Διεύθυνση Συμμόρφωσης

Compliance and Ethics Office

Compliance Makes The Difference

Διαμορφώνοντας το Πλάνο GDPR

Οι Προκλήσεις ενός DPO

Αντώνης Ευαγγελίδης

Chief Ethics & Compliance Officer

VIANEX & VIAN S.A

Αθήνα, July 7th , 2017

Αμφιθέατρο ΒΙΑΝΕΞ

Disclaimer-Διευκρίνηση

"Οι θέσεις και οι απόψεις οι οποίες εκφράζονται στην ακόλουθη παρουσίαση είναι προσωπικές και δεν αντιπροσωπεύουν κατ΄ ανάγκη την επίσημη θέση οποιασδήποτε εταιρείας, εργοδότη ή οργανισμού με τους οποίους συνδέεται ο συντάκτης της παρουσίασης.»

"Statements of fact and opinions expressed in this presentation are those of the author and do not necessarily reflect the official policy or position of any other company, employer or organization connected with the author."

Agenda-Περιεχόμενα

01 EU GDPR: Ένα Μεγάλο Ζήτημα Ευρωπαϊκών +Διαστάσεων

02 Οι 8 Βασικές Προκλήσεις ενός DPO σε σχέση με τον EU GDPR

03 Διαμορφώνοντας το Πλάνο: Στρατηγική και Τακτικές Ενέργειες

04 Χρονοδιάγραμμα Υλοποίησης Πλάνου Συμμόρφωσης EU GDPR

05 Συμπεράσματα -Συστάσεις

1 Το Μεγάλο Ζήτημα

Ο Νέος EU GDPR (ΓΚΠΔ)

The GDPR

General Data Protection Regulation

1

Μεγάλο ζήτημα Ευρωπαϊκών + Διαστάσεων

ΔΙΟΙΚΗΣΗ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΤΩΝ ΕΤΑΙΡΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Ιδιωτικότητα

Προστασία Ατομικών Δικαιωμάτων

Η Νέα Αρχιτεκτονική Διάρθρωση του Νέου EU GDPR

Αποτελείται από ένα ογκώδες πολύπλοκο νομικό κείμενο με 99 άρθρα , σε 88 σελίδες ,98 μη τεχνικά και 1 τεχνικό (άρθρο 32 κρυπτογραφία)

- Κεφάλαιο I: Γενικές Κατευθύνσεις Κανονισμού EU GDPR (άρθρα 1-4)
- Κεφάλαιο II: Βασικές Αρχές του EU GDPR (άρθρα 5-11)
- Κεφάλαιο III: Δικαιώματα των Υποκειμένων των Δεδομένων (άρθρα 5-11)
- Κεφάλαιο IV:Υπεύθυνοι Ελέγχου και Επεξεργασίας (άρθρα 24-43)
- Κεφάλαιο V: Μεταφορά Προσωπ. Δεδομένων σε 3ες χώρες (άρθρα 44-50)
- Κεφάλαιο VI: Ανεξάρτητες Εποπτεύουσες Αρχές (άρθρα 51-59)
- Κεφάλαιο VII: Συνεργασία και Συνέπεια (άρθρα 60-76)
- Κεφάλαιο VIII: Διορθωτικά μέτρα, Ευθύνες και Κυρώσεις (άρθρα 77-84)
- Κεφάλαιο IX : Ρυθμίσεις σχετικές με ειδικές συνθήκες επεξεργασίας (άρθρα 85-91)

Πηγή: Απόδοση από IT Governance,2016

Ο EU GDPR με Γεγονότα και Αριθμούς

Νέος

56.321

Λέξεις στον Νέο EU GDPR

7

Κύρια ατομικά Δικαιώματα Επηρεάζονται από Τον GDPR

28 → 1

Από 28 Νόμους & Αρχές σε 1 Κεντρική Αρχή για Όλους) "One Stop Shop"

80+

Είναι οι επιπλέον απαιτήσεις Του Γενικού Κανονισμού)

190+

Οι Χώρες που περιλαμβάνονται Στον σκοπό του Κανονισμού GDPR)

