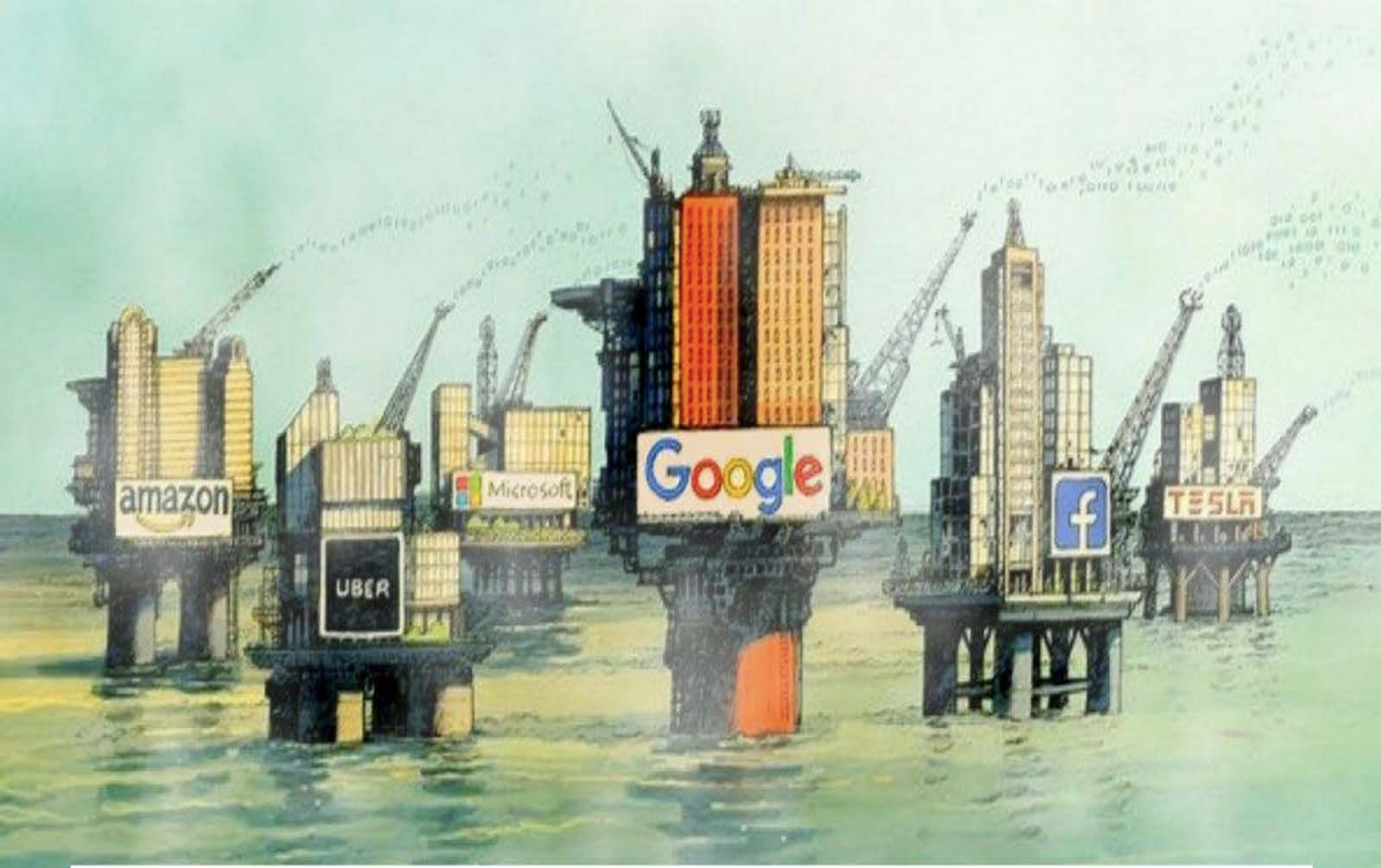
Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) και η επιρροή του στην Επιστημονική Έρευνα

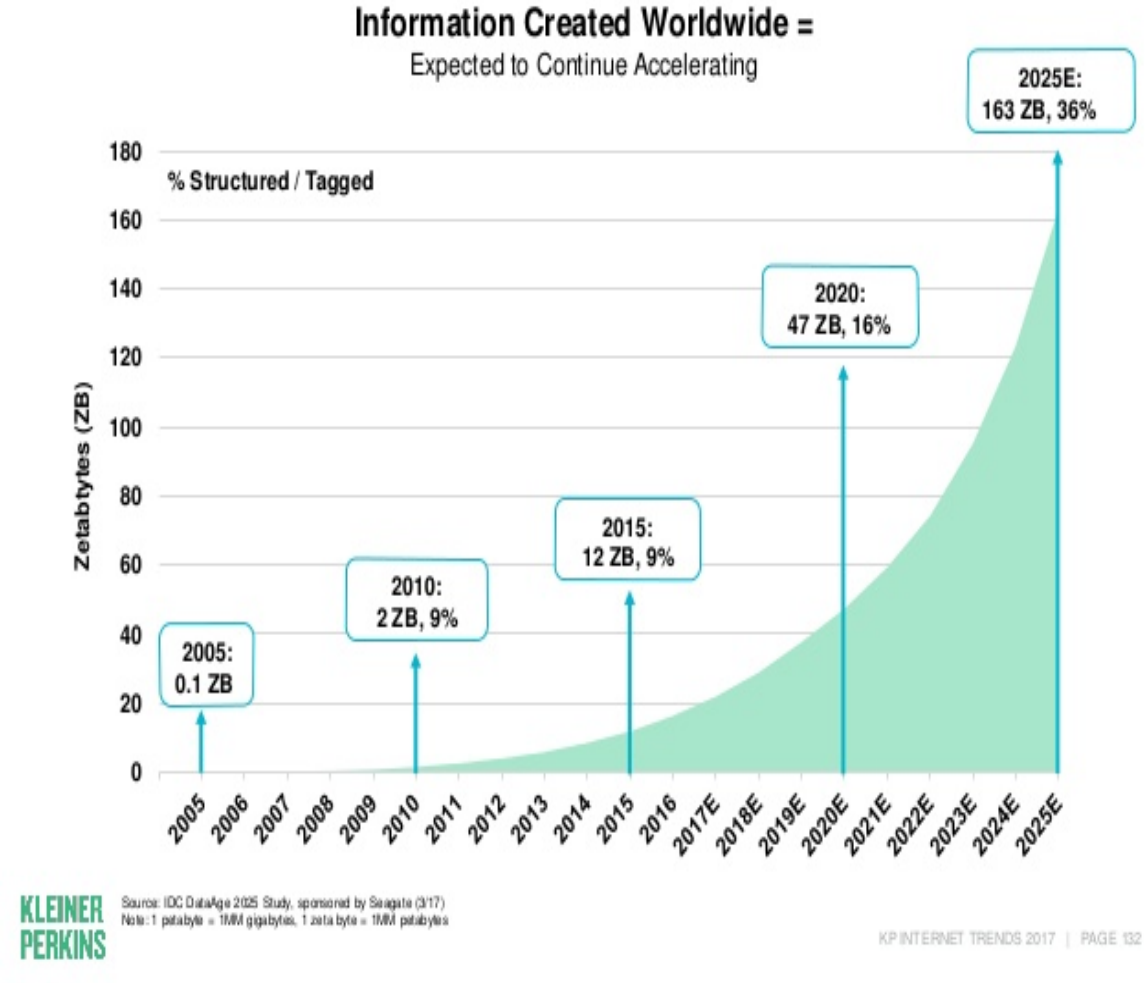
Κωνσταντίνος Λαμπρινουδάκης
Καθηγητής, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιώς
Τακτικό Μέλος Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
clam at unipi.gr



The world's most valuable resource is no longer oil, but data.

The Economist - May 2017

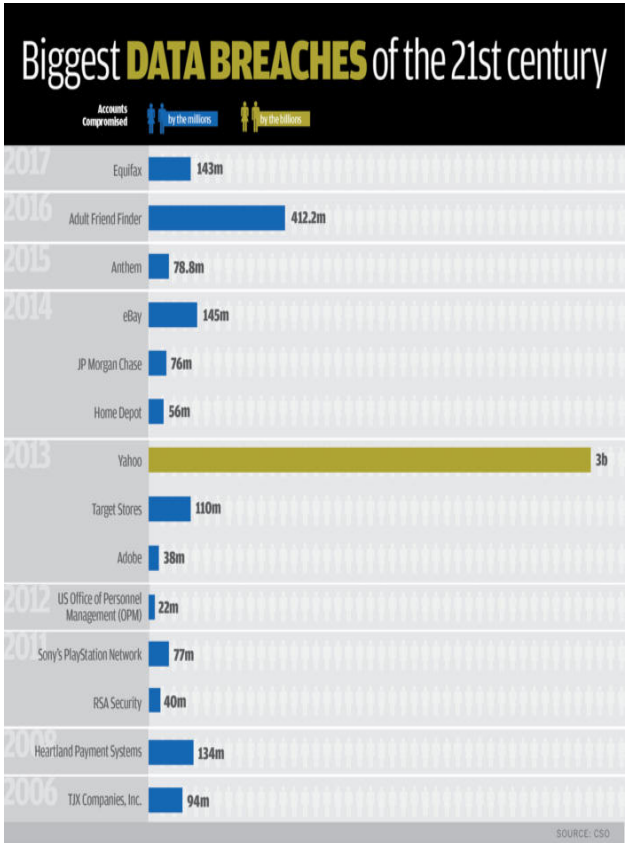
Data Volume Growth Continues @ Rapid Clip…
% Structured / Tagged (~10%) Rising Fast…

