσης συνημμένων μέσω μηνυμάτων ηλεκτρονικής αλληλογραφίας (e-mail attachments)

- Έλεγχος αποστολέα
- Διασταύρωση με τον αποστολέα για την αποστολή συνημένου
- Ενεργοποίηση εμφάνισης κατάληξης αρχείων
- Έλεγχος συνημμένου σε διαδικτυακές υπηρεσίες ανίχνευσης ιών

Διατήρηση αντιγράφων ασφαλείας (Backup)

- Backup σε φυσικό έγγραφο
- Backup σε φυσικό αποθηκευτικό μέσο (USB, Σκληρός δίσκος, DVD κ.α.
- Backup σε cloud υπηρεσίες

Επιμόρφωση προσωπικού

Η επιμόρφωση του προσωπικού είναι το μοναδικό μη τεχνικό μέσο περιορισμού των κινδύνων παραβίασης αλλά ίσως και το σημαντικότερο

Μέσω της επιμόρφωσης περιορίζεται η πιθανότητα επιτυχούς επίθεσης κοινωνικής μηχανής

- Εκπαίδευση μέσω σεμιναρίων / ηλεκτρονικού
- Ενημέρωση για νέες τεχνολογίες από τη διεύθυνση μηχανογράφησης
- Επιμόρφωση με προσομοίωση σε σενάρια κυβερνοεπίθεσης

Σκοπός είναι η ευαισθητοποίηση σε θέματα ασφαλείας (security awareness)

Ερωτήσεις - Απορίες

Alpha Plan Consultants

Κλειδής Μανούσος
Γενικός Διευθυντής

Εθνικής Αντιστάσεως 158 (1ος Όροφος), 71306,
Ηράκλειο Κρήτης
Τηλ.: 2810 289457,Fax: 2810 289428
Website: www.aplan.gr
Personal Email: mkleidis@aplan.gr
Mobile: +30 6972870030

Ευχαριστούμε πολύ

www.eugdpr.gr