*Ημερίδα με θέμα «Γενικός Κανονισμός Προστασίας Δεδομένων – GDPR»*
*ΤΕΕ Κεντρικής και Δυτικής Θεσσαλίας, Λάρισα, 18.05.2018*

# GDPR: η επόμενη μέρα στη διαχείριση δεδομένων προσωπικού χαρακτήρα

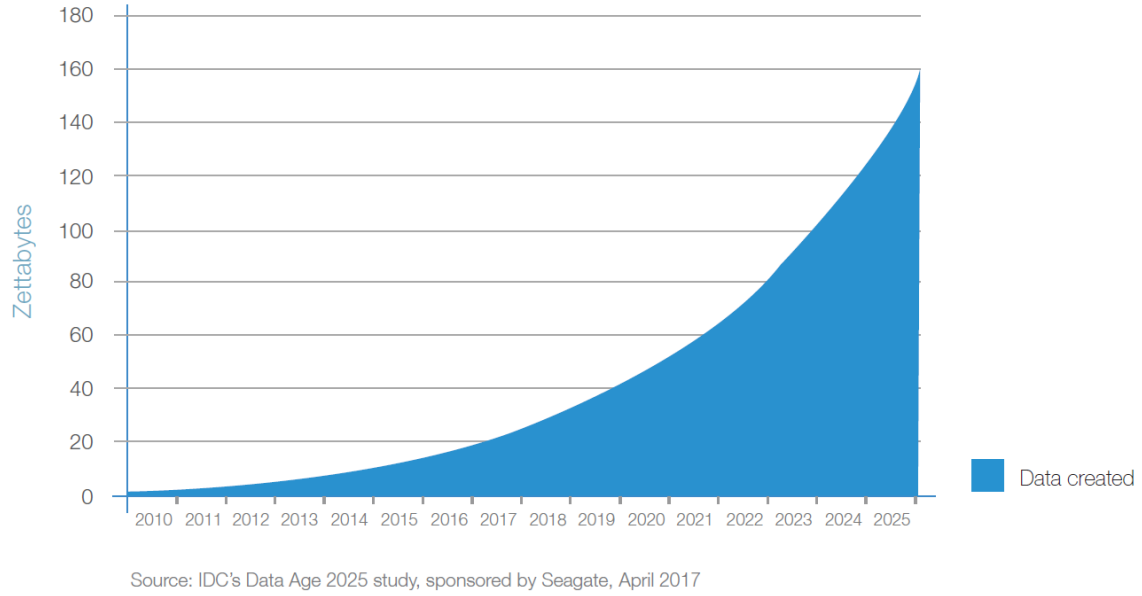
**Δρ. Βασίλης Χ. Γερογιάννης**

Καθηγητής ΤΕΙ Θεσσαλίας
Μηχανικός Η/Υ και Πληροφορικής
Γραμματέας Διοικούσας Επιτροπής ΤΕΕ Κ&Δ Θεσσαλίας
Συντονιστής Μόνιμης Επιτροπής Τεχνολογιών Πληροφορικής και Επικοινωνιών
(gerogian@teilar.gr)

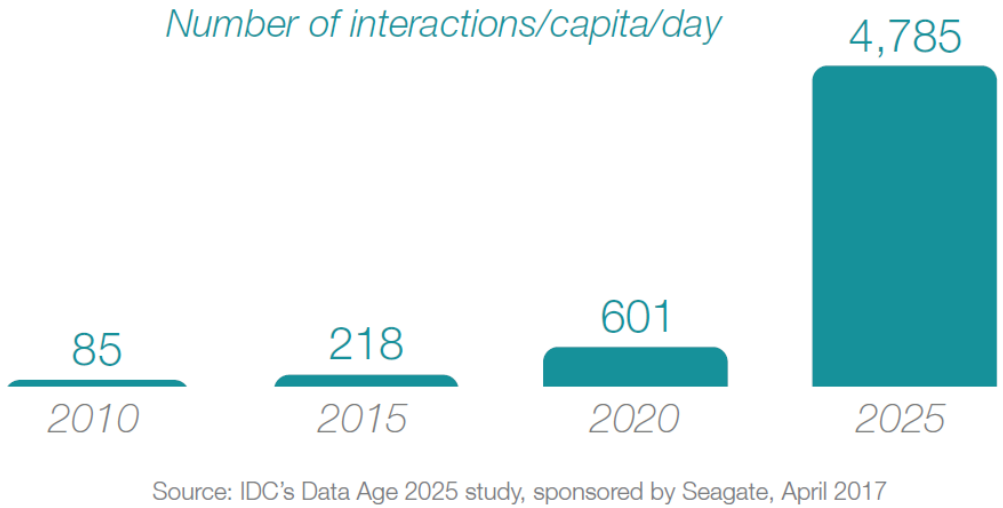
# Η «επόμενη μέρα» στη διαχείριση και στην προστασία των δεδομένων

- Τα δεδομένα (data) είναι το «καύσιμο» της σύγχρονης ψηφιακής βιομηχανίας.
- Η αξία της αγοράς προσωπικών δεδομένων θα ανέλθει σε 1 € τρισ. το 2020.
- Μέχρι το 2025 ο όγκος των δεδομένων θα αυξηθεί από 16,1 ZB σε 163 ZB (1 ZB = $1000^7$bytes = $10^{21}$bytes = 1000000000000000000000 bytes ≈ 36,000 years of HD video = 250 billion DVDs)
- Με την εκθετική αύξηση των δεδομένων αυξάνονται εκθετικά και οι κίνδυνοι παραβίασής των.
- Η διαχείριση των δεδομένων με σεβασμό στην προσωπικότητα και την ιδιωτική ζωή του καθενός μας, θα αποτελεί βασικό κριτήριο αξιολόγησης κάθε επιχείρησης/οργανισμού που χειρίζεται προσωπικά δεδομένα.

# Ρυθμός παραγωγής δεδομένων και αλληλεπιδράσεις ανθρώπου/συσκευών




**Όγκος δεδομένων που δημιουργούνται ανά έτος, σε zettabytes**




**Αλληλεπίδραση μέσου ανθρώπου με μία συνδεδεμένη συσκευή, σε φορές ανά ημέρα**

Πηγή: IDC, "Data Age 2025: The Evolution of Data to Life-Critical", 2017
https://www.seagate.com/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf

# Παραδείγματα περιπτώσεων παραβίασης της ασφάλειας δεδομένων προσωπικού χαρακτήρα (1/3)

**Περίπτωση Yahoo! Inc.**

**Προφίλ:** Εταιρεία διαδικτυακών υπηρεσιών, με έδρα τις ΗΠΑ
**Ημερομηνία συμβάντος:** 2013-2014
**Ημερομηνία ανακοίνωσης συμβάντος:** Σεπτέμβριος 2016 (αρχική) - Οκτώβριος 2017
**Περιγραφή συμβάντος:** Απώλεια προσωπικών δεδομένων (ονομάτων, ημερομηνιών γέννησης, ηλεκτρονικών διευθύνσεων και κωδικών πρόσβασης) 3 δισ. πελατών.
**Εκτίμηση κόστους:** $350 εκ. (εκτίμηση για τις απώλειες της αξίας της τιμής της μετοχής της Yahoo! ενόψει της πώλησής της στην Verizon Communications, καθώς εκείνο το διάστημα εξελίσσονταν οι διαπραγματεύσεις)
**Άλλα στοιχεία:** Η εταιρεία προέβη σε διαδοχικές ανακοινώσεις, το διάστημα από Σεπτέμβριο του 2016 έως τον Οκτώβριο του 2017, σχετικά με τον αριθμό χρηστών των οποίων τα δεδομένα παραβιάστηκαν, αυξάνοντας τον αριθμό από 500 εκ., σε 1 δισ. και τελικά σε 3 δισ. χρήστες. Τα περιστατικά παραβίασης ήταν περισσότερα από ένα, την περίοδο 2013 και 2014.