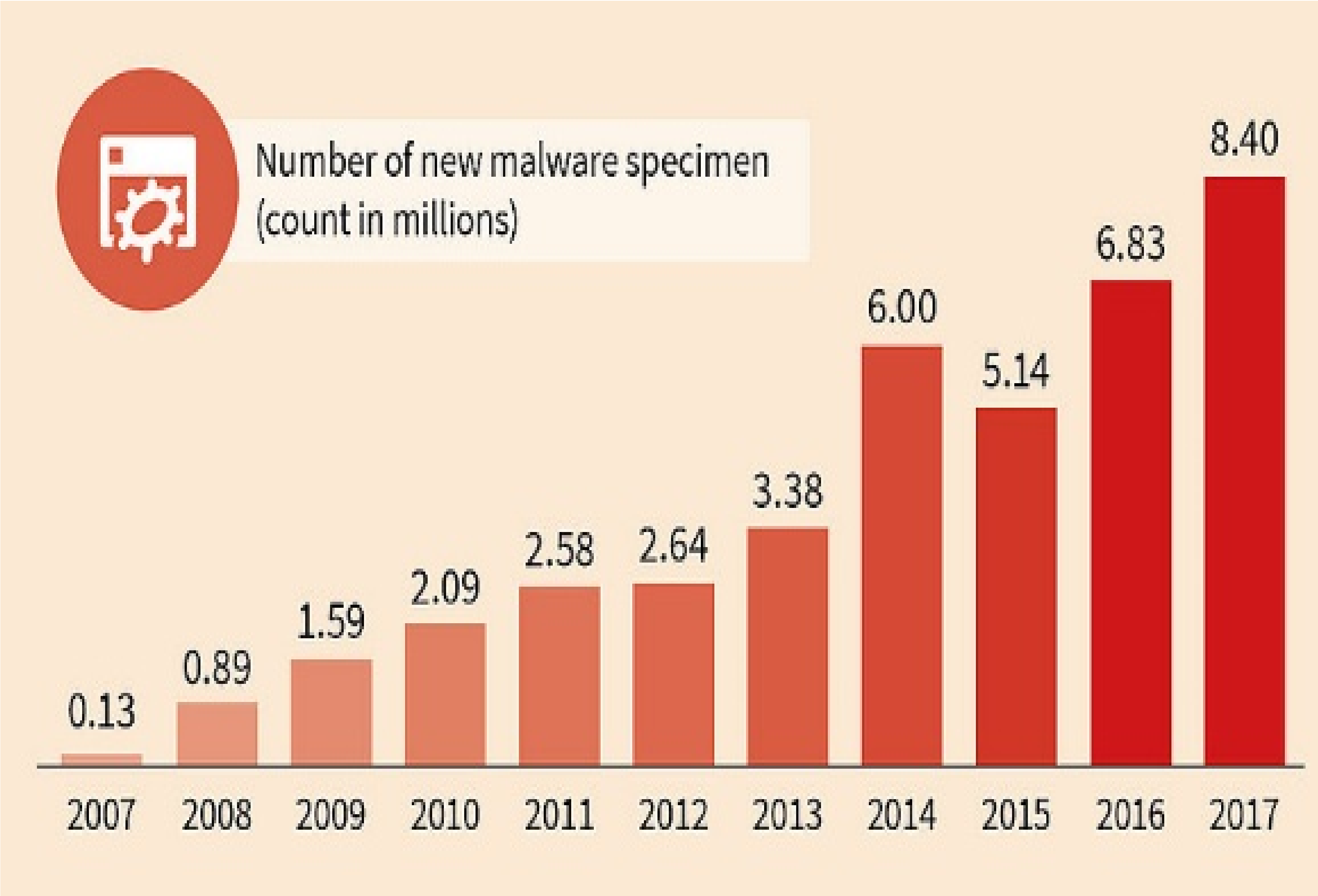


British Airways data breach

- BA announced that **380,000 card payments** were compromised
- Breach relates to bookings made between 10.58pm on 21 August and 9.45pm on 5 September 2018.

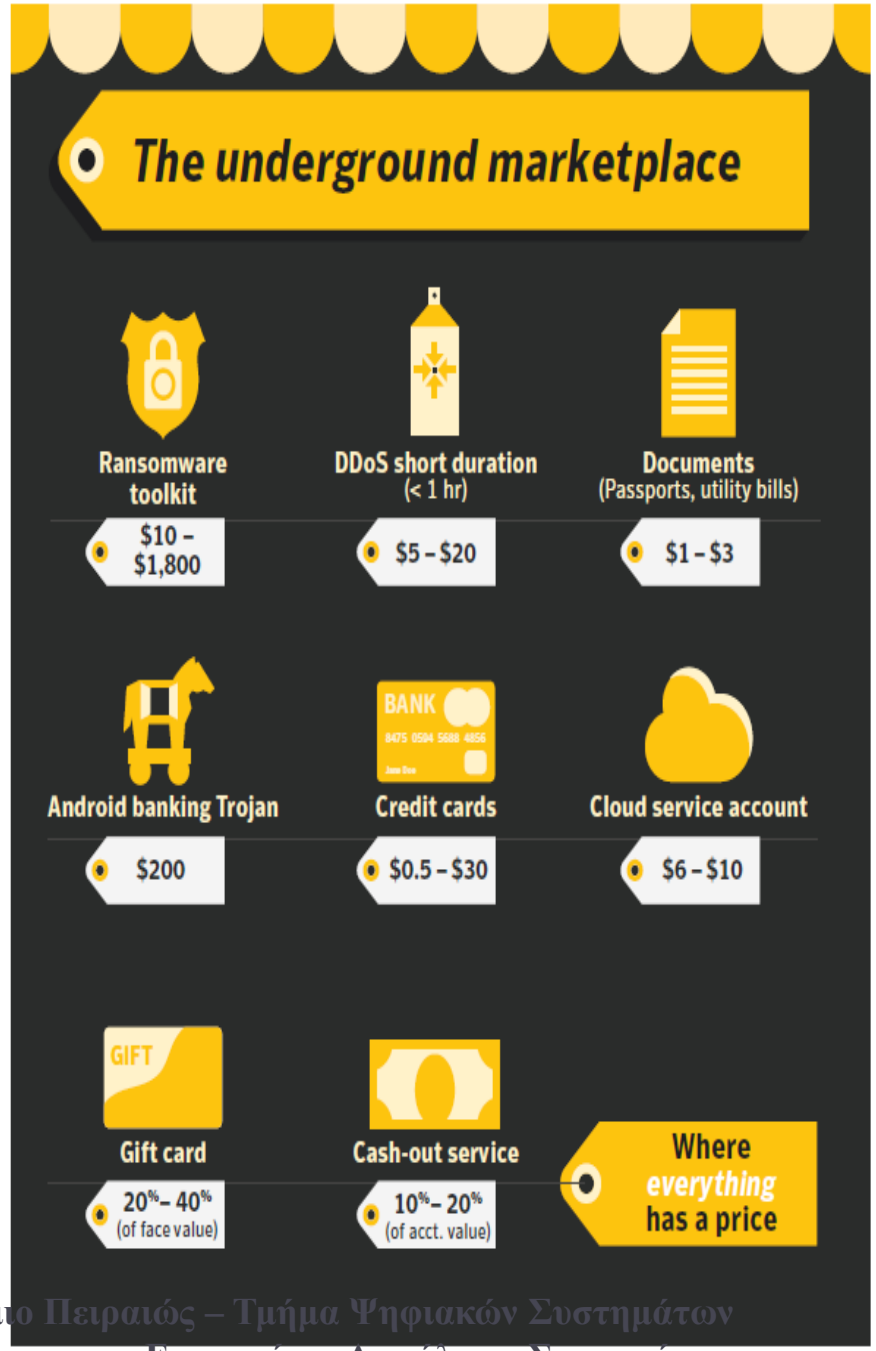
The last 8 years more than 7.1 Billion identities have been exposed in data breaches

