

Προσωπικά Δεδομένα και Ιδιωτικότητα

Σπύρος Ε. Πολυκαλάς
Καθηγητής

Το περιεχόμενο των σημειώσεων του μαθήματος υπάγεται σε Άδεια Χρήσης Creative Commons [Creative Commons](#)
[Αναφορά Δημιουργού - Μη Εμπορική Χρήση - Παρόμοια Διανομή 4.0 Διεθνές](#)



Δομή Μαθήματος

I. Θεωρία

a. 4 ώρες / εβδομάδα

Πλατφόρμα e-class

- Πλατφόρμα Ασύγχρονης Τηλεκπαίδευσης
 - Ύλη μαθήματος, σημειώσεις, ασκήσεις, ανακοινώσεις, επικοινωνία με καθηγητές
- <https://opencourses.ionio.gr/courses/DMC205/>
- Εγγραφή όλων των φοιτητών του μαθήματος
- Κατά την διάρκεια του εξαμήνου δίνονται εργασίες στους φοιτητές
- Οι εργασίες παραδίδονται υποχρεωτικά μέσω του e-class

Εργασίες

- Κατά την διάρκεια του εξαμήνου δίνονται ατομικές ή ομαδικές εργασίες στους φοιτητές
- Οι εργασίες παραδίδονται υποχρεωτικά μέσω του e-class και παρουσιάζονται από τους φοιτητές
- Στον τελικό βαθμό του μαθήματος λαμβάνεται υπόψη ο βαθμός των εργασιών (βαρύτητα από 15% ~ 35% ανάλογα με τον αριθμό των εργασιών)

Περιεχόμενα Μαθήματος (1)

I. Προστασία προσωπικών δεδομένων

- a. Ασφάλεια και προστασία προσωπικών δεδομένων στο Διαδίκτυο
- b. Δικαίωμα στη Λήθη

II. Πνευματική ιδιοκτησία

- a. Πνευματικά Δικαιώματα

III. Ανοικτά Δεδομένα (Open data)

IV. Ουδετερότητα Δικτύων

V. Προσωπικά Δεδομένα και Τεχνητή Νοημοσύνη

Μαθησιακοί Στόχοι

- Η ολοένα και μεγαλύτερη χρήση του Διαδικτύου έχει αναγείρει σημαντικά ζητήματα σχετικά με την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων των χρηστών του Διαδικτύου:
 - μεγάλης χρήσης των κινητών συσκευών,
 - των μέσων κοινωνικής δικτύωσης
 - της αναμενόμενης διείσδυσης του Διαδικτύου των Πραγμάτων (Internet of Things),
- Στα πλαίσια του μαθήματος παρουσιάζεται το γενικό θεωρητικό υπόβαθρο της ιδιωτικότητας και της ασφάλειας στις Ηλεκτρονικές Επικοινωνίες.
- Αναλύεται το εθνικό, ευρωπαϊκό και διεθνές πλαίσιο, σχετικά με τα προσωπικά δεδομένα και την ιδιωτικότητα.
- Έμφαση δίνεται στη πρόσβαση, επεξεργασία και αποθήκευση των προσωπικών δεδομένων από συσκευές, εφαρμογές και υπηρεσίες.
- Με την επιτυχή ολοκλήρωση του μαθήματος οι φοιτητές θα γνωρίζουν:
 - Τις βασικές αρχές της ιδιωτικότητας και της ασφάλειας στις Ηλεκτρονικές Επικοινωνίες.
 - Το θεσμικό πλαίσιο προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων.

Βιβλιογραφία

I. Βιβλία

- a. Το Δίκαιο των ΜΜΕ / Το Δίκαιο των Προσωπικών Δεδομένων
- b. Επιχειρησιακό Δίκαιο, Δίκαιο Διαδικτύου, Δίκαιο ηλεκτρονικού Εμπορίου – Βελέντζας Ιωάννης
- c. Ψηφιακή Ελλάδα: Ιστορική διαδρομή, σύγχρονο ρυθμιστικό πλαίσιο, προτάσεις για το μέλλον – Βαγγέλης Παπακωσταντίνου

Βιβλιογραφία

- I. Σημειώσεις (θα δοθούν μέσω eclass)
- II. Νομοθεσία
 - I. Ελληνική
 - II. Ευρωπαϊκή
- III. Επιστημονικά άρθρα

Μάθημα [601Υ]: Προσωπικά Δεδομένα και Ιδιωτικότητα

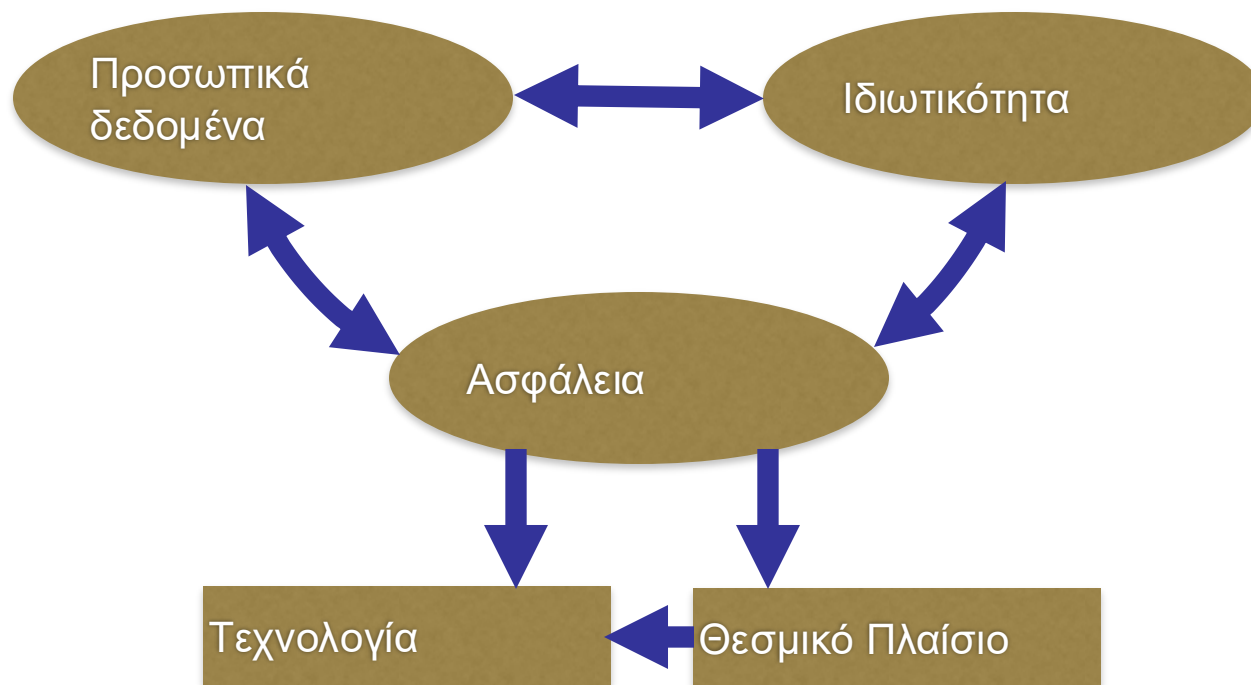
Εξάμηνο 6 - Εαρινό

Επιλογές Συγγραμμάτων:

1. Βιβλίο [77111403]: Ο γενικός κανονισμός προστασίας προσωπικών
2. Βιβλίο [94700768]: ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ
3. Βιβλίο [94689130]: ΔΙΚΑΙΟ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ, ΧΡΙΣ
4. Βιβλίο [94701902]: Ο ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΠΙ

Συνεκτικό πλαίσιο & τεχνολογικές προδιαγραφές

- Η μεγάλη “έκθεση” των προσωπικών δεδομένων ή υψηλός κίνδυνος παραβίασης της Ιδιωτικότητας των φυσικών προσώπων λόγω:
 - της ευρείας χρήσης της τεχνολογίας
 - της παγκοσμιοποίησης των κοινωνιών / οικονομιών
- έκανε επιτακτική την ανάγκη για ύπαρξη ενός συνεκτικού πλαισίου το οποίο θα προστατεύει τα δεδομένα προσωπικού χαρακτήρα των φυσικών προσώπων και θα δίνει την δυνατότητα στα φυσικά πρόσωπα να ελέγχουν τον βαθμό έκθεσης των προσωπικών τους δεδομένων σε τρίτους ή διαφορετικά τον βαθμό άρσης της ιδιωτικότητας τους.
- Πέρα όμως από το θεσμικό πλαίσιο απαιτείται και προστασία των προσωπικών δεδομένων μέσω των επιβολής νέων τεχνολογικών προδιαγραφών τα οποία θα προσδίδουν μεγαλύτερη ασφάλεια σε συστήματα που συλλέγουν αποθηκεύουν και επεξεργάζονται δεδομένων προσωπικού χαρακτήρα



Ενότητα II

- Προστασία Προσωπικών Δεδομένων
 - Προσωπικά Δεδομένα
 - Οδηγία 2002/58
 - Οδηγία 2006/24
 - Οδηγία 2016/680
 - Κοινωνικά δίκτυα & προσωπικά δεδομένα
- Κανονισμός 679/2016
 - Δικαίωμα στη Λήθη (Right to be Forgotten)

- **Οδηγία 2002/58** της ΕΕ για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες
- **Οδηγία 2006/24** της ΕΕ η οποία πρόσθεσε ή / και τροποποίησε ζητήματα που θίγονταν στην Οδηγία 2002/58 σχετικά με την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες ιδίως όσον αφορά την διατήρηση των δεδομένων προσωπικού χαρακτήρα.
- **Κανονισμός 679/2016** της ΕΕ σχετικά με την προστασία των προσωπικών δεδομένων φυσικών προσώπων.

Προσωπικά δεδομένα

- Κάθε άμεση πληροφορία σχετική με ένα φυσικό πρόσωπο. Ενδεικτικά:
 - ονοματεπώνυμο, επάγγελμα, οικογενειακή κατάσταση, ηλικία, τόπος κατοικίας/εργασίας, θρήσκευμα, υπηκοότητα κ.α
- Κάθε έμμεση πληροφορία σχετική με ένα φυσικό πρόσωπο. Ενδεικτικά:
 - πολιτικές πεποιθήσεις, ιστορικό / κατάσταση υγείας, τυχόν ποινικές διώξεις / καταδίκες, τοποθεσία κ.α

Νέες τεχνολογίες και προσωπικά δεδομένα

- Η συγκέντρωση / επεξεργασία και διάδοση δεδομένων προσωπικού χαρακτήρα αποτελεί έναν από τους μεγαλύτερους κινδύνους παραβίασης της προσωπικής ζωής ενός ατόμου.
- Η χρήση των νέων τεχνολογιών επικοινωνιών και πληροφορικής διόγκωσε ακόμη περαιτέρω το πρόβλημα καθώς διευκόλυνε σε μέγιστο βαθμό την συγκέντρωση δεδομένων προσωπικού χαρακτήρα. Ειδικότερα:
 - Η μεγάλη διείσδυση του διαδικτύου,
 - Η χρήση εφαρμογών κινητής τηλεφωνίας / διαδικτυακών εφαρμογών οι οποίες συλλέγουν ευαίσθητα προσωπικά δεδομένα (πχ υπηρεσίες εντοπισμού θέσης),
 - Η χρήση διαδικτυακών εφαρμογών οι οποίες συλλέγουν δεδομένα σχετικά με τις προτιμήσεις του χρήστη στη διαδικτυακή του πλοήγηση.

Συνταγματικό δικαίωμα

- «Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει.
- Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει.» **(άρθρο 9^Α Συντάγματος).**

Οδηγία 2002/58 της ΕΕ

Οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες:

- Διασφάλιση **επιπέδου προστασίας** όσον αφορά την επεξεργασία προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες,
- Ασφάλεια, απόρρητο, δεδομένα κίνησης, αναλυτική χρέωση, ένδειξη ταυτότητας, δεδομένα θέσης, αυτόκλητες κλήσεις,
- **Δεν εφαρμόζεται** σε δραστηριότητες που αφορούν τη δημόσια ασφάλεια, την εθνική άμυνα, την ασφάλεια του κράτους και στις δραστηριότητες του κράτους σε τομείς του ποινικού δικαίου.

Ασφάλεια

- Ο φορέας παροχής διαθέσιμων στο κοινό **υπηρεσιών ηλεκτρονικών επικοινωνιών** οφείλει να λαμβάνει (όπου είναι απαραίτητο από κοινού με τον φορέα παροχής του **δημοσίου δικτύου επικοινωνιών**) τα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα προκειμένου να προστατεύεται η ασφάλεια των υπηρεσιών του.
 - Λογισμικό προστασίας (πχ. antivirus)
 - Υλικό προστασίας (πχ. firewalls)
 - Διαδικασίες πρόσβασης σε ευαίσθητα / προσωπικά δεδομένα
- Σε περίπτωση που υπάρχει **ιδιαίτερος κίνδυνος παραβίασης της ασφάλειας του δικτύου**, ο φορέας που παρέχει διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών **οφείλει να ενημερώνει τους συνδρομητές για τον κίνδυνο** αυτό και, εφόσον ο κίνδυνος κείται εκτός του πεδίου των μέτρων που οφείλει να λαμβάνει ο πάροχος της υπηρεσίας.

Πιστοποιητικά ασφαλείας SSL

- Οι ιστότοποι που χρησιμοποιούν SSL (Secure Socket Layer) εμφανίζουν **πιστοποιητικά ασφαλείας** στο πρόγραμμα περιήγησης στο διαδίκτυο (πχ Chrome) προκειμένου να επαληθεύεται η ταυτότητά τους.
- Μόνο ο πραγματικός ιστότοπος διαθέτει έγκυρο πιστοποιητικό ασφαλείας για τη διεύθυνσή του (URL).
- Τα μη έγκυρα πιστοποιητικά μπορεί να υποδεικνύουν ότι κάποιος προσπαθεί να παρέμβει στη σύνδεσή σας με τον ιστότοπο όπως για παράδειγμα να έχει δημιουργήσει έναν ιστότοπο που προσποιείται ότι είναι άλλος ιστότοπος.
- Στην περίπτωση όπου δώσουμε προσωπικά στοιχεία (πχ username password) σε έναν εικονικό ιστότοπο τότε αυτά θα μπορούσαν να χρησιμοποιηθούν για παράνομη είσοδο στον πραγματικό ιστότοπο.

Απόρρητο

- Τα Κράτη Μέλη κατοχυρώνουν, **το απόρρητο των επικοινωνιών που διενεργούνται μέσω δημόσιου δικτύου επικοινωνιών και των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, κίνησης.**
- **Απαγορεύουν** την ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των επικοινωνιών και των συναφών δεδομένων κίνησης από πρόσωπα πλην των χρηστών, **χωρίς τη συγκατάθεση των ενδιαφερομένων χρηστών**, εκτός αν υπάρχει σχετική νόμιμη άδεια.
- **Δεν επηρεάζει οποιαδήποτε επιτρεπόμενη** από το νόμο καταγραφή συνδιαλέξεων και των συναφών δεδομένων κίνησης όταν πραγματοποιούνται **κατά τη διάρκεια νόμιμης επαγγελματικής πρακτικής με σκοπό την παροχή αποδεικτικών στοιχείων μιας εμπορικής συναλλαγής ή οποιασδήποτε άλλης επικοινωνίας επαγγελματικού χαρακτήρα.**

Δεδομένα Κίνησης (1)

- Τα **δεδομένα κίνησης** που αφορούν συνδρομητές και χρήστες, τα οποία υποβάλλονται σε επεξεργασία και αποθηκεύονται από τον πάροχο δημόσιου δικτύου ή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών, **πρέπει να απαλείφονται ή να καθίστανται ανώνυμα** όταν δεν είναι πλέον απαραίτητα για το σκοπό της μετάδοσης μιας επικοινωνίας.
- Τα δεδομένα κίνησης που είναι απαραίτητα **για τη χρέωση των συνδρομητών** και την πληρωμή των διασυνδέσεων μπορούν να υποβάλλονται σε επεξεργασία. Η επεξεργασία αυτή επιτρέπεται μόνον έως το τέλος της χρονικής περιόδου εντός της οποίας δύναται να αμφισβητείται νομίμως ο λογαριασμός ή να επιδιώκεται η πληρωμή.

Δεδομένα Κίνησης (2)

- Για την εμπορική προώθηση των υπηρεσιών ηλεκτρονικών επικοινωνιών ή για την παροχή υπηρεσιών προστιθέμενης αξίας, ο πάροχος διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών μπορεί να επεξεργάζεται τα δεδομένα που σχετίζονται με δεδομένα κίνησης, **εφόσον ο συνδρομητής ή ο χρήστης τον οποίο αφορούν δίδει τη συγκατάθεσή του**. Στους χρήστες ή συνδρομητές πρέπει να δίνεται η δυνατότητα να ανακαλούν οποτεδήποτε τη συγκατάθεσή τους για την επεξεργασία των δεδομένων κίνησης.
 - Τα προγράμματα / διαδικτυακές εφαρμογές τα οποία χρησιμοποιούν δεδομένα θέσης μας ζητάνε πάντοτε (τουλάχιστον οφείλουν να το κάνουν) πριν από την εγκατάσταση ή την αναβάθμισή τους την συγκατάθεσή μας.

Δεδομένα Κίνησης (3)

- Η επεξεργασία των δεδομένων κίνησης, πρέπει να **περιορίζεται σε πρόσωπα** τα οποία ενεργούν υπό την εποπτεία του φορέα παροχής του δημοσίου δικτύου και της διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών και ασχολούνται με τη **διαχείριση της χρέωσης ή της κίνησης, τις απαντήσεις σε ερωτήσεις πελατών, την ανίχνευση της απάτης, την εμπορική προώθηση των υπηρεσιών ηλεκτρονικών επικοινωνιών ή την παροχή υπηρεσίας προστιθέμενης αξίας, και πρέπει να περιορίζεται στα απολύτως αναγκαία για την εξυπηρέτηση των σκοπών αυτών.**

Αναγνώριση ταυτότητας

- Όταν παρέχεται η υπηρεσία **αναγνώριση ταυτότητας καλούσας γραμμής** ο πάροχος πρέπει να παρέχει **στον χρήστη που καλεί** τη δυνατότητα **να εμποδίζει αυτήν την λειτουργία με απλά μέσα και ατελώς.**
- Όταν παρέχεται ένδειξη της ταυτότητας καλούσας γραμμής, ο πάροχος της υπηρεσίας πρέπει να προσφέρει τη δυνατότητα **στον χρήστη που καλείται να εμποδίζει την ένδειξη της ταυτότητας της καλούσας γραμμής** για τις εισερχόμενες κλήσεις με απλά μέσα και ατελώς, εφόσον κάνει λελογισμένη χρήση αυτής της λειτουργίας.
- Όταν παρέχεται ένδειξη της ταυτότητας καλούσας γραμμής και η ένδειξη αυτή γίνεται πριν από την αποκατάσταση της κλήσης, ο πάροχος της υπηρεσίας πρέπει να προσφέρει τη δυνατότητα **στον χρήστη που καλείται να απορρίπτει με απλά μέσα εισερχόμενες κλήσεις, όταν ο χρήστης ή ο συνδρομητής που καλεί έχει εμποδίσει την ένδειξη της ταυτότητας της καλούσας γραμμής.**
- Όταν παρέχεται ένδειξη της ταυτότητας της συνδεδεμένης γραμμής, ο πάροχος της υπηρεσίας πρέπει να προσφέρει τη δυνατότητα **στον χρήστη που καλείται να απαλείφει, με απλά μέσα και ατελώς, την ένδειξη της ταυτότητας της συνδεδεμένης γραμμής στον χρήστη που καλεί.**

Τηλεφωνικοί κατάλογοι

- Τα κράτη μέλη εξασφαλίζουν **ότι οι συνδρομητές ενημερώνονται, ατελώς και πριν περιληφθούν στον κατάλογο**, σχετικά με τους σκοπούς έντυπων ή ηλεκτρονικών καταλόγων συνδρομητών που διατίθενται στο κοινό ή μπορεί να αποκτηθούν μέσω υπηρεσιών πληροφοριών καταλόγου, στους οποίους μπορεί να περιλαμβάνονται τα προσωπικά τους δεδομένα,
- Τα κράτη μέλη μεριμνούν ώστε οι συνδρομητές να έχουν την ευκαιρία να καθορίζουν **εάν και ποια από τα προσωπικά τους δεδομένα θα περιλαμβάνονται σε δημόσιους καταλόγους**, στο βαθμό που τα εν λόγω στοιχεία είναι συναφή με τους σκοπούς του καταλόγου όπως καθορίζεται από τον φορέα παροχής του καταλόγου, και να επαληθεύουν, να διορθώνουν ή να αποσύρουν τα εν λόγω δεδομένα. **Η μη εγγραφή, η επαλήθευση, η διόρθωση ή η απόσυρση των προσωπικών δεδομένων από το δημόσιο κατάλογο συνδρομητών γίνεται ατελώς.**

Αυτόκλητες Κλήσεις (1)

- Η χρησιμοποίηση **αυτόματων συστημάτων κλήσης χωρίς ανθρώπινη παρέμβαση** (συσκευές αυτόματων κλήσεων), τηλεομοιοτυπικών συσκευών (φαξ) ή **ηλεκτρονικού ταχυδρομείου** για σκοπούς απευθείας εμπορικής προώθησης **επιτρέπεται μόνον στην περίπτωση συνδρομητών οι οποίοι έχουν δώσει εκ των προτέρων τη συγκατάθεσή τους.**
- Αν ένα φυσικό ή νομικό πρόσωπο αποκτά από τους πελάτες του στοιχεία επαφής του ηλεκτρονικού ταχυδρομείου τους στο πλαίσιο της πώλησης ενός προϊόντος ή μιας υπηρεσίας, **μπορεί να χρησιμοποιεί τα εν λόγω στοιχεία για την απευθείας εμπορική προώθηση των δικών του παρόμοιων προϊόντων ή υπηρεσιών, υπό την προϋπόθεση ότι οι πελάτες του έχουν σαφώς και ευδιάκριτα την ευκαιρία να αντιτάσσονται, δωρεάν και εύκολα, σε αυτή τη συλλογή και χρησιμοποίηση ηλεκτρονικών στοιχείων επαφής, και αυτό με κάθε μήνυμα, σε περίπτωση που ο χρήστης αρχικά δεν είχε διαφωνήσει με αυτή τη χρήση.**

Αυτόκλητες Κλήσεις (2)

- Τα κράτη μέλη λαμβάνουν τα ενδεδειγμένα μέτρα προκειμένου να εξασφαλίζεται, ατελώς, ότι **οι αυτόκλητες κλήσεις** με σκοπό την απευθείας εμπορική προώθηση, σε άλλες, εκτός των προβλεπόμενων στις παραγράφους 1 και 2, περιπτώσεις, **δεν επιτρέπονται χωρίς τη συγκατάθεση των ενδιαφερομένων συνδρομητών** ή όταν πρόκειται για συνδρομητές οι οποίοι δεν επιθυμούν να λαμβάνουν αυτές τις κλήσεις. Η σχετική επιλογή καθορίζεται από την εθνική νομοθεσία.
- **Απαγορεύεται** η πρακτική της αποστολής μηνυμάτων ηλεκτρονικού ταχυδρομείου με σκοπό την άμεση εμπορική προώθηση, **τα οποία συγκαλύπτουν ή αποκρύπτουν την ταυτότητα του αποστολέα ή του προσώπου προς όφελος του οποίου αποστέλλεται το μήνυμα, ή δίχως έγκυρη διεύθυνση στην οποία ο αποδέκτης να μπορεί να ζητεί τον τερματισμό της επικοινωνίας αυτής.**

Μητρώο

- Ο εφαρμοστικός νόμος της Οδηγίας 58/2002 (ν. 3471/2006) για την Ελλάδα, προβλέπει ότι όλοι οι πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών (Cosmote, Vodafone, Nova κλπ) είναι υποχρεωμένοι να διατηρούν ένα μητρώο συνδρομητών. Όσοι ανήκουν στο εν λόγω μητρώο δεν επιτρέπεται να δέχονται τηλεφωνικές κλήσεις (στο σταθερό ή/και κινητό τηλέφωνο) με σκοπό την εμπορική προώθηση προϊόντων / υπηρεσιών ή/και για διαφημιστικούς σκοπούς
- Οποιοσδήποτε συνδρομητής μπορεί ατελώς να εγγραφεται στο μητρώο

Cookies (1)

- Τα **cookies** είναι **αρχεία** τα οποία αποθηκεύονται στον υπολογιστή μας όταν συνδεόμαστε με ένα site το οποίο χρησιμοποιεί cookies. Την **πρώτη φορά** που επισκεπτόμαστε ένα site **δημιουργείται ένα cookie** (τα χαρακτηριστικά του έχουν προσδιορισθεί / σχεδιασθεί από το site που επισκεπτόμαστε) **το οποίο αποθηκεύεται στον υπολογιστή μας (στον browser).**
- Η ανάγνωση του cookie βοηθάει **το site που επισκεπτόμαστε να μας ξεχωρίσει από οποιοδήποτε άλλο επισκέπτεται το εν λόγω site.**
- Στον υπολογιστή μας συνήθως δεν αποθηκεύονται προσωπικές πληροφορίες για εμάς απλά **ένας «κωδικός» ο οποίος μας συνδέει με το αντίστοιχο αρχείο το οποίο βρίσκεται στον εξυπηρετητή του site και το οποίο περιέχει πληροφορίες για εμάς.** Όταν επισκεπτόμαστε ξανά το εν λόγω site το αντίστοιχο cookie βοηθάει ώστε το site να αναγνωρίσει τον υπολογιστή / χρήστη.