Source: https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/

# Παραδείγματα περιπτώσεων παραβίασης της ασφάλειας δεδομένων προσωπικού χαρακτήρα (2/3)

**Περίπτωση Uber Technologies Inc.**

**Προφίλ:** Εταιρεία παροχής υπηρεσιών μετακίνησης, με έδρα τις ΗΠΑ
**Ημερομηνία συμβάντος:** Οκτώβριος 2016
**Ημερομηνία ανακοίνωσης συμβάντος:** 22 Νοεμβρίου 2017
**Περιγραφή συμβάντος:** Κλοπή προσωπικών δεδομένων (ονομάτων, ηλεκτρονικών διευθύνσεων και κινητών τηλεφώνων) 57 εκ. χρηστών και 600 χιλ. οδηγών, λόγω κυβερνοεπίθεσης.
**Άλλα στοιχεία:** Η εταιρεία, εκτός του ότι προέβη σε ανακοίνωση του συμβάντος με καθυστέρηση σχεδόν ενός έτους, παραδέχτηκε ότι κατέβαλε λύτρα αξίας $100 χιλ. στους χάκερς, προκειμένου να καταστρέψουν τα προσωπικά δεδομένα που απέκτησαν (δίχως βεβαίως να υπάρχει απόδειξη για τις ενέργειες καταστροφής). Το συμβάν προκάλεσε την απόλυση του Διευθυντή Ασφαλείας.

Source: https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/

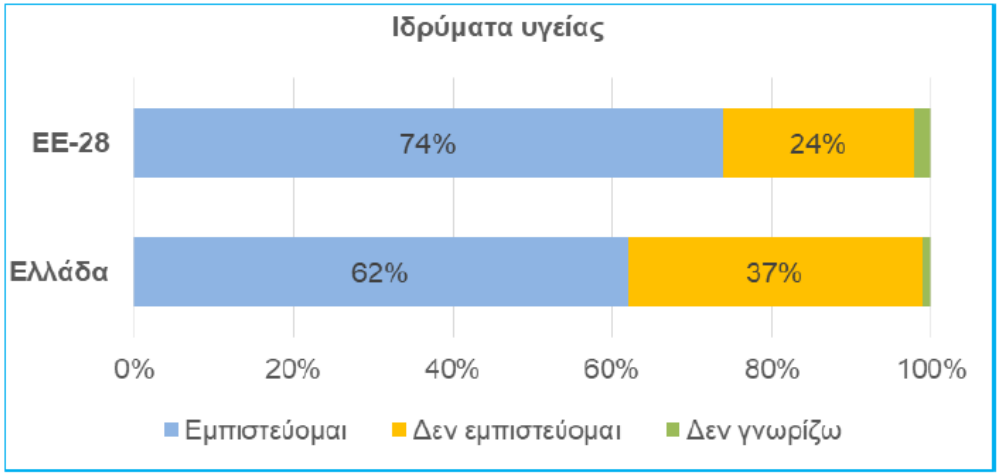
# Παραδείγματα περιπτώσεων παραβίασης της ασφάλειας δεδομένων προσωπικού χαρακτήρα (3/3)

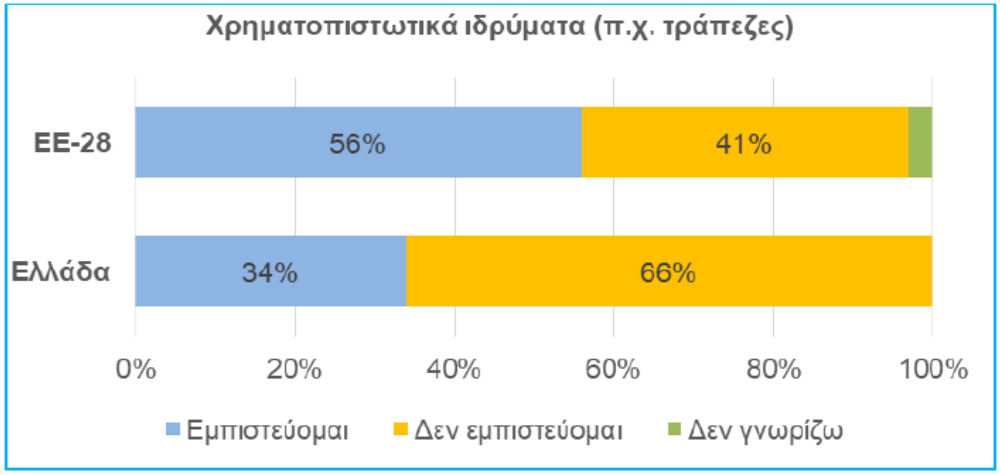
**Περίπτωση Target Stores Inc.**

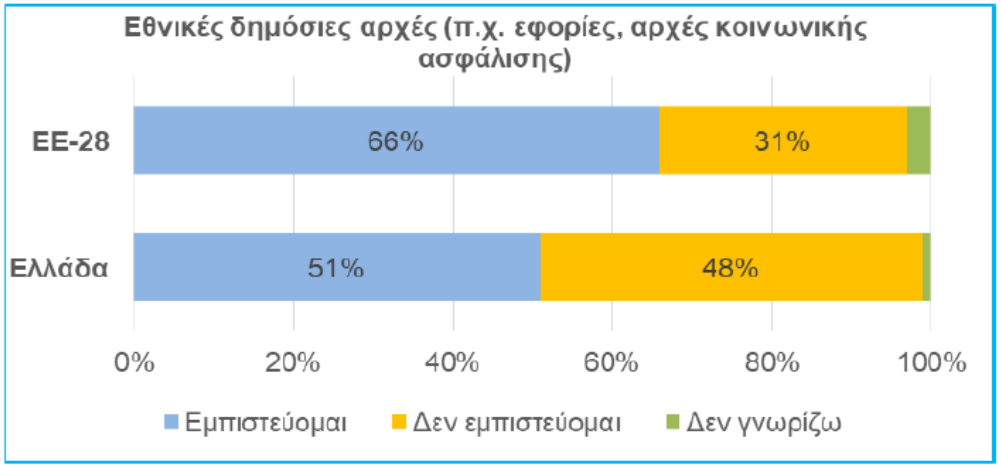
**Προφίλ:** Εταιρεία λιανικού εμπορίου, με έδρα τις ΗΠΑ
**Ημερομηνία συμβάντος:** Δεκέμβριος 2013
**Περιγραφή συμβάντος:** Κλοπή προσωπικών δεδομένων (ονομάτων, ταχυδρομικών διευθύνσεων, ηλεκτρονικών διευθύνσεων και τηλεφώνων) 110 εκ. πελατών, λόγω κυβερνοεπίθεσης.
**Εκτίμηση κόστους:** $162 εκ.
**Άλλα στοιχεία:** Εκτιμάται ότι οι χάκερς απέκτησαν πρόσβαση στα μηχανήματα υποδοχής καρτών (POS) των πελατών, μέσω ενός τρίτου προμηθευτή της εταιρείας. Η παραβίαση των δεδομένων εκτιμάται ότι αποκαλύφθηκε με καθυστέρηση ορισμένων εβδομάδων. Προκάλεσε την παραίτηση του Διευθυντή Πληροφοριακών Συστημάτων το Μάρτιο του 2014 και του Διευθύνοντα Συμβούλου δύο μήνες μετά.

