

GDPR στη Δημόσια Διοίκηση



Μια ακόμη μεγάλη ευκαιρία οργάνωσης

Δαμιανός Κοσμίδης Information Security & Data Protection Consultant,
MSc Πληροφορική και Διοίκηση,
DPO executive



Our Offering



Περιεχόμενο

- Τι είναι ο ΓΚΠΔ (GDPR);
- Προσωπικά Δεδομένα & Επεξεργασία
- Βασικές Αρχές της Επεξεργασίας Προσωπικών Δεδομένων
- Αιτήματα των υποκειμένων των δεδομένων
- Πώς συμμορφωνόμαστε με το ΓΚΠΔ
- Βασικοί κίνδυνοι
- Βασικές προτεραιότητες
- Ευαισθητοποίηση και προστασία στη πράξη
- Συνοψίζοντας τα οφέλη για το Δημόσιο

Τι είναι ο ΓΚΠΔ (GDPR);

Ο Ευρωπαϊκός ΓΚΠΔ θα βελτιώσει την ιδιωτική ζωή των ατόμων και θα δώσει στις ρυθμιστικές αρχές μεγαλύτερες εξουσίες για να αναλάβουν δράση κατά των επιχειρήσεων που παραβιάζουν τους νέους νόμους. Αυτό σημαίνει:

Αυστηρές ποινές: Πρόστιμα έως και το **4%** του ετήσιου παγκόσμιου κύκλου εργασιών ή τα **€20 εκατομμύρια** όποιο από τα δύο είναι **μεγαλύτερο**

Ο Κανονισμός εφαρμόζεται και σε μη **Ευρωπαϊκές εταιρίες** οι οποίες επεξεργάζονται προσωπικά δεδομένα ατόμων στην Ευρωπαϊκή Ένωση.

Η διεθνής μεταφορά των δεδομένων θα συνεχίσει να διέπεται σύμφωνα με τους κανόνες του **Ευρωπαϊκού ΓΚΠΔ**

 **SPACE**

Προσωπικά Δεδομένα σημαίνει...

...κάθε πληροφορία που σχετίζεται με ένα ταυτοποιημένο ή που δύναται να ταυτοποιηθεί φυσικό πρόσωπο (‘υποκείμενο των δεδομένων’)



Τα προσωπικά Δεδομένα είναι ένα περιουσιακό μας στοιχείο με μια αξία

Επεξεργασία σημαίνει...

...κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ... 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, για παράδειγμα:

- Μισθοδοσία εργαζομένων
- Καταγραφή καμερών
- Καταγραφή στοιχείων σε βάση δεδομένων, αρχεία
- Απαντήσεις σε ερωτήματα πολιτών-δημοτών

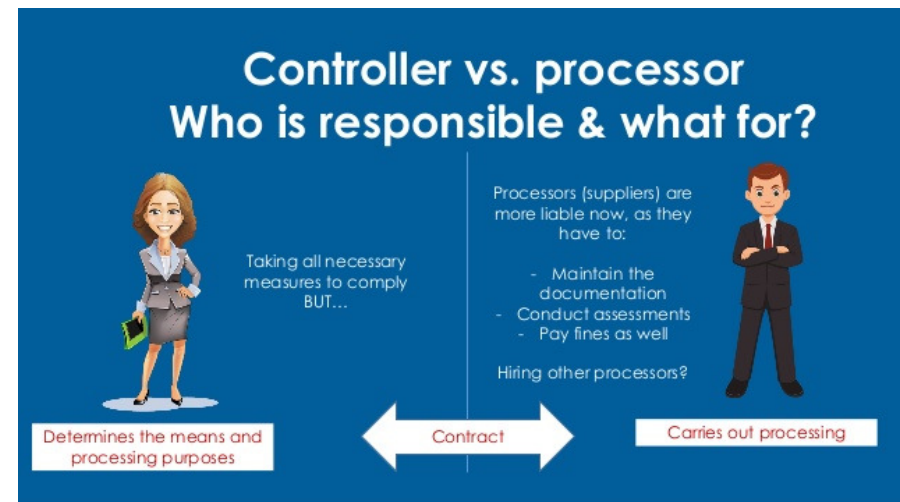
Υπεύθυνος Επεξεργασίας & Εκτελών την Επεξεργασία

Υπεύθυνος Επεξεργασίας
σημαίνει...