Cookies (2)

- Στα cookies αποθηκεύονται διάφορες πληροφορίες όπως **οι προτιμήσεις του χρήστη προκειμένου την επόμενη φορά που ο εν λόγω χρήστης επισκέπτεται το site**, αυτό να έχει προσαρμοσθεί στις δικές του προτιμήσεις.
- Οι προτιμήσεις μπορούν να αφορούν ποιες διαφημίσεις ενδιαφέρουν τον εν λόγω χρήστη, ποιες ειδήσεις διαβάζει, ποιες προσωπικές πληροφορίες δίνει σε ένα site (πχ αριθμό τηλεφώνου κλπ) κα.

Οδηγία 2002/58 – 2009/136

- Η Οδηγία 2002/58 τροποποιήθηκε το 2009 με την Οδηγία 2009/136 η οποία μεταξύ άλλων τροποποίησε και τα σχετικά με τα cookies (άρθρο 5, παράγραφος 3).
- Καταληκτική ημερομηνία εφαρμογής της στα ΚΜ ήταν η 25^η Μαΐου του 2011.

*«Τα κράτη μέλη μεριμνούν ώστε η αποθήκευση πληροφοριών ή η απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη επιτρέπεται **μόνον εάν ο συγκεκριμένος συνδρομητής ή χρήστης έχει δώσει τη συγκατάθεσή του με βάση σαφείς και εκτενείς πληροφορίες** σύμφωνα με την οδηγία 95/46/EK, μεταξύ άλλων για το σκοπό της επεξεργασίας. Τούτο δεν εμποδίζει οιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια της διαβίβασης μιας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή που είναι απολύτως αναγκαία για να μπορεί ο πάροχος υπηρεσίας της κοινωνίας της πληροφορίας την οποία έχει ζητήσει ρητά ο συνδρομητής ή ο χρήστης να παρέχει τη συγκεκριμένη υπηρεσία.»*

Ενημέρωση από Google

- Η Google το καλοκαίρι του 2015 έστειλε email σε όλους τους χρήστες των υπηρεσιών της: **Google AdSense, DoubleClick for Publishers and DoubleClick Ad Exchange** προκειμένου να συμμορφωθούν με την Ευρωπαϊκή νομοθεσία για τα cookies.
- Παρόλο που η νομοθεσία υπήρχε στα περισσότερα ΚΜ από το 2011, μόνο μετά το γράμμα της Google τα περισσότερα sites συμμορφώθηκαν με την νομοθεσία.

Ενημέρωση από Google (Ιούλιος 2015)

Google Ads Policy Team

Dear Publisher,

We want to let you know about a new policy about obtaining EU end-users' consent that reflects regulatory and best practice guidance. It clarifies your duty to obtain end-user consent when you use products like **Google AdSense, DoubleClick for Publishers and DoubleClick Ad Exchange**.

Please review our new EU user consent policy as soon as possible. This requires that you obtain EU end **users' consent to the storing and accessing of cookies and other information**, and to the data collection, sharing and usage that takes place when you use Google products. It does not affect any provisions on data ownership in your contract.

Please ensure that you comply with this policy as soon as possible, **and not later than 30 September 2015**.

If your site or app does not have a compliant consent mechanism, you should implement one now. To make this process easier for you, we have compiled some helpful resources at cookiechoices.org.

This policy change is being made in response to best practice and regulatory requirements issued by the European data protection authorities. These requirements are reflected in changes that have been recently made on Google's own websites.

Thank you in advance for your understanding and cooperation.

Regards,

The Google Policy Team

Οδηγία 2006/24 της ΕΕ

- Πρόσθεσε ή / και τροποποίησε ζητήματα που θίγονταν στην Οδηγία 2002/58 σχετικά με **την προστασία ιδιωτικής ζωής** στις ηλεκτρονικές επικοινωνίες ιδίως **όσον αφορά τη διατήρηση των δεδομένων προσωπικού χαρακτήρα**.
- Σκοπός της Οδηγίας ήταν να καθορίσει ζητήματα σχετικά με **τη διαθεσιμότητα των δεδομένων για τους σκοπούς της διερεύνησης, διαπίστωσης και δίωξης σοβαρών ποινικών αδικημάτων**.
- Η Οδηγία εφαρμόζεται **σε δεδομένα κίνησης και θέσης** τα οποία είναι απαραίτητα για την αναγνώριση του συνδρομητή, ενώ **δεν εφαρμόζεται στο περιεχόμενο των επικοινωνιών**.

Ποια δεδομένα κρατούνται;

- Για κάθε επικοινωνία μέσω των δικτύων ηλεκτρονικών επικοινωνιών (σταθερή - κινητή τηλεφωνία, διαδίκτυο κλπ) **πρέπει να κρατούνται** από τον πάροχο της υπηρεσίας δεδομένα τα οποία προσδιορίζουν:
 - την πηγή και τον προορισμό της επικοινωνίας,
 - την ημερομηνία, ώρα και διάρκεια της επικοινωνίας,
 - το είδος της επικοινωνίας,
 - τον εξοπλισμό επικοινωνίας των χρηστών,
 - την θέση επικοινωνίας στις περιπτώσεις κινητής τηλεφωνίας.

Ενδεικτικά δεδομένα

- **Ενδεικτικά δεδομένα** που θα πρέπει να κρατούνται από τον πάροχο:
 - Τηλεφωνικός αριθμός καλούντος – καλούμενου,
 - Όνομα διεύθυνση συνδρομητών,
 - Κωδικός χρήστη (πρόσβαση στο διαδίκτυο) και διεύθυνση IP,
 - Ημερομηνία σύνδεσης – αποσύνδεσης από διαδίκτυο,
 - Διεθνής ταυτότητα χρήστη κινητής (IMSI – International Mobile Subscriber Identity) και διεθνής ταυτότητα του εξοπλισμού κινητής (IMEI – International Mobile Equipment Identity),
 - Κωδικός θέσης (ταυτότητα κυψέλης) κατά την έναρξη της επικοινωνίας μέσω κινητών δικτύων καθώς επίσης και κατά την διάρκεια όλης της επικοινωνίας.

IMSI - IMEI

- IMSI:
 - Το IMSI είναι μια μοναδική ταυτότητα το οποίο αποδίδεται σε κάθε SIM (Subscriber Identification Module) κάρτα και η οποία προσδιορίζει τον συνδρομητή του δικτύου κινητής τηλεφωνίας.
 - Σε πολλές χώρες η SIM κάρτα δίδεται μόνο με την κατάθεση των προσωπικών στοιχείων του συνδρομητή, άρα το IMSI προσδιορίζει εμμέσως και το φυσικό / νομικό πρόσωπο το οποίο χρησιμοποιεί την συγκεκριμένη σύνδεση κινητής τηλεφωνίας.
- IMEI:
 - Το IMEI είναι ένας αριθμός ο οποίος προσδιορίζει μοναδικά την κινητή συσκευή η οποία συνδέεται σε ένα δίκτυο κινητής τηλεφωνίας ή ένα δίκτυο δορυφορικής επικοινωνίας.
 - Συνήθως εμφανίζεται στην οθόνη του κινητού εάν πληκτρολογήσουμε *#06#.
 - Το IMEI χρησιμοποιείται σε ορισμένες χώρες (συμπεριλαμβανομένου και της Ελλάδας), μεταξύ άλλων, και για απενεργοποίηση κλεμμένων κινητών συσκευών.

Για πόσο διάστημα κρατούνται;

- Τα Κράτη Μέλη υποχρεώνουν τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών να διατηρούν τα δεδομένα τους για διάστημα όχι μικρότερο από 6 μήνες και όχι μεγαλύτερο από 2 χρόνια από την στιγμή που πραγματοποιήθηκε η επικοινωνία. Κάθε ΚΜ μπορεί με αιτιολογημένο αίτημα να ζητήσει την αύξηση του διαστήματος διατήρησης.
- Οι πάροχοι θα πρέπει να διασφαλίζουν ότι για τα δεδομένα που πρέπει να κρατούνται:
 - Πρόσβαση έχουν μόνο εξουσιοδοτημένα άτομα και υπό συγκριμένες διαδικασίες οι οποίες διασφαλίζουν την προστασία προσωπικών δεδομένων
 - Αποτρέπουν την τυχαία ή παράνομη καταστροφή τους πριν από τον προβλεπόμενο χρονικό διάστημα
- Τα δεδομένα πρέπει να παρέχονται στις αρμόδιες αρχές κατόπιν αιτιολογημένου αιτήματος χωρίς αδικαιολόγητη καθυστέρηση.

Ενότητα V

- Προστασία Προσωπικών Δεδομένων
 - Προσωπικά Δεδομένα
 - Οδηγία 2002/58
 - Οδηγία 2006/24
 - Κοινωνικά δίκτυα & προσωπικά δεδομένα
- Δικαίωμα στη Λήθη (Right to be Forgotten)

Κοινωνικά δίκτυα & προσωπικά δεδομένα

- Κοινωνικά Δίκτυα : Facebook
- Υπηρεσίες email : Google / Gmail

Εγγράφομαι στο Facebook

- Εύκολα και απλά:
 - Ελάχιστες απαιτούμενες πληροφορίες για εγγραφή:
 - Ονοματεπώνυμο
 - Email / αριθμό κινητού τηλεφώνου
 - Ημερομηνία Γέννησης
 - Φύλο
- ...και γρήγορα εκτός εάν διαβάσουμε τους όρους χρήσης

Facebook τα πρώτα λεπτά....

- Στα πρώτα λεπτά μετά την εγγραφής μας στο facebook έχουμε δώσει τα ακόλουθα στοιχεία (δεν είναι όλα υποχρεωτικά):
 - ποιοι είμαστε,
 - στοιχεία επικοινωνίας (email, κινητό),
 - ηλικία / φύλο,
 - με ποιους συνεργαζόμαστε,
 - με ποιους μιλάμε,
 - τους πραγματικούς μας φίλους,
 - τα μέλη της οικογένειάς μας (επαφές ηλεκτρονικής αλληλογραφίας),
 - από πού καταγόμαστε,
 - που μένουμε και τέλος
 - μία φωτογραφία μας.

Δικαιώματα αρχείων

- Για οποιοδήποτε υλικό «ανεβάζουμε» στο FB (φωτογραφίες, βίντεο κλπ), παρέχουμε στο FB **δωρεάν τη μη αποκλειστική, μεταβιβάσιμη, παγκόσμια και με δυνατότητα εκχώρησης άδεια χρήσης οποιουδήποτε περιεχομένου**
- Η Άδεια Χρήσης παύει να ισχύει σε περίπτωση που διαγράψουμε το περιεχόμενο ή το λογαριασμό μας, **εκτός εάν το εν λόγω περιεχόμενο έχει κοινοποιηθεί σε τρίτους (πχ σε ψηφιακούς φίλους)**
- Το διαγραφμένο περιεχόμενο IP **“ενδέχεται να παραμείνει αποθηκευμένο σε αντίγραφα ασφαλείας για εύλογο χρονικό διάστημα (χωρίς όμως να είναι διαθέσιμο σε τρίτους)”**

Επίθεση στο Charlie Hebdo



- Τον Ιανουάριο του 2015 ένοπλοι επιτέθηκαν στα γραφεία του σατυρικού περιοδικού Charlie Hebdo στο Παρίσι.
- Μεταξύ των θυμάτων της τρομοκρατικής επίθεσης ήταν και ένας αστυνομικός ο οποίος δολοφονήθηκε από τους ενόπλους στο πεζοδρόμιο έξω από τα γραφεία του περιοδικού.

Επίθεση στο Charlie Hebdo

- Το βίντεο με την δολοφονία του αστυνομικού κυκλοφόρησε και διαδίκτυο (Youtube) λίγα μόλις λεπτά μετά το τραγικό περιστατικό.
- Ποιος είχε βιντεοσκοπήσει το τραγικό περιστατικό;
- Ποιος το είχε ανεβάσει στο διαδίκτυο;

Ανέβασμα αρχείων ...

- Η σκηνή της δολοφονίας του αστυνομικού είχε βιντεοσκοπηθεί από έναν πολίτη ο οποίος διέμενε στο απέναντι κτήριο από το μέρος όπου δολοφονήθηκε ο άτυχος αστυνομικός.
- Ο εν λόγω πολίτης (Jordi Mir), όπως ο ίδιος δήλωσε μόλις βιντεοσκόπησε το περιστατικό, μέσα στον πανικό του, ένιωσε την ανάγκη να μιλήσει με κάποιον και να μοιρασθεί μαζί του το γεγονός.
- Ήταν μόνος του στο διαμέρισμά του και σκέφτηκε ότι θα έπρεπε να το μοιρασθεί με τους 2.500 διαδικτυακούς του φίλους στο Facebook οπότε και ανέβασε το περιεχόμενο του ερασιτεχνικού βίντεο στην σελίδα κοινωνικής δικτύωσης που διατηρούσε.

Απερισκεψία ή εθισμός;

- Μετά από 15 λεπτά αφότου το είχε ανεβάσει συνειδητοποίησε ότι το περιεχόμενό του ίσως να ήταν σοκαριστικό, ιδίως για τους συγγενείς και οικείους του άτυχου αστυνομικού και θα έπρεπε να το κατεβάσει αμέσως, πράγμα που έκανε.
- Αμέσως μετά ανοίγοντας την τηλεόρασή του διαπίστωσε ότι όλα τα διεθνή μέσα ενημέρωσης (CNN, BBC, AP κλπ) πρόβαλαν το βίντεό του. Κάποιος διαδικτυακός του φίλος το είχε ανεβάσει στο Youtube και από εκεί και πέρα διαδόθηκε με αστραπιαίους ρυθμούς.
- Ο εν λόγω χρήστης τους Facebook σε δήλωσή του χαρακτήρισε ηλίθια την ενέργειά του (να ανεβάσει το βίντεο στο Facebook) και δήλωσε ότι «... **μετά από 10 χρόνια στο Facebook έχω εκπαιδευτεί**» (ή καλύτερα έχει εθιστεί) **«να μοιράζομαι ότι βλέπω: μια φωτογραφία, από μια γάτα, την ανεβάζω αμέσως στο Facebook. Ήταν το ίδιο ηλίθιο αντανakλαστικό».**

Διδάγματα

- Σκέψη πριν από την ενέργεια...
- Πνευματικά δικαιώματα...
- Ταχύτητα διάδοσης....
- Δυνατότητα διόρθωσης...

Facebook – Αποποίηση ευθύνης...

- Το FB δεν παρέχει καμία εγγύηση ασφαλούς πλοήγησης
- Ο χρήστης του FB δεσμεύεται μεταξύ άλλων:
 - *Δεν θα παρενοχλεί, τρομοκρατεί, απειλεί οποιοδήποτε χρήση*
 - *Δεν θα χρησιμοποιεί το FB για οποιαδήποτε παράνομη, κακόβουλη και παραπλανητική ενέργεια*
 - *Μη δημοσίευση μη εξουσιοδοτημένων εμποριών πληροφοριών*

Διαδίκτυο $\neq$ Πεδίο Ανομίας & Ανωνυμίας

- Η ευθύνη για τις ενέργειες που κάνω στο FB **είναι δική μου**:
 - Τον Οκτώβριο του 2013 δύο έφηβες συνελήφθησαν στις ΗΠΑ για την εμπλοκή τους στο θάνατο μιας 12χρονης, η οποία αυτοκτόνησε, αφότου έγινε στόχος διαδικτυακής παρενόχλησης και εκφοβισμού. Οι έφηβες “παρενοχλούσαν και εκφόβιζαν κατ’επανάληψη” το θύμα.
 - Τον Αύγουστο του 2013 δύο άτομα συνελήφθησαν στην Ελλάδα για εκβιασμό ανηλίκων, με άσεμνο υλικό μέσα από τις ιστοσελίδες του FB

Facebook – Ακρίβεια στοιχείων

- Ο χρήστης του FB δεσμεύεται ότι:
 - Δεν θα παρέχει **ψευδείς προσωπικές** πληροφορίες
 - Δεν θα δημιουργεί λογαριασμούς **για οποιοδήποτε άλλο πρόσωπο** εκτός από τον ίδιο χωρίς σχετική άδεια
 - Δεν θα δημιουργεί περισσότερους από **έναν προσωπικούς λογαριασμούς**
 - Σε περίπτωση **που απενεργοποιηθεί** ο λογαριασμός, δεν θα δημιουργήσει **άλλο λογαριασμό** χωρίς σχετική άδεια από το FB
 - Δεν θα χρησιμοποιεί **το Facebook εάν είναι κάτω των 13 ετών**

Facebook – Ηλικία κάτω των 13

- Πώς μπορώ να αναφέρω ένα παιδί κάτω των 13 ετών (με βάση τις Οδηγίες από το FB);
 - *“Το Facebook επιτρέπει τη δημιουργία λογαριασμού σε άτομα που έχουν συμπληρώσει τουλάχιστον το 13ο έτος της ηλικίας.*
 - *Αν το παιδί σας δημιούργησε λογαριασμό στο Facebook, χωρίς να έχει συμπληρώσει το νόμιμο όριο ηλικίας, δείξτε του πώς να διαγράψει το λογαριασμό του.*
 -”

Facebook - Διαγραφή Λογαριασμού

- Αν διαγράψουμε οριστικά το λογαριασμό μας τότε:
 - «Δεν θα έχετε ποτέ ξανά πρόσβαση στο λογαριασμό σας.
 - Τα **περισσότερα** προσωπικά δεδομένα που σχετίζονται με το λογαριασμό σας **θα διαγραφούν** από τη βάση δεδομένων μας. Στα δεδομένα αυτά περιλαμβάνονται μεταξύ άλλων **το όνομα, η διεύθυνση email, η ταχυδρομική διεύθυνση και το ψευδώνυμο που χρησιμοποιείτε σε υπηρεσίες συνομιλίας (chat)**. Ίσως παραμείνουν κάποια προσωπικά δεδομένα (όπως το όνομά σας, αν έχετε στείλει μήνυμα σε κάποιον).»
 - «Για τεχνικούς λόγους, **ίσως διατηρήσουμε αντίγραφα κάποιου υλικού** (φωτογραφιών, σημειώσεων κτλ.) στους διακομιστές μας. Όμως, το υλικό αυτό δεν θα σχετίζεται με προσωπικά αναγνωρίσιμα στοιχεία και δεν θα είναι προσβάσιμο **από άλλους χρήστες του Facebook**.»

Facebook – Τι γνωρίζει για εμένα;

- Μετά από λίγο καιρό δραστηριοποίησης στο FB, ποιες πληροφορίες είναι διαθέσιμες στο FB για το άτομό μου;
- «Κατεβάστε» ένα αντίγραφο των δεδομένων που κρατάει το FB για τον λογαριασμό σας για να δείτε τουλάχιστον ένα μέρος των πληροφοριών...

Αντίγραφο Δεδομένων Λογαριασμού

- Ένα zip αρχείο το οποίο περιλαμβάνει όλη την δραστηριότητα του χρήστη στο FB όπως:
 - Φίλους, μηνύματα, χρονολόγιο, συνδέσεις, ρυθμίσεις, προσωπικά στοιχεία, στοιχεία «τοίχου», ρυθμίσεις ασφαλείας, γεγονότα, όλα τα στοιχεία των φίλων και των επαφών, εκδηλώσεις, διαφημίσεις κ.α

Αρχείο security (2)

- Πληροφορίες αρχείου security:
 - Πότε έκανα login (ημερομηνία – ώρα)
 - Πότε έκανα logout (ημερομηνία – ώρα)
 - Από πού (διεύθυνση IP)
 - Με ποιο πρόγραμμα (chrome, internet explorer, mozilla etc)

Πληροφορίες που συλλέγονται...

- «Πληροφορίες **εγγραφής...**
- Πληροφορίες **που κοινοποιούμε...**
- **Πληροφορίες που κοινοποιούν άλλοι για εμάς ...**
- Δεδομένα σχετικά με σας κάθε φορά που **αλληλεπιδράτε με το Facebook**: δηλαδή όταν κοιτάτε το Χρονολόγιο κάποιου, στέλνετε ή λαμβάνετε μήνυμα, αναζητάτε φίλο ή Σελίδα, κλικάρετε ή βλέπετε μια διαφήμιση (ή αλληλεπιδράτε μαζί της με άλλον τρόπο), χρησιμοποιείτε μια εφαρμογή του Facebook, αγοράζετε Μονάδες Facebook ή κάνετε άλλες αγορές μέσω Facebook.»

Πληροφορίες που συλλέγονται...

- «Όταν δημοσιεύετε στο Facebook φωτογραφίες.... η ώρα, η ημερομηνία και το σημείο λήψης της φωτογραφίας ή του βίντεο.
- ...η διεύθυνση IP και άλλες πληροφορίες, όπως είναι ο πάροχος Διαδικτύου, η τοποθεσία, ο τύπος (μαζί με τα αναγνωριστικά) του προγράμματος περιήγησης που χρησιμοποιείτε ή οι σελίδες που επισκέπτεστε..»
- ...ίσως συγκεντρώσουμε δεδομένα σας για να προσδιορίσουμε ποιους φίλους θα σας δείχνουμε
Ενδέχεται να συνδυάσουμε την πόλη στην οποία μένετε με άλλες πληροφορίες GPS και τοποθεσίας που έχουμε για σας.
Επίσης, ενδέχεται να χρησιμοποιήσουμε προσωπικά σας δεδομένα για να σας δείξουμε πιο σχετικές διαφημίσεις.»