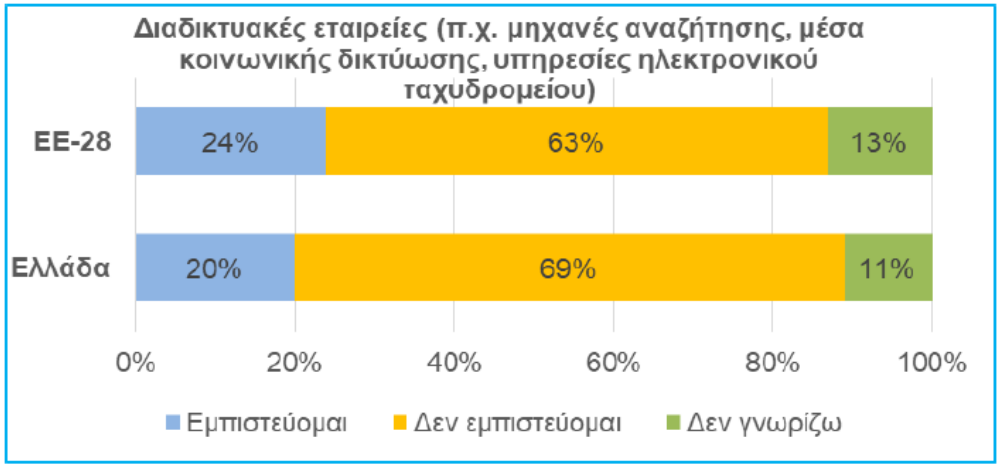
Source: https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/

# Βαθμός εμπιστοσύνης πολιτών προς δημόσιους φορείς και επιχειρήσεις σχετικά με την προστασία προσωπικών στοιχείων



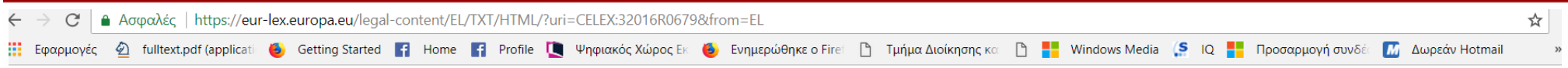

Πηγή: Ευρωβαρόμετρο, Special Eurobarometer 431 DATA PROTECTION, 2015
http://data.europa.eu/euodp/en/data/dataset/S2075_83_1_431_ENG

# Γνώμη για το βαθμό εμπλοκής της κυβέρνησης στα προσωπικά στοιχεία


Πηγή: Ευρωβαρόμετρο, Special Eurobarometer 431 DATA PROTECTION, 2015
http://data.europa.eu/euodp/en/data/dataset/S2075_83_1_431_ENG

# Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR)

https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32016R0679&from=EL






**ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΎ ΚΟΙΝΟΒΟΥΛΊΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΊΟΥ**

**της 27ης Απριλίου 2016**

**για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)**

**(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)**

ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, και ιδίως το άρθρο 16,

Έχοντας υπόψη την πρόταση της Ευρωπαϊκής Επιτροπής,

Μετά από διαβίβαση του σχεδίου νομοθετικής πράξης στα εθνικά κοινοβούλια,

Έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής [1],

Έχοντας υπόψη τη γνώμη της Επιτροπής των Περιφερειών [2],

Αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία [3],

Εκτιμώντας τα ακόλουθα:

(1) Η προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα είναι θεμελιώδες δικαίωμα. Το άρθρο 8 παράγραφος 1 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης («Χάρτης») και το άρθρο 16 παράγραφος 1 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ) ορίζουν ότι κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν.

(2) Οι αρχές και οι κανόνες για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα τους θα πρέπει, ανεξάρτητα από την ιθαγένεια ή τον τόπο διαμονής τους, να σέβονται τα θεμελιώδη δικαιώματα και τις ελευθερίες τους, ιδίως το δικαίωμά τους στην προστασία των δεδομένων προσωπικού χαρακτήρα. Ο παρών κανονισμός σκοπεύει να συμβάλλει στην επίτευξη ενός χώρου ελευθερίας, ασφάλειας και δικαιοσύνης και μιας οικονομικής ένωσης, στην οικονομική και κοινωνική πρόοδο, στην ενίσχυση και σύγκλιση των οικονομιών εντός της εσωτερικής αγοράς και στην ευημερία των φυσικών προσώπων.

(3) Η οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [4] επιδιώκει την εναρμόνιση της προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων όσον αφορά τις δραστηριότητες επεξεργασίας και τη διασφάλιση της ελεύθερης κυκλοφορίας δεδομένων προσωπικού χαρακτήρα μεταξύ κρατών μελών.

(4) Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα θα πρέπει να προορίζεται να εξυπηρετεί τον άνθρωπο. Το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα δεν είναι απόλυτο δικαίωμα· πρέπει να εκτιμάται σε σχέση με τη λειτουργία του στην κοινωνία και να σταθμίζεται με άλλα θεμελιώδη δικαιώματα, σύμφωνα με την αρχή της αναλογικότητας. Ο παρών κανονισμός σέβεται όλα τα θεμελιώδη δικαιώματα και τηρεί τις ελευθερίες και αρχές που αναγνωρίζονται στον Χάρτη όπως κατοχυρώνονται στις Συνθήκες, ιδίως τον σεβασμό της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και των επικοινωνιών, την προστασία των δεδομένων προσωπικού χαρακτήρα, την ελευθερία σκέψης, συνείδησης και θρησκείας, την ελευθερία έκφρασης και πληροφόρησης, την επιχειρηματική ελευθερία, το δικαίωμα πραγματικής προσφυγής και αμερόληπτου δικαστηρίου και την πολιτιστική, θρησκευτική και γλωσσική πολυμορφία.

(5) Η οικονομική και κοινωνική ολοκλήρωση, η οποία προέκυψε από τη λειτουργία της εσωτερικής αγοράς, έχει ως αποτέλεσμα σημαντική αύξηση των διασυνοριακών ροών δεδομένων προσωπικού χα

# Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR)

- Θεσπίστηκε: 26η Απριλίου 2016, Ημερομηνία έναρξης εφαρμογής: η 25η Μαΐου 2018.
- Ο GDPR ορίζει ένα αυστηρό και γραφειοκρατικό πλαίσιο με σκοπό να θωρακίσει την ιδιωτικότητα και να μεταθέσει την ευθύνη προστασίας των δεδομένων στην ίδια την επιχείρηση που τα διατηρεί/διαχειρίζεται.
- Κυρώσεις έως και 4% του συνολικού ετήσιου τζίρου για όσες επιχειρήσεις αποτύχουν να συμμορφωθούν.
- Ο Κανονισμός ορίζει ένα κοινό πλαίσιο ρυθμίσεων (99 άρθρα) για τον τρόπο με τον οποίο συλλέγονται, επεξεργάζονται, φυλάσσονται, διακινούνται, αξιοποιούνται, αλλά και καταστρέφονται, δεδομένα προσωπικού χαρακτήρα των πολιτών της ΕΕ, ανεξαρτήτως του τόπου διαμονής τους, τόσο σε ηλεκτρονική όσο και σε φυσική μορφή.
- Έχει γενική εφαρμογή, αφορά τόσο τις επιχειρήσεις του ιδιωτικού τομέα (ανεξαρτήτως μεγέθους και κλάδου δραστηριοποίησης), όσο και τους φορείς του δημοσίου.
- Η συμμόρφωση με τις απαιτήσεις του Κανονισμού θέτει ένα δίλημμα για κάθε επιχείρηση: άλλη μια κανονιστική/γραφειοκρατική/κοστοβόρα υποχρέωση Ή μια ευκαιρία αλλαγής του επιχειρηματικού μοντέλου/πρόκληση εισαγωγής κάθε επιχείρησης στην ψηφιακή οικονομία;

# Βασικές αρχές του GDPR

- Αρχή της λογοδοσίας: το βάρος για την απόδειξη της συμμόρφωσης μεταφέρεται από τον ρυθμιστή / ελεγκτή στον ρυθμιζόμενο / ελεγχόμενο. Οι «Υπεύθυνοι Επεξεργασίας» είναι εκείνοι που πρέπει να είναι σε θέση να αποδείξουν ότι έχουν λάβει όλα τα απαραίτητα μέτρα για την προστασία των προσωπικών δεδομένων, με την εποπτική Αρχή (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα - ΑΠΔΠΧ) να αναλαμβάνει ρόλο και δράση σε δεύτερο χρόνο, ενώ στο παρελθόν ήταν εκείνη που είχε την πρωτοβουλία για την εποπτεία και τον έλεγχο συμμόρφωσης.
- Έμφαση στα δικαιώματα του ατόμου: Ο Κανονισμός ανανεώνει τα δικαιώματα των υποκειμένων. Οι ιδιοκτήτες των προσωπικών δεδομένων έχουν ενισχυμένα δικαιώματα, γεγονός στο οποίο οι επιχειρήσεις-υπεύθυνοι επεξεργασίας οφείλουν να προσαρμοστούν και συνεπώς να μεταβάλλουν ανάλογα τη λειτουργία και τις αποφάσεις τους.