20 εκ. €

Το πρόστιμο για μια Εταιρεία

Πηγή: Γενικός Κανονισμός Προστασίας Δεδομένων

Ο EU GDPR με Λίγα Λόγια

Πρόστιμα	Πρόστιμα επί μη συμμόρφωσης έως και > του 4% του ετήσιου τζίρου (ή 10-20 εκ.€)
Υπεύθυνος Προστασίας (DPO)	Ο DPO είναι απαραίτητος σε Οργανισμούς και Εταιρείες που επεξεργάζονται μαζικά Ειδικά Δεδομένα
Ενισχυμένα Δικαιώματα Εποπτεύουσας Αρχής	Η Ευρωπαϊκή Εποπτεύουσα Αρχή έχει ευρυζωνική εξουσία.Οι τοπικές ενισχυμένα
Καταγραφή Δεδομένων	Οι Εταιρείες πρέπει να καταγράφουν τα προσωπικά δεδομένα-Τήρηση Αρχείου
Ενημέρωση Παραβιάσεων	Απαίτηση άμεσης ενημέρωσης της Εποπτεύουσας Αρχής εντός 72 h και δυνητικά σε Υποκ. Δεδομένων
Ασφάλεια	Αυστηρές απαιτήσεις για ανωνυμοποίηση, ψευδωνυμοποίηση, κρυπτογράφηση
Εφαρμογή	Εφαρμογή σε όλες ανεξαιρέτως τις Εταιρείες που επεξεργάζονται δεδομένα Ευρωπαίων Πολιτών

Πηγή: Γενικός Κανονισμός Προστασίας Δεδομένων

Το 1ο Ερώτημα(& Πρόκληση)

Το GDPR έρχεται
Είμαστε έτοιμοι;

GDPR

322	09	27	49
DAYS	HOURS	MINUTES	SECONDS

Time until **Παρασκευή**, 25 **Μαΐου** 2018 (Athens, Greece time)

2.Οι 8+1 Προκλήσεις για τις Εταιρείες ως προς τον EUGDPR

Οι Βασικότερες Προκλήσεις στον EU GDPR Κανονισμό

Οι 8 Βασικότερες Προκλήσεις του Κανονισμού

- 1.Διευρύνει τον Ορισμό των Προσωπικών Δεδομένων
  - Γενετικά , βιομετρικά
- 2.Νέα Δικαιώματα για τα Υποκείμενα των Δεδομένων (άρθρα 5-11)

- 3.Διευρύνει τις Αρμοδιότητες των Υπεύθυνων (DP) και των Εκτελούντων (DC) την Επεξεργασία
- 4.Υποχρεωτικές Γνωστοποιήσεις της Αρχής και των Υ.Δ. επί Παραβιάσεων των Δεδομένων

- 5.Διευρυμένα Δικαιώματα των Αρχών ΠΔ
- 6.Επιβολή Υψηλών Προστίμων για μη συμμόρφωση (άρθρα 83,84)

- 7.Ορίζει Υποχρεωτικά τον Data Protection Officer (DPO)
- 8.Μελέτες Εκτίμησης Επιπτώσεων /Αντικτύπου Ιδιωτικότητας (DPIA)(άρθρο 35)

EU GDPR:Τα Νέα Ενισχυμένα Δικαιώματα Πολιτών/Πελατών

2

6 **Συγκατάθεση (Consent) Του Υποκειμένου**

Ο Καταναλωτής πρέπει να είναι πληροφορημένος με «ξεκάθαρη και σαφή γλώσσα» .Η συναίνεση μπορεί να αποσυρθεί σε οποιαδήποτε στιγμή (άρθρο 7)

7 **Ειδοποίηση επί Παραβιάσεων**

Ανταπόκριση σε αιτήματα και παροχή Δεδομένων σε χρονικό διάστημα 1 μήνα (2 μήνες σε περίπλοκες περιπτώσεις)