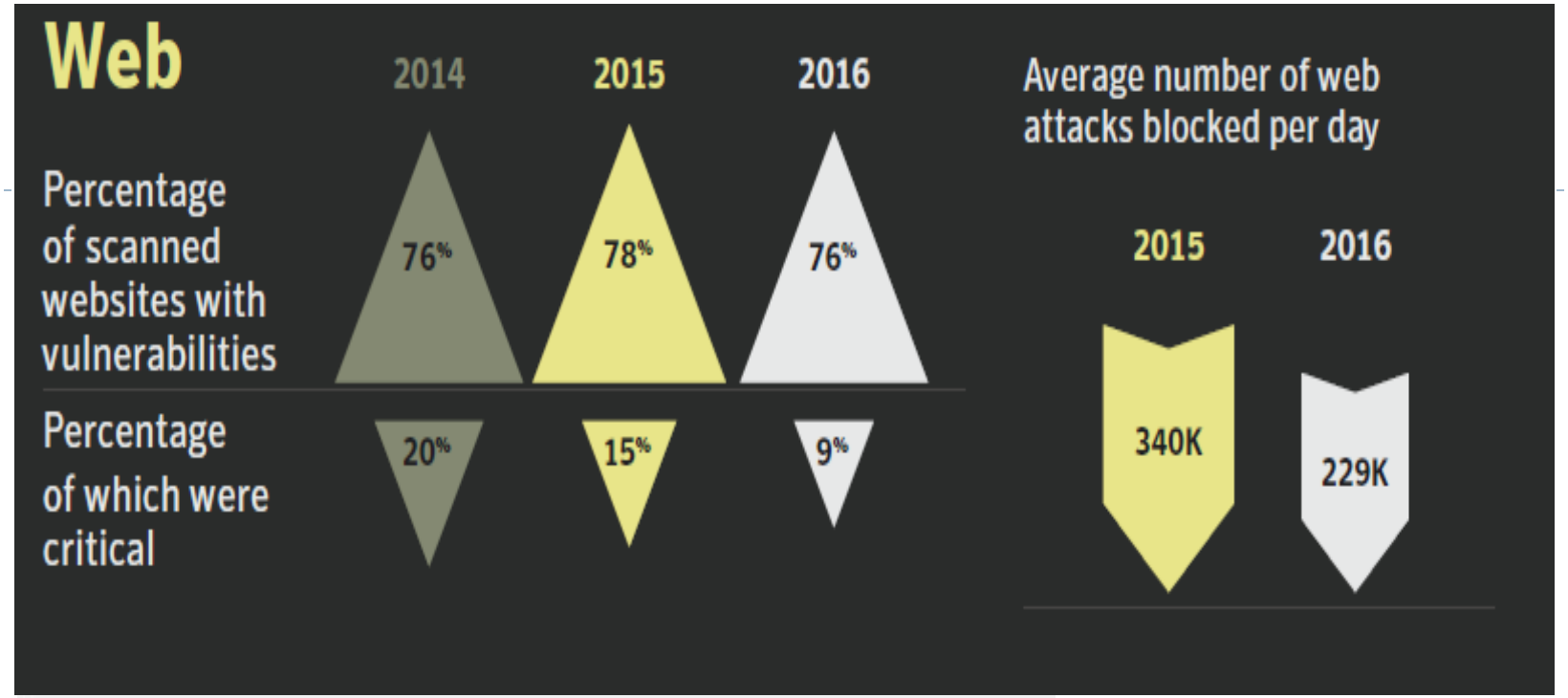




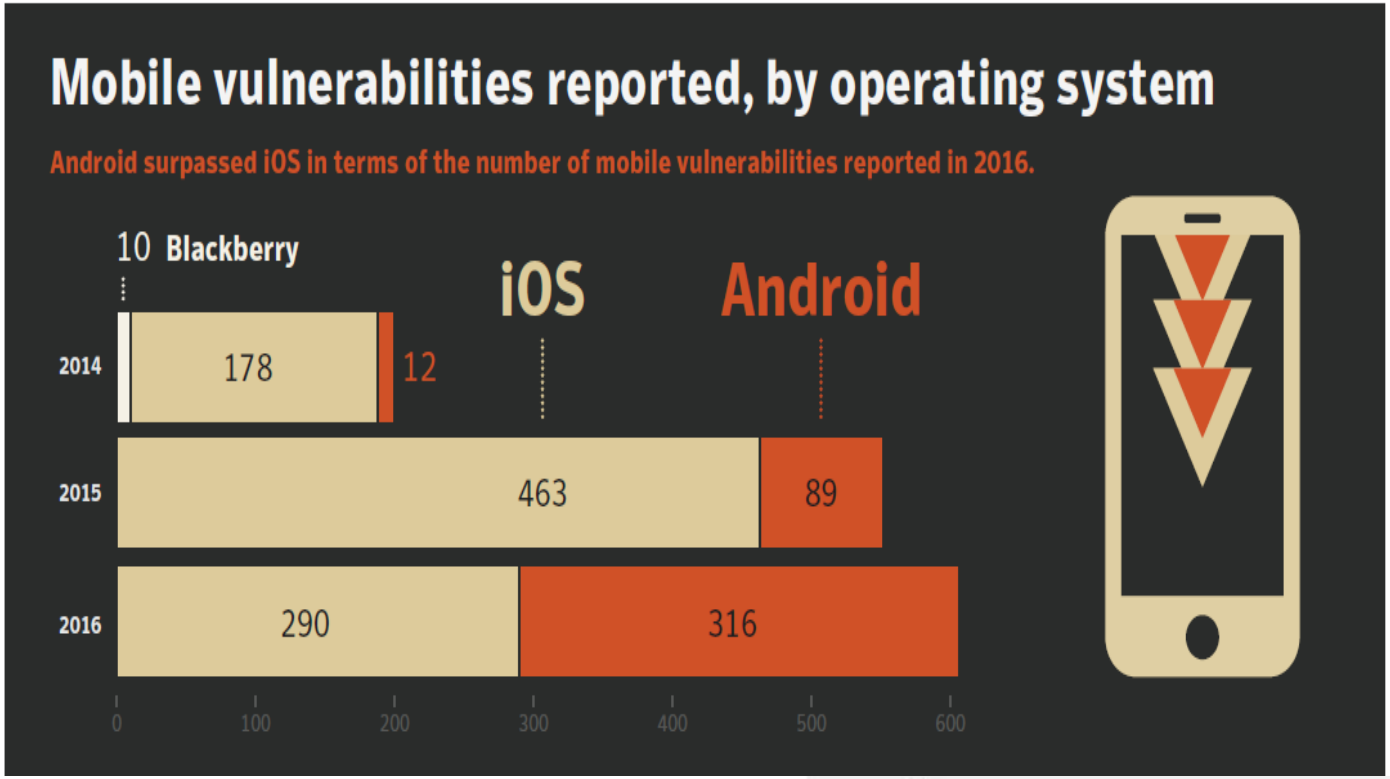
https://www.gdatasoftware.com/blog/2018/03/30610-malware-number-2017


ΚΑΛΜΟΛ
ΚΑΛΜΟΛ

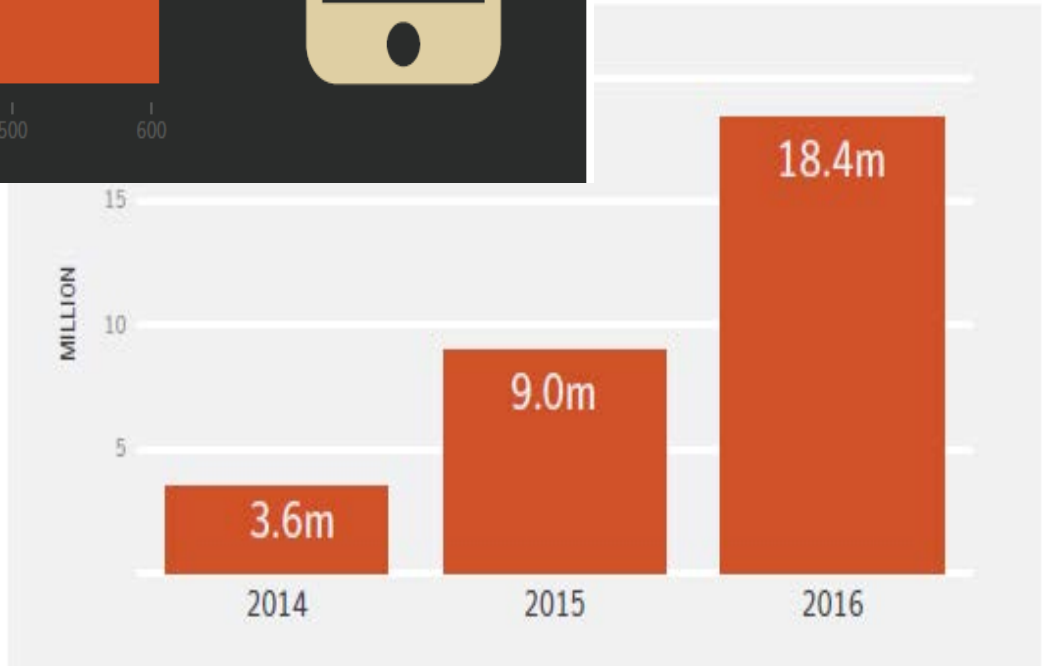

The underground marketplace
Ransomware toolkit
$10 – $1,800
DDoS short duration (< 1 hr)
$5 – $20
Documents (Passports, utility bills)
$1 – $3
Android banking Trojan
$200
BANK
Credit cards
$0.5 – $30
Cloud service account
$6 – $10
GIFT
Gift card
20% – 40% (of face value)
Cash-out service
10% – 20% (of acct. value)
Where everything has a price