Περιήγηση στο Διαδίκτυο & Σύνδεση στο FB

- **Περιήγηση στο Διαδίκτυο χωρίς να είμαι συνδεδεμένος στο FB:**
 - Ανώνυμος χρήστης, οι διαφημίσεις είναι γενικού ενδιαφέροντος (με ενημερώνει ότι η εν λόγω ιστοσελίδα «αρέσει» σε 259.943 άτομα)
- **Περιήγηση στο Διαδίκτυο όντας συνδεδεμένος στο FB:**
 - Το FB γνωρίζει ότι επισκέπτομαι τον εκάστοτε ιστότοπο οπότε και προσαρμόζει άμεσα και δυναμικά τις σχετικές διαφημίσεις στο δικό μου προφίλ (με ενημερώνει ότι η εν λόγω ιστοσελίδα «αρέσει» σε δύο ψηφιακούς φίλους μου και σε άλλα 259.942 άτομα ακόμη)

Facebook – Χρήση Δεδομένων

Χρήση δεδομένων χρηστών

- «Πριν κοινοποιήσουμε αυτά τα δεδομένα στους διαφημιστικούς συνεργάτες ή στους πελάτες μας, **αφαιρούμε το όνομά σας και κάθε άλλο προσωπικό δεδομένο σας. Εναλλακτικά, συνδυάζουμε τα δεδομένα σας με τα δεδομένα άλλων ατόμων, ώστε να μην είναι πλέον αναγνωρίσιμα.**»...
-
- «Δεν κοινοποιούμε τις πληροφορίες σας σε άλλους, εκτός από τις εξής περιπτώσεις:
 - μας έχετε δώσει την άδειά σας,
 - **σας έχουμε ειδοποιήσει σχετικά** (π.χ. σας έχουμε ενημερώσει γι' αυτό στην πολιτική μας) ή
 - έχουμε αφαιρέσει το όνομά σας ή άλλα προσωπικά στοιχεία ταυτότητας από τις συγκεκριμένες πληροφορίες»

Όροι Χρήσης Διαδικτυακών Υπηρεσιών

- Κοινωνικά Δίκτυα : Facebook
- Υπηρεσίες email : Google / Gmail

Τι στοιχεία συλλέγει η Google (1);

- Συλλογή στοιχείων:
 - **Στοιχεία εγγραφής:** όνομα, email, αριθμός τηλεφώνου ή στοιχεία πιστωτικής κάρτας, φωτογραφία.
 - **Στοιχεία χρήσης:** αναγνωριστικά συσκευής, ερωτήματά μας, αριθμός καλούμενου, IP, ρυθμίσεις συσκευής, λογισμικό συσκευής, ημερομηνία και ώρα αιτήματος, cookies.....
 - **Στοιχεία τοποθεσίας:** σήματα GPS, σημεία πρόσβασης WiFi ή κεραιών κινητής τηλεφωνίας

Κοινοποίηση προσωπικών δεδομένων (1)

- Πληροφορίες τις οποίες μοιράζεται η Google με άλλους φορείς / οργανισμούς / εταιρίες :
 - **Δεν κοινοποιούνται προσωπικά** στοιχεία σε εταιρίες, οργανισμούς και μεμονωμένα άτομα εκτός του Google, **εκτός αν ισχύει μία από τις παρακάτω περιπτώσεις:**
 - Για νομική επεξεργασία, με ρητή συναίνεση των χρηστών, με διαχειριστές τομέα, για εξωτερική επεξεργασία: *«Παρέχουμε προσωπικά στοιχεία στους συνεργάτες μας και σε επιχειρήσεις ή άτομα που εμπιστευόμαστε για να τα επεξεργαστούν για δική μας χρήση»*

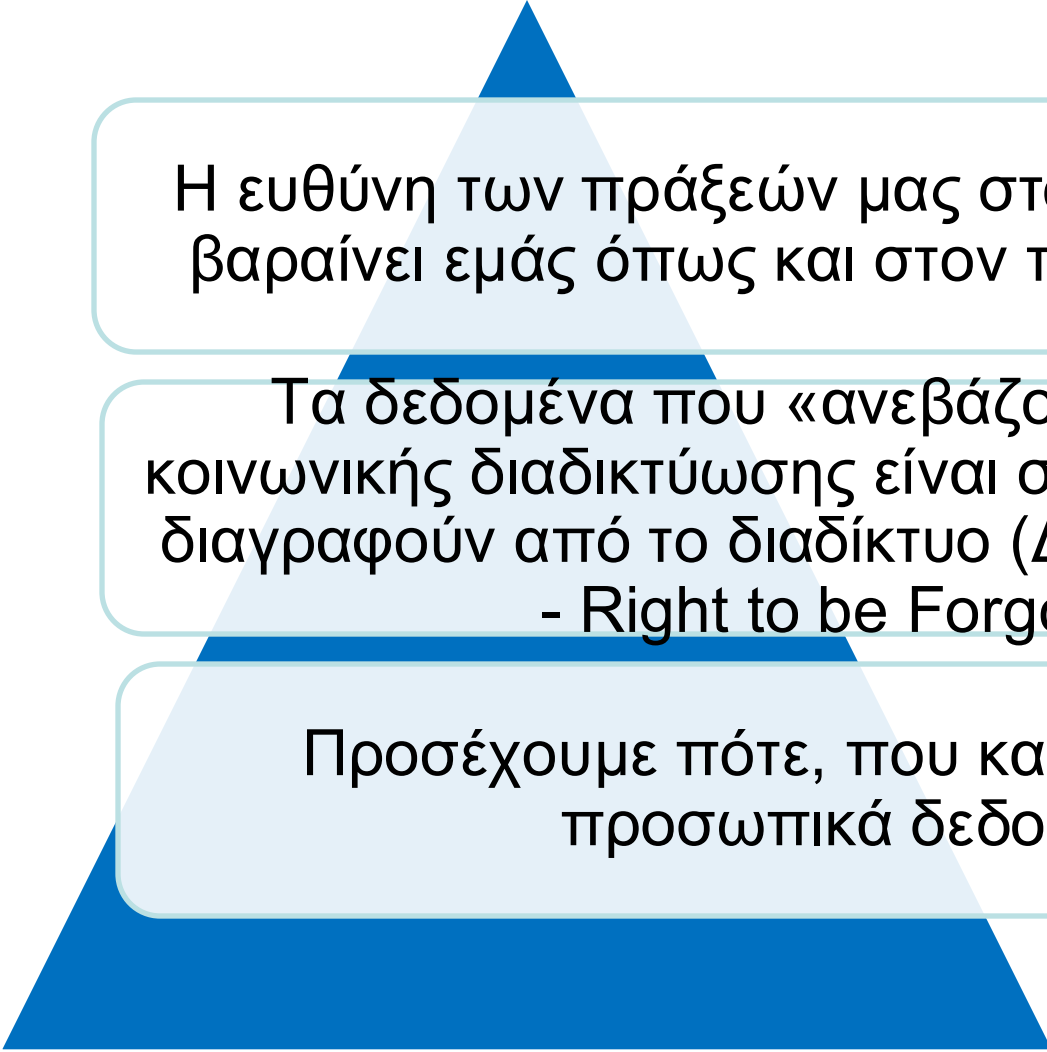
Κοινοποίηση προσωπικών δεδομένων (2)

- ***“Ενδέχεται να μοιραστούμε συγκεντρωτικά στοιχεία μη προσωπικής ταυτοποίησης δημόσια και με τους συνεργάτες μας – όπως εκδότες, διαφημιζόμενους ή συνδεδεμένους ιστότοπους. Για παράδειγμα, ενδέχεται να μοιραστούμε πληροφορίες δημόσια για να δείξουμε τις τάσεις όσον αφορά τη γενική χρήση των υπηρεσιών μας.”***

Χρήση Google Search

- Η χρήση της υπηρεσίας Google search χρησιμοποιεί μεταξύ άλλων πληροφορίες σχετικά με την τοποθεσία που ήμασταν όταν κάναμε χρήση της εν λόγω υπηρεσίας (από διεύθυνση IP του υπολογιστή).
- Εάν δεν έχουμε κάνει login υπάρχει συσχέτιση του χρήστη της εφαρμογής Chrome με τις προτιμήσεις αναζήτησης και την τοποθεσία από όπου έχουμε κάνει τις σχετικές αναζητήσεις.
- Εάν έχουμε κάνει και login στις σχετικές υπηρεσίες της Google τότε υπάρχει πλήρη συσχέτιση του χρήστη των υπηρεσιών Google (Gmail, Google+, Youtube κλπ) με τις αναζητήσεις που κάνει αλλά και από ποιες τοποθεσίες τις κάνει.
- Σε κάθε περίπτωση όμως υπάρχουν συσχετίσεις μεταξύ των χρηστών των υπηρεσιών της Google (Gmail, Google+, Youtube κλπ) με τους χρήστες των εφαρμογών της Google (Chrome).

Χρήση Διαδικτυακών Υπηρεσιών



Η ευθύνη των πράξεών μας στον ψηφιακό κόσμο
βαραίνει εμάς όπως και στον πραγματικό κόσμο

Τα δεδομένα που «ανεβάζουμε» στα μέσα
κοινωνικής διαδικτύωσης είναι σχεδόν αδύνατον να
διαγραφούν από το διαδίκτυο (Δικαίωμα στη Λήθη
- Right to be Forgotten)

Προσέχουμε τότε, που και πώς δίνουμε
προσωπικά δεδομένα

Εφαρμογή: Χάρτες

- Εγκαθιστώντας ή ενημερώνοντας την εφαρμογή “Χάρτες” της Google για κινητές συσκευές Android....

Εφαρμογή: Χάρτες

- Δεδομένα που έχει πρόσβαση η εφαρμογή (και στα οποία έχουμε δώσει την συγκατάθεσή μας):
 - Τηλέφωνο
 - Τηλέφωνο, αρχείο καταγραφής κλήσεων
 - Αναγνωριστικό συσκευή / στοιχεία κλήσεων
 - Αριθμό τηλεφώνου, μία ενεργή κλήση, αριθμό καλούμενου κλπ

Snapchat case

- Η δημοφιλής εφαρμογή Snapchat ανέφερε στην πολιτική ασφαλείας: «not ask for, track, or access any location specific information»
- Το 2014 ένας ερευνητής δημοσίευσε την εργασία του στην οποία αποδύκνειε ότι η εν λόγω εφαρμογή συλλέγει και στέλνει σε τρίτους πληροφορίες σχετικές με την τοποθεσία των χρηστών όπως πληροφορίες για τα δίκτυα WiFi και για τις κεραίες κινητής τηλεφωνίας.
- Η αρμόδια υπηρεσία στις ΗΠΑ (FDC - Federal Trade Comission) ανάγκασε το Snapchat να τροποποιήσει την πολιτική ασφαλείας του ενημερώνοντας τους χρήστες για τις πρακτικές της (Πηγή: In the Matter of Snapchat, Inc., FTC No. 132 3078 (December 31, 2014, Complaint)).

Ενότητα V

- Προστασία Προσωπικών Δεδομένων
 - Προσωπικά Δεδομένα
 - Οδηγία 2002/58
 - Οδηγία 2006/24
 - Κοινωνικά δίκτυα & προσωπικά δεδομένα
- Δικαίωμα στη Λήθη (Right to be Forgotten)

Προϋπάρχει από το 1995

- Η Οδηγία 1995/46/EK προβλέπει μεταξύ άλλων (άρθρο 12):
- *“...Τα ΚΜ εγγυώνται ότι στα πρόσωπα στα οποία αναφέρονται τα δεδομένα προσωπικού χαρακτήρα έχουν το δικαίωμα να ζητήσουν από τον υπεύθυνο της επεξεργασίας την κατά περίπτωση διόρθωση, διαγραφή ή το κλείδωμα των δεδομένων τα οποία είναι ελλιπή ή ανακριβή.”*

Ερώτημα στο ΔΕΚ (1)

- Το 2010 ένας Ισπανός πολίτης κατέθεσε αγωγή εναντίον μιας Ισπανικής εφημερίδας και της Google, διότι και οι δύο εμφάνιζαν δεδομένα τα οποία αφορούσαν μία υπόθεση του 1998 και ειδικότερα τις διαδικασίες πλειστηριασμού της κατοικίας τους, λόγω οφειλών του, υπόθεση η οποία είχε ολοκληρωθεί και διευθετηθεί προ πολλού και επομένως σύμφωνα με τον αιτούνται δεν υπήρχε λόγος αναφοράς στην υπόθεση.
- Ειδικότερα η εφημερίδα περιείχε πληροφορίες για τον εν λόγω πλειστηριασμό, ενώ η Google περιείχε σύνδεσμο προς τον ιστότοπο της εφημερίδας, όταν κάποιος χρησιμοποιούσε τις υπηρεσίες αναζήτησης της Google για να αναζητήσει πληροφορίες σχετικά με το ονοματεπώνυμο του εν λόγω Ισπανού πολίτη.

Ερώτημα στο ΔΕΚ (2)

- Ο Ισπανός πολίτης είχε αιτηθεί από την εφημερίδα να διαγράψει τις σχετικές πληροφορίες και από την Google να διαγράψει τον σύνδεσμο από την μηχανή αναζήτησης προς τις σχετικές πληροφορίες.
- Το εθνικό δικαστήριο απεύθυνε εξωδικαστικό ερώτημα στο ΔΕΚ το οποίο περιελάμβανε τα ακόλουθα υπο-ερωτήματα :
 - Κατά πόσο οι διατάξεις της Οδηγίας 1995/46 έβρισκαν εφαρμογή σε δεδομένα της μηχανής αναζήτησης της Google.
 - Κατά πόσο είχε αρμοδιότητα να επιβάλει μέτρα στην Google με δεδομένο ότι η εν λόγω εταιρεία είχε έδρα στις ΗΠΑ.
 - Κατά πόσο έχει δικαίωμα ένας πολίτης να ζητήσει την διαγραφή των δεδομένων από μία μηχανή αναζήτησης.

Απάντηση από ΔΕΚ (1)

- Το ΔΕΚ γνωμοδότησε στις 13-5-2014 ως ακολούθως:
 - Οι μηχανές αναζήτησης επεξεργάζονται προσωπικά δεδομένα και άρα εμπίπτουν στο πεδίο της Οδηγίας 1995/46 περί επεξεργασίας προσωπικών δεδομένων, άρα και στην αρχή του Δικαιώματος στη Λήθη.
 - Παρόλο που η Google εδρεύει στις ΗΠΑ το γεγονός ότι έχει θυγατρική σε ένα ΚΜ η οποία προωθεί τις υπηρεσίες της Google (μέσω διαφημίσεων στον σχετικό ιστότοπο) συνεπάγεται ότι έχει όλες τις υποχρεώσεις που προβλέπονται από το σχετικό νομικό πλαίσιο για μία εταιρία που εδρεύει σε χώρα της ΕΕ.
 - Οι πολίτες έχουν δικαίωμα στη λήθη και σε δεδομένα που περιέχονται σε μηχανές αναζήτησης και προβάλλονται κατά την αναζήτηση πληροφοριών για το ονοματεπώνυμο ενός φυσικού προσώπου, όταν αυτά είναι ανακριβή, ελλιπή, ή μη σχετικά με τους σκοπούς της επεξεργασίας των δεδομένων.

Απάντηση από ΔΕΚ (2)

- Το ΔΕΚ επίσης γνωμοδότησε ότι η αναγνώριση του Δικαιώματος στη Λήθη δεν θα πρέπει να έρχεται σε αντίθεση με την θεμελιώδη αρχή της ελευθερίας της έκφρασης και των μέσων.
- Κάθε περίπτωση θα πρέπει να εξετάζεται αναλυτικά και ξεχωριστά και δεν μπορεί να διατυπωθεί ένας απόλυτος κανόνας. Για κάθε περίπτωση θα πρέπει να εξετάζεται:
 - Ο τύπος των πληροφοριών και δεδομένων.
 - Η ευαισθησία των δεδομένων όσον αφορά την ιδιωτική ζωή του κάθε ατόμου.
 - Το ενδιαφέρον του κοινού για την πρόσβαση στις ανωτέρω πληροφορίες / δεδομένα.
 - Ο ρόλος του ατόμου που ζητά την διαγραφή των δεδομένων στα κοινά και στον δημόσιο βίο.

Απάντηση από ΔΕΚ (3)

- Το κάθε δικαστήριο για να αποφασίσει θα πρέπει να σταθμίζει κατά πόσο η επέμβαση στα δικαιώματα του κάθε ατόμου ιδίως όπως αυτά περιέχονται στον Χάρτη των Θεμελιωδών Δικαιωμάτων δικαιολογείται ή όχι από το συμφέρον του κοινού για πρόσβαση στην επίμαχη πληροφορία. Βασικό κριτήριο αποτελεί ο ρόλος του ατόμου στο δημόσιο βίο.
- Στην υπόθεση του Ισπανού πολίτη το δικαστήριο έκανε εν μέρει δεκτό το αίτημα του εν λόγω πολίτη. Ειδικότερα το δικαστήριο αποφάσισε ότι η Google θα πρέπει να διαγράψει τον σύνδεσμο που εμφανίζεται στην μηχανή αναζήτησης όταν κάποιος πληκτρολογήσει το ονοματεπώνυμο του εν λόγω Ισπανού πολίτη. Όμως στην ίδια απόφαση το δικαστήριο θεώρησε ότι δεν είναι απαραίτητο να διαγραφούν τα σχετικά δεδομένα τα οποία είναι αποθηκευμένα στον ιστότοπο της εφημερίδας και αφορούν τον συγκεκριμένο πολίτη.

Η Google συμμορφώθηκε ...

- Η Google 15 ημέρες μετά την δημοσιοποίηση της γνωστοποίησης του Δικαστηρίου παρουσίασε μία πλατφόρμα προκειμένου οι χρήστες των σχετικών υπηρεσιών της μηχανής αναζήτησης να μπορούν να στείλουν σχετικά αιτήματα για απόκρυψη των διασυνδέσεων οι οποίες αναφέρονται σε δεδομένα προσωπικού χαρακτήρα.

Οι πολίτες επωφελήθηκαν

- Μέσα σε 24 ώρες από την ημερομηνία που δημοσιοποιήθηκε η γνωμοδότηση του Δικαστηρίου η Google έλαβε παραπάνω από 12.000 αιτήσεις για αφαίρεση συνδέσεων προς δεδομένα τα οποία οι πολίτες θεωρούσαν ότι θα πρέπει να διαγραφούν.
- Μέσα σε έξι μήνες η Google είχε λάβει πάνω από 145.000 αιτήσεις για κατάργηση συνδέσεων σε ιστότοπους και έλεγξε περίπου 500.000 διαδικτυακές διευθύνσεις (URL). Πάνω από τις μισές συνδέσεις σε URL καταργήθηκαν.
- Από Ελλάδα στο αντίστοιχο διάστημα οι αιτήσεις ήταν πάνω από 800 και αφορούσαν σχεδόν 3.000 URLs. Περίπου το 40% των URLs καταργήθηκαν.

Σημαντικές λεπτομέρειες...

- Η γνωμοδότηση αφορά μόνο τις συνδέσεις που εμφανίζονται σε μηχανές αναζήτησης όταν πληκτρολογούμε το ονοματεπώνυμο ενός ατόμου:
 - Δεν αφορά δεδομένα τα οποία περιέχονται σε ιστότοπους
 - Δεν αφορά συνδέσμους οι οποίοι εμφανίζονται στις μηχανές αναζήτησης όταν πληκτρολογούμε κάποια λέξη / φράση η οποία δεν σχετίζεται με το ονοματεπώνυμο κάποιου πολίτη.
- Υπάρχουν περιπτώσεις όπου κάποιοι σύνδεσμοι διαγράφονται από τις μηχανές αναζήτησης, όμως:
 - Οι σύνδεσμοι μπορεί να εμφανίζονται όταν πληκτρολογούμε στην μηχανή αναζήτησης κάποια άλλη λέξη ή φράση,
 - Το περιεχόμενο μπορεί να εξακολουθεί να βρίσκεται στους ιστοτόπους που παρέπεμπαν τα αποτελέσματα της μηχανής αναζήτησης όταν πληκτρολογούσαμε το ονοματεπώνυμο κάποιου πολίτη.

ΗΠΑ: Results about You

- Η Google έχει διαθέσει στις ΗΠΑ την υπηρεσία Results about You
- Μέσω της υπηρεσίας κάθε ένας χρήστης της Google μπορεί να πληροφορηθεί για ποιες προσωπικές πληροφορίες είναι διαθέσιμες στο διαδίκτυο όταν κάποιος πληκτρολογεί το ονοματεπώνυμό του ή κάποιο προσωνύμιο σχετικό με αυτόν
- Προσωπικές πληροφορίες: Ονοματεπώνυμο, διεύθυνση κατοικίας, τηλέφωνο, ΑΦΜ, ΑΔΤ, τραπεζικοί λογαριασμοί κα.
- Ο κάθε χρήστης έχει δικαίωμα να ζητήσει με αιτιολογημένο αίτημα από την Google να μην εμφανίζονται οι εν λόγω πληροφορίες (ο σύνδεσμος που οδηγεί στις εν λόγω πληροφορίες) όταν κάποιος πληκτρολογεί το ονοματεπώνυμό του στη μηχανή αναζήτησης της Google
- Η Google δεν είναι υποχρεωμένη να ικανοποιήσει το αίτημα
- Επίσης υπάρχει η δυνατότητα η Google να ενημερώνει τον χρήστη κάθε φορά που προστίθεται στο διαδίκτυο μια προσωπική πληροφορία για τον εν λόγω χρήστη.

Ασφάλεια Πληροφοριών

- Η **ασφάλεια πληροφοριών** (information security) ενός υπολογιστικού συστήματος προσδιορίζεται από **τα μέτρα που έχουν ληφθεί για την προστασία των πόρων** του υπολογιστικού συστήματος από ενέργειες ή γεγονότα τα οποία:
 - άμεσα ή έμμεσα
 - με ή χωρίς πρόθεση
- μπορούν **να μειώσουν την αξία** των πόρων του συστήματος
- Η αξία των πόρων ενός συστήματος μπορεί να μειωθεί:
 - **καταστρέφοντας** τους πόρους
 - **υποκλέπτοντας / αφαιρώντας** τους πόρους
 - **υποκλέπτοντας (χωρίς να αφαιρεθούν)** τους πόρους (δεδομένα / πληροφορίες)
 - **αποκτώντας** (χωρίς να υπάρχει εξουσιοδότηση) **πρόσβαση** και δικαιώματα στους πόρους

Συνέπειες παραβίασης ασφάλειας

- Οι συνέπειες της παραβίασης της ασφάλειας ενός πληροφορικού συστήματος ποικίλουν:
 - **Διαρροή δεδομένων / πληροφοριών** τα οποία είναι αποθηκευμένα στο πληροφοριακό σύστημα
 - **Αλλοίωση δεδομένων / πληροφοριών** τα οποία είναι αποθηκευμένα στο πληροφορικό σύστημα
 - **Καταστροφή ή Δυσλειτουργία υπολογιστικών πόρων** το οποίο μπορεί να έχει ως αποτέλεσμα τη δυσλειτουργία ή ακόμη και την διακοπή των υπηρεσιών που παρέχονται από το πληροφοριακό σύστημα.
- Οι συνέπειες της παραβίασης των ασφάλειας ενός συστήματος προκαλούν ορισμένες φορές **μη επανορθώσιμες ζημιές** στο πληροφοριακό σύστημα οι οποίες μπορεί να συνδέονται: με **δυσφήμιση** της υπηρεσίας, με **υπέρογκο κόστος επιδιόρθωσης** των ζημιών, με **υπέρογκο κόστος** από την καταβολή **αποζημιώσεων** στους χρήστες που έχουν υποστεί ζημιά, κ.α

Πρόληψη - Ανίχνευση - Αντίδραση

- Η ασφάλεια ενός υπολογιστικού συστήματος σχετίζεται με την **πρόληψη (prevent)** και την **ανίχνευση (detect)** γεγονότων τα οποία άμεσα ή έμμεσα με ή χωρίς πρόθεση (εσκεμμένα ή τυχαία) έχουν ως αποτέλεσμα την φθορά κάποιων συστατικών του συστήματος (υλικού ή λογισμικού) καθώς επίσης και με την εκ των υστέρων **αντίδραση (react)** του συστήματος.
- **Πρόληψη (prevention) φθορών:** λήψη μέτρων προκειμένου να προληφθούν ενέργειες οι οποίες μπορούν να βλάψουν συστατικά του συστήματος.
- **Ανίχνευση (detection) φθορών:** ύπαρξη μηχανισμών οι οποίοι είναι σε θέση να ανιχνεύσουν τότε με ποιον τρόπο και από ποιον έγινε προσπάθεια (ή επιτεύχθηκε τελικά) φθοράς κάποιου ή κάποιων συστατικών του συστήματος.
- **Αντίδραση (reaction):** ύπαρξη μηχανισμών αντίδρασης και αποκατάστασης τυχόν φθορών σε συστατικά του συστήματος.

Ασφάλεια Πληροφοριών (Δεδομένων)

- Η πρόληψη, ανίχνευση και αντίδραση ενός υπολογιστικού συστήματος σε γεγονότα / ενέργειες που μπορεί να μειώσουν την αξία των πόρων του συστήματος συνεισφέρουν στην ύπαρξη **τριών βασικών ποιοτικών χαρακτηριστικών** ενός υπολογιστικού συστήματος τα οποία σχετίζονται κυρίως με τα δεδομένα (ή την πληροφορία) που διακινείται στα υπολογιστικά συστήματα:
 - **Διαθεσιμότητα (Availability)**
 - **Εμπιστευτικότητα (Confidentiality)**
 - **Ακεραιότητα (Integrity)**

Διαθεσιμότητα - Εμπιστευτικότητα - Ακεραιότητα

- **Διαθεσιμότητα (availability):** ο βαθμός διαθεσιμότητας σχετίζεται με το **διάστημα** (σε σχέση με μία συγκεκριμένη χρονική περίοδο πχ διάρκεια ενός έτους) κατά το οποίο τα συστατικά ή/και οι υπηρεσίες ενός συστήματος **προσφέρονται** χωρίς “μεγάλες” χρονικές καθυστερήσεις κατόπιν εξουσιοδοτημένων αιτήσεων. Για την μέτρηση της διαθεσιμότητας ενός δικτύου λαμβάνονται υπόψη τόσο κακόβουλες ενέργειες (όπως για παράδειγμα επιθέσεις DOS – Denial of Service) όσο και μη κακόβουλες ενέργειες / γεγονότα όπως φυσικές ή τυχαίες καταστροφές (πχ σεισμός, ή κόψιμο καλωδίων).
- **Εμπιστευτικότητα (confidentiality):** σχετίζεται με το κατά πόσο τα δεδομένα (ή οι πληροφορίες) που διακινούνται στο υπολογιστικό σύστημα μπορούν να **αναγνωρισθούν από μη εξουσιοδοτημένα άτομα**.
- **Ακεραιότητα (integrity):** αφορά κατά πόσο τα δεδομένα / πληροφορίες που διακινούνται στο υπολογιστικό σύστημα **δεν έχουν υποστεί αλλοίωση** (διαγραφή, τροποποίηση, αντιγραφή). Η οποιαδήποτε τροποποίηση **συμπεριλαμβανομένης και της αντιγραφής** θα πρέπει να γίνεται μόνο από εξουσιοδοτημένα άτομα.