1 **Δικαίωμα στη Λήθη (Άρθρα 15,17)**

Διεύρυνση

5 **Δικαίωμα στην**

4 **Πρόσβαση/ Διόρθωση (Άρθρα 15 & 16)**

Νέα Ενισχυμένα Δικαιώματα

8

- **Δικαίωμα Άσκησης Κατηγορίας κατά ΥΕ** (άρθρο 79)
- **Αποζημίωση**
- **Δικαίωμα Άρνησης Profiling**
- **Δικαίωμα Αντίρρησης**
- **Δικαίωμα στον Περιορισμό της Επεξεργασίας**

3 **Περιορισμένη Επεξεργασία**

Νέο

2 **Δικαίωμα Φορητότητας (Άρθρο 20)**

Νέο

EU GDPR: Υποχρεώσεις Των Εταιρειών ως Υ.Ε-D.P*

3 Διευρύνει τις Υποχρεώσεις του Υπευθύνου Επεξεργασίας (D.P*)

Διατήρηση Αρχείου Τεκμηρίωσης σχετικά με τις εκτελούμενες διεργασίες επεξεργασίας και **υποβολή της τεκμηρίωσης στην Εποπτεύουσα Αρχή** (ΑΔΠΧ) αν του ζητηθεί (άρθρο 33,34)

Εκτελεί **Μελέτες Εκτίμησης Επιπτώσεων Ιδιωτικότητας, Privacy Impact Assessments (PIA)** όταν επεξεργάζεται ευαίσθητα δεδομένα από τα οποία προκύπτει κίνδυνος για τους καταναλωτές (άρθρο 35)

Είναι από Κοινού Υπεύθυνος με τον Εκτελούντα την Επεξεργασία (DP) για τον **ορισμό Υπευθύνου Προστασίας Δεδομένων (DPO**.Αρθρο 37)

Ενημερώνει τον Εκτελούντα την Επεξεργασία (DC) για **την παραβίαση των προσωπικών δεδομένων** χωρίς αδικαιολόγητη καθυστέρηση, αφού λάβει γνώση αυτής της παραβίασης

Περιορίζει το ποιος Βλέπει/ έχει πρόσβαση στα Δεδομένα. Μόνο εξουσιοδοτημένα άτομα μπορούν να έχουν πρόσβαση στα Δεδομένα

Περιορίζει την Επεξεργασία προς τον σκοπό για τον οποίο τα δεδομένα συγκεντρώθηκαν

* Υ.Ε=Υπεύθυνος Επεξεργασίας, Data Processor

- Πηγή: Απόδοση από Ernst & Young

Παραβίαση των Δεδομένων, Εταιρική Φήμη και Κόστος

4

Υποχρεωτικές Γνωστοποιήσεις σε Παραβιάσεις των Δεδομένων

Άρθρο 33

- **Η Παραβίαση των Δεδομένων** είναι από τους μεγαλύτερους κινδύνους (30%) που μπορούν να έχουν επίδραση στην **Φήμη μιας Εταιρείας**
  - Ύστερα και μαζί με την Κακή Εξυπηρέτηση Πελατών(75%) και μια Πιθανή Περιβαντολλογική Καταστροφή(33%)
- **Το Μέσο κατά κεφαλήν κόστος αντιμετώπισης** μιας παραβίασης στις Φαρμακευτικές Επιχειρήσεις **είναι 227 $**

2011:Κλοπή Στοιχείων 77 εκ. πελατών

Πηγή: The Aftermath of a data breach Consumer Sentiment. Ponemon Institute Report,2014

Διαδικασία Γνωστοποίησης σε Περίπτωση Παραβίασης

4

Υποχρεωτικές Γνωστοποιήσεις σε Παραβιάσεις των Δεδομένων

Άρθρο 33

Παραβιάσεις

Εξωτερικές
- Κυβερνοεπιθέσεις
- Υποκλοπή Κωδικών Πρόσβασης
- Phishing
- Κακόβουλο Λογισμικό