# Έργο της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

| | Προσφυγές / Καταγγελίες | Ερωτήματα | Αποφάσεις | Γνωμοδοτήσεις |
|---|---|---|---|---|
| 2008 | 670 | 1.118 | 69 | 0 |
| 2009 | 702 | 1.106 | 91 | 4 |
| 2010 | 674 | 1.261 | 84 | 4 |
| 2011 | 812 | 1.432 | 168 | 7 |
| 2012 | 675 | 1.330 | 194 | 5 |
| 2013 | 562 | 1.421 | 158 | 6 |
| 2014 | 659 | 1.615 | 202 | 5 |
| 2015 | 506 | 1.299 | 138 | 7 |
| 2016 | 714 | 1.465 | 132 | 8 |
| **Μέσος όρος** | **664** | **1.339** | **137** | **5** |

Πηγή: Ετήσια έκθεση Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), 2016
http://www.dpa.gr/portal/page?_pageid=33,15078&_dad=portal&_schema=PORTAL

# Οι 10 βασικότερες έννοιες του Κανονισμού (1/2)

| | |
|---|---|
| **Προσωπικά Δεδομένα ή Δεδομένα Προσωπικού Χαρακτήρα** | Κάθε πληροφορία που αφορά ταυτοποιημένο, ή ταυτοποιήσιμο, φυσικό πρόσωπο («υποκείμενο των δεδομένων»). Παραδείγματα αποτελούν: όνομα, επώνυμο, αριθμός ταυτότητας, ΑΜΚΑ, ΑΦΜ, τηλέφωνο, ταχυδρομική και ηλεκτρονική διεύθυνση, διεύθυνση πρωτοκόλλου διαδικτύου (IP address), γεωχωρικά δεδομένα (GPS), δηλαδή στοιχεία που μπορούν να ταυτοποιήσουν ένα φυσικό πρόσωπο. |
| **Υποκείμενο των Δεδομένων** | Πρόκειται για το φυσικό πρόσωπο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας. |
| **Επεξεργασία δεδομένων** | Κάθε πράξη που πραγματοποιείται επί των προσωπικών δεδομένων, όπως συλλογή, καταχώριση, οργάνωση, αποθήκευση, μεταβολή, ανάκτηση, αναζήτηση πληροφοριών, χρήση, διαγραφή, καταστροφή κ.λπ. |
| **Υπεύθυνος Επεξεργασίας Δεδομένων** | Το φυσικό, ή νομικό, πρόσωπο, ή δημόσια αρχή / υπηρεσία, που καθορίζει τους σκοπούς και τον τρόπο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. |
| **Εκτελών την Επεξεργασία** | Το φυσικό, ή νομικό, πρόσωπο, ή δημόσια αρχή / υπηρεσία, που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του Υπευθύνου Επεξεργασίας. Παραδείγματα Εκτελούντων την Επεξεργασία αποτελούν οι επιχειρήσεις ενημέρωσης οφειλετών και παροχής υπηρεσιών “cloud”. |
| **Υπεύθυνος Προστασίας Δεδομένων** | Ορίζεται από τον Υπεύθυνο Επεξεργασίας και τον Εκτελούντα την Επεξεργασία και συμμετέχει, δεόντως και εγκαίρως, σε όλα τα ζητήματα τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα. Αποτελεί το πρόσωπο επικοινωνίας τόσο με τα υποκείμενα των δεδομένων όσο και με την εποπτική Αρχή. |

(άρθρο 4 του Κανονισμού)

# Οι 10 βασικότερες έννοιες του Κανονισμού (2/2)

| | |
|---|---|
| **Εκτίμηση Αντικτύπου σχετικά με την προστασία δεδομένων** | Όταν ένα είδος επεξεργασίας δεδομένων, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο Υπεύθυνος Επεξεργασίας οφείλει να διενεργήσει, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία προσωπικών δεδομένων. |
| **Συγκατάθεση Υποκειμένου** | Κάθε ένδειξη βούλησης (ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει), με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν. |
| **Παραβίαση Δεδομένων Προσωπικού Χαρακτήρα** | Παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας αποκάλυψη ή πρόσβαση δεδομένων προσωπικού χαρακτήρα, τα οποία διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία. |
| **Εποπτική Αρχή Προστασίας Δεδομένων** | Πρόκειται για την ανεξάρτητη δημόσια Αρχή, καθ' ύλην αρμόδια για την εποπτεία εφαρμογής του Κανονισμού. Επικεφαλής ορίζεται η Αρχή του κράτους-μέλους όπου βρίσκεται η «κύρια εγκατάσταση»[21] του Υπευθύνου Επεξεργασίας. Ο Κανονισμός ενθαρρύνει την επικοινωνία και συνεργασία μεταξύ των διάφορων Αρχών («μηχανισμός μιας στάσης»), ώστε να διασφαλίζεται ομοιογένεια στην αντιμετώπιση υποθέσεων διευρωπαϊκού ενδιαφέροντος και ασφάλεια δικαίου. |

(άρθρο 4 του Κανονισμού)

# Ερώτηση

- **Τι είναι τα δεδομένα προσωπικού χαρακτήρα;**

Τα δεδομένα προσωπικού χαρακτήρα είναι πληροφορίες που αφορούν ένα **ταυτοποιημένο ή ταυτοποιήσιμο εν ζωή άτομο**. Διαφορετικές πληροφορίες οι οποίες, εάν συγκεντρωθούν όλες μαζί, μπορούν να οδηγήσουν στην ταυτοποίηση ενός συγκεκριμένου ατόμου, αποτελούν επίσης δεδομένα προσωπικού χαρακτήρα. Τα δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα, έχουν κρυπτογραφηθεί ή για τα οποία **έχουν χρησιμοποιηθεί ψευδώνυμα** αλλά τα οποία μπορούν να χρησιμοποιηθούν για την επαναταυτοποίηση ενός ατόμου παραμένουν δεδομένα προσωπικού χαρακτήρα και εμπίπτουν στο πεδίο εφαρμογής του ΓΚΠΔ.

**Παραδείγματα:**

- όνομα και επώνυμο·
- διεύθυνση κατοικίας· και ηλεκτρονική διεύθυνση, π.χ. όνομα.επώνυμο@εταιρεία.com·
- αναγνωριστικός αριθμός κάρτας
- δεδομένα τοποθεσίας (π.χ. η λειτουργία δεδομένων τοποθεσίας σε κινητό τηλέφωνο)
- διεύθυνση διαδικτυακού πρωτοκόλλου (IP)·
- δεδομένα που φυλάσσονται από νοσοκομείο ή γιατρό, που θα μπορούσαν να είναι ένα σύμβολο που προσδιορίζει αποκλειστικά ένα άτομο.