← **Zero-day vulnerabilities**



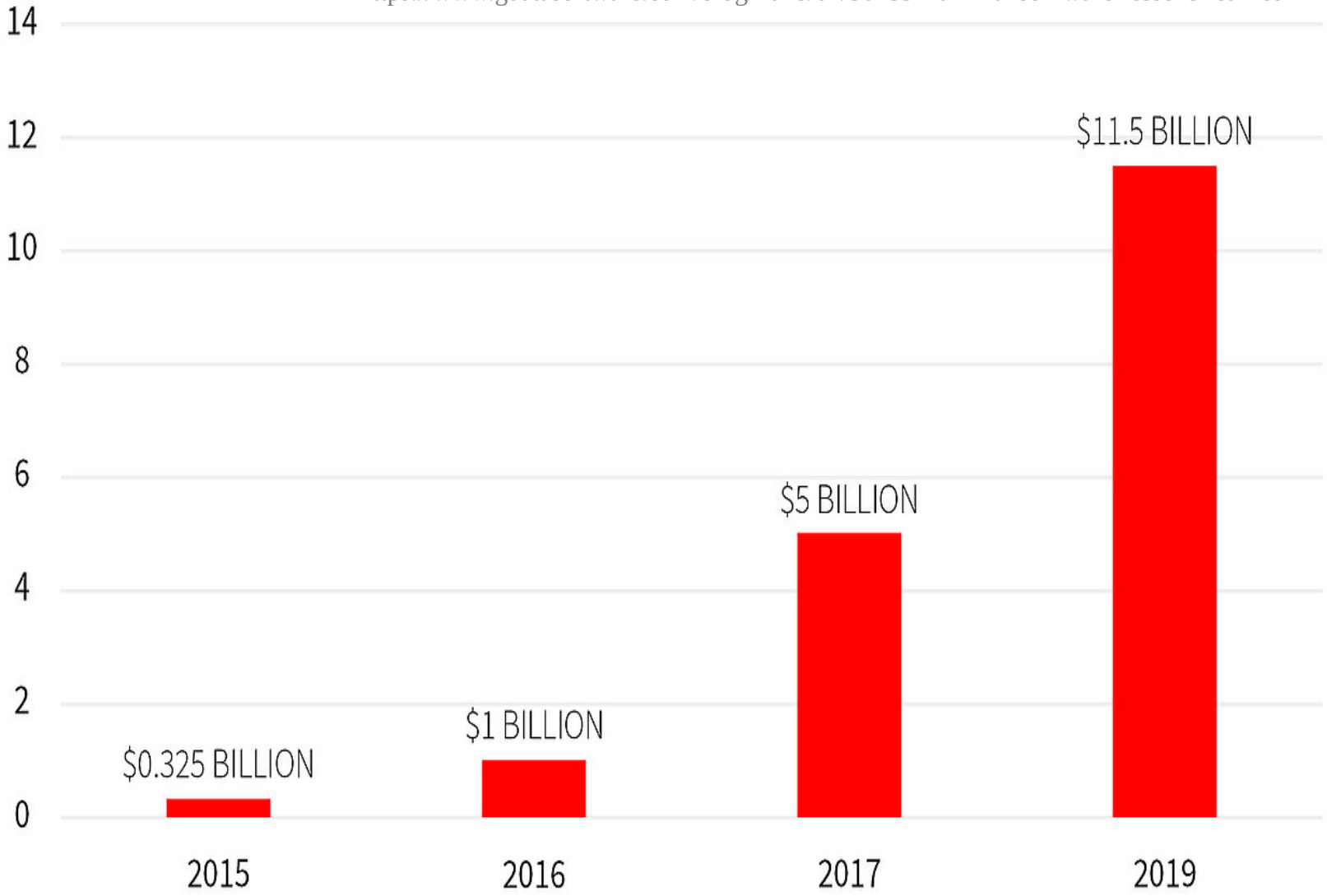
Number of mobile malware detection ➔



https://www.symantec.com/security-center/threat-report

RANSOMWARE: TOTAL DAMAGE COST

https://www.gdatasoftware.com/blog/2018/02/30439-2017-ransomware-lessons-learned



Shodan: The IoT search engine for watching sleeping kids and bedroom antics

[Opinion] Shodan is not the devil, but rather a messenger which should make us take responsibility for our own security in a world of webcams and mobile devices.

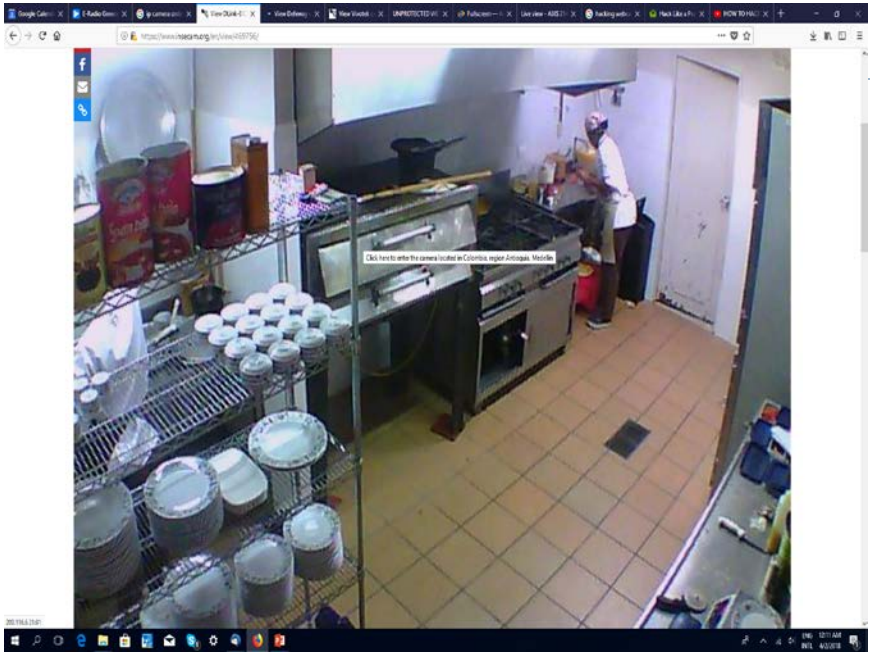
By Charlie Osborne for Zero Day | January 26, 2016 -- 11:43 GMT (11:43 GMT) | Topic: Security