▣ 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
σημαίνει ...

▣ το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας



Βασικές Αρχές της Επεξεργασίας Προσωπικών Δεδομένων

1. Νομιμότητα, αντικειμενικότητα και διαφάνεια
2. Περιορισμός του σκοπού
3. Ελαχιστοποίηση των δεδομένων
4. Ακρίβεια
5. Περιορισμός της περιόδου αποθήκευσης
6. Ακεραιότητα και εμπιστευτικότητα
7. Λογοδοσία

Δικαιώματα των υποκειμένων των δεδομένων

Το υποκείμενο των δεδομένων (ανάλογα με τη νόμιμη βάση) έχει το δικαίωμα:



ΑΠΔΠΧ – Ενημέρωση των Φυσικών Προσώπων



Γενικοί όροι επιβολής διοικητικών προστίμων

[Άρθρο 83]

- η φύση, η βαρύτητα και η διάρκεια της παράβασης, λαμβάνοντας υπόψη και τον αριθμό των υποκειμένων που έθιξε η παράβαση και το βαθμό ζημίας που υπέστησαν
- ο δόλος ή η αμέλεια που προκάλεσε την παράβαση,
- οποιεσδήποτε ενέργειες για τον μετριασμό της βλάβης των υποκείμενων των δεδομένων,
- ο βαθμός ευθύνης, λαμβάνοντας υπόψη τα τεχνικά και οργανωτικά μέτρα
- τυχόν σχετικές προηγούμενες παραβάσεις
- ο βαθμός συνεργασίας με την αρχή ελέγχου για την επανόρθωση της παράβασης
- οι κατηγορίες δεδομένων προσωπικού χαρακτήρα που επηρεάζει η παράβαση
- ο τρόπος με τον οποίο η εποπτική αρχή πληροφορήθηκε την παράβαση
- τα οικονομικά οφέλη που αποκομίστηκαν ή ζημιών που αποφεύχθηκαν, άμεσα ή έμμεσα, από την παράβαση

Προσέγγιση του GDPR

- Πολιτικές και διαδικασίες προστασίας των Προσωπικών Δεδομένων

Διασφάλιση των Πληροφοριών



- Κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας

Προστασία συστημάτων & δικτύων



- Εντοπισμός ενδιαφερομένων μερών. Καταγραφή & ικανοποίηση των απαιτήσεών τους

Ικανοποίηση Ενδιαφερόμενων μερών



- συμμόρφωση με τον **GDPR** και την Ελληνική Νομοθεσία

GDPR



- Δημιουργία κουλτούρας προστασίας προσωπικών δεδομένων

Culture eats Strategy for Breakfast



Εμπιστευτικότητα – **Ακεραιότητα** – **Διαθεσιμότητα**

Πως Συμμορφωνόμαστε με τον GDPR



ΑΝΑΛΥΣΗ ΚΑΤΑΣΤΑΣΗΣ

- ▣ Ενότητα 01 - Προετοιμασία Έργου για τον ΓΚΠΔ
- ▣ Ενότητα 02 - Συλλογή Πληροφοριών και Εκτίμηση της Κατάστασης
- ▣ Ενότητα 03 - Ανάλυση Προσωπικών Δεδομένων
- ▣ Ενότητα 04 - Χαρτογράφηση Ροής και Επεξεργασίας Προσωπικών Δεδομένων

ΕΝΔΙΑΦΕΡΟΜΕΝΑ ΜΕΡΗ

- ▣ Ενότητα 05 - Ενημέρωση των Υποκειμένων των Δεδομένων
- ▣ Ενότητα 06 - Δικαιώματα των Υποκειμένων Δεδομένων
- ▣ Ενότητα 07 - Πολιτικές Ασφάλειας Πληροφοριών και προστασίας δεδομένων
- ▣ Ενότητα 08 - Διεθνείς Μεταφορές
- ▣ Ενότητα 09 - Διαχείριση Παραβιάσεων Προσωπικών Δεδομένων
- ▣ Ενότητα 10 - Υπεύθυνοι και Εκτελούντες την Επεξεργασία