Εσωτερικές
- Πρώην Υπάλληλοι
- USB sticks

- **Οι επεξεργαστές των δεδομένων (DP) πρέπει να αναφέρουν τις παραβιάσεις των προσωπικών δεδομένων** στους **εκτελούντες τα δεδομένα DP**(Clouds)
- **Επιβεβαίωση της Παραβίασης και Διαχείριση της Νομικά και Επικοινωνιακά (Crisis Management)-Φήμη-Απώλεια Εσόδων**
- **Οι Υπεύθυνοι Επεξεργασίας πρέπει να αναφέρουν τις παραβιάσεις στην Εποπτεύουσα Αρχή ΠΔΠΧ και σε ορισμένες περιπτώσεις** στα υποκείμενα των **δεδομένων που επηρεάστηκαν σε κάθε περίπτωση για πιθανούς κινδύνους**
- Οι Υπεύθυνοι Επεξεργασίας πρέπει να τηρούν **ένα εσωτερικό μητρώο κινδύνων**
- Η μη συμμόρφωση οδηγεί σε **μεγάλα διοικητικά πρόστιμα**

5 Διευρυμένα Δικαιώματα της Εποπτεύουσας Αρχής

Ενισχυμένα Δικαιώματα της Εποπτεύουσας Αρχής

Άρθρο 56

- Έργο της Αρχής Προστασίας Δεδομένων (ΑΠΔ) είναι:
  - Η Προστασία των Προσωπικών Δεδομένων και της Ιδιωτικότητας και
  - Να λαμβάνει μέτρα για όσους δεν συμμορφώνονται με την Νομοθεσία Προσωπικών Δεδομένων
- Η Ευρωπαϊκή Εποπτεύουσα Αρχή (EDPB) έχει Ευρυζωνικά (ΕΟΧ , 28 χώρες,+190 χώρες) Δικαιώματα και είναι υπεύθυνη για την επίλυση διαφορών μεταξύ των ΑΠΔ των κρατών μελών
- Η Ελληνική ΑΠΔ έχει ενισχυμένα δικαιώματα
- Όταν μια περίπτωση αφορά μόνο μια εγκατάσταση υπεύθυνου επεξεργασίας ή εκτελούντα την επεξεργασία σε ένα κράτος μέλος ή επηρεάζει ουσιαστικά τους κατοίκους μόνο σε ένα συγκεκριμένο κράτος- μέλος, η ΑΠΔ του οικείου κράτους μέλους θα είναι αρμόδια για την υπόθεση. (GDPR, Άρθ. 56 (2)).

6 Το Κόστος της μη Συμμόρφωσης προς τον EU GDPR

Επιβολή Υψηλών Προστίμων για μη Συμμόρφωση

Αρθρα 83.84

- Η Ελληνική Αρχή Προστασίας των Δεδομένων (ΑΠΔΠΧ) παρακολουθεί τη συμμόρφωση. Οι εργασίες της συντονίζονται σε επίπεδο ΕΕ.
- Το κόστος Παραβίασης του EU Κανονισμού είναι Υψηλό

Προειδοποίηση

Επίπληξη

Αναστολή της Επεξεργασίας Των Δεδομένων

Υψηλό Πρόστιμο

Πηγή: Ευρωπαϊκή Ένωση και Ελληνική Αρχή Προστασίας Δεδομένων,2017

6 Εξαντλητικά Πρόστιμα Στον Νέο EU GDPR (Άρθρο 83)

Προετοιμαστείτε Τώρα. Ή αλλιώς Πληρώστε το Τίμημα…

Τα Πρόστιμα Προσδιορίζονται από την Φύση και Σοβαρότητα της Παράβασης

Μέγιστο Πρόστιμο των

€20M / ~$22M

Ή το **4%** *Του ετήσιου τζίρου Της προηγούμενης χρονιάς*

(whichever is greater)

Failure to adhere to core principles of data processing, infringement of personal rights, or the **transfer of personal data** to other countries or international organizations that do not ensure an adequate level of data protection

ARTICLE: 44

Μέγιστο Πρόστιμο των

€10M / ~$11M

Ή το **2%** *Του ετήσιου τζίρου Της προηγούμενης χρονιάς*

(whichever is greater)

Failure to comply with technical and organizational requirements such as **impact assessments, breach communications**, and certifications