Ασφάλεια και πρόσβαση σε πόρους

- Πώς παρέχεται πρόσβαση στους πόρους τους υπολογιστικού συστήματος σεβόμενοι τις αρχές της ασφάλειας;
 - Αναγνώριση ταυτότητας
 - Αυθεντικοποίηση χρήστη
 - Εξουσιοδότηση χρήστη
- **Αναγνώριση (Identification):** σχετίζεται με τις διαδικασίες που ακολουθούνται από ένα υπολογιστικό σύστημα για την **αναγνώριση της ταυτότητας** ενός χρήστη στο σύστημα.
- **Αυθεντικοποίηση (Authentication):** σχετίζεται με τις διαδικασίες **εξακρίβωσης και επιβεβαίωσης της ταυτότητας** του χρήστη που αιτείται πρόσβαση στο σύστημα (ταυτοπροσωπία, γνήσιο υπογραφής).
- **Εξουσιοδότηση (Authorization):** σχετίζεται με το **εύρος της πρόσβασης στο σύστημα** που θα έχει ένας αυθεντικοποιημένος χρήστης του συστήματος. Το εύρος της πρόσβασης ή τα δικαιώματα πρόσβασης έχουν προκαθοριστεί για κάθε έναν αυθεντικοποιημένο χρήστη πριν από το αίτημα πρόσβασης και τα οποία μπορεί να διαφοροποιούνται τόσο μεταξύ των χρηστών του συστήματος όσο και από άλλους παράγοντες όπως είναι η συσκευή του χρήστη ή/και η τοποθεσία του χρήστη.

Αυθεντικοποίηση

- Πώς επιτυγχάνεται η αυθεντικοποίηση;
 - Με κάτι που **γνωρίζω**: Όνομα χρήστη (username) και κωδικό πρόσβαση (password))
 - Με κάτι που **έχω**: Κωδικούς μιας χρήσης (pin) που συνήθως παράγονται από μια εφαρμογή ή ένα μηχάνημα
 - Με κάτι που **είμαι**: Βιομετρικά στοιχεία (δακτυλικά αποτυπώματα, ή σάρωση ίριδας ματιού)
- Μεθοδολογίες αυθεντικοποίησης:
 - Αυθεντικοποίηση ενός παράγοντα / βήματος (**Single-Factor Authentication**): η χρήση μιας μεθόδου για την αυθεντικοποίηση του χρήστη
 - Αυθεντικοποίηση πολλαπλών παραγόντων / τμημάτων (**Multi-Factor Authentication**): η χρήση δύο ή περισσότερων μεθόδων για την αυθεντικοποίηση του χρήστη. Για την επιτυχή αυθεντικοποίηση ενός χρήστη θα πρέπει να είναι έγκυρα και τα δύο βήματα / στάδια της αυθεντικοποίησης. Η πιο συνήθης αυθεντικοποίηση πολλαπλών παραγόντων είναι η αυθεντικοποίηση δύο βημάτων (**Two-Factor Authentication**) η οποία χρησιμοποιείται κατά κόρον πλέον στις ηλεκτρονικές επικοινωνίες

Two-Factor Authentication

- Η αυθεντικοποίηση συναντιέται και σε υπηρεσίες πέρα από τις υπηρεσίες Διαδικτύου:
 - Ανάληψη χρημάτων από μια τράπεζα:
 - Από το γκισέ: 1) βιβλιάριο καταθέσεων (παλιότερα) και 2) αστυνομική ταυτότητα δικαιούχου
 - Από ένα ATM: 1) κάρτα και 2) pin κάρτας
- Στην πλειονότητα των υπηρεσιών ηλεκτρονικών επικοινωνιών χρησιμοποιείται πλέον η **αυθεντικοποίηση δύο παραγόντων**:
 - e-banking: 1) όνομα και κωδικό χρήστη 2) pin που στέλνεται μέσω κινητών τηλεφώνων (ή μέσω διαδικτύου)
 - Όλες σχεδόν οι μεγάλες εταιρίες που παρέχουν υπηρεσίες ηλεκτρονικών επικοινωνιών (Microsoft / Google / Apple / Amazon / Facebook) χρησιμοποιούν (και κάποιες πλέον απαιτούν) αυθεντικοποίηση χρηστών δύο παραγόντων

Multi Factor Authentication

Αλλαγή κωδικού ebanking

- Απαιτεί γνώση / κατοχή των:
 1. User name
 2. Χρεωστικής κάρτας
 3. Κινητού τηλεφώνου (έχει ήδη επαληθευθεί)
 4. Κωδικού χρεωστικής κάρτας

Διαδικασία:

1. Αίτηση στο web
2. Αποστολή στο κινητό κωδικού για extrapin (ισχύς για 2 λεπτά)
3. Εγγραφή στο web του κωδικού για extrapin
4. Φωνητική κλήση στην οποία ζητείται ο κωδικός χρεωστικής κάρτας
5. Αποστολή στο κινητό νέου κωδικού πρόσβασης (ισχύς 72 ώρες)
6. Υποχρεωτική αλλαγή κωδικού πρόσβασης κατά την πρώτη εισαγωγή και ανά τακτά χρονικά διαστήματα

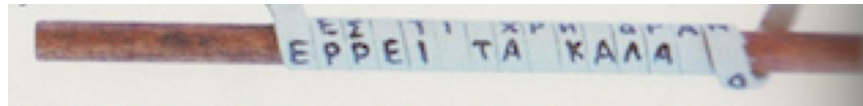
Ορισμοί σχετικοί με την ασφάλεια στο Διαδίκτυο

- Κρυπτογραφία
- Ψηφιακά πιστοποιητικά / υπογραφές
- Ψευδωνυμοποίηση - ανωνυμοποίηση

Κρυπτογραφία

- Η κρυπτογραφία (cryptography) είναι σύνθετη λέξη: κρύπτω - γραφή και σημαίνει η γραφή κειμένου με συνθηματικά στοιχεία
- Στην πληροφορική η κρυπτογραφία σχετίζεται με την συνθηματική μετατροπή των δεδομένων της πληροφορίας σε τέτοια μορφή ώστε να μην είναι δυνατή η ανάγνωση των δεδομένων από μη εξουσιοδοτημένα άτομα (ή από άτομα που δεν γνωρίζουν τα συνθηματικά κρυπτογράφησης)
- Η κρυπτογραφία χρησιμοποιούνταν από αρχαιοτάτων χρόνων

Κρυπτογραφία: κρυπτεία σκυτάλη

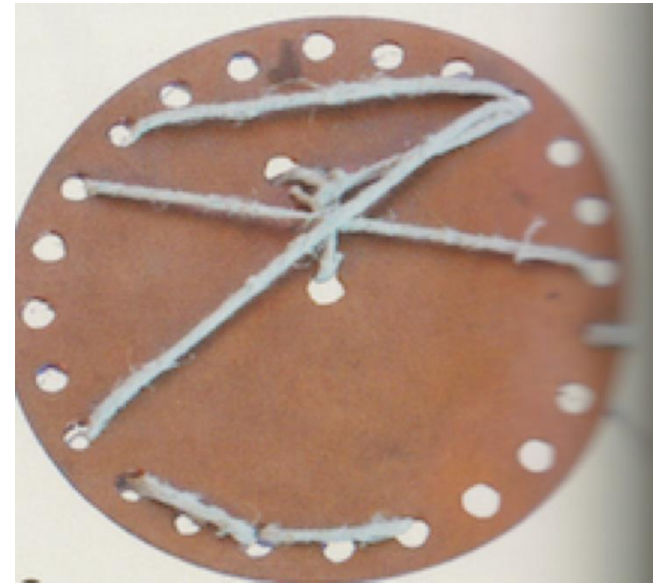


- Ο αποστολέας έγραφε το μήνυμα σε κατεργασμένο δέρμα το οποίο είχε τυλίξει σε μια ράβδο. Ο αποστολέας έστελνε μόνο το δέρμα στον παραλήπτη. Για να διαβαστεί σωστά το μήνυμα θα έπρεπε το δέρμα να τυλιχθεί σε ράβδο του ίδιου πάχους.

Πηγή: Οι εφευρέσεις των Αρχαίων Ελλήνων, Κ. Κοτσανάς

Κρυπτογραφικός δίσκος Αινεία

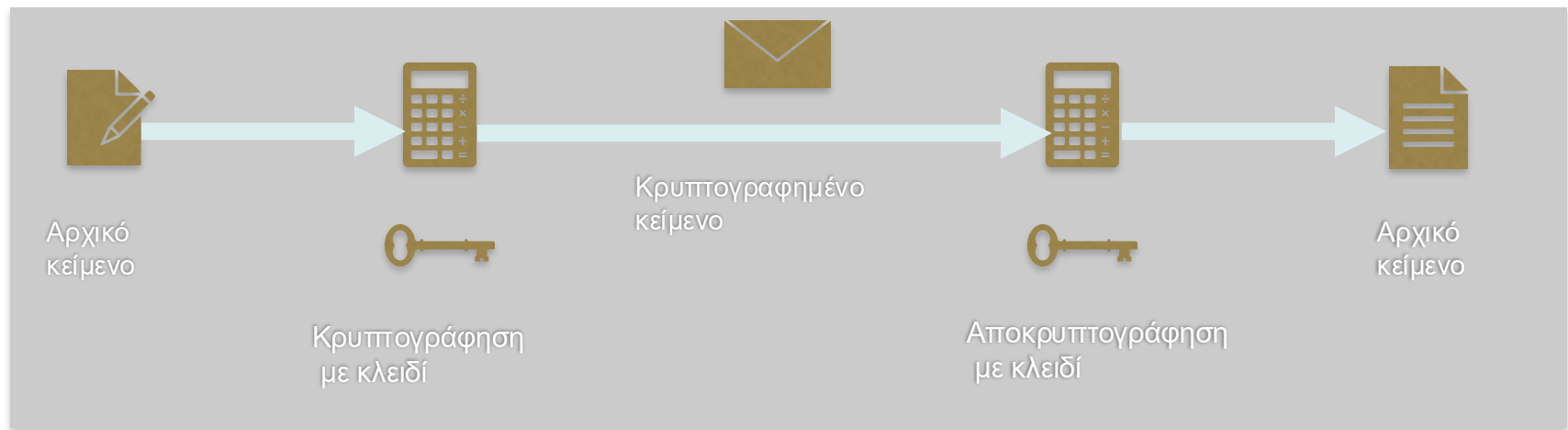
- Κάθε οπή αντιστοιχούσε σε ένα γράμμα. Ο παραλήπτης για να διαβάσει το μήνυμα ξετύλιγε το νήμα και για κάθε οπή που ήταν τυλιγμένο το μήνυμα έγραφε και το αντίστοιχο γράμμα (από δεξιά προς αριστερά).



Πηγή: Οι εφευρέσεις των Αρχαίων Ελλήνων, Κ. Κοτσανάς

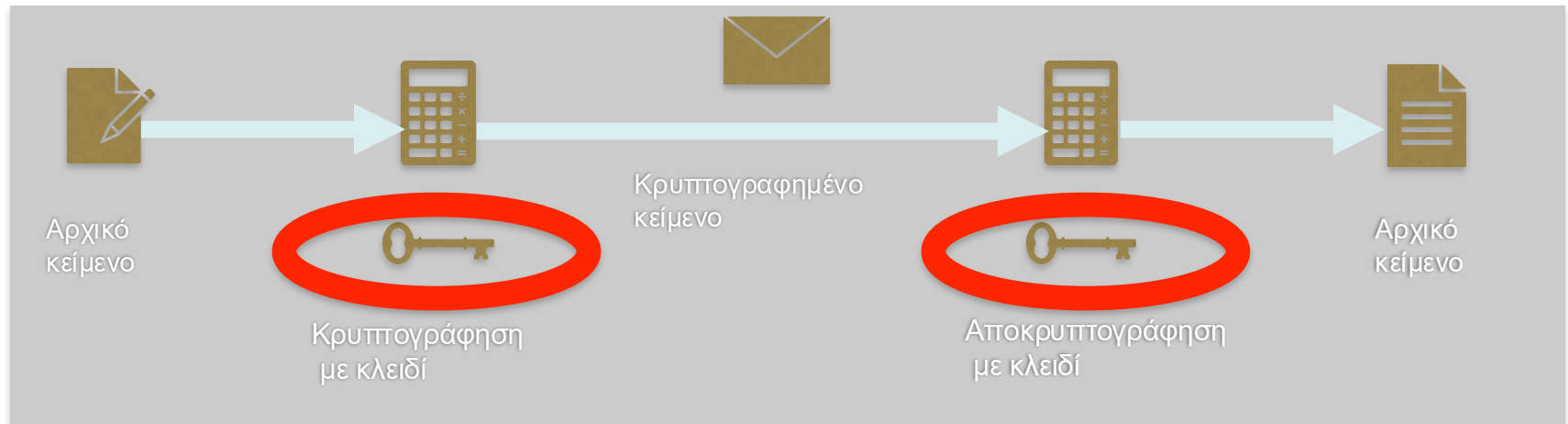
Κρυπτογραφία

- Πώς λειτουργεί;



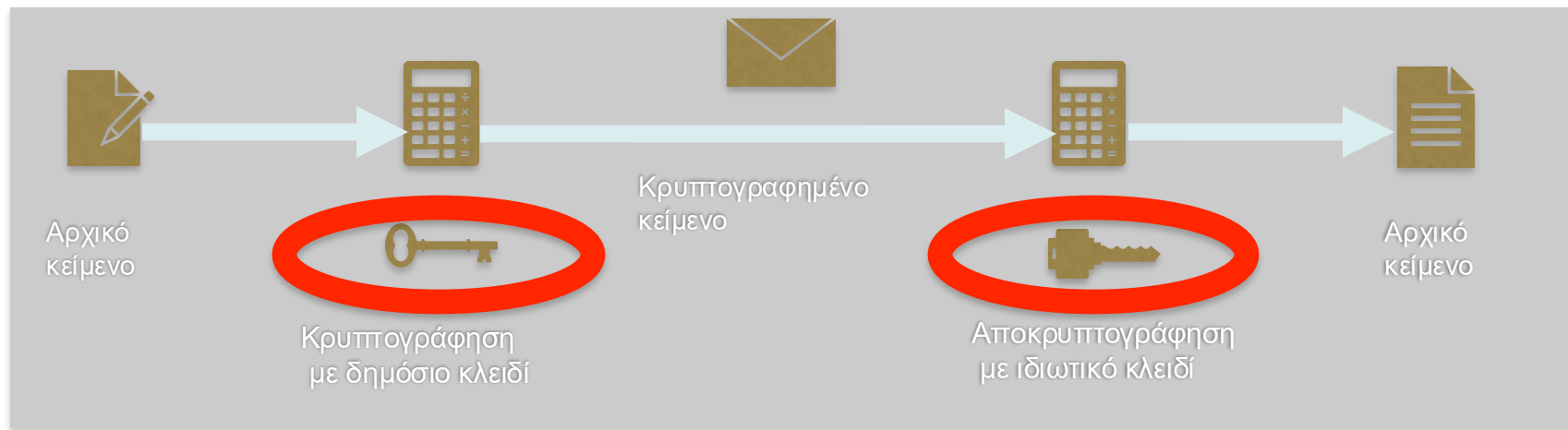
Συμμετρική

- Στη **συμμετρική κρυπτογραφία** χρησιμοποιείται **το ίδιο κλειδί** για την κρυπτογράφηση και την αποκρυπτογράφηση. Ο αποστολέας κρυπτογραφεί και ο παραλήπτης αποκρυπτογραφεί **με το ίδιο κλειδί**. Το κλειδί θα πρέπει να παραμένει μυστικό και να είναι γνωστό μόνο στους συναλλασσόμενους. Η μέθοδος αυτή **παρουσιάζει μειονεκτήματα** όσον αφορά την εφαρμογή της σε ανοιχτά δίκτυα με πολλούς χρήστες και τις αυξημένες απαιτήσεις της για την ασφάλεια (π.χ. αποθήκευση των κλειδιών κλπ).



Ασύμμετρη

- Στην **ασύμμετρη κρυπτογραφία** (ή κρυπτογραφία δημοσίου κλειδιού- public key cryptography) χρησιμοποιούνται **δύο διαφορετικά κλειδιά**, ένα για την κρυπτογράφηση και ένα για την αποκρυπτογράφηση. Κάθε χρήστης έχει στη διάθεσή του δύο κλειδιά. Το **δημόσιο κλειδί** είναι αυτό που ο χρήστης μπορεί να το γνωστοποιήσει σε τρίτους ενώ το **ιδιωτικό** είναι εκείνο που το φυλάσσει με ασφάλεια και μόνο αυτός θα πρέπει να το γνωρίζει και κατέχει. Για να επιτευχθεί η εμπιστευτικότητα, ο αποστολέας κρυπτογραφεί το μήνυμα με το **δημόσιο κλειδί του παραλήπτη**. Έτσι, το μήνυμα μπορεί να αποκρυπτογραφηθεί **μονάχα από τον παραλήπτη** (που είναι ο κάτοχος του αντίστοιχου ιδιωτικού κλειδιού εκτός και αν η μυστικότητα του ιδιωτικού κλειδιού έχει παραβιαστεί).



Ψηφιακά πιστοποιητικά - Ψηφιακή υπογραφή

- Κρυπτογράφηση
- Ασύμμετρη κρυπτογράφηση
- Συνάρτηση κατακερματισμού

Ψηφιακή (ή ηλεκτρονική)
Υπογραφή η οποία βασίζεται σε
ένα ψηφιακό πιστοποιητικό

Γιατί είναι απαραίτητη η ψηφιακή υπογραφή;

Διάφορα

Παρακαλούνται τα τακτικά μέλη της Συγκλήτου σε περίπτωση απουσίας ή κωλύματος να ενημερώσουν τα αναπληρωματικά τους.

Ο Πρύτανης του Ιονίου Πανεπιστημίου



Καθηγητής Ανδρέας Φλώρος

Εσωτερική Διανομή:

- Γραφείο Πρύτανη Ι.Π.,
- Αντιπρυτάνεις Ι.Π.,
- Γραμματείες όλων των Ακαδημαϊκών Τμημάτων του Ι.Π.,
- Συντονιστή Υπηρεσιών Ι.Π.,
- Νομική Υπηρεσία Ι.Π.,
- Όλες τις Διευθύνσεις και τα αυτοτελή Γραφεία και Τμήματα Ι.Π.,
- Γραμματεία Συγκλήτου & Πρυτανικού Συμβουλίου Ι.Π.

Λαμβάνοντας ένα ηλεκτρονικό κείμενο ο παραλήπτης θέλει:

1. Να είναι σίγουρος για την αυθεντικότητα του αποστολέα ή του υπογράφοντος (**αυθεντικότητα**)
2. Να είναι βέβαιος ότι το περιεχόμενο του εγγράφου δεν έχει τροποποιηθεί κατά την μετάδοσή του (**ακεραιότητα**)
3. Να είναι σίγουρος ότι το έγγραφο δεν έχει αποκαλυφθεί και σε άτομα που δεν είναι εξουσιοδοτημένα (**εμπιστευτικότητα**)
4. Να είναι σίγουρος ότι ο αποστολέας δεν θα αρνηθεί ότι το έχει στείλει αυτός (**μη αποποίηση ευθύνης**)

Τι γίνεται στον πραγματικό κόσμο;

- Συστημένη αποστολή εγγράφου:
 - Κατά την αποστολή ο υπάλληλος του ταχυδρομείου απαιτεί ένα έγγραφο για να αυθεντικοποιήσει τον αποστολέα (όχι τον υπογράφοντα): **αυθεντικοποίηση, μερική μη αποποίηση ευθύνης**
 - Κατά την αποστολή απαιτείται ο αποστολέας να εισάγει το έγγραφο σε ένα φάκελο ο οποίος σφραγίζεται μπροστά του: **ακεραιότητα - εμπιστευτικότητα**
 - Κατά την παράδοση ο υπάλληλος του ταχυδρομείου παραδίδει σε σφραγισμένο φάκελο το έγγραφο στον παραλήπτη, μόνο με την επίδειξη εγγράφου το οποίο πιστοποιεί την ταυτότητα του παραλήπτη: **ακεραιότητα, αυθεντικοποίηση, εμπιστευτικότητα**
- Ζητήματα:
 - Δεν είμαστε σίγουροι ότι υπογράφων έχει λάβει γνώση
 - Δεν είμαστε σίγουροι για την ακεραιότητα της αποστολής
 - Δεν είμαστε σίγουροι για την εμπιστευτικότητα
 - Δεν είμαστε σίγουροι ότι ο υπογράφων δεν θα αποποιηθεί το έγγραφο

Βοηθάει η ψηφιακή υπογραφή;

Ψηφιακή υπογραφή και κρυπτογραφία:

- Οι ψηφιακές υπογραφές χρησιμοποιούν την **κρυπτογραφία δημοσίου κλειδιού**. Η διαφοροποίηση από την κρυπτογράφηση, έγκειται στο ότι για τη δημιουργία της ψηφιακής υπογραφής **ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα**.

Κατακερματισμός

- Μια συνάρτηση κατακερματισμού (hashing function) δέχεται **σαν είσοδο** μια σειρά από δεδομένα (bits) **μεταβλητού μήκους** και παράγει **σαν έξοδο** μια σειρά από δεδομένα (bits) **σταθερού μήκους** το οποίο ονομάζεται και σύνοψη μηνύματος (hash)
- Άρα η συνάρτηση κατακερματισμού παράγει **μια έξοδο σταθερού μεγέθους** (μήκους) (πχ 64 bits) **ανεξάρτητα με το μέγεθος** (μήκος) **της εισόδου**:
 - Είσοδος μήκους 2.000bits -> έξοδος μήκους 64bits
 - Είσοδος μήκους 10.000bits -> έξοδος μήκους 64bits
 - Είσοδος μήκους 180.00bits -> έξοδος μήκους 64bits

Ακεραιότητα και ψηφιακή υπογραφή

- Στη διαδικασία της δημιουργίας και επαλήθευσης της υπογραφής χρησιμοποιείται **μια συνάρτηση κατακερματισμού** (one way hash). Με την εφαρμογή της συνάρτησης κατακερματισμού, από ένα μήνυμα ανεξαρτήτου μεγέθους, παράγεται η «σύνοψή του», η οποία είναι μία σειρά από bits συγκεκριμένου μεγέθους (π.χ. 128 ή 160 bits). **Η σύνοψη του μηνύματος (fingerprint ή message digest) είναι μία ψηφιακή αναπαράσταση του μηνύματος και είναι μοναδική για το μήνυμα που αντιπροσωπεύει.**

Ακεραιότητα και ψηφιακή υπογραφή

- Η συνάρτηση κατακερματισμού είναι μονόδρομη διότι από την σύνοψη που δημιουργεί, **είναι υπολογιστικά αδύνατον κάποιος να εξάγει το αρχικό μήνυμα**. Η πιθανότητα δύο μηνύματα να έχουν την ίδια σύνοψη είναι εξαιρετικά μικρή σχεδόν μηδενική. Αυτό σημαίνει ότι **αν το μήνυμα του αποστολέα έχει κάποια συγκεκριμένη σύνοψη και το μήνυμα που λάβει ο παραλήπτης** (χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού) **παράγει διαφορετική σύνοψη**, τότε το μήνυμα κατά την μετάδοσή του **έχει αλλοιωθεί** (μη ακεραιότητα). Οποιαδήποτε αλλαγή σε ένα μήνυμα συνεπάγεται και τη δημιουργία διαφορετικής σύνοψης.
- Η ηλεκτρονική υπογραφή, στην ουσία είναι **η κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα σύνοψη**. Δηλαδή, η ψηφιακή υπογραφή (σε αντίθεση με την ιδιόχειρη υπογραφή) είναι διαφορετική για κάθε μήνυμα!