The most shocking of Shodan

SEE FULL GALLERY

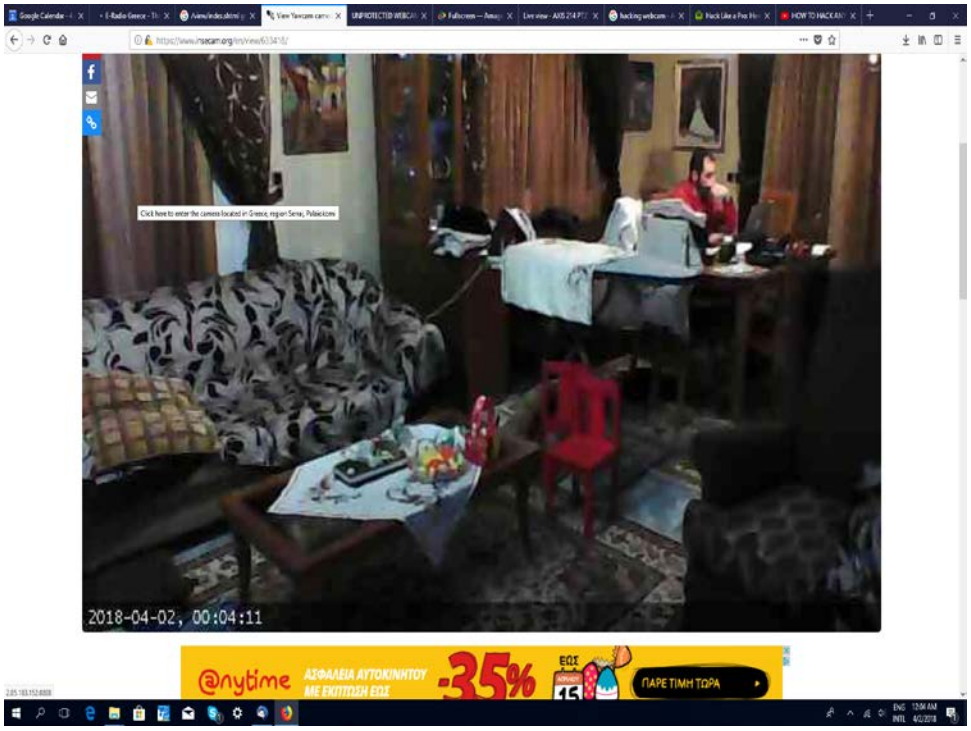
The most shocking of Shodan

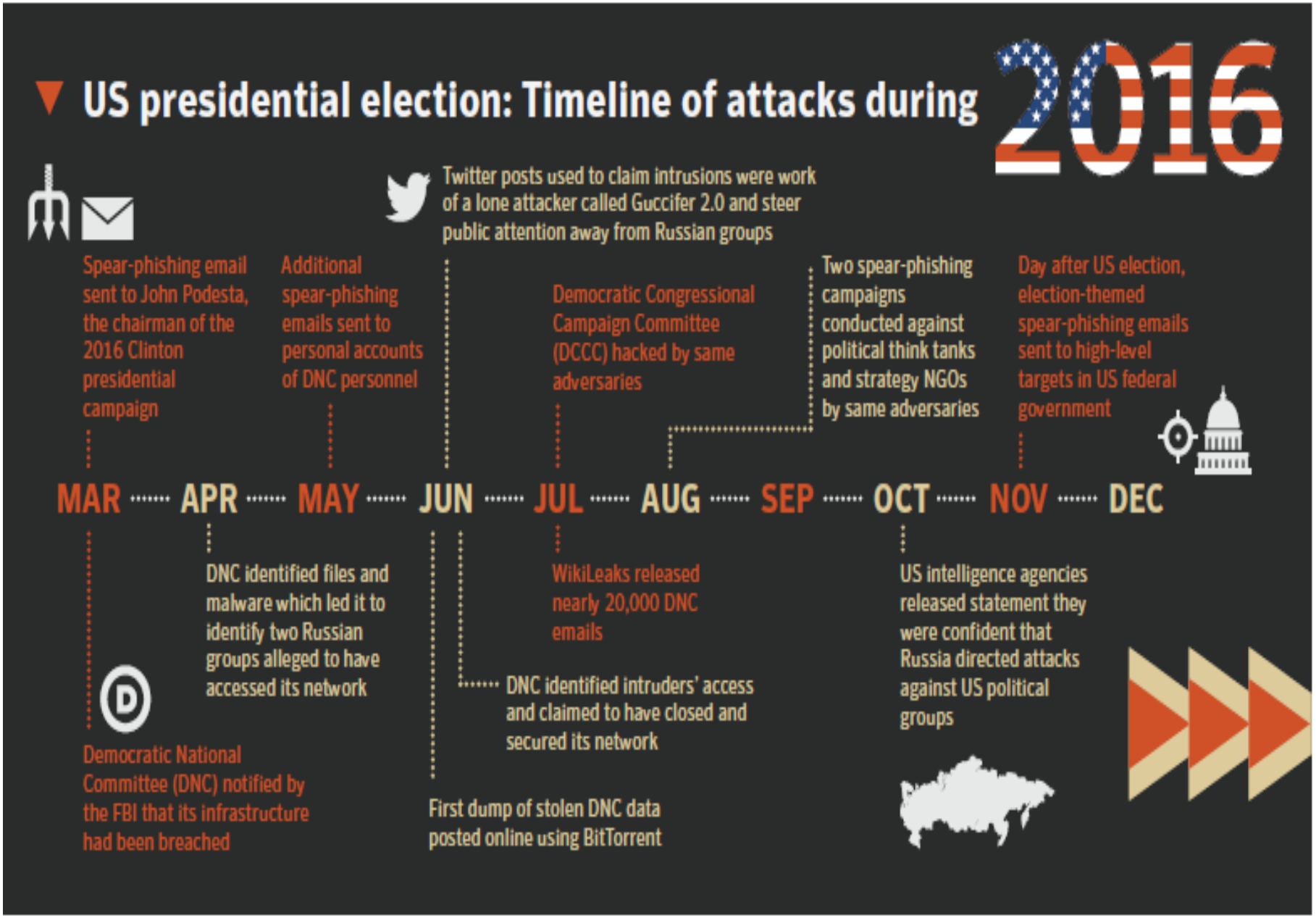
SEE FULL GALLERY



https://www.insecam.org/

/view/index.s
html greece

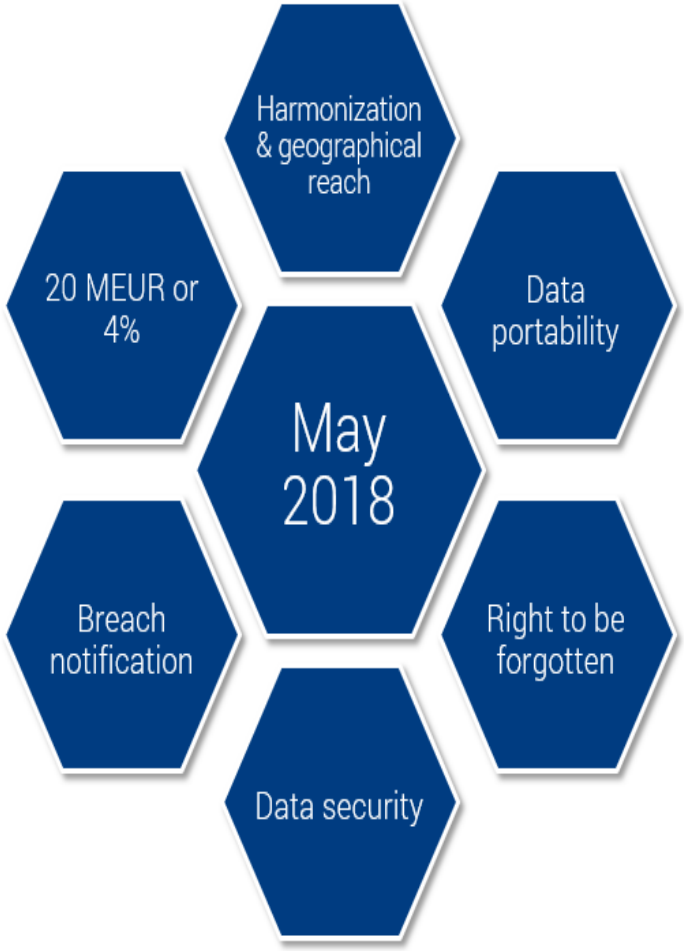




https://www.symantec.com/security-center/threat-report

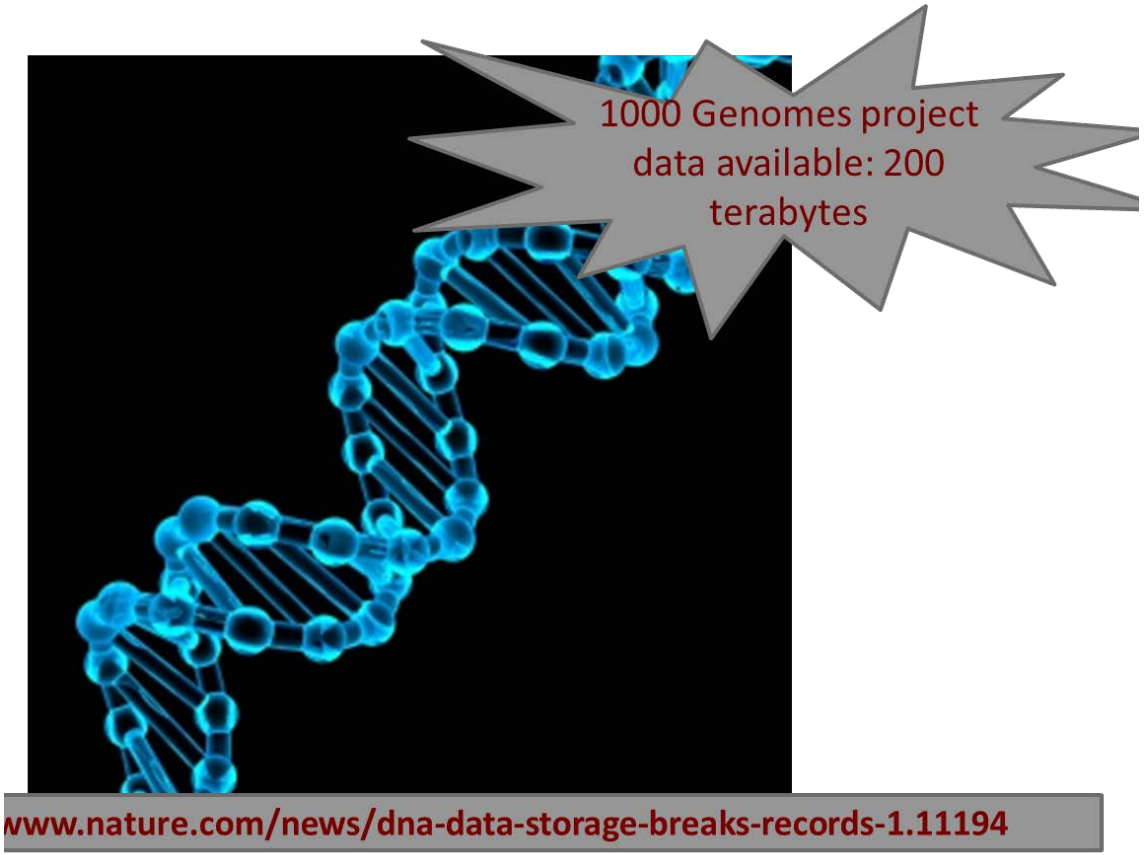
General Data Protection Regulation – GDPR

Cybercrime can no longer be considered as an acceptable 'running cost' of business



Biological Data - Έρευνα

- Έρευνα για αποκωδικοποίηση του DNA
- Ανάλυση Γονιδίων

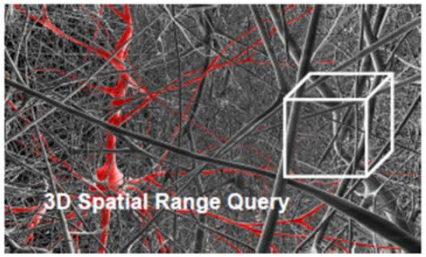


Human Brain Project- Έρευνα

- Τεράστιος Όγκος Δεδομένων
- Χωρική Ανάλυση

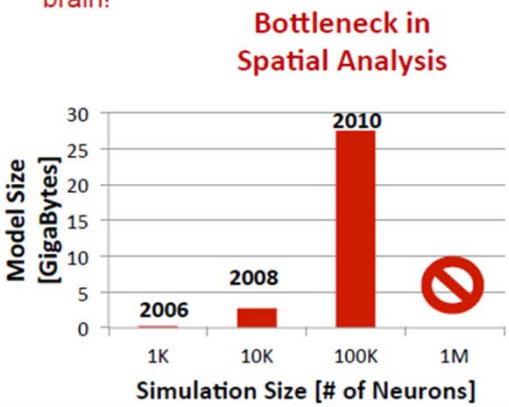
- *"The goal of the Human Brain Project is to build a completely new information computing technology infrastructure for neuroscience and for brain-related research in medicine and computing, catalysing a global collaborative effort to understand the human brain and its diseases and ultimately to emulate its computational capabilities"*

FET Flagship project, funded >1billion euro, with 135 partner institutions from 26 countries



86 billion of neurons
100 trillion of synapses

develop platform to simulate human brain!



Source: Timos Sellis talk @Univ.of Piraeus, 12/1/2015
Slides: http://www.datastories.org/wp-content/uploads/2014/09/Timos_Sellis_Big_Data_UNIPI.compressed.pdf

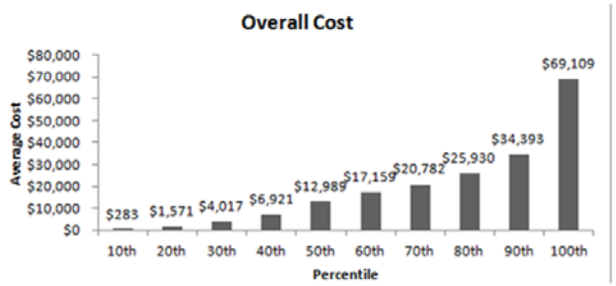
Εξαγωγή Συμπερασμάτων ....

- Ιατρική Πρόοδος
- Βελτίωση Υπηρεσιών
- Εξοικονόμηση Πόρων

MASSACHUSETTS GENERAL HOSPITAL

MGH Cancer Center
"Super-Database"

- Largest cancer database in the world (173,301 patients)
- Based on national tumor registry
- Cross linked with death registry
- Includes billing, reports, labs, imagery, genome SNPs



Question:
What are the factors driving costs for lung cancer patients?

Some results:
No correlation of cost with
- **Stage of presentation**
- **Survival**

Source: Sam Madden's VLDB'13 keynote talk

ΓΚΠΔ (GDPR)

- Καθορίζει τις απαιτήσεις για την προστασία των φυσικών προσώπων όσον αφορά στην επεξεργασία δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών
- Είναι υποχρεωτικός για τους οργανισμούς που διαχειρίζονται προσωπικά δεδομένα Ευρωπαίων πολιτών

Προσωπικά Δεδομένα

- Κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο
- Το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου

Ειδικές Κατηγορίες Προσωπικών Δεδομένων

- Δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό

Υπεύθυνος Επεξεργασίας Δεδομένων

- Φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με τις γενικές αρχές του ΓΚΠΔ (#5)
- Εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον ΓΚΠΔ, λαμβάνοντας υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων (#24)

Αρχεία Δραστηριοτήτων Επεξεργασίας

Τεκμηρίωση κάθε πράξης επεξεργασίας

Καταργείται η υποχρέωση γνωστοποίησης στις εποπτικές Αρχές.