*Πηγή: Ευρωπαϊκή Επιτροπή. Κανόνες για επιχειρήσεις και οργανισμούς για την προστασία των δεδομένων*
https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_el

# Ερώτηση

- **Σε τι εφαρμόζεται ο Κανονισμός;**

Ο Κανονισμός ρυθμίζει την επεξεργασία από **άτομο, εταιρεία ή οργανισμό** των **δεδομένων προσωπικού χαρακτήρα** που αφορούν **άτομα** στην ΕΕ.

Δεν υπάγεται σε αυτόν η επεξεργασία δεδομένων προσωπικού χαρακτήρα αποθανόντων προσώπων ή νομικών προσώπων.

Οι κανόνες δεν εφαρμόζονται σε δεδομένα που υποβάλλονται σε επεξεργασία από ένα άτομο για αυστηρά προσωπικούς λόγους ή για δραστηριότητες που διενεργούνται κατ' οίκον, υπό την προϋπόθεση ότι δεν συνδέονται με κάποια επαγγελματική ή εμπορική δραστηριότητα.

**Πότε εφαρμόζεται ο κανονισμός**

- Μια εταιρεία με επαγγελματική εγκατάσταση στην ΕΕ παρέχει ταξιδιωτικές υπηρεσίες σε πελάτες που βρίσκονται στις χώρες των Βαλκανίων και σε αυτό το πλαίσιο υποβάλλει σε επεξεργασία δεδομένα προσωπικού χαρακτήρα φυσικών προσώπων.

**Πότε δεν εφαρμόζεται ο κανονισμός**

- Ένα άτομο χρησιμοποιεί το ιδιωτικό του βιβλίο διευθύνσεων για να προσκαλέσει φίλους μέσω ηλεκτρονικού μηνύματος σε μια γιορτή που διοργανώνει.

*Πηγή: Ευρωπαϊκή Επιτροπή. Κανόνες για επιχειρήσεις και οργανισμούς για την προστασία των δεδομένων*
https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_el

# Ερώτηση

- **Τι αποτελεί επεξεργασία δεδομένων;**

Η **συλλογή, καταχώριση, οργάνωση, διάρθρωση, αποθήκευση, προσαρμογή ή μεταβολή, ανάκτηση, αναζήτηση πληροφοριών, χρήση, κοινολόγηση με διαβίβαση, διάδοση** ή κάθε άλλη μορφή διάθεσης, **συσχέτιση ή συνδυασμό, περιορισμό, διαγραφή ή καταστροφή** δεδομένων προσωπικού χαρακτήρα. **Πότε εφαρμόζεται ο κανονισμός**

**Παραδείγματα:**

- διαχείριση προσωπικού και μισθοδοσία·
- προσπέλαση/αναζήτηση πληροφοριών σε βάση δεδομένων επαφών που περιλαμβάνει δεδομένα προσωπικού χαρακτήρα·
- αποστολή διαφημιστικών ηλεκτρονικών μηνυμάτων
- καταστροφή διά τεμαχισμού εγγράφων που περιέχουν δεδομένα προσωπικού χαρακτήρα
- δημοσίευση/ανάρτηση φωτογραφίας ενός ατόμου σε ιστότοπο
- αποθήκευση διευθύνσεων IP ή διευθύνσεων MAC
- μαγνητοσκόπηση (τηλεόραση κλειστού κυκλώματος).

*Πηγή: Ευρωπαϊκή Επιτροπή. Κανόνες για επιχειρήσεις και οργανισμούς για την προστασία των δεδομένων*
https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_el

# Ερώτηση

- **Ποιος είναι ο υπεύθυνος επεξεργασίας και ποιος ο εκτελών την επεξεργασία ;**

Μια ζυθοποιία έχει πολλούς εργαζομένους. Υπογράφει σύμβαση με εταιρεία πληρωμών για την καταβολή των μισθών. Η ζυθοποιία ενημερώνει την εταιρεία πληρωμών για το πότε πρέπει να γίνεται η πληρωμή των μισθών, πότε ένας εργαζόμενος αποχωρεί ή παίρνει αύξηση και παρέχει όλα τα υπόλοιπα στοιχεία που είναι απαραίτητα για το εκκαθαριστικό σημείωμα αποδοχών και την πληρωμή. Η εταιρεία πληρωμών παρέχει πληροφοριακό σύστημα και αποθηκεύει τα δεδομένα των εργαζομένων. Η ζυθοποιία είναι ο υπεύθυνος επεξεργασίας δεδομένων και η εταιρεία πληρωμών είναι ο εκτελών την επεξεργασία των δεδομένων.

Πηγή: Ευρωπαϊκή Επιτροπή. Κανόνες για επιχειρήσεις και οργανισμούς για την προστασία των δεδομένων
https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_el

# Ερώτηση

- **Οι υποχρεώσεις παραμένουν οι ίδιες ανεξάρτητα από τον όγκο των δεδομένων που χειρίζεται η εταιρεία ή ο οργανισμός μου;**

Ο Κανονισμός βασίζεται στην προσέγγιση με βάση τον κίνδυνο. Οι εταιρείες/οργανισμοί που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα ενθαρρύνονται να εφαρμόζουν μέτρα προστασίας **που να αντιστοιχούν στο επίπεδο κινδύνου των δραστηριοτήτων επεξεργασίας δεδομένων που εκτελούν**.

**Για παράδειγμα**, η πιθανότητα πρόσληψης ενός υπεύθυνου προστασίας δεδομένων για μια εταιρεία/έναν οργανισμό που επεξεργάζεται πολλά δεδομένα είναι υψηλότερη συγκριτικά με μια εταιρεία/οργανισμό που επεξεργάζεται μικρό όγκο δεδομένων (σε αυτήν την περίπτωση αυτό σχετίζεται με την έννοια της επεξεργασίας δεδομένων προσωπικού χαρακτήρα σε «μεγάλη κλίμακα»). Ταυτόχρονα, η φύση των δεδομένων προσωπικού χαρακτήρα και η επίδραση της σχεδιαζόμενης επεξεργασίας διαδραματίζουν επίσης έναν ρόλο. Η επεξεργασία μικρού όγκου δεδομένων, τα οποία όμως είναι ευαίσθητα (π.χ. δεδομένα υγείας), απαιτεί την εφαρμογή πιο αυστηρών μέτρων για συμμόρφωση.

Πηγή: Ευρωπαϊκή Επιτροπή. Κανόνες για επιχειρήσεις και οργανισμούς για την προστασία των δεδομένων
https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_el

# Ερώτηση

- **Τι σημαίνει η προστασία δεδομένων «ήδη από τον σχεδιασμό» και «εξ ορισμού»;**

Οι εταιρείες/οργανισμοί ενθαρρύνονται να εφαρμόζουν τεχνικά/οργανωτικά μέτρα, στα αρχικά στάδια του σχεδιασμού των πράξεων επεξεργασίας, με τρόπο ώστε να διασφαλίζονται οι αρχές ιδιωτικού απορρήτου και προστασίας δεδομένων ήδη από την αρχή («προστασία δεδομένων ήδη από τον σχεδιασμό»). Εξ ορισμού, οι εταιρείες/οργανισμοί πρέπει να διασφαλίζουν ότι τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία με το υψηλότερο επίπεδο προστασίας της ιδιωτικής ζωής.

**Παραδείγματα:**

**Προστασία δεδομένων ήδη από τον σχεδιασμό**
Χρήση ψευδωνυμοποίησης (αντικατάσταση προσωπικά ταυτοποιήσιμου υλικού με τεχνητά αναγνωριστικά στοιχεία) και κρυπτογράφησης (κωδικοποίηση μηνυμάτων ώστε μόνο όσοι είναι εξουσιοδοτημένοι να μπορούν να τα διαβάζουν).

**Προστασία δεδομένων εξ ορισμού**
Μια πλατφόρμα κοινωνικής δικτύωσης θα πρέπει να ενθαρρύνεται να ορίζει τις ρυθμίσεις των προφίλ των χρηστών ώστε να προστατεύουν όσο το δυνατόν περισσότερο το ιδιωτικό απόρρητο, για παράδειγμα, περιορίζοντας από την αρχή την προσβασιμότητα στα προφίλ των χρηστών έτσι ώστε να μην είναι προσβάσιμα εξ ορισμού από αόριστο αριθμό ατόμων.