Αυθεντικότητα και ψηφιακή υπογραφή

- Θεωρώντας ότι ο αποστολέας έχει ένα συγκεκριμένο ζευγάρι κλειδιών και το ιδιωτικό του κλειδί είναι στην πλήρη κατοχή του, τότε το γεγονός ότι ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει το μήνυμα, **πιστοποιεί στον παραλήπτη που το αποκρυπτογραφεί με το αντίστοιχο δημόσιο κλειδί (του αποστολέα) την ταυτότητα του αποστολέα (αυθεντικότητα)**. Η ψηφιακή υπογραφή είναι ένας τρόπος αυθεντικοποίησης του αποστολέα του μηνύματος.
- Μία ψηφιακή υπογραφή μπορεί να πλαστογραφηθεί **εάν ο δικαιούχος του ιδιωτικού κλειδιού δεν το έχει υπό τον πλήρη έλεγχό του** (π.χ. χάσει το μέσο στο οποίο έχει αποθηκευτεί το ιδιωτικό κλειδί).

Πώς λειτουργεί η ψηφιακή υπογραφή;

Αποστολέας:

1. **Ο αποστολέας** χρησιμοποιώντας κάποιον αλγόριθμο κατακερματισμού (one way hash) **δημιουργεί τη σύνοψη** του μηνύματος (message digest) που θέλει να στείλει. Ανεξάρτητα από το μέγεθος του μηνύματος, αυτό που θα παραχθεί θα είναι μία συγκεκριμένου μήκους σειρά ψηφίων.
2. Με το ιδιωτικό του κλειδί, **ο αποστολέας κρυπτογραφεί τη σύνοψη**. Αυτό που **παράγεται είναι η ψηφιακή υπογραφή**. Η υπογραφή είναι ουσιαστικά μία σειρά ψηφίων συγκεκριμένου πλήθους.
3. Η κρυπτογραφημένη σύνοψη (**ψηφιακή υπογραφή**) **προσαρτάται στο κείμενο** και το μήνυμα με τη ψηφιακή υπογραφή μεταδίδονται μέσω του δικτύου. Εάν ο αποστολέας το επιθυμεί μπορεί να κρυπτογραφήσει το μήνυμά του με το δημόσιο κλειδί του παραλήπτη. Σε αυτήν την περίπτωση το μήνυμα είναι αναγνώσιμο μόνο με το ιδιωτικό κλειδί του παραλήπτη.

Πώς λειτουργεί η ψηφιακή υπογραφή;

Παραλήπτης

1. Ο παραλήπτης **αποσπά (κάνει κλικ) από το μήνυμα την ψηφιακή υπογραφή** (κρυπτογραφημένη, με το ιδιωτικό κλειδί του αποστολέα, σύνοψη).
2. Εφαρμόζοντας στο μήνυμα που έλαβε τον ίδιο αλγόριθμο κατακερματισμού, **ο παραλήπτης δημιουργεί (κάνοντας κλικ) τη σύνοψη του μηνύματος**.
3. Στη συνέχεια, αποκρυπτογραφεί **με το δημόσιο κλειδί του αποστολέα**, την κρυπτογραφημένη σύνοψη του μηνύματος (ψηφιακή υπογραφή).
4. **Συγκρίνονται οι δύο συνόψεις** και αν βρεθούν ίδιες, αυτό σημαίνει ότι το μήνυμα που έλαβε ο παραλήπτης είναι ακέραιο. Αν το μήνυμα έχει μεταβληθεί, η σύνοψη που θα παράγει ο παραλήπτης θα είναι διαφορετική από την σύνοψη που έχει κρυπτογραφηθεί.

Μη αποποίηση

Πώς επιτυγχάνεται η μη αποποίηση;

- Απαιτείται η ύπαρξη ενός μηχανισμού, ώστε ο παραλήπτης να μπορεί να είναι σίγουρος για την ταυτότητα του προσώπου με το δημόσιο κλειδί. Ο μηχανισμός αυτός θα πρέπει να υλοποιείται από μία οντότητα που εμπνέει εμπιστοσύνη και που **εγγυάται ότι σε ένα συγκεκριμένο πρόσωπο αντιστοιχεί το συγκεκριμένο δημόσιο κλειδί: Πάροχος Υπηρεσιών Πιστοποίησης.**
- Ο Πάροχος Υπηρεσιών Πιστοποίησης είναι η οντότητα που παρέχει την υπηρεσία (έκδοση πιστοποιητικού - ηλεκτρονικό αρχείο) εκείνη με την οποία πιστοποιείται η σχέση ενός προσώπου με το δημόσιο κλειδί του.

Μητρώο Υπηρεσιών Πιστοποίησης (ΠΥΠ) Παρόχων

Για να γίνει κάποιος
ΠΥΠ πρέπει να
πληροί συγκεκριμένα
κριτήρια

Επωνυμία	Αριθμός Μητρώου ΕΕΤΤ	Ημερομηνία Καταχώρισης	Παροχή εγκεκριμένων υπηρεσιών εμπιστοσύνης	Ιστοσελίδα
ΑΝΤΑΚΟΜ-ΠΡΟΗΓΜΕΝΕΣ ΕΦΑΡΜΟΓΕΣ ΔΙΑΔΙΚΤΥΟΥ ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ	02-902	1/10/2002	ΝΑΙ (https://webgate.ec.europa.eu/ti-browser/#/trustmark/EL/VATEL-099554476)	www.adacom.com
ΕΛΛΗΝΙΚΑ ΧΡΗΜΑΤΙΣΤΗΡΙΑ- ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ ΣΥΜΜΕΤΟΧΩΝ	10-164	17/3/2006	ΝΑΙ (https://webgate.ec.europa.eu/ti-browser/#/trustmark/EL/VATEL-099755108)	https://www.athexgroup.gr/el/web/guest/digital-certificates
ΑΡΧΗ ΠΙΣΤΟΠΟΙΗΣΗΣ ΕΛΛΗΝΙΚΟΥ ΔΗΜΟΣΙΟΥ	07-901	20/6/2007	ΝΑΙ (https://webgate.ec.europa.eu/ti-browser/#/trustmark/EL/Hellenic Public Administration Certification Services)	http://www.aped.gov.gr
BYTE COMPUTER A.B.E.E.	15-062	29/10/2014	ΝΑΙ (https://webgate.ec.europa.eu/ti-browser/#/trustmark/EL/VATEL-094265075)	www.byte.gr
ΑΚΑΔΗΜΑΪΚΟ ΔΙΑΔΙΚΤΥΟ	91-222	3/6/2015	ΝΑΙ (https://webgate.ec.europa.eu/ti-browser/#/trustmark/EL/VATEL-099028220)	https://www.gunet.gr/el/ https://harica.gr/
EDPS ΕΠΕΞΕΡΓΑΣΙΑ ΠΛΗΡΟΦΟΡΙΩΝ ΤΗΛΕΜΑΤΙΚΗΣ ΑΕ	10-166	18/3/2005		https://edps.gr
ΕΛΛΗΝΙΚΟ ΑΝΟΙΚΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ	10-167	15/4/2009		https://www.eap.gr/el/
ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΑΕ	10-010	18/1/2010		www.ktpae.gr
ΡΙΤΕΙΛ – LINK ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ ΥΠΗΡΕΣΙΩΝ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ	13-056	2/5/2013		www.retail-link.gr
SINGULAR LOGIC ΑΕ	13-063	2/12/2013		https://portal.singularlogic.eu/
INFORMATION SYSTEMS IMPACT ΑΕ	14-022	24/1/2014		https://www.impact.gr
ΕΛΜΗΣΥΣΤΕΜΣ ΕΛΛΗΝΙΚΑ ΜΗΧΑΝΟΓΡΑΦΙΚΑ ΣΥΣΤΗΜΑΤΑ ΑΕ	14-156	14/10/2014		https://elmisystems.gr/
INTELLI SOLUTIONS ΑΕ	18-052	30/5/2018		https://intelli-corp.com/

Πλαίσιο Ψηφιακών Πιστοποιητικών / Υπογραφών

- Κανονισμός **EETT 248/2002**
(τροποποιήθηκε με την 775/2016)
- **Ευρωπαϊκός Κανονισμός 910/2014**
σχετικά με την ηλεκτρονική ταυτοποίηση
και τις υπηρεσίες εμπιστοσύνης για τις
ηλεκτρονικές συναλλαγές
- Κανονισμός **EETT 837/2017** σχετικά με την
παροχή υπηρεσιών εμπιστοσύνης

Ευρωπαϊκός Κανονισμός 910/2014 (eIDAS - electronic Identification and Trust Services)

- Αποσκοπεί στην επίτευξη **ενός επαρκούς επιπέδου ασφάλειας** στα μέσα ηλεκτρονικής ταυτοποίησης και στις υπηρεσίες εμπιστοσύνης:
 - **“επιβάλλει” αναγνώριση** μέσω ηλεκτρονικής ταυτοποίησης μεταξύ κρατών μελών
 - **θεσπίζει κανόνες για τις ηλεκτρονικές υπηρεσίες εμπιστοσύνης** (δημιουργία, επικύρωση, διαφύλαξη ηλεκτρονικών εγγράφων/υπογραφών κλπ) ιδίως για ηλεκτρονικές συναλλαγές
 - **θεσπίζει πλαίσιο για τις ηλεκτρονικές υπογραφές / σφραγίδες / χρονοσφραγίδες, ηλεκτρονικά έγγραφα, ηλεκτρονικές υπηρεσίες συστημένης παράδοσης και για υπηρεσίες πιστοποιητικών για ιστότοπους.**

3 τύπους ηλεκτρονικών υπογραφών

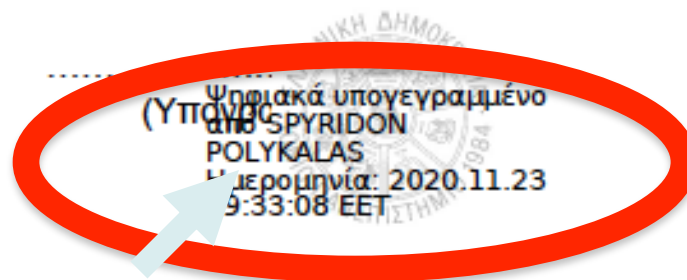
- **Ηλεκτρονική υπογραφή:** δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα και χρησιμοποιούνται για ηλεκτρονική υπογραφή
- **Προηγμένη ηλεκτρονική υπογραφή:** ηλεκτρονική υπογραφή η οποία συνδέεται κατά μοναδικό τρόπο με τον υπογράφοντα, ταυτοποιεί τον υπογράφοντα, χρησιμοποιείται κατά αποκλειστικό τρόπο από τον υπογράφοντα (με υψηλό βαθμό εμπιστοσύνης) και συνδέεται με δεδομένα για τα οποία μπορεί να ανιχνευθεί οποιαδήποτε τροποποίηση αυτών
- **Εγκεκριμένη ηλεκτρονική υπογραφή:** προηγμένη ηλεκτρονική υπογραφή η οποία δημιουργείται από εγκεκριμένη διάταξη και βασίζεται σε εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής
- **Η εγκεκριμένη ηλεκτρονική υπογραφή έχει την ίδια νομική ισχύ με την ιδιόχειρη υπογραφή**

Ψηφιακή Υπογραφή;

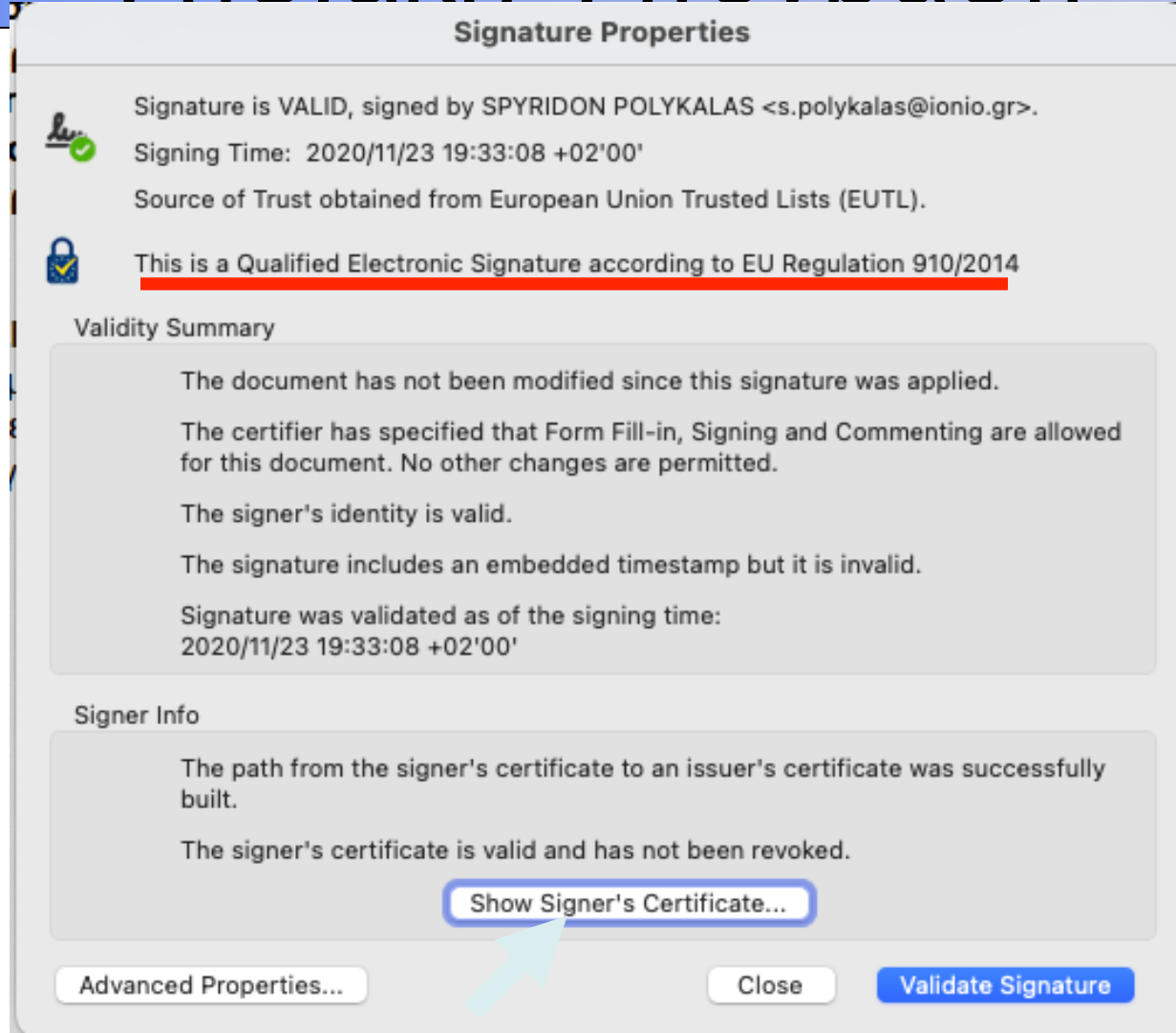
και συνδέεται με το Πακέτο Εργασίας «ΕΕ2 ΚΑΤΑΓΡΑΦΗ & ΑΝΑΛΥΣΗ ΛΕΙΤΟΥΡΓΙΚΩΝ ΠΡΟΔΙΑΓΡΑΦΩΝ», σύμφωνα με τις συμβατικές υποχρεώσεις του συμβαλλόμενου προς την Επιτροπή Ερευνών και σύμφωνα με τις υποχρεώσεις που απορρέουν από το Τεχνικό Δελτίο του έργου.

Ο Επιστημονικά Υπεύθυνος

.....
(ΥΠΟΝΥΣ)
Ψηφιακά υπογεγραμμένο
από SPYRIDON
POLYKALAS
Ημερομηνία: 2020.11.23
9:33:08 EET



Ψηφιακή Υπογραφή



Ψηφιακή Υπογραφή

Certificate Viewer

This dialog allows you to view the details of a certificate and its entire issuance chain. The details correspond to the selected entry.

☐ Show all certification paths found

Ionian University Client

SPYRIDON POLYKA

Summary

Details

Revocation

Trust

Policies

Legal Notice



SPYRIDON POLYKALAS <s.polykalas@ionio.gr>
Class A - Private Key created and stored in hardware

Issued by:

Ionian University Client CA R1
Ionian University

Valid from:

2019/06/28 08:57:47 +02'00'

Valid to:

2021/06/27 08:57:47 +02'00'

Intended usage:

Digital Signature, Non-Repudiation, Client Authentication, Email Protection, Document Signing,
1 3 6 1 4 1 3 11 30 2 2



This certificate is Qualified according to EU Regulation 910/2014 Annex I
The private key related to this certificate resides in a Qualified Signature Creation Device (QSCD)

Export...

 The selected certificate path is valid.

Γενικές Πληροφορίες

- Νέα / Ανακοινώσεις
- Διαβουλεύσεις
- Προδικαστικές Προσφυγές
- Ετήσια Στατιστικά Στοιχεία
- Αρχείο Ειδών - Κωδικολόγιο CPV
- Μητρώο Ενσώτων Τεχνικών Προδιαγραφών
- Κέντρο Αριστείας για τις Δημόσιες Συμβάσεις Καινοτομίας
- Χρήσιμοι Σύνδεσμοι
- Διαγωνισμοί Φορέων Εξωτερικού

Εθνικό Σύστημα Ηλεκτρονικών Δημοσίων Συμβάσεων (ΕΣΗΔΗΣ) - Προμήθειες και Υπηρεσίες

- Ηλεκτρονικοί Διαγωνισμοί
- Δυναμικό Σύστημα Αγορών
- Ανταγωνιστικός Διάλογος & Ανταγωνιστική Διαδικασία με Διαπραγμάτευση
- Οικονομικοί Φορείς (εγγραφή, πληροφορίες κ.α.) - Supplier's registration & Information
- Αναθέτουσες Αρχές (εγγραφή χρηστών, πληροφορίες κ.α.)
- Ενιαίο Πρόγρ. Προμηθειών Φορέων Υγείας
- Εισοδος Χρηστών ΕΣΗΔΗΣ
- Εγχειρίδια Χρήσης
- e-Learning
- Στατιστικά Στοιχεία Προμηθειών &

Οπτικοποίηση δεδομένων (data visualization)
Ηλεκτρονικών Διαγωνισμών ΕΣΗΔΗΣ
(Προμηθειών, Υπηρεσιών και Δημοσίων Έργων) και
Συμβάσεων ΚΗΜΔΗΣ



ΑΝΑΚΟΙΝΩΣΗ

Υποστήριξη των χρηστών του ΕΣΗΔΗΣ Προμήθειες και Υπηρεσίες, του ΚΗΜΔΗΣ και του Promitheus ESPDint, κατά το διάστημα ισχύος των έκτακτων μέτρων αντιμετώπισης του κινδύνου διασποράς του κορωνοϊού COVID -19.

Λεπτομέρειες ανακοίνωσης (pdf)

ΠΙΣΤΟΠΟΙΗΣΗ ΤΕΧΝΙΚΗΣ ΔΥΣΛΕΙΤΟΥΡΓΙΑΣ ΤΟΥ ΥΠΟΣΥΣΤΗΜΑΤΟΣ ΕΣΗΔΗΣ ΔΗΜΟΣΙΑ ΕΡΓΑ

Σας πληροφορούμε ότι διαπιστώθηκε τεχνική δυσλειτουργία του υποσυστήματος ΕΣΗΔΗΣ Δημόσια Έργα σήμερα Παρασκευή 23/10/2020 και από 14:45.

Λεπτομέρειες ανακοίνωσης (pdf)

ΣΥΜΦΩΝΙΕΣ - ΠΛΑΙΣΙΟ ΕΤΟΥΣ 2020

Σας γνωρίζουμε ότι δημοσιεύθηκε στην Εφημερίδα της Κυβερνήσεως η απόφαση με αρ. πρωτ.: 88408/24-8-2020, ΦΕΚ Β' 3810/09-09-2020 με θέμα: «Συμφωνίες - πλαίσιο έτους 2020 που συνάπτονται από την Εθνική Κεντρική Αρχή Αγορών της παρ. 1β) του άρθρου 41 του ν. 4412/2016»

ΦΕΚ Β' 3810/09/09/2020

ΣΗΜΑΝΤΙΚΗ ΕΝΗΜΕΡΩΣΗ

Η υποβολή
προσφορών για
δημόσια έργα
γίνεται
αποκλειστικά μέσω
της πύλης
[eprocurements.gov](http://eprocurements.gov.gr)
[.gr](http://eprocurements.gov.gr) αποκλειστικά
με την χρήση
ψηφιακής
υπογραφής

 Signed and all signatures are valid.

Signature Panel

Πιστοποίηση ολοκλήρωσης ατομικού παραδοτέου
Κωδικός Σύμβασης: 22592

Βεβαιώνεται ότι:

Ο συμβαλλόμενος ΠΟΛΥΚΑΛΑΣ ΣΠΥΡΙΔΩΝ ολοκλήρωσε την εργασία **Συμμετοχή στην Ενότητα Εργασίας ΕΕ2** η οποία αποτελεί μέρος των παραδοτέων:

«Π2.1 Διαδικασίες Ποιοτικού Ελέγχου, Π2.2: Τεύχος λειτουργικών απαιτήσεων» του έργου με κωδικό «80384» και τίτλο «Ανάπτυξη του συστήματος "PharmaTron" μέσω του οποίου οι Ασθενείς/Πολίτες θα ενημερώνονται για το πλησιέστερο φαρμακείο που μπορεί να εκτελέσει την συνταγή τους (που έχει καταχωρηθεί στην Ηλεκτρονική Συνταγογράφηση <https://www.e-prescription.gr> της Γενικής Γραμματείας Κοινωνικών Ασφαλίσεων) και προαιρετικά να παραδώσει τα φάρμακα στο χώρο του ασθενή»

και συνδέεται με το Πακέτο Εργασίας «ΕΕ2 ΚΑΤΑΓΡΑΦΗ & ΑΝΑΛΥΣΗ ΛΕΙΤΟΥΡΓΙΚΩΝ ΠΡΟΔΙΑΓΡΑΦΩΝ», σύμφωνα με τις συμβατικές υποχρεώσεις του συμβαλλόμενου προς την Επιτροπή Ερευνών και σύμφωνα με τις υποχρεώσεις που απορρέουν από το Τεχνικό Δελτίο του έργου.

Ο Επιστημονικά Υπεύθυνος

Ψηφιακά υπογεγραμμένο
(Υπογραφή)
ΠΟΛΥΚΑΛΑΣ
Ημερομηνία: 2020.11.22
22:27:49 EET

- Έχω ένα έγκυρο, ψηφιακά υπογεγραμμένο, κείμενο: Signed and all signatures are valid

♦ Κάνω μια αλλαγή (έστω και ασήμαντη όπως για παράδειγμα να κάνω highlight μια φράση)

Πιστοποίηση ολοκλήρωσης ατομικού παραδοτέου
Κωδικός Σύμβασης: 22592

Βεβαιώνεται ότι:

Ο συμβαλλόμενος ΠΟΛΥΚΑΛΑΣ ΣΠΥΡΙΔΩΝ ολοκλήρωσε την εργασία Συμμετοχή στην Ενότητα Εργασίας ΕΕ2 η οποία αποτελεί μέρος των παραδοτέων:

«Π2.1 Διαδικασίες Ποιοτικού Ελέγχου, Π2.2: Τεύχος λειτουργικών απαιτήσεων» του έργου με κωδικό «80384» και τίτλο «Ανάπτυξη του συστήματος “PharmaTron” μέσω του οποίου οι Ασθενείς/Πολίτες θα ενημερώνονται για το πλησιέστερο φαρμακείο που μπορεί να εκτελέσει την συνταγή τους (που έχει καταχωρηθεί στην Ηλεκτρονική Συνταγογράφηση <https://www.e-prescription.gr> της Γενικής Γραμματείας Κοινωνικών Ασφαλίσεων) και προαιρετικά να παραδώσει τα φάρμακα στο χώρο του ασθενή»

και συνδέεται με το Πακέτο Εργασίας «ΕΕ2 ΚΑΤΑΓΡΑΦΗ & ΑΝΑΛΥΣΗ ΛΕΙΤΟΥΡΓΙΚΩΝ ΠΡΟΔΙΑΓΡΑΦΩΝ», σύμφωνα με τις συμβατικές υποχρεώσεις του συμβαλλόμενου προς την Επιτροπή Ερευνών και σύμφωνα με τις υποχρεώσεις που απορρέουν από το Τεχνικό Δελτίο του έργου.