Τα αρχεία αυτά περιλαμβάνουν

- **Ποιος**; (ταυτότητα υπευθύνου, τρόπος επικοινωνίας, εκπρόσωπος και DPO)
- **Γιατί**; (σκοπός επεξεργασίας)
- **Τι**; (κατηγορίες υποκειμένων δεδομένων, κατηγορίες δεδομένων)
- **Σε ποιον**; (κατηγορίες αποδεκτών)
- **Διαβιβάσεις**: (σε χώρες εκτός Ε.Ε.)
- **Για πόσο**; (προθεσμία διαγραφής κάθε κατηγορίας δεδομένων)
- **Πώς**; (γενική περιγραφή μέτρων ασφάλειας)

> 250 εργαζόμενοι => Εσωτερικά αρχεία κάθε επεξεργασίας

< 250 εργαζόμενοι => Αρχεία επεξεργασιών με διακινδύνευση

Υπεύθυνος Προστασίας Δεδομένων

- **Υποχρέωση ορισμού Υπεύθυνου Προστασίας Δεδομένων (DPO):**
  - Δημόσιες αρχές
  - Τακτική και συστηματική παρακολούθηση υποκειμένων σε μεγάλη κλίμακα
  - Μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων (και ποινικών)
- **Ρόλος DPO:**
  - Συμβουλεύει τον υπεύθυνο/εκτελούντα
  - Εκπαίδευση – ευαισθητοποίηση προσωπικού
  - Εσωτερικοί έλεγχου σε ζητήματα προσωπικών δεδομένων – παρακολούθηση συμμόρφωσης
  - Σημείο επαφής με Εποπτική Αρχή – συνεργασία μαζί της
  - Τα υποκείμενα των δεδομένων μπορούν να επικοινωνούν μαζί του
- **Το προφίλ ενός DPO:**
  - Εμπειρία στον τομέα του Δικαίου και των πρακτικών περί προστασίας δεδομένων
  - Λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο
  - Ενεργεί ανεξάρτητα – δεν λαμβάνει εντολές για την εκτέλεση των καθηκόντων του
  - Διαθέτει επαρκείς πόρους
  - Μπορεί να είναι υπάλληλος ή εξωτερικός συνεργάτης

Data protection by Design by Default

- **...από το σχεδιασμό** :
  - Τεχνολογίες ιδιωτικότητας και προστασία προσωπικών δεδομένων κατά το σχεδιασμό συστήματος/επεξεργασίας και όχι εκ των υστέρων
  - **Λαμβάνοντας υπόψη:**
    - Τελευταίες εξελίξεις τεχνολογίας
    - Κόστος εφαρμογής μέτρων
    - Φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας,
    - Ελαχιστοποίηση πιθανότητας κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων από την επεξεργασία
  - **Μέσα επίτευξης:**
    - Ελαχιστοποίηση δεδομένων
    - Ψευδωνυμοποίηση

- **...εξ ορισμού**:
  - Οι «προ-καθορισμένες» ρυθμίσεις πρέπει να είναι οι πιο φιλικές προς την ιδιωτικότητα

Ασφάλεια επεξεργασίας

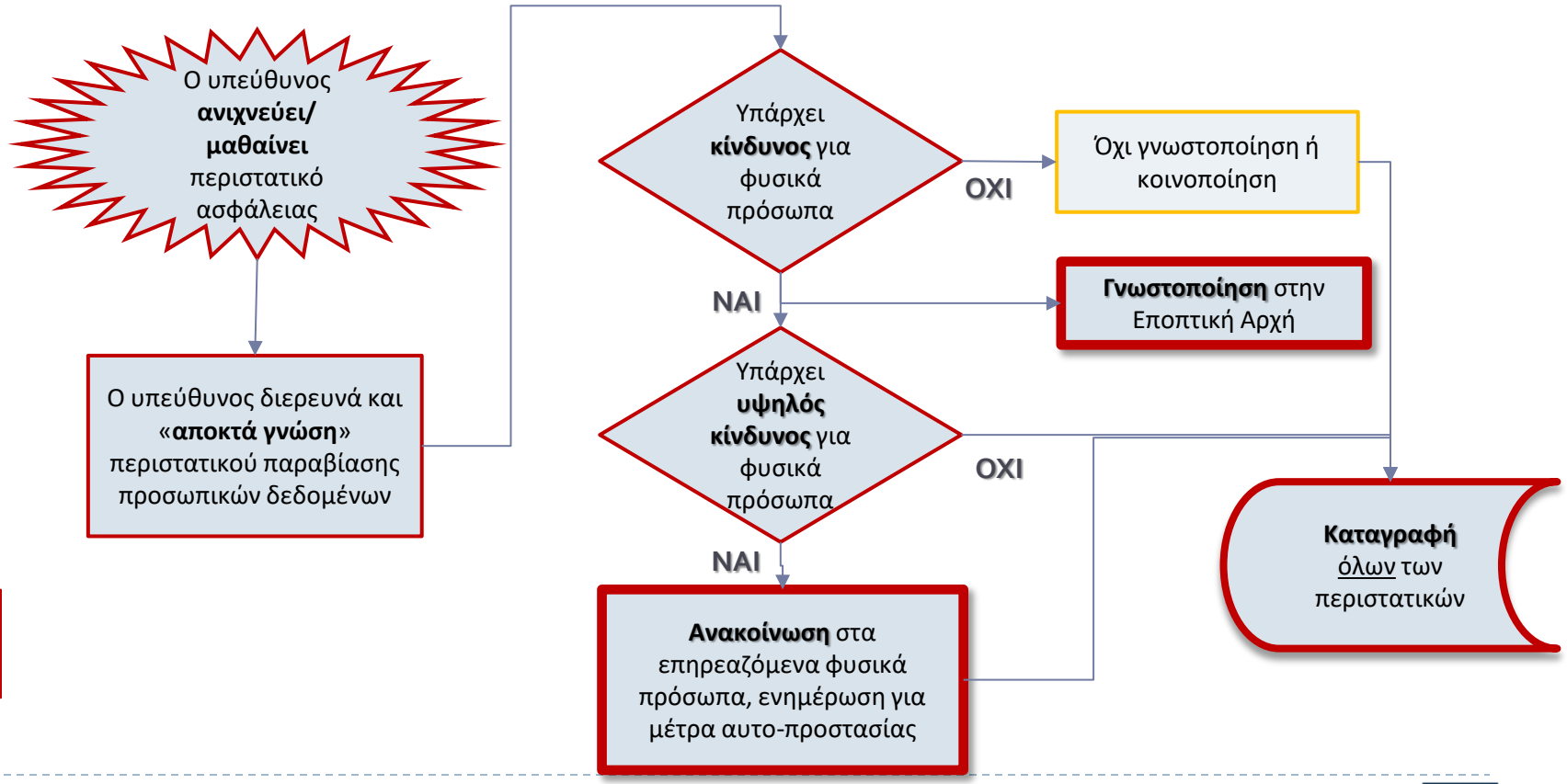
Όπως και με το προηγούμενο νομικό πλαίσιο, απαιτήσεις για ασφαλή επεξεργασία και με το ΓΚΠΔ. Αλλά…

- **Νέες ρυθμίσεις:**
  - Εξειδίκευση, με πρόταση «ενδεδειγμένων» τεχνικών και οργανωτικών μέτρων:
    - ***Ψευδωνυμοποίηση*** και ***Κρυπτογράφηση***
    - Διασφάλιση **Απορρήτου**, **Ακεραιότητας**, ***Διαθεσιμότητας*** και ***Αξιοπιστίας***
    - Αποκατάσταση ***Διαθεσιμότητας*** και της πρόσβασης σε περίπτωση συμβάντος
    - Δοκιμή, εκτίμηση και ***διαρκής αξιολόγηση*** της αποτελεσματικότητας των μέτρων
  - Χρήση εγκεκριμένου κώδικα δεοντολογίας ή μηχανισμού πιστοποίησης (προαιρετικά μεν, αλλά ο ΓΚΠΔ σαφώς ενθαρρύνει)
  - «Αναβαθμίζεται» η σχετική υποχρέωση ασφαλείας και για τους εκτελούντες την επεξεργασία
  - Κοινοποίηση περιστατικών παραβίασης……

Περιστατικά Παραβίασης Προσωπικών Δεδομένων

Ορισμός:

- παραβίαση της ασφάλειας (C-I-A) που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα.



Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

- **Data Protection Impact Assessment (DPIA)**
  - συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας, των σκοπών της επεξεργασίας και της νομικής βάσης
  - εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας
  - εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων
  - τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων

DPIA : εργαλείο ελέγχου & απόδειξης συμμόρφωσης με GDPR

- Υποχρεωτικό όταν "*…ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων*"
- Οι Αρχές θα ορίσουν καταλόγους με επεξεργασίες που απαιτείται DPIA
- Αν μετά την εκπόνηση της DPIA προκύπτει ακόμα «υψηλός κίνδυνος» => Διαβούλευση με την Εποπτική Αρχή

Δικαιώματα Υποκειμένων

- α) Αρχή της Διαφάνειας (12)
- β) Δικαίωμα Ενημερώσεως (13 & 14)
- γ) Δικαίωμα Προσβάσεως (15)
- δ) Δικαίωμα Διορθώσεως (16)
- ε) Δικαίωμα Διαγραφής (17)
- στ) Δικαίωμα Περιορισμού της Επεξεργασίας (18)
- ζ) Δικαίωμα στη Φορητότητα των Δεδομένων (άρθρο 20)
- η) Δικαίωμα Εναντιώσεως (21)
- θ) Δικαίωμα στην Ανθρώπινη Παρέμβαση (22)

ΓΚΠΔ και Επιστημονική Έρευνα

- **Περιορισμός του σκοπού**: Η περαιτέρω επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς επιστημονικής έρευνας δεν θεωρείται ασύμβατη με τους σκοπούς για τους οποίους αρχικά συλλέχθηκαν τα δεδομένα.
- **Επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα**: Η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, δηλαδή των δεδομένων των Άρθρων 9 και 10 του ΓΚΠΔ, είναι κατ' εξαίρεση δυνατή για ερευνητικούς σκοπούς, οι οποίοι είναι ανάλογοι με τον επιδιωκόμενο σκοπό και σέβονται το κατοχυρωμένο από το Σύνταγμα δικαίωμα στην προστασία των δεδομένων.