ARTICLES: 25, 32, 33, 35

Πηγή: Ευρωπαϊκός Κανονισμός Προστασίας Δεδομένων. Άρθρο 83,2016

7

Ο Ρόλος του DPO (Άρθρο 37)

Καθιερώνει Υποχρεωτικά τον DPO

DPO:Υποχρεωτικός σε 3 Περιπτώσεις/Χαρακτηριστικά

7

Άρθρο 37 και Οδηγία της Επιτροπής του Άρθρου 29

Ποιος Μπορεί να Είναι DPO-Συγκρούσεις Συμφερόντων;

7

Το 2ο Ερώτημα:

ARTICLE 29 DATA PROTECTION WORKING PARTY

16/EN
WP 243 rev.01

Guidelines on Data Protection Officers ('DPOs')

Adopted on 13 December 2016
As last Revised and Adopted on 5 April 2017

3.5. Conflict of interests

Article 38(6) allows DPOs to '*fulfil other tasks and duties*'. It requires, however, that the organisation ensure that '*any such tasks and duties do not result in a conflict of interests*'.

The absence of conflict of interests is closely linked to the requirement to act in an independent manner. Although DPOs are allowed to have other functions, they can only be entrusted with other tasks and duties provided that these do not give rise to conflicts of interests. This entails in particular that the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case.

As a rule of thumb, conflicting positions within the organisation may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing. In addition, a conflict of interests may also arise for example if an external DPO is asked to represent the controller or processor before the Courts in cases involving data protection issues.

Διευκρινιστική Οδηγία της Επιτροπής του Άρθρου 29/05.04.2017

In addition, a conflict of interests may also arise for example if an external DPO is asked to represent the controller or processor before the Courts in cases involving data protection issues.»

Εξέλιξη Τεχνολογίας-Κανονισμοί

8+1

3. Στρατηγική GDPR

Στρατηγικό και Τακτικό Σχέδιο (Πλάνο)

Όταν ο Harry γνώρισε την Sally ή .....

Εκεί όπου

ΤΟ Ethical Marketing

συναντά την

Ethical Συμμόρφωση

Πως Πρέπει να Δούμε την Εισαγωγή του EU GDPR

- **Εισαγωγή** Νέου Φαρμακευτικού Προϊόντος
- **Πανευρωπαϊκή Έγκριση**/4 χρόνια Διαδικασία Έγκρισης
- **Φάρμακο Υψηλού Κόστους** (ΦΥΚ)=20.000.000€
- **Launch Date**: 25 Μαΐου 2018/**Co-Promotion** όλες οι Φ.Ε

Μορφές

Σπάνια Ένδειξη

EU General Data Protection Regulation

Ο Οδικός Χάρτης Προετοιμασίας του EU GDPR

Source:GDPR Program in VIANEX SA

4.Σχέδιο Δράσης
Action Plan-Χρονοδιάγραμμα

Φάσεις Έργου GDPR

Φάσεις Έργου EU GDPR

Προετοιμασία Οργάνωση (Awareness)

Εκτίμηση Διάγνωση (Assessment)

Υλοποίηση (Implementation)

1

2

3

Ορισμός Ομάδας Έργου (Privacy Team) και Ρόλων GDPR

*SOPs, Processes,σε συνεργασία με DPO ,Εργοστάσια. Audits Πιστοποιήσεις ISO.

Προσοχή: Δεν πρέπει να επαναπαυθούμε μόνον σε αυτούς

Δημιουργία Διεταιρικής Ομάδας Υποστήριξης GDPR

Η Συμμόρφωση με τοις απαιτήσεις του GDPR είναι ένα Διεταιρικό Θέμα!! Μας αφορά όλους!

- Γενικοί Διευθυντές (GMs)

- Διευθυντή Ανθρώπινων Υπηρεσιών
- **Τμήματα Επικοινωνίας & Ε.Κ.Ε**
- Τηλεφωνικά Κέντρα, Πύλη
- ΕΣ, ΚΑΜ, Πωλητές Φαρμακείων…….