Ο Επιστημονικά Υπεύθυνος

Ψηφιακά υπογεγραμμένο
(Υπογραφή)
ΠΟΛΥΚΑΛΑΣ ΣΠΥΡΙΔΩΝ
Ημερομηνία: 2020.11.22
22:27:49 EET

- Στο έγγραφο αμέσως εμφανίζεται μήνυμα το οποίο μας ενημερώνει ότι θα πρέπει εκ νέου να υπογραφεί

“At least one signature requires validating”

Εάν κάνω αποθήκευση τότε...

Πιστοποίηση ολοκλήρωσης ατομικού παραδοτέου
Κωδικός Σύμβασης: 22592

Βεβαιώνεται ότι:



και συνδέεται με το Εγχείρημα «ΕΡΕΥΝΑ ΚΑΙ ΑΝΑΛΥΣΗ
ΛΕΙΤΟΥΡΓΙΚΩΝ ΠΡΟΔΙΑΓΡΑΦΩΝ»,
σύμφωνα με τις συμβατικές υποχρεώσεις του συμβαλλόμενου προς την Επιτροπή
Ερευνών και σύμφωνα με τις υποχρεώσεις που απορρέουν από το Τεχνικό Δελτίο του
έργου.

Ο Επιστημονικά Υπεύθυνος

Υπογραφή υπογεγραμμένο
(Υπογραφή)
SPYRIDON
POLYKALAS
Ημερομηνία: 2020.11.22
22:27:49 EET

- Signed and all signatures are valid, but with unsigned changes after the last signatures

The revision of the document that was covered by this signatures has not been altered; however, there have been subsequent changes to the document

Ψευδονυμοποίηση & Ανωνυμοποίηση

Ψευδονυμοποίηση και Ανωνυμοποίηση

- **Ψευδονυμοποίηση (Pseudonymization):** είναι η επεξεργασία προσωπικών δεδομένων με τέτοιο τρόπο ώστε **από αυτά να μην είναι δυνατόν να προσδιορισθεί ένα πρόσωπο χωρίς την χρήση επιπρόσθετων δεδομένων,**
- τα επιπρόσθετα δεδομένα είναι αποθηκευμένα σε ξεχωριστό μέσο και η πρόσβαση σε αυτά υπόκειται σε **τεχνικούς και οργανωτικούς περιορισμούς** προκειμένου να διασφαλίσουν ότι τα προσωπικά δεδομένα δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο

Ψευδονυμοποίηση

- Ορισμένα **στοιχεία προσδιορίζουν μοναδικά κάποια εγγραφή** και επομένως είναι ανεξάρτητα του μεγέθους / πλήθους των δεδομένων και **επομένως δεν μπορούμε σε καμία περίπτωση** να τα συμπεριλάβουμε σε “ψευδονυμοποιημένα” υποτίθεται δημόσια στοιχεία. Ενδεικτικά:
 - Αριθμός δελτίου ταυτότητας
 - Αριθμός διαβατηρίου
 - Αριθμός Μητρώου Κοινωνικής Ασφάλισης (ΑΚΜΑ)
- **Ο καθορισμός των στοιχείων** τα οποία προσδιορίζουν μοναδικά (με άμεσο ή έμμεσο τρόπο) κάποια εγγραφή (στην περίπτωσή μας κάποιο φυσικό πρόσωπο) εξαρτάται **τόσο από το στοιχείο** (την μοναδικότητά του) **όσο και από το μέγεθος (πλήθος) των δεδομένων που έχουμε**
- Εάν θα έπρεπε να ψευδονυμοποιήσουμε το σύνολο των μελών ΔΕΠ των ελληνικών πανεπιστημίων (ο αριθμός μελών ΔΕΠ των ελληνικών πανεπιστημίων είναι μερικές χιλιάδες) τότε **η βαθμίδα από μόνης της** δεν θα αποτελούσε στοιχείο με το οποίο θα μπορούσαμε να προσδιορίσουμε ένα φυσικό πρόσωπο **(σε συνδυασμό όμως με άλλα στοιχεία ενδεχομένως να αποτελούσε)**

Ανωνυμοποίηση

- **Ανωνυμοποίηση (Anonymisation):** είναι η επεξεργασία προσωπικών δεδομένων με τέτοιο τρόπο ώστε **το υποκείμενο των δεδομένων να μην μπορεί να ταυτοποιηθεί με οποιοδήποτε τρόπο είτε άμεσα είτε εμμέσως από τον κάτοχο των δεδομένων (με ή χωρίς την συνεργασία τρίτου μέρους)**

Επιλογή στοιχείων για απαλοιφή

- Ποια στοιχεία πρέπει να επιλέξουμε από ένα σετ δεδομένων για να πετύχουμε ψευδονυμοποίηση / ανωνυμοποίηση;

General Data Protection Regulation

Κανονισμός 679 / 2016

- Ο Κανονισμός (Regulation) 679/2016 ψηφίσθηκε στις 16-04-2016 από το ΕΚ και αφορά: την προστασία φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία αυτών
- Έχει άμεση ισχύ σε όλα τα ΚΜ της ΕΕ
- Καταργεί την Οδηγία 1995/46
- Είναι συμπληρωματικός στην Οδηγία 2002/58

ΣΚΟΠΟΣ

- Σκοπός: θέσπιση κανόνων για την προστασία των προσωπικών δεδομένων φυσικών προσώπων αναφορικά με την **συλλογή, επεξεργασία και διακίνηση αυτών**.
- Ο κανονισμός εφαρμόζεται ανεξάρτητα εάν η επεξεργασία των δεδομένων γίνεται εντός ή εκτός της ΕΕ.
- Ο κανονισμός εφαρμόζεται για τα δεδομένα που **συλλέγονται στα πλαίσια παροχής υπηρεσιών ή/και αγαθών** ανεξάρτητα εάν αυτές οι υπηρεσίες / αγαθά παρέχονται έναντι αμοιβής ή όχι.
- Προσωπικά δεδομένα (δεδομένα προσωπικού χαρακτήρα): κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. **Ταυτοποιήσιμο φυσικό πρόσωπο είναι το πρόσωπο του οποίου η ταυτότητα μπορεί να εξακριβωθεί άμεσα ή έμμεσα μέσω αναφοράς σε στοιχείο ταυτότητας όπως όνομα, δεδομένα θέσης κλπ.**

Ορισμοί

- **Ψευδονυμοποίηση (pseudonymisation):** η επεξεργασία προσωπικών δεδομένων με τέτοιο τρόπο ώστε τα δεδομένα να μην μπορούν να αποδοθούν σε συγκεκριμένο πρόσωπο.
- **Παραβίαση δεδομένων προσωπικού χαρακτήρα:** η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα.

Αρχές επεξεργασίας δεδομένων προσωπικού χαρακτήρα

- Νομίμως και διαφανώς
- **Συλλογή για συγκεκριμένο σκοπό και δεν θα πρέπει να επεκτείνεται η επεξεργασία τους για λόγους οι οποίοι δεν συμβαδίζουν με τους σκοπούς που συλλέχθηκαν**
- Ακριβή και να είναι επικαιροποιημένα
- Διατηρούνται σε τέτοια μορφή που επιτρέπουν την ταυτοποίηση των υποκειμένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας. Εάν αποθηκεύονται για μεγαλύτερο διάστημα να αποθηκεύονται σε τέτοια μορφή όπου **μετά από ένα διάστημα δεν θα είναι δυνατή η ταυτοποίηση του φυσικού προσώπου**
- Μία νόμιμη επεξεργασία θα προϋποθέτει μεταξύ άλλων το φυσικό πρόσωπο να έχει δώσει εκ των προτέρων την συγκατάθεσή του για την επεξεργασία των προσωπικών του δεδομένων

Νομιμότητα επεξεργασίας

- Η επεξεργασία είναι **σύννομη μόνο εάν ισχύει** ένα από τα ακόλουθα:
 - το υποκείμενο των δεδομένων **έχει συναινέσει** στην επεξεργασία αυτών για έναν ή περισσότερους σκοπούς
 - η επεξεργασία **είναι απαραίτητη** για την εκτέλεση σύμβασης με συμβαλλόμενο το υποκείμενο των δεδομένων
 - **έννομη υποχρέωση** του υπευθύνου της επεξεργασίας
 - είναι απαραίτητη **για την διαφύλαξη ζωτικού συμφέροντος** του υποκειμένου των δεδομένων

Συγκατάθεση φυσικού προσώπου

- Ο υπεύθυνος επεξεργασίας των προσωπικών δεδομένων θα πρέπει να είναι σε θέση **να αποδείξει ότι το φυσικό πρόσωπο** έχει δώσει την συγκατάθεσή του για την συλλογή των προσωπικών του δεδομένων.
- Εάν η συγκατάθεση έχει γίνει στα πλαίσια μια έγγραφης συμφωνίας **η οποία αφορά και άλλα θέματα**, η συγκατάθεση για την επεξεργασία των προσωπικών δεδομένων θα πρέπει να είναι **διακριτή, κατανοητή, εύκολα προσβάσιμη και η διατύπωση να είναι σαφής και απλή.**
- Κατά την εκτίμηση κατά πόσο η συγκατάθεση έχει γίνει ελεύθερα θα πρέπει να λαμβάνεται υπόψη κατά πόσο η παροχή των προσωπικών δεδομένων **τα οποία δεν είναι απαραίτητα για την παροχή των υπηρεσιών έχουν τεθεί ως προϋπόθεση για την παροχή της υπηρεσίας.**
- Εάν ο χρήστης των υπηρεσιών **είναι κάτω από 16 ετών τότε για την συλλογή και επεξεργασία των προσωπικών δεδομένων απαιτείται η συγκατάθεση του ατόμου που έχει την κηδεμονία του παιδιού.**

Δικαιώματα φυσικού προσώπου

- Κάθε φυσικό πρόσωπο **έχει δικαίωμα να ζητήσει από τον κάτοχο των προσωπικών του δεδομένων:**
 - τον σκοπό της επεξεργασίας των δεδομένων,
 - τις κατηγορίες των προσωπικών δεδομένων που συλλέγονται
 - τυχόν τρίτους παραλήπτες των προσωπικών του δεδομένων
 - την περίοδο που θα είναι αποθηκευμένα τα προσωπικά του δεδομένα
 - την διαγραφή των προσωπικών του δεδομένων ή τον περιορισμό της επεξεργασίας τους
- Ο υπεύθυνος επεξεργασίας παρέχει αντίγραφο των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία.

Δικαίωμα διόρθωσης – διαγραφής (right to be forgotten)

- Κάθε φυσικό πρόσωπο έχει δικαίωμα να ζητήσει από τον κάτοχο των προσωπικών του δεδομένων **την διόρθωση ανακριβών δεδομένων** προσωπικού χαρακτήρα που το αφορούν
- Κάθε φυσικό πρόσωπο έχει δικαίωμα να ζητήσει **την διαγραφή προσωπικών δεδομένων** εάν ισχύει ένα από τα ακόλουθα:
 - τα δεδομένα δεν είναι απαραίτητα σε σχέση με τους σκοπούς που συλλέχθηκαν
 - το φυσικό πρόσωπο ανακαλεί την συγκατάθεση που είχε δώσει
 - τα δεδομένα υποβλήθηκαν σε επεξεργασία παράνομα
 - υπάρχει σχετική νομική υποχρέωση
- Φορητότητα προσωπικών δεδομένων: κάθε φυσικό πρόσωπο μπορεί να ζητήσει να λάβει τα δεδομένα που έχουν συλλεχθεί και μπορεί να τα μεταβιβάσει σε άλλον φορέα επεξεργασίας

Δικαίωμα εναντίωσης (right to object)

- Κάθε φυσικό πρόσωπο έχει δικαίωμα να ζητήσει από τον κάτοχο των προσωπικών του δεδομένων να σταματήσει την επεξεργασία τους και ο κάτοχος θα πρέπει να το κάνει εκτός και εάν υπάρχουν ειδικοί νόμιμοι λόγοι.
- Εάν τα προσωπικά δεδομένα επεξεργάζονται **για σκοπούς απευθείας εμπορικής διάθεσης προϊόντων** τότε το φυσικό πρόσωπο μπορεί να αντιταχθεί οποιαδήποτε στιγμή και ο κάτοχος θα πρέπει να σταματήσει την επεξεργασία τους άμεσα.

Προστασία προσωπικών δεδομένων

- Ο κάτοχος των προσωπικών δεδομένων λαμβάνει όλα εκείνα τα μέτρα, οργανωτικά και τεχνικά **για την προστασία των προσωπικών δεδομένων** όπως είναι η ψευδονυμοποίηση (pseudonymisation) και η κρυπτογράφηση.
- Ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει ότι, εξ ορισμού, υφίστανται επεξεργασία **μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας**. Τα εν λόγω μέτρα διασφαλίζουν ότι, εξ ορισμού, τα δεδομένα προσωπικού χαρακτήρα δεν καθίστανται προσβάσιμα χωρίς την παρέμβαση του φυσικού προσώπου σε αόριστο αριθμό φυσικών προσώπων.
- **Εάν υπάρξει παραβίαση** των προσωπικών δεδομένων ο υπεύθυνος επεξεργασίας ενημερώνει **την εποπτική αρχή** αλλά και το **φυσικό πρόσωπο** στην περίπτωση όπου η παραβίαση μπορεί να θέσει σε κίνδυνο τα δικαιώματα και προσωπικές ελευθερίες του φυσικού προσώπου.
- Μεταβιβάσεις προσωπικών δεδομένων σε τρίτες χώρες εκτός ΕΕ είναι δυνατή μόνο εάν οι τρίτες χώρες συμπεριλαμβάνονται σε σχετικό κατάλογο της ΕΕ.

Μηχανές αναζήτησης και προστασία προσωπικών δεδομένων

- Εάν κάποιος πολίτης θεωρεί ότι οι μηχανές αναζήτησης εμφανίζουν στα αποτελέσματα της αναζήτησης για το ονοματεπώνυμό του, συνδέσμους των οποίων το περιεχόμενο σχετίζεται με την προστασία των προσωπικών του δεδομένων τότε μπορεί να κάνει αίτηση στον διαχειριστή των μηχανών αναζήτησης (πχ Google) για να εξετάσει το εν λόγω αίτημα.
- Εάν ο διαχειριστής των μηχανών αναζήτησης (πχ Google) εξετάσει το αίτημα και αποφανθεί ότι δεν πρέπει να διαγράψει τους σχετικούς συνδέσμους ή αρνηθεί να εξετάσει το αίτημα, τότε ο πολίτης μπορεί να απευθυνθεί στις αρμόδιες αρχές του Κράτους Μέλους (για την Ελλάδα είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα).

Κριτήρια

- Ο Κανονισμός περιέχει μία σειρά από κριτήρια τα οποία θα πρέπει να εξετάζονται από τον διαχειριστή των προσωπικών δεδομένων (πχ μία μηχανή αναζήτησης / Google) όταν κάποιος Ευρωπαίος πολίτης καταθέτει αίτημα.
- Τα εν λόγω κριτήρια σχετίζονται κυρίως με:
 - Την ακρίβεια των δεδομένων.
 - Τη σχετικότητα των δεδομένων.
 - Τον χρόνο που αναφέρονται τα δεδομένα (δηλαδή πόσος χρόνος έχει περάσει από τον χρόνο που αναφέρονται τα δεδομένα).
 - Τον ρόλο που διαδραματίζει ο αιτούμενος στο δημόσιο βίο.

Ανεξάρτητο έδρας...

- Εφαρμογή και σε εταιρίες εκτός ΕΕ: η εφαρμογή της αρχής του Δικαιώματος της Λήθης δεν πρέπει να σχετίζεται με την έδρα της εταιρίας που παρέχει τις σχετικές υπηρεσίες αναζήτησης. Με το νέο Κανονισμό οι σχετικές πληροφορίες θα πρέπει να διαγράφονται όχι μόνο από την μηχανή αναζήτησης στο σχετικό Κράτος Μέλος (πχ. www.google.gr ή www.google.com.uk) αλλά και από τις βάσεις δεδομένων της βασικής μηχανής αναζήτησης (πχ. www.google.com) προκειμένου στις περιπτώσεις όπου κριθεί η διαγραφή δεδομένων με βάση την αρχή του Δικαιώματος στη Λήθη αυτό να γίνει από όλες τις σχετικές βάσεις δεδομένων.
- Το βάρος της απόδειξης ότι τα αιτούμενα δεδομένα δεν μπορούν να διαγραφούν διότι είναι απαραίτητα ακόμη ή είναι ακόμη σχετικά το έχει η εταιρία και όχι αυτός που έχει κάνει το σχετικό αίτημα.

Ενημέρωση τρίτων μερών – άμεση εφαρμογή

- Ο Κανονισμός επιβάλλει την υποχρέωση στο διαχειριστή των προσωπικών δεδομένων να πληροφορήσει τρίτα μέρη σχετικά με την επιθυμία του προσώπου να διαγραφούν τα προσωπικά δεδομένα. Επίσης ο διαχειριστής των προσωπικών δεδομένων είναι υποχρεωμένος να επιβεβαιώσει την διαγραφή των δεδομένων (διαγράφοντας οποιοδήποτε σύνδεσμο προς αυτά, η αναδημοσίευσή τους, ή αντιγραφή τους).
- Παράλληλα επιβάλλει στο διαχειριστή την υποχρέωση να συμμορφώνεται άμεσα με τις σχετικές Αποφάσεις των εθνικών δικαστηρίων ή των σχετικών Ρυθμιστικών Αρχών σχετικά με την διαγραφή των σχετικών προσωπικών δεδομένων.

Εφαρμογή Κανονισμού

Ο Κανονισμός τέθηκε σε εφαρμογή στις 25-05-2018

Ποινές

- Στο Κανονισμό προβλέπονται ποινές για τις περιπτώσεις όπου ο διαχειριστής των προσωπικών πληροφοριών δεν λαμβάνει υπόψη του τις διατάξεις του Κανονισμού.
- Ο αρμόδιος εθνικός φορέας ο οποίος είναι υπεύθυνος για την τήρηση των διατάξεων μπορεί να επιβάλει πρόστιμο έως 1 εκ. € ή έως το 2% των ετήσιων εσόδων στον διαχειριστή των προσωπικών πληροφοριών ο οποίος εσκεμμένα ή από αμέλεια δεν εφαρμόζει τις σχετικές διατάξεις περί προστασίας των προσωπικών δεδομένων.
- Σε επιχειρήσεις και για παραβάσεις που σχετίζονται με βασικές αρχές του Κανονισμού επιβάλλονται πρόστιμα που μπορούν να φθάσουν έως το 4% του παγκόσμιου τζίρου ή έως 20 εκ. €.

50M€ πρόστιμο στην Google

- Τον Ιανουάριο του 2019 η Γαλλική Αρχή για την Προστασία των Προσωπικών Δεδομένων (CNIL) επέβαλε πρόστιμο 50M€ στην Google για παραβίαση όσον αφορά την διαφάνεια, τις υποχρεώσεις πληροφόρησης και της ύπαρξης συναίνεσης αναφορικά με τις πρακτικές που ακολουθεί η Google στο προσωπική – στοχευμένη διαφήμιση.
- Ήταν η πρώτη Απόφαση ρυθμιστικής αρχής στην Ευρώπη η οποία επέβαλε πρόστιμο σε ένα παγκόσμιο παίκτη του Διαδικτύου βασιζόμενη στις προβλέψεις του GDPR.

Ιστορικό Απόφασης CNIL

- Τον Μάιο του 2018 δύο οργανισμοί καταναλωτών (εκπροσωπούσαν 10.000 καταναλωτές) έκαναν καταγγελία για παραβίαση των προβλέψεων του GDPR εφαρμόζοντας το άρθρο 80 του Κανονισμού (ο Κανονισμός προβλέπει τη δυνατότητα στα φυσικά πρόσωπα να εκπροσωπούνται από μη κερδοσκοπηκούς φορείς).
- Τον Ιούνιο του 2018 η CNIL κατέθεσε τα παράπονα στις αντίστοιχες ρυθμιστικές αρχές των άλλων ΚΜ. Ο GDPR προβλέπει ότι κάθε οργανισμός ο οποίος έχει έδρα στην ΕΕ θα εποπτεύεται από μια ρυθμιστική αρχή ενός ΚΜ της ΕΕ (one-stop-shop, European Single Market).
- Η Google έχει έδρα στην Ευρώπη στην Ιρλανδία αλλά η CNIL έκρινε ότι η έδρα στην Ιρλανδία δεν έχει διοικητικές εξουσίες (management power) και επομένως η CNIL έχει την αρμοδιότητα να χειριστεί την υπόθεση.
- Τον Σεπτέμβριο του 2018 η CNIL έκανε online έρευνα προκειμένου να διαπιστώσει κατά πόσο η επεξεργασία των προσωπικών δεδομένων που διενεργεί η Google είναι σε συμφωνία με τις προβλέψεις του GDPR.

Παραβάσεις Google (1)

- Η CNIL διαπίστωσε ότι η Google παραβιάζει δύο βασικές αρχές του GDPR:
 1. Έλλειψη διαφάνειας και πληροφόρησης
 2. Έλλειψη έγκυρης συναίνεσηςαναφορικά με την επεξεργασία των προσωπικών δεδομένων που χρησιμοποιούνται για σκοπούς προσωπικής διαφήμισης.
- Έλλειψη διαφάνειας και πληροφόρησης:
 - Η πληροφόρηση που παρέχει η Google **δεν είναι εύκολα προσβάσιμη** από τους χρήστες διότι ουσιώδης πληροφόρηση (όπως σκοπός επεξεργασίας, διάστημα που κρατούνται τα δεδομένα, κατηγορίες δεδομένων που κρατούνται) **είναι διασκορπισμένη σε διάφορα κείμενα** και απαιτούνται 5 ή έξι ενέργειες από τον χρήστη (ενεργοποίηση buttons και συνδέσμων) προκειμένου οι χρήστες να είναι πλήρως ενήμεροι.
 - Η πληροφόρηση που παρέχει η Google δεν είναι επαρκώς ακριβής και ολοκληρωμένη διότι **οι σκοποί** της επεξεργασίας περιγράφονται **με έναν γενικό και ασαφή τρόπο**.
 - Λείπει ουσιώδης πληροφορία η οποία είναι απαιτητή σύμφωνα με το άρθρο 13 του GDPR η οποία σχετίζεται **με την περίοδο που κρατούνται τα δεδομένα**.

Παραβάσεις Google (2)

- **Μή έγκυρη συναίνεση από τους χρήστες:**
 - ***Οι χρήστες δεν είναι επαρκώς ενημερωμένοι:***
 - Οι χρήστες δεν είναι επαρκώς ενημερωμένοι διότι η πληροφόρηση για την επεξεργασία είναι διασκορπισμένη σε διάφορα κείμενα το οποίο δεν επιτρέπει στον χρήστη να πληροφορηθεί με επάρκεια. Για παράδειγμα στην ενότητα "Personalization of ads" δεν είναι σαφές ποιες υπηρεσίες αφορά η επεξεργασία (google search, youtube, maps, home, playstore, photo) και επομένως η χρήστης δεν αντιλαμβάνεται τον όγκο της πληροφορίες που συλλέγεται και επεξεργάζεται.
 - ***Δεν είναι συγκεκριμένη και δεν υπάρχει σαφήνεια:***
 - Η συναίνεση των χρηστών δεν είναι συγκεκριμένη διότι κάνοντας κλικ το button «*I accept Google's terms of use*» και "*I agree that my information may be used as described above and as specified in the privacy policy*", και επιλέγοντας "*Create an account*", η χρήστης τα επιλέγει σαν ένα σύνολο.

Απόφαση CNIL

- Η συναίνεση των χρηστών δεν είναι ξεκάθαρη διότι η επιλογή για προσωποποιημένη διαφήμιση **είναι προ-επιλεγμένη** και δεν απαιτεί καμία ενέργεια από τον χρήστη όπως απαιτεί ο GDPR (opt in vs. opt out), όπως για παράδειγμα κάνοντας κλικ ένα button το οποίο δεν είναι εκ των προτέρων επιλεγμένο.