Πηγή: Ευρωπαϊκή Επιτροπή. Κανόνες για επιχειρήσεις και οργανισμούς για την προστασία των δεδομένων
https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_el

# Ποιος είναι ο ρόλος του DPO;

- Ενημερώνει και συμβουλεύει τη διοίκηση του οργανισμού για τις υποχρεώσεις της σε σχέση με τα ΔΠΧ
- Παρακολουθεί τη συμμόρφωση με το σχετικό Ευρωπαϊκό και Εθνικό δίκαιο
- Παρέχει κατευθύνσεις σε σχέση με τις επιθεωρήσεις Data Protection Impact Assessments (DPIA), σύμφωνα με το άρθρο 35 του GDPR
- Λειτουργεί ως το σημείο επαφής με άτομα και θεσμούς περιλμβανόμενων των αρχών προστασίας ΔΠΧ (DPA).

# Πρόβλεψη για ορισμό DPO

- Οργανισμοί για τους οποίους είναι υποχρεωτικός ο ορισμός
- Δημόσιο (ευρύτερο). Δημόσιος τομέας (περιλ. συμπράξεις με ιδιωτικό), μουσεία, οργανισμοί μεταφορικού έργου, πολιτιστικά ιδρύματα, κλπ.
- Οργανισμοί που παρέχουν συστηματική επεξεργασία σε μεγάλη κλίμακα. Παράδειγμα εταιρίες που κάνουν έρευνες γνώμης, καταγραφή καταναλωτικών συμπεριφορών, profiling, etc.
- Οργανισμοί που εκτελούν επεξεργασία μεγάλης κλίμακας ειδικών τύπων δεδομένων όπως ιατρικά δεδομένα, ποινικά μητρώα. Παράδειγμα ιδιωτικές κλινικές, επιδημιολογικά δεδομένα, ασφαλιστικοί οργανισμοί.

# Εταιρίες που πρέπει να διαθέτουν DPO

- Εταιρία ύδρευσης σε μικρό δήμο. Δημοτική επιχείρηση. Παρέχει νερό σε 500 οικογένειες σε απομακρυσμένη περιοχή.
  - Επειδή ανήκει σε ευρύτερο δημόσιο φορέα, θεωρείται Public Authority, ακόμα και αν δεν πραγματοποιεί μεγάλης κλίμακας επεξεργασία
  - Απαραίτητος ο DPO

- Ιατρείο βελονισμού για θεραπεία πόνου. Έχει μια βάση 400 ασθενών. Προκειμένου να παράσχουν τις υπηρεσίες τους με ακρίβεια ζητούν στοιχεία ιατρικού ιστορικού από τους ασθενείς Αποθηκεύουν τα δεδομένα αυτά σε ηλεκτρονικό σύστημα που στέλνει υπενθυμίσεις στους ασθενείς
  - Παρόλο που έχει μικρό αριθμό ασθενών, επεξεργάζεται ιατρικά δεδομένα. Τα ιατρικά δεδομένα ανήκουν στις ειδικές κατηγορίες
  - Απαραίτητος ο DPO.

# Περιπτώσεις που δεν απαιτείται ορισμός DPO

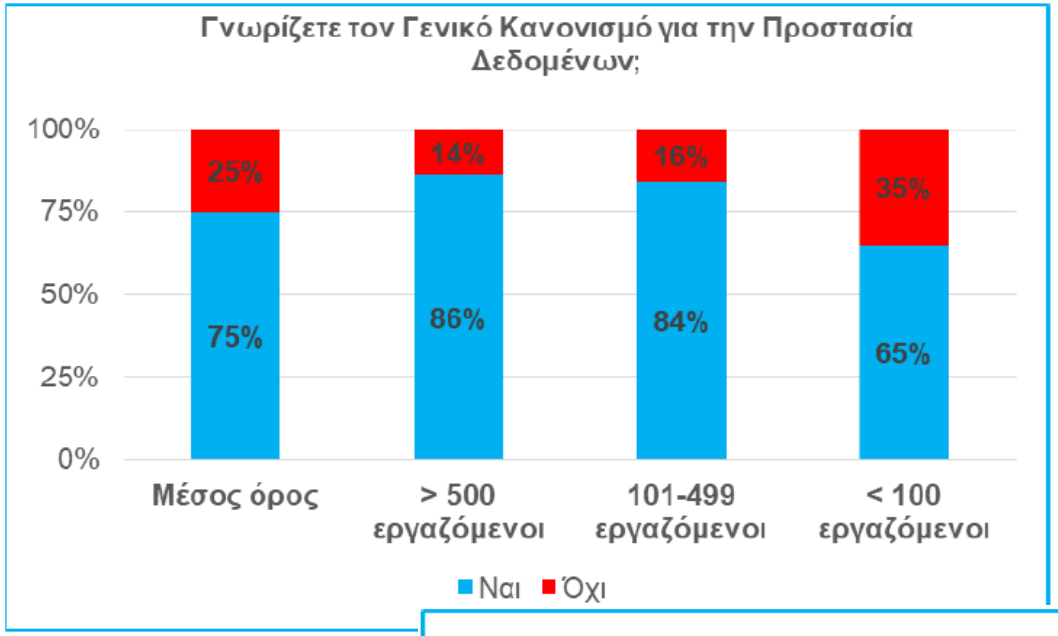
- Καθαριστήριο με 1300 πελάτες στους οποίες παρέχει εξειδικευμένες υπηρεσίες. Έχει ΒΔ με στοιχεία πελατών για να βελτιώσει τη λειτουργία του.
  - Παρόλο τον αριθμό των πελατών δεν πραγματοποιεί παρακολούθηση (monitoring) των πελατών ούτε αναλύει καταναλωτικές συμπεριφορές
  - Δεν απαιτείται ορισμός DPO.

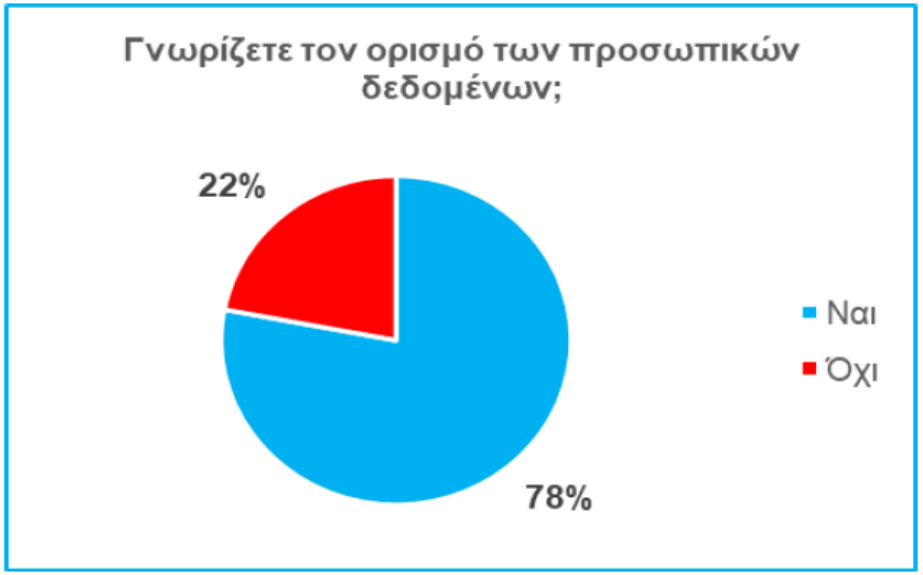
- Μικρή εταιρία συμβούλων παρέχει συμβουλευτικές μελετητικές υπηρεσίες.
  - Έχει μικρό αριθμό πελατών (15 πελάτες) για τους οποίους διατηρεί ΒΔ.
  - Οι ίδιες οι εταιρίες διατηρούν μεγάλο όγκο δεδομένων, αλλά η συμβουλευτική δεν έχει πρόσβαση σε αυτά.
  - Δεν απαιτείται ορισμός DPO.