ΕΣΩΤΕΡΙΚΗ ΟΡΓΑΝΩΣΗ

- Ενότητα 11 - Εκτίμηση Αντικτύπου για την Προστασία των Δεδομένων
- Ενότητα 12 - Τεχνικά και οργανωτικά μέτρα
- Ενότητα 13 - Ρόλοι, Ευαισθητοποίηση και Εκπαίδευση
- Ενότητα 14 - Έλεγχος Συμμόρφωσης
- Ενότητα 15 - Ενημέρωση της Διοίκησης

Βασικοί κίνδυνοι...

(1/2)

Διακίνηση των εγγράφων –
Κλητήρες - υπάλληλοι

Κατακερματισμένη και πολλαπλή πληροφορία
στα πληροφοριακά συστήματα και στα φυσικά αρχεία –
Αδυναμία ελέγχου και υψηλό κόστος προστασίας

Υψηλός κίνδυνος λαθροακρόασης σε υπηρεσίες που επεξεργάζονται ευαίσθητα
προσωπικών δεδομένων (πχ Υπηρεσίες Υγείας, Δήμοι, ΚΕΠ)

Δεν υπάρχουν συμφωνίες εμπιστευτικότητας με εργαζόμενους, εξωτερικούς
συνεργάτες κλπ.

Βασικοί κίνδυνοι...

(2/2)

Ελλιπής φύλαξη των φυσικών και ηλεκτρονικών αρχείων

Αδυναμία ικανοποίησης των δικαιωμάτων των φυσικών προσώπων

Πιθανότητα καταγγελιών που συνεπάγονται πρόστιμα

Βασικές προτεραιότητες...

1. Εκπαίδευση όλων των εργαζομένων γραφείου - Ευαισθητοποίηση

2. Ανάθεση DPO

3. Κατάργηση των υπολογιστών με XP.

Άμεση προτεραιότητα σε κρίσιμες υπηρεσίες

4. Δημιουργία κεντρικής υποδομής file server και backup

5. Ηλεκτρονική Διαχείριση Διαδικασιών και Εγγράφων

6. Πολιτικές καθαρού γραφείου – καθαρής οθόνης

7. Εγκύκλιος - οδηγίες/κανονισμός/πολιτικές

Ευαισθητοποίηση και προστασία στη πράξη

- Φυσική Προστασία της Πληροφορίας
- Ηλεκτρονική Προστασία της Πληροφορίας
- Πρόσβαση και Passwords
- Email
- Χρησιμοποιώντας το διαδίκτυο

- Προστασία από ιούς (Anti-Virus)
- Κινητές συσκευές
- Αφαιρούμενα μέσα
- Διαγραφή Πληροφοριών
- Περιστατικά ασφάλειας

Η μη συμμόρφωση με εγκεκριμένες πολιτικές είναι πειθαρχικό παράπτωμα.

Συνοψίζοντας τα οφέλη για το Δημόσιο



Ευχαριστώ και πάντα να θυμάστε

Το κλίμα εμπιστοσύνης

χρειάζεται χρόνια για να χτιστεί
δευτερόλεπτα για να γκρεμιστεί
και αιώνες για να επανέρθει...

Νομιμότητα της επεξεργασίας [Άρθρο 6]

το υποκείμενο έχει **συναινέσει** στην επεξεργασία για έναν ή περισσότερους συγκεκριμένους σκοπούς

η επεξεργασία είναι απαραίτητη για την **εκτέλεση σύμβασης**

η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με **έννομη υποχρέωση** του Υ.Ε.

η επεξεργασία είναι απαραίτητη για τη **διαφύλαξη ζωτικού συμφέροντος**

η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος για το **δημόσιο συμφέρον**

η επεξεργασία είναι απαραίτητη για τα **έννομα συμφέροντα** που επιδιώκει ο Υ.Ε ή τρίτος