ΓΚΠΔ και Επιστημονική Έρευνα

- **Περιορισμός της περιόδου αποθήκευσης**: Τα δεδομένα προσωπικού χαρακτήρα που χρησιμοποιούνται για ερευνητικούς σκοπούς απαλλάσσονται από την απαίτηση του ΓΚΠΔ αναφορικά με τη τήρησή τους μόνο για το χρονικό διάστημα που είναι αναγκαίο για την εκπλήρωση του σκοπού της επεξεργασίας.

ΓΚΠΔ και Επιστημονική Έρευνα

- **Διαφανής ενημέρωση του υποκειμένου των δεδομένων**:
  - Στην περίπτωση που τα δεδομένα έχουν συλλεχθεί από το ίδιο το υποκείμενο και πρόκειται να χρησιμοποιηθούν για κάποιον άλλο σκοπό από εκείνον για τον οποίο αρχικά συλλέχθηκαν που όμως αφορά επιστημονική έρευνα, τότε υπάρχει μια ελαστικότητα σχετικά με τη διαφανή ενημέρωση του σκοπού της επεξεργασίας και το υποκείμενο μπορεί να συγκατατεθεί είτε στον ερευνητικό σκοπό με γενικότερο τρόπο είτε μόνο για συγκεκριμένους τομείς / στάδια της επιστημονικής έρευνας.

ΓΚΠΔ και Επιστημονική Έρευνα

- **Διαφανής ενημέρωση του υποκειμένου των δεδομένων**:
  - Στην περίπτωση που τα δεδομένα προσωπικού χαρακτήρα του υποκειμένου έχουν συλλεχθεί μέσω κάποιου άλλου (π.χ. δημόσια πηγή, άλλη δημόσια αρχή) και όχι από το ίδιο το υποκείμενο των δεδομένων, ο ερευνητής δεν υποχρεούται από τον Κανονισμό να ενημερώσει τα υποκείμενα των δεδομένων όταν η ενέργεια αυτή αποδεικνύεται αδύνατη ή απαιτεί δυσανάλογες προσπάθειες, καθώς και όταν η εν λόγω ενημέρωση ενδέχεται να καταστήσει αδύνατη ή να βλάψει σε μεγάλο βαθμό την επίτευξη των σκοπών της έρευνας.

ΓΚΠΔ και Επιστημονική Έρευνα

- **Δικαιώματα των υποκειμένων των δεδομένων:** Όταν η επεξεργασία των δεδομένων προσωπικού χαρακτήρα εκτελείται για ερευνητικούς σκοπούς, ο ΓΚΠΔ παρέχει τη δυνατότητα στα κράτη μέλη της Ε.Ε. να προβλέπουν παρεκκλίσεις από τα δικαιώματα που μπορούν να ασκήσουν τα υποκείμενα των δεδομένων.
  - Οι εν λόγω παρεκκλίσεις δύναται να αφορούν το δικαίωμα πρόσβασης, το δικαίωμα διόρθωσης, το δικαίωμα του περιορισμού της επεξεργασίας και το δικαίωμα εναντίωσης. **Οι παρεκκλίσεις είναι εφαρμόσιμες μόνο εάν τα εν λόγω δικαιώματα μπορεί να καταστήσουν αδύνατη την επιστημονική έρευνα ή να παρεμποδίσουν την επίτευξη των σκοπών τη**ς. Επιπροσθέτως, ο ΓΚΠΔ ρητώς αναφέρει ότι σε περίπτωση που η επεξεργασία των δεδομένων είναι απαραίτητη για σκοπούς επιστημονικής έρευνας το δικαίωμα της διαγραφής δεν είναι ικανοποιήσιμο.

ΓΚΠΔ και Επιστημονική Έρευνα

- **Οι προαναφερόμενες παρεκκλίσεις και εξαιρέσεις που αφορούν την επεξεργασία δεδομένων για ερευνητικούς σκοπούς, ισχύουν μόνο όταν**:
  - Η επεξεργασία υπόκειται σε κατάλληλες, τεχνικές και οργανωτικές, εγγυήσεις σχετικά με την προστασία των δεδομένων, όπως η αρχή της ελαχιστοποίησης, η ψευδωνυμοποίηση, ο έλεγχος λογικής πρόσβασης.
  - Η επεξεργασία δεν πρόκειται να οδηγήσει σε λήψη μέτρων ή αποφάσεων που θα επηρεάσουν τα φυσικά πρόσωπα.
  - Η επεξεργασία δε δύναται να προκαλέσει κάποια σημαντική βλάβη ή κίνδυνο για το υποκείμενο των δεδομένων.
  - Η εφαρμογή των προβλεπόμενων από το ΓΚΠΔ απαιτήσεων ενδέχεται να καταστήσει αδύνατη ή να βλάψει σε μεγάλο βαθμό την επίτευξη των σκοπών της έρευνας

Ενέργειες πριν την έναρξη της Επιστημονικής Έρευνας

Βήμα 1: **Προσδιορισμός του σκοπού ή των σκοπών επεξεργασίας**

- Αρχικά, ο ερευνητής (-ές) πρέπει να εντοπίσει και να προσδιορίσει τον σκοπό (ή τους σκοπούς) της επεξεργασίας των δεδομένων στο πλαίσιο της επιστημονικής έρευνας. Καθότι αρκετές φορές είναι αρκετά δύσκολο να προσδιοριστούν εξαρχής οι εν λόγω σκοποί, ο ερευνητής πρέπει, τουλάχιστον, να περιγράφει σε γενικότερο επίπεδο τον σκοπό της έρευνας

Ενέργειες πριν την έναρξη της Επιστημονικής Έρευνας

Βήμα 2: **Δυνατότητα χρήσης ανωνυμοποιημένων δεδομένων στην έρευνα**

- Ο ερευνητής πρέπει να εξακριβώσει εάν για την εκπλήρωση της επιστημονικής του έρευνας χρειάζεται να γνωρίζει την ταυτότητα των συμμετεχόντων φυσικών προσώπων. Σε περίπτωση που η έρευνα μπορεί να πραγματοποιηθεί με την επεξεργασία ανωνυμοποιημένων δεδομένων, τότε η εκπλήρωση των σκοπών της πρέπει να γίνεται κατά αυτόν τον τρόπο.

Ενέργειες πριν την έναρξη της Επιστημονικής Έρευνας

Βήμα 3: Προσδιορισμός της Νομικής Βάσης

- Σύμφωνα με το ΓΚΠΔ, για να είναι σύννομη μια επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να βασίζεται σε μία από τις νομικές βάσεις του Άρθρου 6.1. Πιο συγκεκριμένα, τα δεδομένα μπορούν να επεξεργαστούν για ερευνητικούς σκοπούς όταν:
  - το υποκείμενο έχει δώσει τη συγκατάθεσή του,
  - το υποκείμενο έχει ήδη συγκατατεθεί από κάποια προηγούμενη έρευνα στην περαιτέρω χρήση των δεδομένων του ή στη χρήση τους για παρεμφερείς σκοπούς,
  - τα δεδομένα προσωπικού χαρακτήρα που αφορούν στο υποκείμενο προέρχονται από κάποια δημόσια προσβάσιμη πηγή,
  - η επεξεργασία είναι απαραίτητη για τους σκοπούς της έρευνας και ο ερευνητής μπορεί να αποδείξει ότι οι σκοποί της επιστημονικής έρευνας δεν υπερισχύουν των συμφερόντων και των δικαιωμάτων του υποκειμένου των δεδομένων

Ενέργειες πριν την έναρξη της Επιστημονικής Έρευνας

Βήμα 3: Προσδιορισμός της Νομικής Βάσης

- Είναι σημαντικό να σημειωθεί ότι η συγκατάθεση των υποκειμένων ως νομική βάση της επεξεργασίας για ερευνητικούς σκοπούς δεν προτείνεται και πρέπει να αποτελεί την τελευταία επιλογή του ερευνητή, καθώς κάθε έρευνα που βασίζεται στη συγκατάθεση υπόκειται σε πρόσθετες απαιτήσεις βάσει του ΓΚΠΔ (π.χ. ανάκληση της συγκατάθεσης), οι οποίες ενδέχεται να έχουν ζημιογόνο αντίκτυπο στην έρευνα.
- Επιπροσθέτως, όταν τα δεδομένα προσωπικού χαρακτήρα ανήκουν σε ειδική κατηγορία δεδομένων (άρθρα 9 και 10 του ΓΚΠΔ) ο σκοπός της έρευνας πρέπει να είναι ανάλογος του πρόσθετου κινδύνου που συνεπάγεται η επεξεργασία τέτοιου είδους δεδομένων προσωπικού χαρακτήρα.

Ενέργειες πριν την έναρξη της Επιστημονικής Έρευνας

Βήμα 4: Διασφάλιση των κατάλληλων Εγγυήσεων

- Η επεξεργασία δεδομένων προσωπικού χαρακτήρα για ερευνητικούς σκοπούς πρέπει, βάσει του ΓΚΠΔ, να υπόκειται σε κατάλληλες εγγυήσεις για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Οι εν λόγω εγγυήσεις θα πρέπει να διασφαλίζουν ότι έχουν υλοποιηθεί από τον ερευνητή διάφορα αποτελεσματικά τεχνικά και οργανωτικά μέτρα.