# Περιπτώσεις εθελοντικής εμπλοκής DPO

- Μια ιδιωτικού δικαίου ΜΚΟ με αντικείμενο την προστασία δημόσιας πολιτιστικής κληρονομιάς. Χρηματοδοτείται από το Δημόσιο
  - Διατηρεί ΒΔ με τους επισκέπτες των συλλογών που τηρεί, όμως δεν πραγματοποιεί κάποια επεξεργασία τους
  - Αν και δεν απαιτείται DPO, καλό είναι να ορίσει έναν για να επιδείξει συμμόρφωση με το νόμο δεδομένης της δημόσιας χρηματοδότησης των υπηρεσιών της

# Πόσο κοντά είναι οι Ελληνικές Επιχειρήσεις στο βαθμό συμμόρφωσης με τον Κανονισμό ;





Πηγή: ICAP Management Consultants, Φεβρουάριος 2018 (δείγμα: 210 επιχειρήσεις)
http://www.icap.gr/Default.aspx?id=10594&nt=146&lang=1

# Σε ποιες ενέργειες προβαίνουν οι Επιχειρήσεις (διεθνώς) για να συμμορφωθούν με τον Κανονισμό ;


Πηγή: International Association of Privacy Professionals (IAPP), "Annual Privacy Governance Report«, 2017
https://iapp.org/media/pdf/resource_center/IAPP-2016-GOVERNANCE-SURVEY-FINAL2.pdf

# Προσέγγιση συμμόρφωσης του GDPR

- Ο κανονισμός GDPR εισάγει μια προσέγγιση βασισμένη στην επικινδυνότητα (risk-based) σε σχέση με τη συμμόρφωση με την προστασία δεδομένων.
- Στο άρθρο 37 αναφέρονται οι προϋποθέσεις, αλλά δεν μπορούν να οδηγήσουν σε κατάρτιση μιας σαφούς checklist
- Έτσι οι οργανισμοί που ορίζουν DPO προσθέτουν επιπλέον επιχειρήματα στη συνολική στρατηγική τους
  - αυτό θα τους βοηθήσει να υπερασπιστούν τα συμφέροντά τους σε περιπτώσεις επίθεσης και απώλειας δεδομένων.

# 10+1 προτεινόμενα (ΕΝΔΕΙΚΤΙΚΑ) βήματα για ορθή εφαρμογή του Κανονισμού στις Επιχειρήσεις / Οργανισμούς

Πηγή:

Σύνδεσμος Επιχειρήσεων και Βιομηχανιών (ΣΕΒ)
Τομέας Επιχειρηματικού Περιβάλλοντος και Ρυθμιστικών Πολιτικών
Special Report: Προστασία Προσωπικών Δεδομένων

http://www.sev.org.gr/Uploads/Documents/50953/SPECIAL%20REPORT_14_3_2018.pdf

# 10+1 προτεινόμενα (ΕΝΔΕΙΚΤΙΚΑ) βήματα για ορθή εφαρμογή του Κανονισμού στις Επιχειρήσεις / Οργανισμούς

## Βήμα 1: Σύσταση Ομάδας Εργασίας

Σύσταση Ομάδα Εργασίας, η οποία θα απαρτίζεται από εκπροσώπους Διευθύνσεων που εμπλέκονται περισσότερο με την προστασία των προσωπικών δεδομένων (π.χ. Πληροφορικής, Νομικής και Ανθρώπινου Δυναμικού). Σε κάθε περίπτωση, η Ομάδα Εργασίας πρέπει να έχει μικρό και ευέλικτο μέγεθος, αλλά και δυνατότητα λήψης αποφάσεων.

# 10+1 προτεινόμενα (ΕΝΔΕΙΚΤΙΚΑ) βήματα για ορθή εφαρμογή του Κανονισμού στις Επιχειρήσεις / Οργανισμούς

## Βήμα 2: Ορισμός Υπεύθυνου Προστασίας Δεδομένων (ΥΠΔ)

Υποχρεωτικό βήμα για όσες επιχειρήσεις προβαίνουν σε μεγάλης κλίμακας επεξεργασία προσωπικών δεδομένων, προαιρετικό για τις υπόλοιπες. Ο ΥΠΔ συμβουλεύει την επιχείρηση για τις υποχρεώσεις που απορρέουν από τον Κανονισμό και παρακολουθεί τις ενέργειες συμμόρφωσης με αυτόν. Συμμετέχει ενεργά σε όλα τα ζητήματα που σχετίζονται με τον Κανονισμό και αποτελεί το πρόσωπο επικοινωνίας τόσο με τα υποκείμενα των δεδομένων όσο και με την εποπτική Αρχή. Ο ΥΠΔ πρέπει να είναι άτομο κατάλληλα καταρτισμένο και προσεκτικά επιλεγμένο.

# 10+1 προτεινόμενα (ΕΝΔΕΙΚΤΙΚΑ) βήματα για ορθή εφαρμογή του Κανονισμού στις Επιχειρήσεις / Οργανισμούς

## Βήμα 3: Χαρτογράφηση της ροής των δεδομένων

Η χαρτογράφηση της πορείας των δεδομένων προσωπικού χαρακτήρα που τηρούνται και επεξεργάζονται εντός επιχείρησης (δηλαδή των δεδομένων προσωπικού, πελατών, προμηθευτών και τρίτων προσώπων) αποτελεί μια διαδικασία μέσω της οποίας απαντώνται τα εξής ερωτήματα: τί είδους δεδομένα, για ποιο σκοπό, πόσο συχνά, πώς αποκτώνται, πού υπάρχουν, ποιος έχει πρόσβαση και τα επεξεργάζεται, για πόσο χρόνο διακρατούνται. Προτείνεται η χρήση ερωτηματολογίων και η πραγματοποίηση «συνεντεύξεων» ανά Διεύθυνση προκειμένου να γίνει πλήρης καταγραφή.

# 10+1 προτεινόμενα (ΕΝΔΕΙΚΤΙΚΑ) βήματα για ορθή εφαρμογή του Κανονισμού στις Επιχειρήσεις / Οργανισμούς

## Βήμα 4: Εντοπισμός και ανάλυση κινδύνων και ελλείψεων

Αξιοποιώντας την πλήρη γνώση της ροής των προσωπικών δεδομένων (βήμα 3), η επιχείρηση οφείλει να καταγράψει τους πιθανούς κινδύνους και τις ελλείψεις που - ενδεχομένως - εντοπίστηκαν. Ενδεικτικά παραδείγματα σχετικών «κενών» είναι: πολύ μεγάλη περίοδος διατήρησης των δεδομένων άνευ λόγου, διατήρηση των ίδιων δεδομένων σε περισσότερα (του ενός) σημεία και ανεμπόδιστη πρόσβαση σε δεδομένα από όλα τα στελέχη ενώ δεν χρειάζεται.

# 10+1 προτεινόμενα (ΕΝΔΕΙΚΤΙΚΑ) βήματα για ορθή εφαρμογή του Κανονισμού στις Επιχειρήσεις / Οργανισμούς

## Βήμα 5: Εκπόνηση Εκτίμησης Αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑ)

Υποχρεωτικό βήμα για όσες επιχειρήσεις προβαίνουν σε επεξεργασία που ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, προαιρετικό για τις υπόλοιπες. Η εκπόνηση της ΕΑ εξ' ορισμού προηγείται της επεξεργασίας των δεδομένων και περιλαμβάνει ανάλυση για τις πιθανότητες επέλευσης κινδύνων και τις συνέπειες στα προσωπικά δεδομένα. Καταλήγει σε κατηγοριοποίηση των δραστηριοτήτων επεξεργασίας σε υψηλού, μεσαίου και χαμηλού κινδύνου και σε επανεξέταση των απαιτούμενων διαδικασιών σε κάθε περίπτωση.