ης

ονας

με στόχο να ελαχιστοποιήσουμε τους κινδύνους μη συμμόρφωσης προς τις απαιτήσεις του GDPR

Διαχείριση Δεδομένων GDPR στις Εταιρείες

Data Type	HR	Finance	Marketing	Sales
Name	✓	✓	✓	✓
Job Title	✓	✓	✓	✓
Telephone Number	✓	✓	✓	✓
Email Address	✓	✓	✓	✓
Home Address	✓	✓		
Business Address	✓	✓	✓	✓
Salary	✓	✓		
Personal Bank Details	✓	✓	✓	
Business Bank Details		✓		
Purchases		✓	✓	✓
Payments	✓	✓		✓

Εργασιακές Σχέσεις και Προσωπικά Δεδομένα

1.
Δικαιούται ο Εργοδότης μου να παρακολουθεί τον ηλεκτρονικό μου υπολογιστή;
Η πρόληψη πιο σημαντική από την ανίχνευση. Ενημέρωση. Προειδοποίηση εργαζομένων

2.
Δικαιούται ο Εργοδότης να με παρακολουθεί με Σύστημα Βιντεοεπιτήρησης;

3.
Δικαιούται ο εργοδότης μου να εγκαταστήσει σύστημα γεωγραφικού προσδιορισμού (GPS) στο αυτοκίνητό μου, στο κινητό μου;

4.
Δικαιούται ο εργοδότης μου να παρακολουθεί μυστικά το ηλεκτρονικό ταχυδρομείο μου;
Σε εξαιρετικές περιπτώσεις (Εγκληματικές δραστηριότητες Διατ. Άρθρου 13/Οδ.95/46/ΕΟ)

5.
Δικαιούται ο εργοδότης μου να παρακολουθεί τις τηλεφωνικές συνδιαλέξεις μου;
Οι τηλεφωνικές κλήσεις αποτελούν μέρος της ιδιωτικής Ζωής των εργαζομένων)

6.
Μπορώ να μάθω στατιστικές πληροφορίες για μια επιχείρηση;
Τα συγκεντρωτικά στοιχεία δεν λογίζονται ως Προσωπικά Δεδομένα)

7.
Οι στενοί συγγενείς έχουν δικαίωμα να λαμβάνουν γνώση δεδομένων κοινωνικής πρόνοιας κάποιου ;
Όχι είναι Τρίτα Πρόσωπα. Μόνον με εξουσιοδότηση του εργαζομένου .

Συνεντεύξεις-Χαρτογράφηση/Αποτύπωση Υφιστάμενης Κατάστασης (Data Mapping)

Ερωτηματολόγια-Οδηγίες-Workshops

Χαρτογράφηση Δεδομένων: Ποιες είναι οι Προκλήσεις;

+

+

=

Ο Προσδιορισμός Των Προσωπικών Δεδομένων

Ο Προσδιορισμός Των Κατάλληλων Τεχνικών και Οργανωτικών Διασφαλίσεων

Η κατανόηση των Νομικών και Κανονιστικών Υποχρεώσεων

Πηγή :IT Governance 2016

Άγνωστα –Αδόμητα Δεδομένα

10GB αδόμητων δεδομένων ανά εργαζόμενο

Ροή Δεδομένων-Πληροφοριών (Data/Information Flow)

Προσδιορίστε τα Σημεία-Κλειδιά

Στοιχεία Δεδομένων

Ονόματα,E-mails, Διευθύνσεις	Δεδομένα Υγείας Ποινικά Δεδομένα	Βιομετρικά Δεδομένα Θέσης

Μορφές

Έγχαρτα (Hardcopy)	Ψηφιακά (USB)	Βάσεις Δεδομένων (Databases)

Μέθοδοι Μεταφοράς

Ταχυδρομεία ,τηλέφωνο, Μέσα Κοινωνικής Δικτύωσης (Social Media)	Εσωτερικά (Ενδοεταιρικά)	Εξωτερικά (Data Sharing)

Τοποθεσίες

Γραφεία	Σύννεφα (Clouds)	Τρίτα Μέρη (Third Parties)