Ποινή CNIL

- Ο GDPR προβλέπει πρόστιμα έως 20M€ ή 4% επί του ταγκόσμιου τζίρου του πλέον πρόσφατου οικονομικού έτους.
- Η Google το 2017 είχε έσοδα περίπου 96 G€ (96 δισ. €) που σημαίνει ότι η CNIL θα μπορούσε να επιβάλει πρόστιμο της τάξης των 3,8 δισ. €.
Ωστόσο επιλέχθηκε να επιβληθεί πρόστιμο της τάξης των 50M€ (0,05% των εσόδων).
- Για τον προσδιορισμό του ύψους του προστίμου η CNIL έλαβε υπόψη της:
 - οι παραβιάσεις έρχονται σε αντίθεση με ουσιώδεις αρχές του GDPR
 - οι παραβιάσεις είναι συνεχόμενες
 - αφορούν ένα μεγάλο αριθμό χρηστών
 - το επιχειρηματικό μοντέλο της Google βασίζεται σε ένα μέρος στην στοχευμένη διαφήμιση και επομένως η Google θα πρέπει να λάβει σοβαρά υπόψη της τον GDPR όταν υλοποιεί πολιτικές στοχευμένης διαφήμισης.

ENISA

- Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (European Union Agency for Network and Information Security – ENISA) δημοσίευσε το 2012 μια αναλυτική έκθεση με την οποία προσπάθησε να αναλύσει τις τεχνικές λεπτομέρειες από την εφαρμογή του Δικαιώματος στη Λήθη.

Τεχνικές πτυχές Δικαιώματος στη Λήθη (1)

- Οι φορείς χάραξης πολιτικής και οι αρχές προστασίας δεδομένων προσωπικού χαρακτήρα θα πρέπει να συνεργαστούν ώστε να διευκρινίσουν ορισμούς που θα συμβάλλουν στην εφαρμογή του δικαιώματος:
 - ποιος δύναται να ζητήσει τη διαγραφή των κοινών προσωπικών δεδομένων;
 - υπό ποιες συνθήκες;
 - ποια είναι τα σχετικά κόστη;

Τεχνικές πτυχές Δικαιώματος στη Λήθη (2)

- Μια απολύτως τεχνική λύση για την υλοποίηση αυτού του δικαιώματος στο ανοιχτό Διαδίκτυο είναι αδύνατη. Γιατί;
 - Απαιτείται διατομεακή προσέγγιση και οι ιθύνοντες θα πρέπει να γνωρίζουν το γεγονός αυτό.
- Πιθανή λύση:
 - Απαίτηση από τους λειτουργούς των μηχανών αναζήτησης και των υπηρεσιών διάδοσης εντός της ΕΕ να φιλτράρουν αναφορές σε «λησμονηθείσες» πληροφορίες που έχουν αποθηκευτεί εντός και εκτός της περιφέρειας της ΕΕ.

Τεχνικές πτυχές Δικαιώματος στη Λήθη (3)

- Θα πρέπει να δοθεί ιδιαίτερη προσοχή στη διαγραφή δεδομένων προσωπικού χαρακτήρα που είναι αποθηκευμένα σε αποσυρμένες και εκτός σύνδεσης συσκευές αποθήκευσης.

Ενότητα III

- Πνευματική Ιδιοκτησία
 - Πνευματικά Δικαιώματα
 - Ψηφιακά πνευματικά δικαιώματα
 - Creative commons

Συνθήκη της ΕΕ

- Άρθρο 118 :

*«Στο πλαίσιο της εγκαθίδρυσης και της λειτουργίας της εσωτερικής αγοράς, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία, θεσπίζουν μέτρα για τη δημιουργία ευρωπαϊκών τίτλων, ώστε να εξασφαλισθεί **ενιαία προστασία των δικαιωμάτων διανοητικής ιδιοκτησίας στο εσωτερικό της Ένωσης**, και για τη δημιουργία κεντρικών καθεστώτων έγκρισης, συντονισμού και ελέγχου στο επίπεδο της Ένωσης.»*

Πνευματική Ιδιοκτησία

- Τι είναι η πνευματική ιδιοκτησία;
 - Το αποκλειστικό δικαίωμα των δημιουργών στα πνευματικά έργα
- Πνευματική ιδιοκτησία ή πνευματικά δικαιώματα υπάρχουν για όλα τα πνευματικά έργα. Ενδεικτικά: βιβλία, φωτογραφίες, αρχιτεκτονική, οπτικοακουστικά αρχεία, θεατρικά έργα, μουσικές συνθέσεις, λογισμικό κλπ.
- Ένα πνευματικό έργο εμπίπτει στο πεδίο της πνευματικής ιδιοκτησίας και μπορεί να προστατεύεται ανεξάρτητα από την πνευματική / καλλιτεχνική / επιστημονική αξία του.
- Δεν αποτελούν έργα τα οποία εμπίπτουν στο πεδίο της προστασίας της πνευματικής ιδιοκτησίας:
 - Μαθηματικοί τύποι, ειδήσεις, νόμοι / δικαστικές αποφάσεις, ιδέες (πχ η πλοκή σε ένα έργο) κ.α

Απόκτηση πνευματικής ιδιοκτησίας

- Η πνευματική ιδιοκτησία ενός έργου αποκτάται αυτόματα από τον δημιουργό από την στιγμή της δημιουργίας του.
- Για να υπάρξει όμως καλύτερη προστασία και να αποφευχθούν οι διαμάχες περί πατρότητας του έργου ο δημιουργός του έργου θα πρέπει να κατοχυρώσει την πατρότητα αυτού (πχ με μία συμβολαιογραφική πράξη).



Copyright

Ηθικό – Περιουσιακό - Συγγενικό

- Το δικαίωμα της πνευματικής ιδιοκτησίας μπορεί να διαχωρισθεί σε:
 - **Ηθικό δικαίωμα**: σχέση έργου με δημιουργό η οποία περιλαμβάνει την αναγνώριση της πατρότητας, την εξουσία δημοσίευσης, την εξουσία προέλευσης κλπ
 - **Περιουσιακό δικαίωμα**: υπάρχει η δυνατότητα οικονομικής εκμετάλλευσης του έργου μέσω της διανομής του, της αναπαραγωγής του, της δημιουργία παράγωγου, της δημόσιας εκτέλεσής του κλπ
- Τα **συγγενικά πνευματικά δικαιώματα** έχουν αυτοί που παρουσιάζουν ή επενδύουν ένα / σε ένα, πνευματικό έργο χωρία απαραίτητα να είναι οι δημιουργοί του: πχ ερμηνευτές ενός τραγουδιού, ραδιοτηλεοπτικοί οργανισμοί, οι εκδότες,

Διάρκεια – Εξαιρέσεις - Μεταβίβαση

- Η διάρκεια ενός πνευματικού δικαιώματος έχει καθορισθεί διεθνώς (ΕΕ & ΗΠΑ) στα 70 χρόνια από τον θάνατο του δημιουργού (μετά το θάνατο δικαιούχοι είναι οι κληρονόμοι) ή στα 50 για τα συγγενικά πνευματικά δικαιώματα.
- Δεν είναι απαραίτητο όλα τα πνευματικά έργα να έχουν και περιορισμούς στα πνευματικά δικαιώματα πχ ελεύθερο λογισμικό.
- Επίσης επιτρέπεται η παράθεση σύντομων αποσπασμάτων για κριτική, η αναπαραγωγή έργων για εκπαιδευτικούς σκοπούς κλπ.
- Ένας δημιουργός μπορεί να εκχωρήσει το περιουσιακό πνευματικό δικαίωμα εν όλο ή εν μέρει σε ένα τρίτο πρόσωπο για ένα χρονικό διάστημα. Το ηθικό πνευματικό δικαίωμα δεν εκχωρείται.

Διαδίκτυο και πνευματική ιδιοκτησία

- Η μεγάλη διείσδυση της πληροφορικής και των ηλεκτρονικών επικοινωνιών ανέδειξε με έντονο ρυθμό και τα πνευματικά δικαιώματα που σχετίζονται με τον ψηφιακό κόσμο του διαδικτύου και το περιεχόμενο των ψηφιακών αρχείων όπως: τραγούδια, ταινίες, ιστοσελίδες, λογισμικό, βάσεις δεδομένων κλπ.

Πολυσύνθετο πρόβλημα

- Τα ζητήματα της πνευματικής ιδιοκτησίας στο διαδίκτυο ή στην Κοινωνία της Πληροφορίας γενικότερα είναι ένα πολυσύνθετο πρόβλημα λόγω της φύσης του διαδικτύου.
- Από την μία πλευρά έχουμε:
 - το δικαίωμα στην ελεύθερη πληροφόρηση και στην συμμετοχή στην Κοινωνία της Πληροφορίας (συνταγματικό δικαίωμα).
 - τη δομή του διαδικτύου η οποία προάγει την ελευθερία στην έκφραση, την πρόσβαση στην Κοινωνία της Πληροφορίας, την συνεργατικότητα, την ουδετερότητα δικτύου, την καινοτομία, την ελευθερία λόγου.
- Από την άλλη:
 - Τα χαρακτηριστικά του ψηφιακού κόσμου διευκολύνουν την παράβαση των δικαιωμάτων της πνευματικής ιδιοκτησίας.

Ψηφιακά αρχεία

- Ευκολία στην αντιγραφή (παράνομη ή χωρίς να υπάρχει το σχετικό δικαίωμα) και διακίνηση έργων τα οποία εγείρουν ζητήματα πνευματικών δικαιωμάτων:
 - Κείμενο (αντιγραφή, διακίνηση)
 - Φωτογραφίες (ψηφιακή σάρωση, διακίνηση)
 - Μουσική («κατέβασμα», αποθήκευση, διακίνηση)
 - Ταινίες («κατέβασμα», προβολή, διακίνηση)
 - Προγράμματα – software («κατέβασμα», εγκατάσταση)
- Τη διακίνηση των ψηφιακών έργων διευκολύνουν ακόμη περισσότερο προγράμματα τα οποία επιτρέπουν την ισότιμη διακίνηση ψηφιακών αρχείων μεταξύ των χρηστών του διαδικτύου.

ΗΠΑ – Πνευματική ιδιοκτησία (1)

- Το 1998 ψηφίσθηκε στις ΗΠΑ νόμος στον οποίο καθορίσθηκε για πρώτη φορά ένα αυστηρό πλαίσιο σχετικά με τα ψηφιακά πνευματικά δικαιώματα (Digital Millennium Copyright Act - DCMA) .
- Στον εν λόγω νόμο για πρώτη φορά περιλαμβάνονταν διατάξεις σχετικά με την εναρμόνηση του θεσμικού πλαισίου των ΗΠΑ με την συνθήκη του 1996 του Παγκόσμιου Οργανισμού Πνευματικής Ιδιοκτησίας (World Intellectual Property Organization - WIPO) η οποία μεταξύ άλλων προέβλεπε και την ποινικοποίηση τεχνολογιών, συσκευών, υπηρεσιών οι οποίες είχαν ως στόχο την εξάλειψη των τεχνολογιών της ψηφιακής προστασίας των πνευματικών δικαιωμάτων (Digital Rights Management).

ΗΠΑ – Πνευματική ιδιοκτησία (2)

- Επίσης για πρώτη φορά υιοθετήθηκε η αρχή της αποποίησης της ευθύνης του παροχέα πρόσβασης σχετικά με τις ενέργειες του χρήστη του διαδικτύου συμπεριλαμβανομένου και του κατεβάσματος περιεχομένου το οποίο προστατεύεται από πνευματικά δικαιώματα.
- Υπήρχαν πολλές περιπτώσεις όπου ο πάροχος πρόσβασης έχει κατηγορηθεί για την «συμπεριφορά» των χρηστών του στο διαδίκτυο σχετικά με την πρόσβαση σε περιεχόμενο το οποίο προστατεύεται από πνευματικά δικαιώματα. Ενδειτικά:
 - Στις ΗΠΑ το 1997 η εταιρία πρόσβασης CompuServe κατηγορήθηκε από την National Music Publishers Association ότι επέτρεπε στους συνδρομητές της να «κατεβάζουν» τραγούδια τα οποία προστατεύονταν από πνευματικά δικαιώματα. Η δικαστική διαμάχη έληξε με εξωδικαστικό συμβιβασμό στον οποίο η CompuServe πλήρωσε ένα μεγάλο χρηματικό ποσό.

ΗΠΑ – Πνευματική ιδιοκτησία (3)

- Πολλοί υποστήριξαν ότι ο DCMA ήταν πολύ αυστηρός όσον αφορά την προστασία της πνευματικής ιδιοκτησίας αφού περιορίζει σε μεγάλο βαθμό την επικοινωνία μεταξύ συστημάτων λογισμικού που σχετίζονται με την πνευματική ιδιοκτησία (π.χ. αλγόριθμους αποκρυπτογράφησης).
- Υπήρχαν πολλοί επικριτές του Νόμου ακόμη και στην ΗΠΑ οι οποίοι θεωρούσαν ότι είναι αντίθετος με το Σύνταγμα των ΗΠΑ σχετικά με την ελευθερία της διακίνησης ιδεών και την ανάπτυξη της καινοτομίας (*“Congress shall make no law abridging the freedom of speech”*)

Πρόβλημα πριν από το διαδίκτυο

- Υπόθεση “**Sony Safe Harbor Rule**” (Betamax case)
 - Το 1978 η Universal μήνυσε την Sony η οποία είχε κατασκευάσει συσκευές οι οποίες είχαν την δυνατότητα αποθήκευσης βίντεο (τεχνολογίας Betamax)
 - Ο βασικός ισχυρισμός της Universal ήταν ότι με τις συσκευές που κατασκεύασε η Sony οι καταναλωτές θα είχαν τη δυνατότητα να αντιγράφουν το τηλεοπτικό πρόγραμμα και να τα αναπαράγουν σε όσα αντίγραφα ήθελαν με αποτέλεσμα να παραβιάζονται τα σχετικά πνευματικά δικαιώματα.
 - Το 1984 το Ανώτατο Δικαστήριο των ΗΠΑ με μία ιστορική Απόφαση αθώωσε την Sony καθώς αποδέχθηκε το γεγονός ότι η εφεύρεση της Sony επέτρεπε στους καταναλωτές να μαγνητοσκοπούν μία εκπομπή και να την δουν όποτε το επιθυμούν, πράξη που δεν παραβίαζε τα πνευματικά δικαιώματα.

“Sony Safe Harbor” Rule

- Η ιστορική Απόφαση βασίσθηκε στο επιχείρημα ότι δεν τίθεται απαγόρευση κυκλοφορίας μια συσκευής λόγω πιθανής παραβίασης πνευματικών δικαιωμάτων, όταν τουλάχιστον μία κύρια χρήση της συσκευής δεν παραβιάζει την πνευματική ιδιοκτησία.
- Το σκεπτικό της Απόφασης έχει χρησιμοποιηθεί έκτοτε σε πληθώρα σχετικών Αποφάσεων οι οποίες σχετίζονται με παραβιάσεις πνευματικών δικαιωμάτων. Πέρα του ανωτέρω σκεπτικού η Απόφαση βασίστηκε και στο επιχείρημα ότι εάν η Απόφαση απαγόρευε την κυκλοφορία της συσκευής της Sony τότε αυτό θα ήταν καταστρεπτικό για το εμπόριο, τον ανταγωνισμό και την έρευνα σχετικά με νέα προϊόντα και τεχνολογίες.

Διαδίκτυο και πνευματικά δικαιώματα

- **Υπόθεση Napster**

- Ένα από τα πρώτα προγράμματα διακίνησης ψηφιακών αρχείων ήταν το Napster (διακίνηση μουσικών ψηφιακών αρχείων), ενώ ακολούθησαν πάρα πολλά άλλα (torrent, emule κλπ).
- Το Napster ήταν ένα πρόγραμμα το οποίο επέτρεπε στους χρήστες του να μοιρασθούν ψηφιακά μουσικά κομμάτια (mp3) τα οποία ήταν αποθηκευμένα στους υπολογιστές των χρηστών και όχι σε κάποια βάση δεδομένων της εταιρίας. Βέβαια το Napster ήταν έτσι σχεδιασμένο ώστε όλα τα αρχεία τα οποία αντάλλασσαν οι χρήστες περνούσαν από τους κεντρικούς εξυπηρετητές της εταιρίας και επομένως η εταιρία γνώριζε τα αρχεία που διακινούνταν.
- Το γεγονός ότι το Napster δεν αποθήκευε αρχεία ήταν ένα από τα βασικότερα επιχειρήματα με τα οποία το Napster προσπάθησε να αποποιηθεί οποιαδήποτε ευθύνη σχετικά με τα πνευματικά δικαιώματα των μουσικών κομματιών τα οποία διακινούνταν μέσω της εφαρμογής Napster.
- Οι χρήστες του Napster έφταναν να αντιγράφουν περίπου 14.000 τραγούδια το λεπτό.

Napster (1)

- Η ένωση δισκογραφικών εταιρειών της Αμερικής (RIAA) κατέθεσε το 2000 αγωγή κατά του Napster διεκδικώντας αποζημιώσεις της τάξεως του 1 δισ.\$ η οποία βασίζονταν μεταξύ άλλων και στο πρόσφατα νέο νόμο των ΗΠΑ για τα ψηφιακά πνευματικά δικαιώματα (Digital Millennium Copyright Act - DCMA). Η εξέταση της υπόθεσης του Napster ανέδειξε για πρώτη φορά σε παγκόσμιο επίπεδο το ζήτημα των ψηφιακών πνευματικών δικαιωμάτων.
- Το βασικό επιχείρημα του Napster ήταν ότι δεν έκανε καμία αντιγραφή ή αποθήκευση μουσικού κομματιού αλλά έδινε τη δυνατότητα στους χρήστες του να ανταλλάζουν τα μουσικά κομμάτια τα οποία είχαν αποθηκευμένα στους υπολογιστές τους.
- Η Απόφαση του δικαστηρίου υποχρέωνε το Napster να εμποδίζει την αντιγραφή μεταξύ των χρηστών της εφαρμογής των μουσικών κομματιών για τα οποία οι δισκογραφικές εταιρίες έθεταν ζητήματα προστασίας των πνευματικών δικαιωμάτων.

Napster (2)

- Παρόλο την αρνητική έκβαση (για το Napster) της δικαστικής διαμάχης μεταξύ των κατόχων των πνευματικών δικαιωμάτων και της εταιρείας η δημιουργία και η τεράστια επιτυχία του Napster άνοιξε τον δρόμο σε μία σειρά άλλα σχετικά προγράμματα ενώ άσκησε τεράστιες ανταγωνιστικές πιέσεις στις σχετικές βιομηχανίες οι οποίες πέρα πάσας αμφιβολίας είχαν σαν αποτέλεσμα στην μείωση των τιμών για τα σχετικά προϊόντα.
- Οι απόγονοι του Napster (Kazza, Grokster, Morpheus) σχεδιάσθηκαν με τέτοιο τρόπο ώστε τα προγράμματα (και επομένως και οι εταιρίες) να μην γνωρίζουν τα αρχεία τα οποία διακινούνται μεταξύ των χρηστών.

MGM vs. Grokster

- Η MGM (εταιρία των ΗΠΑ παραγωγής κυρίως κινηματογραφικών και τηλεοπτικών παραγωγών) κατέθεσε αγωγή εναντίον της Grokster σχετικά με το ομώνυμο πρόγραμμα file sharing.
- Το 2003 το δικαστήριο του Λος Άντζελες αθώωσε την Grokster βασιζόμενο κυρίως στην υπόθεση Sony Safe Harbor
- Η δικαστική διαμάχη συνεχίστηκε και έφθασε στο Ανώτατο Δικαστήριο των ΗΠΑ όπου το 2005 απεφάνθη ότι η υπόθεση θα πρέπει να εκδικασθεί εκ νέου διότι το δικαστήριο του LA ερμήνευσε το Sony Safe Harbor rule με πολύ ευρύ σκεπτικό και αφετέρου υπήρχαν ενδείξεις ότι η Grokster με ενεργό τρόπο ωθούσε τους χρήστες να κατεβάσουν ταινίες / μουσικά κομμάτια τα οποία προστατεύονταν από πνευματικά δικαιώματα.
- Η εν λόγω Απόφαση θεωρείται ιστορική διότι για πρώτη φορά από το 1984 αμφισβητήθηκε η Απόφαση Sony Safe Harbor και έθεσε νέες βάσεις (νομολογία) για τις μελλοντικές εκδικάσεις για ζητήματα που άπτονται των ψηφιακών πνευματικών δικαιωμάτων.

DRM - Digital Rights Management

- Τα DRM είναι όλα εκείνα τα τεχνικά μέτρα τα οποία έχουν ως στόχο την προστασία των ψηφιακών πνευματικών δικαιωμάτων και τον περιορισμό / έλεγχο της διάδοσης του ψηφιακού περιεχομένου ενός έργου το οποίο προστατεύεται από πνευματικά δικαιώματα.
- Τα DRM περιορίζουν / ελέγχουν την αντιγραφή, εκτέλεση, εκτύπωση, προβολή, ψηφιακού περιεχομένου το οποίο προστατεύεται από πνευματικά δικαιώματα.
- Τα DRM έχουν διάφορες μορφές. Ενδεικτικά:
 - Περιορισμός της πρόσβασης σε τελικούς χρήστες λαμβάνοντας υπόψη την τοποθεσία του τελικού χρήστη (IP).
 - Κωδικοποίηση για την αποφυγή αντιγραφής (DVD).
 - Χρήση κωδικού για τον έλεγχο της πρόσβασης ή της εκτέλεσης (product Key, license Key κλπ).

Οδηγία 2001/29/ΕΚ (1)

- Η Οδηγία 2001/29 αντιμετώπισε για πρώτη φορά σε επίπεδο Ευρωπαϊκής Ένωσης τα ζητήματα της πνευματικής ιδιοκτησίας στην κοινωνία της πληροφορίας. Έως τότε στα Κράτη Μέλη υπήρχαν μεγάλες διαφοροποιήσεις στον τρόπο αντιμετώπισης το οποίο έθετε κινδύνους στον στόχο της ΕΕ περί δημιουργίας μία εννιαίας κοινής εσωτερικής αγοράς. Η εν λόγω Οδηγία εναρμονίστηκε στο εθνικό πλαίσιο με τον ν.3057/2002.
- **Βασικά ζητήματα Οδηγίας:**
 - **Δικαιώματα αναπαραγωγής & δικαιώματα παρουσίασης των έργων στο κοινό:** τα δικαιώματα αναπαραγωγής και τα δικαιώματα παρουσίασης των έργων στο κοινό παρέχονται αποκλειστικά στους δημιουργούς, καλλιτέχνες (για καλλιτεχνικές εκτελέσεις), παραγωγούς φωνογραφημάτων, ραδιοτηλεοπτικούς οργανισμούς.

Οδηγία 2001/29/ΕΚ (2)

- **Βασικά ζητήματα Οδηγίας:**
 - **Δικαιώματα διανομής:** οι δημιουργοί των έργων έχουν το αποκλειστικό δικαίωμα να επιτρέπουν ή να απαγορεύουν τη διανομή των πρωτότυπων ή των αντιγράφων των έργων τους στο κοινό με οποιαδήποτε μορφή μέσω πώλησης ή άλλως.
 - **Προστασία δικαιωμάτων:** έννομη προστασία κατά της κατασκευής, εισαγωγής, διανομής, προϊόντων, παροχής υπηρεσιών οι οποίες έχουν σκοπό την εξουδαιτέρωση της προστασίας, ή επιτρέπουν ή διευκολύνουν την εξουδετέρωση της προστασίας των δικαιωμάτων.
 - **Πληροφορίες σχετικά με τα δικαιώματα:** έννομη προστασία κατά οποιουδήποτε ο οποίος εν γνώσει του προβαίνει σε αφαίρεση ή αλλοίωση ηλεκτρονικής πληροφορίας σχετική με τα δικαιώματα.

Οδηγία 2001/29/ΕΚ (3)

- **Βασικά ζητήματα Οδηγίας:**
 - **Κυρώσεις :**
 - Τα ΚΜ προβλέπουν κατάλληλες κυρώσεις και μέσα έννομης προστασίας έναντι της προστασίας των πνευματικών δικαιωμάτων...
 - ...Οι κυρώσεις είναι αποτελεσματικές, ανάλογες και αποτρεπτικές.
 - ...οι δικαιούχοι μπορούν αν ζητούν την λήψη ασφαλιστικών μέτρων κατά των διαμεσολαβητών οι υπηρεσίες των οποίων χρησιμοποιούνται από τρίτους για την προσβολή των πνευματικών δικαιωμάτων.