# 10+1 προτεινόμενα (ΕΝΔΕΙΚΤΙΚΑ) βήματα για ορθή εφαρμογή του Κανονισμού στις Επιχειρήσεις / Οργανισμούς

## Βήμα 6: Αναθεώρηση πολιτικών και διαδικασιών

Με βάση τα συμπεράσματα των βημάτων 4 και 5, η επιχείρηση προβαίνει σε αναθεώρηση των πολιτικών και των διαδικασιών τήρησης και επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Παραδείγματα αποτελούν: οριστική διαγραφή και καταστροφή δεδομένων με το πέρας Χ ετών, διαμόρφωση κοινού γλωσσάριου ώστε να υπάρχει η σωστή κατανόηση από όλο το προσωπικό, θέσπιση πολιτικής «καθαρού γραφείου» (από έντυπα), κλείδωμα συρταριών, απαγόρευση εξόδου από την επιχείρηση USB sticks και laptops, ανάπτυξη πολιτικής διαβαθμισμένης πρόσβασης, ανάπτυξη πολιτικής για τις διαδρομές των φυσικών αρχείων εντός της επιχείρησης, θέσπιση ορισμένου χρόνου διατήρησης CVs κ.λπ.

# 10+1 προτεινόμενα (ΕΝΔΕΙΚΤΙΚΑ) βήματα για ορθή εφαρμογή του Κανονισμού στις Επιχειρήσεις / Οργανισμούς

## Βήμα 7: Αξιοποίηση των εργαλείων πληροφορικής

Κάθε επιχείρηση ανάλογα με τη φύση των εργασιών της, τα μεγέθη και τις δυνατότητές της, οφείλει να αξιοποιήσει κάποια από τα εργαλεία πληροφορικής που ενισχύουν την ασφάλεια των συστημάτων. Ενδεικτικά παραδείγματα αποτελούν: εργαλεία που με αυτοματοποιημένο τρόπο χαρτογραφούν τα δεδομένα (βήμα 3), εργαλεία που αξιολογούν την αποτελεσματικότητα των πολιτικών και διαδικασιών που έχουν αναπτυχθεί και εργαλεία που βοηθούν στην αποτροπή ή τον εντοπισμό των αποπειρών παραβίασης δεδομένων. Επιπλέον, η κρυπτογράφηση και η ψευδωνυμοποίηση αποτελούν δύο εκ των απλούστερων τεχνικών μέτρων προστασία.

# 10+1 προτεινόμενα (ΕΝΔΕΙΚΤΙΚΑ) βήματα για ορθή εφαρμογή του Κανονισμού στις Επιχειρήσεις / Οργανισμούς

## Βήμα 8: Ανάπτυξη διαδικασιών γνωστοποίησης εποπτικής Αρχής και ανακοίνωσης υποκειμένου

Υποχρεωτικές διαδικασίες για κάθε επιχείρηση. Η πρώτη αφορά στη διαδικασία γνωστοποίησης της παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική Αρχή, εντός μόλις 72 ωρών από τη στιγμή που η επιχείρηση αποκτά γνώση του γεγονότος. Η δεύτερη αφορά στη διαδικασία άμεσης ανακοίνωσης της παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων, όταν υπάρχει ενδεχόμενο να τεθούν σε υψηλό κίνδυνο τα δικαιώματα και οι ελευθερίες του. Ο επικοινωνιακός χειρισμός σε αυτήν την περίπτωση είναι κρίσιμης σημασίας και μπορεί να κάνει τη διαφορά όσον αφορά στη φήμη της επιχείρησης.

# 10+1 προτεινόμενα (ΕΝΔΕΙΚΤΙΚΑ) βήματα για ορθή εφαρμογή του Κανονισμού στις Επιχειρήσεις / Οργανισμούς

## Βήμα 9: Δοκιμαστικοί έλεγχοι συστημάτων και διαδικασιών

Αναφέρεται σε δοκιμαστικούς ελέγχους επί των συστημάτων και διαδικασιών που έχει αναπτύξει η επιχείρηση στα προηγούμενα βήματα, προκειμένου να εξασφαλιστεί ότι οι ενέργειες συμμόρφωσης θα δουλέψουν αποτελεσματικά στην πράξη. Ενδεχομένως, οδηγήσει σε ανάγκη υλοποίησης διορθωτικών παρεμβάσεων.

# 10+1 προτεινόμενα (ΕΝΔΕΙΚΤΙΚΑ) βήματα για ορθή εφαρμογή του Κανονισμού στις Επιχειρήσεις / Οργανισμούς

## Βήμα 10: Διαρκής παρακολούθηση και επικαιροποίηση των διαδικασιών και των συστημάτων

Η συμμόρφωση στον Κανονισμό είναι μια δυναμική «άσκηση» και στο πλαίσιο αυτό οι επιχειρήσεις οφείλουν συνεχώς να επικαιροποιούν τις διαδικασίες τους (ή έστω να εξετάζουν την αναγκαιότητα επικαιροποίησής τους) και να αναβαθμίζουν τα συστήματά τους. Όπως στο βήμα 9 συστήνονται δοκιμαστικοί έλεγχοι των συστημάτων και διαδικασιών πριν την έναρξη εφαρμογής του Κανονισμού, όμοια προτείνονται αντίστοιχες δοκιμές και μετά την έναρξη εφαρμογής του.

# 10+1 προτεινόμενα (ΕΝΔΕΙΚΤΙΚΑ) βήματα για ορθή εφαρμογή του Κανονισμού στις Επιχειρήσεις / Οργανισμούς

## Βήμα 11: Εκπαίδευση προσωπικού

Η επιχείρηση οργανώνει εκπαιδευτικές δράσεις, προς το σύνολο του προσωπικού, προκειμένου να εξασφαλίσει ότι όλοι γνωρίζουν τις πολιτικές και τις διαδικασίες που έχουν αναπτυχθεί για την προστασία των προσωπικών δεδομένων, γιατί είναι σημαντικές για την επιχείρηση, αλλά και τί πρέπει να κάνουν σε περίπτωση που αντιληφθούν απειλή παραβίασης. Οι εν λόγω δράσεις προτείνεται να επαναλαμβάνονται, με βάση τις ανάγκες και τα χαρακτηριστικά κάθε επιχείρησης (π.χ. δραστηριότητα υψηλού κινδύνου, μεγάλη / συχνή αλλαγή προσωπικού, σημαντικές αλλαγές επί των πολιτικών και διαδικασιών κ.λπ.).

# Συμπέρασμα:

Σκοπός δεν πρέπει να είναι η εφαρμογή του Κανονισμού «μόνο στα χαρτιά».

Σκοπός είναι να αλλάξουμε ουσιαστικά την κουλτούρα των επιχειρήσεων/οργανισμών μας, διαφυλάττοντας τα προσωπικά δεδομένα που διαχειριζόμαστε, δείχνοντας έμπρακτα σεβασμό στην ιδιωτική ζωή του κάθε ατόμου, είτε είναι εργαζόμενος είτε είναι πελάτης είτε είναι οποιοσδήποτε πολίτης.

## Προτεινόμενη πηγή ενημέρωσης:

Special Report: Προστασία Προσωπικών Δεδομένων
Σύνδεσμος Επιχειρήσεων και Βιομηχανιών (ΣΕΒ)
Τομέας Επιχειρηματικού Περιβάλλοντος και Ρυθμιστικών Πολιτικών
http://www.sev.org.gr/Uploads/Documents/50953/SPECIAL%20REPORT_14_3_2018.pdf