Ανάλυση Ελλείψεων (Gap Analysis) ως προς τον ΓΚΠΔ

Βασικές αρχές προστασίας προσωπικών δεδομένων

Εξασφάλιση δικαιωμάτων φυσικών προσώπων

Γνωστοποίηση παραβίασης προσωπικών δεδομένων

Ασφάλεια Πληροφοριών

Οργανωτική δομή

Πολιτικές και Διαδικασίες

Επιθεωρήσεις και συνεχής βελτίωση

Σχεδιασμός Προγράμματος Προστασίας ΠΔ (Compliance Plan)- Εξασφάλιση Δικαιωμάτων Φυσικών Προσώπων

- Αλλαγές σε Πρακτικές
  - Συναινέσεις
  - Πληροφόρηση Πελατών
  - Χρόνος διαγραφής PII
  - Προσβάσεις
  - Ανωνυμοποίηση δεδομένων
  - Συμβάσεις με processors
  - Συμβάσεις με συνεργάτες
  - Πρακτικές ασφάλειας
- Νέοι μηχανισμοί
  - Εξασφάλισης δικαιωμάτων φυσικών προσώπων
  - Παρακολούθησης, ελέγχου και βελτίωσης
- Αναβάθμιση υποδομών ασφάλειας
- Αναθεώρηση και σύνταξη πολιτικών και διαδικασιών
- Εκπαίδευση

Σχεδιασμός του Προγράμματος Προστασίας των Π.Δ*

- Καθορισμός του Πλαισίου Εταιρικής Διακυβέρνησης (Governance) και Διαχείρισης Κινδύνων (Risk Management) για την προστασία των προσωπικών δεδομένων (υπευθυνότητες, αρμοδιότητες)
- Καθορισμός των βασικών σημείων Πολιτικής και των Διαδικασιών για την προστασία των προσωπικών δεδομένων

*ΠΔ=Προσωπικά Δεδομένα

Συγγραφή Μελέτης Αντικτύπου Ιδιωτικότητας/ Privacy Impact Assessment (DPIA)

Άρθρο 35

- **Αξιολόγηση Κινδύνων**
  - Ανά κατηγορία προσωπικών δεδομένων
  - Ανά έργο/προϊόν
- **Αναγνώριση Κινδύνων ποσοτικοποίηση ή εκτίμηση αντίκτυπου/επιπτώσεων** σχετικά με την προστασία δεδομένων
- **Απαραίτητο σε καταστάσεις που εμπλέκουν:**
  - Ευαίσθητα Προσωπικά Δεδομένα
  - Profiling
  - Νομικές Επιπτώσεις/Χρήση Νέων Τεχνολογιών
- **Προσδιορισμός απαραίτητων ενεργειών, οργανωτικών και τεχνικών μέτρων αποκατάστασης** που θα πρέπει να εκτελεστούν.
  - Με έγκυρη μεθοδολογία
  - ISO 29134, οδηγίες από DPAs
- Τακτική επανάληψη, επικαιροποίηση
- Συσχέτιση με άλλες εκτιμήσεις κινδύνων **Αναφορά για τον CISO/DPO/Διοίκηση**

IT Λύσεις Ιδιωτικότητας Πληροφοριακών Συστημάτων

- Privacy Impact Assessment & data flow mapping
- Data inventory/ discovery/ mapping/ classification
- Data masking / Data encryption
- Monitoring
- E-mail encryption
- Mobile Device Management
- Management of PII owner rights
- Data deletion and data portability

Information Security Management System

- Πολιτικές και Διαδικασίες Ασφάλειας
  - Έλεγχος πρόσβασης
  - Αντίγραφα ασφάλειας
  - Διακίνηση πληροφοριών και ασφάλεια επικοινωνιών
  - Ασφάλεια στις σχέσεις με προμηθευτές
  - Κρυπτογραφία
  - Ασφάλεια δεδομένων ανθρωπίνων πόρων
- Δείκτες (KPIs) και Στόχοι
- Μηχανισμοί Παρακολούθησης και Ελέγχου (Auditing & Monitoring)
- Συστηματική διερεύνηση μη συμμορφώσεων
  - παράπονα, καταγγελίες, ευρήματα, παραβιάσεις, συστάσεις