Ενέργειες πριν την έναρξη της Επιστημονικής Έρευνας

Βήμα 4: Διασφάλιση των κατάλληλων Εγγυήσεων

- Προκειμένου να χρησιμοποιηθούν τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς της έρευνας, πρέπει να εφαρμοστούν οπωσδήποτε τα εξής:
  - Τι δεδομένα προσωπικού χαρακτήρα πραγματικά χρειάζεται. Ο ερευνητής πρέπει να συλλέγει και να επεξεργάζεται μόνο τα δεδομένα εκείνα που είναι αναγκαία και συναφή προς τους ειδικούς σκοπούς της εκάστοτε επιστημονικής έρευνας. Για παράδειγμα, εάν η επιστημονική έρευνα μπορεί να εκπληρωθεί μόνο με το έτος γέννησης ή την ηλικία των συμμετεχόντων, ο ερευνητής δε χρειάζεται να γνωρίζει την πλήρη ημερομηνία γέννησής τους.

Ενέργειες πριν την έναρξη της Επιστημονικής Έρευνας

Βήμα 4: Διασφάλιση των κατάλληλων Εγγυήσεων

- Προκειμένου να χρησιμοποιηθούν τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς της έρευνας, πρέπει να εφαρμοστούν οπωσδήποτε τα εξής:
  - Τη δυνατότητα ψευδωνυμοποίησης των δεδομένων, εφόσον οι σκοποί της έρευνας μπορούν να εκπληρωθούν κατ' αυτόν τον τρόπο. Με αυτόν τον τρόπο ελαχιστοποιείται το ενδεχόμενο διαρροής πληροφορίας και ταυτοποίησης των συμμετεχόντων φυσικών προσώπων.
  - Ποιος θα έχει πρόσβαση στα δεδομένα. Για παράδειγμα, αρκετές φορές προκειμένου να εκπληρωθούν οι σκοποί της εκάστοτε έρευνας δεν χρειάζεται όλα τα μέλη της ερευνητικής ομάδας να γνωρίζουν την ταυτότητα των συμμετεχόντων. Αντίστοιχα, τα δεδομένα προσωπικού χαρακτήρα πρέπει να αποστέλλονται μόνο στα τρίτα μέρη που είναι απαραίτητα για τις ανάγκες της έρευνας

Ενέργειες πριν την έναρξη της Επιστημονικής Έρευνας

- **Βήμα 5: Αναγνώριση των εμπλεκόμενων τρίτων μερών**
  - Σε περίπτωση που τον σκοπό και τον τρόπο με τον οποίο θα διεξαχθεί η επιστημονική έρευνα, τους καθορίζει ένας φορέας τότε υπεύθυνος επεξεργασίας είναι ο Φορέας αυτός.
  - Σε περίπτωση που τον σκοπό ή / και τον τρόπο διεξαγωγής της έρευνας δύναται να τον καθορίσουν και άλλοι συνεργάτες ερευνητές, τότε ο Φορέας και οι εν λόγω συνεργάτες ερευνητές δρουν ως από κοινού υπεύθυνοι επεξεργασίας.
  - Σε περίπτωση που συνεργάτες ερευνητές επεξεργάζονται δεδομένα προσωπικού χαρακτήρα συμμετεχόντων στην έρευνα υπό την καθοδήγηση και υπό τις εντολές του Φορέα, τότε οι συνεργάτες ερευνητές δρουν ως εκτελούντες την επεξεργασία.

Ενέργειες πριν την έναρξη της Επιστημονικής Έρευνας

Βήμα 6: Απόφαση για τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων

- Προτού αρχίσει η έρευνα, ο ερευνητής πρέπει να αξιολογήσει κατά πόσο η επεξεργασία των δεδομένων προσωπικού χαρακτήρα ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων. Συγκεκριμένα, πρέπει να διερευνηθεί κατά πόσο η επεξεργασία εμπεριέχεται στον κατάλογο της αρχής (ΑΠΔΠΧ) με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων.

Ενέργειες πριν την έναρξη της Επιστημονικής Έρευνας

Βήμα 6: Απόφαση για τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων

- Σε περίπτωση που η επεξεργασία δεν ανήκει στον ανωτέρω κατάλογο, τότε πρέπει να ελεγχθούν τα παρακάτω κριτήρια:
  - Αξιολόγηση ή βαθμολόγηση και κατάρτιση προφίλ φυσικών προσώπων
  - Λήψη αυτοματοποιημένων αποφάσεων σχετικά με το φυσικό πρόσωπο
  - Συστηματική παρακολούθηση των υποκειμένων των δεδομένων, συμπεριλαμβανομένης της παρακολούθησης μέσω δικτύων

Ενέργειες πριν την έναρξη της Επιστημονικής Έρευνας

Βήμα 6: Απόφαση για τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων

- Σε περίπτωση που η επεξεργασία δεν ανήκει στον ανωτέρω κατάλογο, τότε πρέπει να ελεγχθούν τα παρακάτω κριτήρια:
  - Επεξεργασία δεδομένων που αφορούν ευάλωτα φυσικά πρόσωπα, όπως παιδιά, εργαζόμενοι, άτομα με ειδικές ανάγκες κ.λπ.
  - Μεγάλης κλίμακας επεξεργασία δεδομένων προσωπικού χαρακτήρα,
  - Καινοτόμος χρήση ή εφαρμογή νέων τεχνολογικών ή οργανωτικών λύσεων, όπως το «διαδίκτυο των πραγμάτων» (IOT), βιομετρικές τεχνολογίες κ.λπ. [10]

Ενέργειες πριν την έναρξη της Επιστημονικής Έρευνας

Βήμα 7: Υλοποίηση επιπλέον οργανωτικών και τεχνικών μέτρων

- Είναι ζωτικής σημασίας τα δεδομένα της έρευνας που αφορούν σε δεδομένα προσωπικού χαρακτήρα να συλλέγονται, να τηρούνται, να διαβιβάζονται και να καταστρέφονται με ασφάλεια. Για το λόγο αυτό η εκάστοτε ερευνητική ομάδα, είτε επειδή εντοπίστηκε η ανάγκη πρόσθετων μέτρων για τον μετριασμό των κινδύνων (μη εξουσιοδοτημένη πρόσβαση / χρήση, μη εξουσιοδοτημένη τροποποίηση, τυχαία (ή μη) απώλεια, καταστροφή ή βλάβη) που αναγνωρίστηκαν στην ΕΑΠΔ είτε επειδή κρίνει ότι απαιτείται η λήψη μέτρων προστασίας, εφαρμόζει τα απαραίτητα, κάθε φορά, τεχνικά και οργανωτικά μέτρα.

Ενέργειες πριν την έναρξη της Επιστημονικής Έρευνας

Βήμα 8: Δημιουργία εντύπου ενημέρωσης σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και δήλωσης συγκατάθεσης

- Αφού γίνουν τα ανωτέρω βήματα, ο ερευνητής πρέπει να σχεδιάσει ένα έντυπο σχετικά με την επεξεργασία που διενεργείται στο πλαίσιο της έρευνας επί των δεδομένων προσωπικού χαρακτήρα. Το έντυπο ενημέρωσης θα πρέπει να διασφαλίζει ότι τα υποκείμενα των δεδομένων έχουν λάβει όλη την απαραίτητη πληροφορία σχετικά με την επεξεργασία των δεδομένων τους.

Ενέργειες πριν την έναρξη της Επιστημονικής Έρευνας

Τι πρέπει να περιλαμβάνει το έντυπο της ενημέρωσης:	Όταν τα δεδομένα συλλέγονται απευθείας από το υποκείμενο	Όταν τα δεδομένα <u>δε</u> συλλέγονται απευθείας από το υποκείμενο
Την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και του ΥΠΔ.	✓	✓
Τη δραστηριότητα επεξεργασίας και τη νομική βάση αυτής.	✓	✓
Τον σκοπό ή τους σκοπούς της επεξεργασίας.	✓	✓
Τις κατηγορίες των δεδομένων προσωπικού χαρακτήρα.		✓
Τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων, εφόσον υπάρχουν.	✓	✓
Πληροφορίες σχετικά με τη διαβίβαση των δεδομένων σε τρίτη χώρα και τις κατάλληλες εγγυήσεις, εφόσον υφίσταται.	✓	✓
Το χρονικό διάστημα αποθήκευσης των δεδομένων ή τα κριτήρια που το καθορίζουν.	✓	✓
Πληροφορίες σχετικά με τα δικαιώματα του υποκειμένου βάσει του ΓΚΠΔ.	✓	✓
Ενημέρωση σχετικά με την ύπαρξη του δικαιώματος ανάκλησης της συγκατάθεσής του οποτεδήποτε, εφόσον υφίσταται.	✓	✓
Ενημέρωση σχετικά με την ύπαρξη του δικαιώματος υποβολής καταγγελίας στην ΑΠΔΠΧ.	✓	✓
Την πηγή από την οποία προέρχονται τα δεδομένα προσωπικού χαρακτήρα και εάν τα δεδομένα προήλθαν από δημόσια προσβάσιμες πηγές.		✓
Την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ.	✓	✓

Ενέργειες πριν την έναρξη της Επιστημονικής Έρευνας

Βήμα 9: Δημοσίευση Έρευνας

- Μετά το πέρας της έρευνας, σε περίπτωση που ο ερευνητής επιθυμεί να δημοσιεύσει δεδομένα προσωπικού χαρακτήρα που επεξεργάστηκε κατά την επιστημονική του έρευνα ή τα αποτελέσματά της, συμπεριλαμβανομένων δεδομένων που αφορούν στους συμμετέχοντες, πρέπει να έχει τη ρητή συγκατάθεση των υποκειμένων. Για το λόγο αυτό προτείνεται, σε κάθε περίπτωση, ο ερευνητής να δημιουργεί πριν την ολοκλήρωση της έρευνας μια ανωνυμοποιημένη έκδοση των δεδομένων προσωπικού χαρακτήρα, προκειμένου να μπορεί όποτε επιθυμεί να τα δημοσιεύσει.

Σας ευχαριστώ !!