Διαμόρφωση Κώδικα Επιχειρηματικής Συμπεριφοράς για ΠΔ

Εταιρικοί και Κλαδικοί (πχ Κώδικας EFPIA για ΠΔ, Παράρτημα στον Κώδικα ΣΦΕΕ)

Πηγές:

9/7/2017

Χρονοδιάγραμμα Υλοποίησης Έργου EU GDPR

Επίλογος-Συμπεράσματα Συστάσεις

Συμπέρασμα:Το GDPR είναι ένα Τεράστιο Project…

EU GDPR
679/2016
680/2016

Οδηγία
95/46/EC
N 2472/2006

Το EU GDPR έρχεται…

10

ΜΗΝΕΣ

Ακόμα…
Είμαστε Έτοιμοι;

Μύθος # 1243

Μάϊος 2018;Ελα, έχουμε πολύ χρόνο ακόμα!

Προειδοποίηση:Η άγνοια, η απάθεια και ο εθελοτυφλισμός σκοτώνουν

Ξεκινήστε Τώρα… Προετοιμαστείτε Κατάλληλα

Η ανάγκη Υποστήριξης Top-Down Ακρογωνιαίος Λίθος

"Preparation has to start early, ideally you've already begun. In terms of actually doing something, the best advice is: *make sure top management and key decision makers appreciate the impact GDPR will have.*"

Τα 20 Βήματα του Οδικού Χάρτη για την Υλοποίηση του GDPR

Εξασφαλίστε Στήριξη της Διοίκησης Top-Down

Οικοδόμηση Προγράμματος & Ομάδας	Προσδιορίστε την Ομάδα & Εντοπίστε τους κύριους Εταίρους	Κατανείμετε Πόρους , Χρόνο & Προϋπολογισμό	Ορίστε τον Υπεύθυνο (Στέλεχος) Προστασίας Δεδομένων (DPO)	Προσδιορίστε Ρόλους ,Στόχους και την Αποστολή
Εκτίμηση Κινδύνων & Κινητοποίηση	Χαρτογραφήστε Κάντε Απογραφή & Ροή Δεδομένων	Εκτιμήστε τους Κινδύνους & Προσδιορίστε Ελλείψεις	Αναπτύξτε Πολιτικές και Διαδικασίες (SOPs) Ιδιωτικότητας	Επικοινωνήστε τις Προσδοκίεσσας και Εκπαιδεύστε
Σχεδιασμός και Υλοποίηση Λειτουργικών Ελέγχων	Διαχειριστείτε τις Συγκαταθέσεις	Μεταβίβαση Δεδομένων & Διαχείριση 3ων Μερών	Ατομικά Δικαιώματα Προστασίας Δεδομένων	Φυσικές, Τεχνικές, Διοικητικές Διασφαλίσεις
Διαχείριση & Ενίσχυση των Ελέγχων	Πραγματοποιήστε PIAs (DPIAs)	Διατήρηση Αναγκαίων Δεδομένων, & Διάθεση	Ακεραιότητα & Ποιότητα Δεδομένων	Σχέδιο Απόκρισης Επί Παραβίασης Δεδομένων
Επίδειξη Διαρκούς GDPR Συμμόρφωσης	Έλεγχος & Αξιολόγηση Αποτελεσματικότητας	Εσωτερικές& Εξωτερικές Αναφορές	Μηχανισμοί Ειδοποίησης Προσωπικών Δεδομένων	Πιστοποίηση GDPR Ready

9/7/2017 Πηγή:TRUSTE,2017

Εαν Νομίζετε…

"If you think compliance is expensive – try non-compliance."

Former U.S. Deputy Attorney General Paul McNulty

Τίποτα δεν είναι Αδύνατον…

Καλή Δύναμη, Καλή Επιτυχία

Ερωτήσεις ή/και Σχόλια

Σας Ευχαριστώ πολύ!

Για Περισσότερες Πληροφορίες

Αντώνης Ευαγγελίδης
Chief Compliance Officer
VIANEX & VIAN SA
+30-2108009422
+30-6979004043
Evaggelidisa@vianex.gr
www,vianex.gr