Οδηγία 2019/790/ΕΚ

- **Στόχοι:**

- Μείωση της ανασφάλειας δικαίου για τους πολίτες σχετικά με την ψηφιακά δικαιώματα χρήσης υλικού καθώς και αποσαφήνιση των ψηφιακών τους δικαιωμάτων
- Οι διαδικτυακές πλατφόρμες που συμμετέχουν οι χρήστες θα πρέπει να μεριμνούν για τη δυνατότητα ή μη χρήσης πνευματικών έργων
- Με βάση τις προβλεπόμενες εξαιρέσεις που σχετίζονται με την ελευθερία της έκφρασης όλοι οι χρήστες είναι ελεύθεροι να ανεβάζουν υλικό που δημιουργείται από άλλους χρήστες για σχολιασμό για κριτική, για γελοιογραφία, για μίμηση κ.α
- Οι χρήστες έχουν ξεκάθαρα δικαιώματα όταν το περιεχόμενο που έχουν μεταφορτώσει έχει διαγραφεί λόγω παραβίασης πνευματικών δικαιωμάτων. Μπορούν να υποβάλουν ένσταση και οι πλατφόρμες θα πρέπει να τους απαντήσουν χωρίς καθυστέρηση
- Οι πολίτες θα πρέπει να έχουν διαδικτυακή πρόσβαση σε μουσική, αρχεία, ταινίες, βιβλία τα οποία δεν είναι πλέον εμπορικά διαθέσιμα στην Ευρώπη

Οδηγία 2019/790/ΕΚ

- **Στόχοι:**

- Διευκόλυνση συμφωνιών μεταξύ των εμπλεκόμενων μερών: κατόχων πνευματικών δικαιωμάτων, αντιπροσώπων αυτών, εκπροσώπων του τύπου κλπ
- Οι δημιουργοί των μουσικών και οπτικοακουστικών έργων θα πρέπει να αποκτήσουν μεγαλύτερο έλεγχο στην χρήση των έργων τους τα οποία αναφορτώνονται από χρήστες διαδικτυακών υπηρεσιών
- Οι εκδότες θα πρέπει να αποκτήσουν ένα νέο δικαίωμα να διαπραγματεύονται και να αμείβονται καλύτερα από την χρήση των εφημερίδων και των περιοδικών από διαδικτυακές υπηρεσίες. Οι δημοσιογράφοι θα πρέπει να λαμβάνουν ένα κατάλληλο μερίδιο των εσόδων που δημιουργούνται από το νέο δικαίωμα

Οδηγία 2019/790/ΕΚ

- **Στόχοι:**

- Περισσότερες εξαιρέσεις για χρήση έργων που προστατεύονται από πνευματικά δικαιώματα για επιστημονικούς και εκπαιδευτικούς λόγους καθώς και για λόγους διάδοσης της πολιτιστικής κληρονομιάς
- Η έρευνα και η ανάπτυξη της τεχνικής νοημοσύνης στο τομέα της εξόρυξης δεδομένων δίνει νέα ώθηση στην ανάλυση μεγάλου όγκου δεδομένων, η οποία δεν θα πρέπει να προστατεύεται από αποκλειστικότητα και από πνευματικά δικαιώματα όταν η ανάλυση πραγματοποιείται για ερευνητικούς ή εκπαιδευτικούς σκοπούς
- Τα μουσεία, οι βιβλιοθήκες, αρχεία ταινιών και άλλοι πολιτισμικοί φορείς θα μπορούν να ψηφιοποιήσουν καλλιτεχνικά έργα για την διάδοση της πολιτισμικής κληρονομιάς
- Προστασία αυτο-αποσχολούμενων δημοσιογράφων και δημιουργών και θέσπιση διαδικασιών / κανόνων προκειμένου να αποκομίζουν οφέλη από την διάδοση των έργων τους μέσω της ψηφιακής αγοράς
- Θέσπιση κανόνων για ευκολότερη διαπραγμάτευση μεταξύ αυτοαπασχολούμενων καλλιτεχνών / συγγραφέων / δημοσιογράφων και των εκδοτών / παραγωγών

Οδηγία 2019/790/ΕΚ

- Θεσπίζει κανόνες σε επίπεδο ΕΕ σχετικά με τα δικαιώματα πνευματικής ιδιοκτησίας και τα συγγενικά δικαιώματα λαμβάνοντας υπόψη τις εξελίξεις στην τεχνολογία και την ύπαρξη μιας ενιαίας ψηφιακής αγοράς
- Προβλέπει διευκολύνσεις χρήσης περιεχομένου που προστατεύεται από πνευματικά δικαιώματα όταν η χρήση αφορά έρευνα, εκπαίδευση και διατήρηση πολιτιστικής κληρονομιάς
- Προωθεί και διευκολύνει την χρήση νέων τεχνολογιών όπως αυτής της εξόρυξης δεδομένων και της τεχνικής νοημοσύνης

Οδηγία 2019/790/ΕΚ

- Ενίσχυση διαπραγματευτικής ισχύς και οικονομικής θέσης των εμπλεκόμενων που σχετίζονται με την δημιουργία / παραγωγή περιεχομένου: δημιουργούς, εκδότες, παραγωγούς ιδίως με μεγάλες εταιρίες που δραστηριοποιούνται στο Διαδίκτυο (Google, Facebook κλπ)
- Προστασία φυσικών προσώπων (με μικρή διαπραγματευτική ισχύ) όπως οι δημιουργοί, ερμηνευτές έναντι των μεγάλων εκδοτών και παραγωγών

Άδειες Creative Commons

- Ο Creative Commons (CC) είναι ένας μη κερδοσκοπικός οργανισμός ο οποίος ιδρύθηκε το 2001 με έδρα το Σαν Φρανσίσκο των ΗΠΑ.
- Σκοπός του CC είναι η υποστήριξη του ανοικτού και προσβάσιμου διαδικτύου.
- Ο CC έχει δημιουργήσει διαφορετικές κατηγορίες δικαιωμάτων πνευματικής ιδιοκτησίας προκειμένου να διευκολύνει την χρήση πνευματικών έργων στο διαδίκτυο.
- Τα περισσότερα πνευματικά έργα στο διαδίκτυο προστατεύονται με την χρήση του όρου “All rights Reserved” ή «Με την επιφύλαξη παντός νομίμου δικαιώματός».
- Η ιδέα του CC ήταν να δώσει την εύκολη δυνατότητα σε δημιουργούς πνευματικών έργων στο διαδίκτυο να μεταπηδήσουν σε μία ελαστικότερη μορφή πνευματικών δικαιωμάτων σχετικά με τα έργα τους προκειμένου να δώσουν τη δυνατότητα για ευκολότερη και ταχύτερη διάδοση των έργων τους.

ΣΚΕΠΤΙΚΟ CC...

- Η μορφή του διαδικτύου και ο πλούτος των πληροφοριών που περιέχονται σε αυτόν επηρεάζει σημαντικά τη διαμόρφωση του θεσμικού πλαισίου της προστασίας της πνευματικής ιδιοκτησίας ιδίως της ψηφιακής.
- Η ευκολία με την οποία μπορεί κάποιος να «κατεβάσει» από το διαδίκτυο περιεχόμενο που καλύπτεται από πνευματική ιδιοκτησία είχε ως αποτέλεσμα πολλοί οργανισμοί και κυβερνήσεις να προσπαθήσουν να δημιουργήσουν ένα αυστηρό πλαίσιο σχετικά με τα πνευματικά δικαιώματα ψηφιακού περιεχομένου.
- Από την άλλη μεριά το διαδίκτυο διευκολύνει σε μεγάλο βαθμό την ανάπτυξη της συνεργατικότητας μεταξύ πνευματικών δημιουργών όχι μόνο για εμπορικούς σκοπούς αλλά και για την επίτευξη εκπαιδευτικών και ερευνητικών στόχων.
- Ο CC δημιούργησε τύπους αδειών για πνευματικά δικαιώματα προκειμένου αφενός να απονέμει με εύκολο και προσιτό τρόπο πνευματικά δικαιώματα στους δημιουργούς αλλά παράλληλα να τους διευκολύνει για ευρύτερη, αμεσότερη και σαφέστερη διάδοση των έργων τους.

Επίπεδα αδειών CC

- Οι άδειες CC έχουν τρία επίπεδα κώδικα:
 - **Νομικό**: προκειμένου να καλύπτονται οι άδειες νομικά (στο βαθμό που αυτό είναι εφικτό λαμβάνοντας υπόψη το σχετικό εθνικό νομικό πλαίσιο)
 - **Κοινό**: οι δεσμεύσεις γίνονται κατανοητές και από μη νομικούς
 - **Μηχανικό**: η άδεια μπορεί να γίνει κατανοητή και από κατάλληλο λογισμικό χωρίς την παρέμβαση ανθρώπου (πχ σύνθετη αναζήτηση εικόνων από Google)

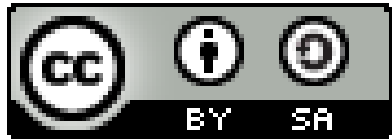
Τύποι αδειών CC

- Οι άδειες CC έχουν 4 βασικά στοιχεία:
 - Αναφορά στον αρχικό δημιουργό (attribution)
 - Απαγόρευση ή μη εμπορικής χρήσης του έργου (non-commercial)
 - Απαγόρευση ή μη δημιουργίας παράγωγων έργων (no derivatives)
 - Διανομή ή μη του παράγωγου έργου με τους όρους της αρχικής άδειας (share alike)
- Τα αρχικά των 4 βασικών στοιχείων των αδειών:
 - BY: **A**tribution only
 - ND: **N**o **D**erivatives
 - NC: **N**on **C**ommercial
 - SA: **S**hare **A**like

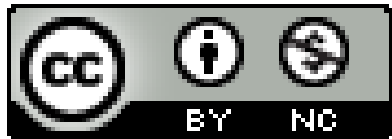
Παραδείγματα αδειών CC



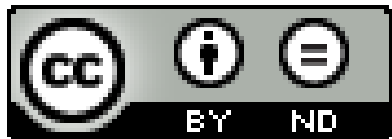
Μόνη υποχρέωση: Αναφορά στον δημιουργό



Αναφορά στον δημιουργό, παρόμοια διανομή



Αναφορά στον δημιουργό, και μη εμπορική χρήση



Αναφορά στον δημιουργό, όχι παράγωγα έργα



Αναφορά στον δημιουργό, όχι εμπορική χρήση, παρόμοια διανομή



Αναφορά στον δημιουργό, όχι εμπορική χρήση, όχι παράγωγα

Παραδείγματα αδειών CC

- Ενδεικτικά δημοφιλή παραδείγματα χρήσης αδειών CC:
 - Wikipedia
 - Youtube
 - Opencourses.gr

Ενότητα IV

- Ανοικτά δεδομένα

Open Data – Ανοικτά Δεδομένα

- Ως ανοικτά δεδομένα (open data) ορίζονται εκείνα τα δεδομένα τα οποία είναι δημοσίως διαθέσιμα και μπορούν να χρησιμοποιηθούν (re-use) εκ νέου χωρίς περιορισμούς.
- Με το πέρασμα του χρόνου ο όρος επαναχρησιμοποίηση (re-use) έχει τροποποιηθεί ως προς την πρακτική του σημασία:
 - Δημοσίως διαθέσιμα σε οποιαδήποτε μορφή (πχ έντυπη)
 - Δημοσίως διαθέσιμα σε ηλεκτρονική μορφή (πχ pdf)
 - Δημοσίως διαθέσιμα σε συγκεκριμένη επεξεργάσιμη ηλεκτρονική μορφή (πχ .doc ή .xls)
 - Δημοσίως διαθέσιμα σε συγκεκριμένη επεξεργάσιμη ηλεκτρονική μορφή αναγνώσιμη από μηχανές
 - Δημοσίως διαθέσιμα σε συγκεκριμένη επεξεργάσιμη ηλεκτρονική μορφή αναγνώσιμη από μηχανές με συγκεκριμένα διαλειτουργικά και με βάση διεθνή στάνταρτ (API)
- Και ο όρος χωρίς περιορισμούς μπορεί να ερμηνευθεί ποικιλοτρόπως (πχ. βλέπε άδειες CC)

Πού χρησιμοποιούνται;

- Πολλές εφαρμογές & υπηρεσίες βασίζονται στη διαθεσιμότητα των ανοικτών δεδομένων. Ενδεικτικά:
 - εφαρμογές πρόγνωσης καιρού
 - εφαρμογές παρακολούθησης αεροσκαφών / πλοίων

Εξόρυξη δεδομένων: Data mining

- Εξόρυξη δεδομένων: οι νέες τεχνολογίες παρέχουν δυνατότητες αυτοματοποιημένης υπολογιστικής ανάλυσης πληροφοριών σε ψηφιακή μορφή όπως: κειμένων, ήχων, εικόνων κλπ
- Με την εξόρυξη δεδομένων είναι δυνατή η επεξεργασία μεγάλου όγκου δεδομένων (big data analysis) με στόχο την απόκτηση νέων γνώσεων και την ανακάλυψη νέων τάσεων
- Σε ορισμένες περιπτώσεις η εξόρυξη δεδομένων ενδέχεται να περιλαμβάνει πηγές που προστατεύονται από δικαιώματα πνευματικής ιδιοκτησίας (όπως πνευματικά δικαιώματα σε βάσεις δεδομένων), οπότε σε αυτές τις περιπτώσεις θα πρέπει να υπάρχει η σχετική άδεια από τους κατόχους των δικαιωμάτων
- Η εξόρυξη δεδομένων είναι μια τεχνολογία στην οποία βασίζεται η παγκόσμια οικονομία. Πέρα όμως από αυτό αποτελεί σημαντικό εργαλείο της ερευνητικής κοινότητας προς όφελος της καινοτομίας

Open Data στο Δημόσιο Τομέα

- Τα ανοικτά δεδομένα στο δημόσιο τομέα (Public Sector Information) σχετίζονται με τα δεδομένα που παράγονται / συλλέγονται από δημόσιους οργανισμούς.
- Σε επίπεδο ΕΕ υπάρχει από το 2003 Ευρωπαϊκή Οδηγία (2003/98/ΕΚ – PSI Directive) η οποία επιβάλλει την υποχρέωση σε δημόσιους οργανισμούς να παρέχουν πρόσβαση στα έγγραφά τους (δεδομένα) σε έντυπη και όπου αυτό είναι εφικτό και σε ηλεκτρονική μορφή, χωρίς περιορισμούς και σεβόμενοι την αρχή της μη διακριτικής μεταχείρισης. Έγγραφα / δεδομένα που περιέχουν προσωπικά δεδομένα ή εμπιστευτικά στοιχεία εξαιρούνται από την υποχρέωση.
- Οι δημόσιοι φορείς μπορούσαν να χρεώνουν για την πρόσβαση στα εν λόγω στοιχεία/ δεδομένα προκειμένου να καλύψουν το σχετικό κόστος. Τα στοιχεία δεν μπορούσαν να επαναχρησιμοποιηθούν.

Open Data στο Δημόσιο Τομέα

- Το 2013 η ΕΕ τροποποίησε την Οδηγία:
 - διευρύνοντας τους δημόσιους φορείς (περιλαμβάνονται μουσεία, βιβλιοθήκες).
 - παρέχοντας δυνατότητα επαναχρησιμοποίησης των δεδομένων.
 - οι δημόσιοι φορείς θα μπορούσαν να χρεώνουν μόνο εάν αποδείκνυαν ότι έχουν επιπλέον κόστος για την παροχή της σχετικής πρόσβασης στα δεδομένα.
 - τα δεδομένα θα έπρεπε να είναι προσβάσιμα και από μηχανές / προγράμματα.

Public Sector Information

- Στην ΕΕ λόγω της υφιστάμενης Οδηγίας (2003/98) τα ανοικτά δεδομένα σχετίζονται με την ανοικτότητα των δεδομένων του ευρύτερου δημόσιου τομέα.
- Τέτοια δεδομένα μπορεί να είναι σχετικά με (ενδεικτικά):
 - πρόγνωσης καιρού (πχ meteo.gr)
 - αποτελέσματα δημόσιων ερευνητικών φορέων (www.demokritos.gr)
 - στατιστικά (www.statistics.gr)
 - data.gov.gr

Οικονομικό αντίκτυπο PSI

- Μελέτη που έχει εκπονηθεί για λογαριασμό της ΕΕ εκτιμά ότι τα άμεσα οικονομικά οφέλη από την ύπαρξη της PSI για το **2018 ανέρχονται στα 21 δις. ευρώ** ενώ το 2030 θα εκτιναχθούν **στα 180 δις. Ευρώ**.

Νέα Οδηγία 1024/2019

- Η νέα Οδηγία της ΕΕ (1024/2019) (Οδηγία για τα ανοικτά δεδομένα) αντικαθιστά την PSI και ορίζει το πλαίσιο ΕΕ για τα ανοικτά δεδομένα σε επίπεδο ΕΕ. Τα βασικά σημεία της Οδηγίας είναι:
 - Σκοπός της Οδηγίας είναι να προαχθεί η χρήση ανοικτών δεδομένων και η καινοτομία στην παροχή υπηρεσιών που βασίζονται στα ανοικτά δεδομένα
 - Εφαρμόζεται σε δεδομένα του δημόσιου τομέα καθώς και σε ερευνητικά δεδομένα τα οποία έχουν παραχθεί με δημόσιους πόρους
 - Προωθεί την δημοσίευση δυναμικών δεδομένων μέσω διαθέσιμων API (Application Program Interface)
 - Περιορίζει τις εξαιρέσεις μέσω των οποίων οι δημόσιοι φορείς επιτρέπεται να χρεώνουν πέρα από το κόστος για την επαναχρησιμοποίηση των δεδομένων τους
 - Ενδυναμώνει την διαφάνεια για συμφωνίες μεταξύ ιδιωτικών και δημόσιων φορέων προκειμένου να αποτρέψει συμφωνίες αποκλειστικής χρήσης για δεδομένα που παράγονται από δημόσιους φορείς

Δεδομένα υψηλής αξίας

- Απαιτεί από την Επιτροπή την υιοθέτηση μια λίστας δεδομένων τα οποία θα διατίθενται χωρίς χρέωση και τα οποία θεωρούνται ως δεδομένα υψηλής αξίας και τα οποία θα επιταχύνουν την ανάπτυξη καινοτόμων προϊόντων και υπηρεσιών τα οποία βασίζονται σε δεδομένα. Αυτά τα δεδομένα είναι απαραίτητα για την ανάπτυξη εφαρμογών Τεχνητής Νοημοσύνης (Artificial Intelligence)
- Τα εν λόγω δεδομένα έχουν ιδιαίτερα σημαντική αξία για την κοινωνία και την οικονομία και θα πρέπει να διατίθενται δωρεάν σε μορφή αναγνωρίσιμη από μηχανές μέσω APIs.
- Τέτοια δεδομένα είναι:
 - Γεω-χωρικά δεδομένα (Geospatial)
 - Δεδομένα σχετικά με παρατηρήσεις για την γη και για το περιβάλλον
 - Μετεωρολογικά δεδομένα
 - Στατιστικά δεδομένα
 - Δεδομένα σχετικά με εταιρίες και το ιδιοκτησιακό καθεστώς αυτών
 - Κινητικότητα

Μελέτη περίπτωσης Open Data

- Δύο ερευνητές στην Αμερική συνέδεσαν ανοικτά δεδομένα
 - καιρού: προγνώσεις
 - γεωργίας: ανάλυση χωραφιών και συστατικά εδάφους
- Ανάπτυξαν εφαρμογή η οποία μπορούσε να προβλέψει την αποδοτικότητα ενός χωραφιού σε οποιοδήποτε μέρος των ΗΠΑ λαμβάνοντας υπόψη τις προγνώσεις καιρού (καταιγίδες κλπ), συστατικά χωραφιών, είδος καλλιεργειών.
- Την εφαρμογή την χρησιμοποιούσαν τόσο οι γεωργοί όσο και οι ασφαλιστικές εταιρίες
- Μετά από λίγα χρόνια την εταιρία την εξαγόρασε για πολλά εκ. \$ μία από τις μεγαλύτερες εταιρίες παραγωγής γεωργικών προϊόντων στις ΗΠΑ.

Μελέτη περίπτωσης Big Data

- Τον Ιανουάριο του 2019 η εταιρία data Artisans εξαγοράσθηκε από την Alibaba έναντι του ποσού των 90M€.
- Η data Artisans ιδρύθηκε το 2014 και ο ένας εκ των δύο ιδρυτών ήταν Έλληνας (απόφοιτος ΕΜΠ το 2007 ο οποίος στην συνέχεια εκπόνησε το διδακτορικό του σε πανεπιστήμιο της Δανίας και στη συνέχεια μεταδιδακτορική έρευνα στην Γερμανία)
- Η data Artisans υλοποίησε πλατφόρμα ανοικτού κώδικα (Apache Flink) προκειμένου να επεξεργάζεται μεγάλου όγκου δεδομένα (big data) σε πραγματικό χρόνο (την στιγμή που δημιουργούνται – data stream processing)
- Μέχρι τότε τα δεδομένα μεγάλου όγκου επεξεργάζονταν αφού πρώτα αποθηκεύονταν σε βάσεις δεδομένων

Ηλεκτρονική Διακυβέρνηση & Ανοικτά Δεδομένα – Διαύγεια

Νόμος 3861/2010

- Σκοπός:
 - **Υποχρέωσης ανάρτησης** των νόμων, των προεδρικών διαταγμάτων, και των πράξεων που εκδίδουν οι υπόχρεοι στο Διαδίκτυο και η δημιουργία των προϋποθέσεων **και διαδικασιών για τη διασφάλιση ευρύτατης δημοσιότητας** αυτών.
- Υπόχρεοι:
 - Πρωθυπουργός, Υπουργεία, Ν.Π.Δ.Δ. οι ανεξάρτητες και ρυθμιστικές διοικητικές αρχές, το Νομικό Συμβούλιο του Κράτους, τα όργανα των φορέων των Οργανισμών Τοπικής Αυτοδιοίκησης πρώτου και δεύτερου βαθμού.

Ανάρτηση στο Διαδίκτυο

- Τι αναρτάται (περιληπτικά):
- Νόμοι, Προεδρικά Διατάγματα, πράξεις κανονιστικού χαρακτήρα **με εξαίρεση** τις πράξεις η δημοσιοποίηση των οποίων προκαλεί βλάβη στην **εθνική άμυνα** και **ασφάλεια της χώρας**, εγκύκλιοι, οι προϋπολογισμοί, απολογισμοί, ισολογισμοί δημόσιων υπηρεσιών και φορέων του ευρύτερου δημόσιου τομέα, προκηρύξεις πλήρωσης θέσεων με διαγωνισμό ή με επιλογή, το σύνολο των συμβάσεων και των πράξεων που αναφέρονται σε αναπτυξιακούς νόμους, πράξεις αποδοχής δωρεών στο Ελληνικό Δημόσιο, οι γνωμοδοτήσεις του Νομικού Συμβουλίου του Κράτους, οι πράξεις και γνωμοδοτήσεις των ανεξάρτητων και ρυθμιστικών διοικητικών αρχών, κλπ.

Ανάρτηση - Ισχύς – Προσωπικά Δεδομένα

- Οι πράξεις **αναρτώνται αμελλητί** στο Διαδίκτυο με μέριμνα του οργάνου που τις εξέδωσε.
- Οι πράξεις **δεν εκτελούνται**, εάν δεν έχει προηγηθεί η ανάρτησή τους στο δικτυακό τόπο et.diavgeia.gov.gr. Με την ολοκλήρωση της ανάρτησης η κάθε απόφαση αποκτά έναν μοναδικό αριθμό Αριθμό Διαδικτυακής Ανάρτησης ([ΑΔΑ](#)), ο οποίος την πιστοποιεί.
- **Δεν αναρτώνται** πράξεις, στις οποίες περιλαμβάνονται **ευαίσθητα δεδομένα προσωπικού χαρακτήρα**, όπως αυτά ορίζονται στην κείμενη νομοθεσία.

Διαδικασία Ανάρτησης

- Σε κάθε δημόσιο φορέα **συγκροτείται ομάδα διοίκησης** έργου με αντικείμενο την τεχνική, διαδικαστική και οργανωτική υποστήριξη της ανάρτησης νόμων και πράξεων στο Διαδίκτυο.
- Στο Εθνικό Τυπογραφείο δημιουργείται και τηρείται **κεντρικό αρχείο νόμων, προεδρικών διαταγμάτων και πράξεων που αναρτώνται στο Διαδίκτυο**, το οποίο είναι προσιτό σε κάθε ενδιαφερόμενο και με ηλεκτρονικά μέσα.

ΑΔΑ – Αριθμός Διαδικτυακής Ανάρτησης

- Είναι ένας μοναδικός κωδικός που αποκτά κάθε πράξη μετά την ολοκλήρωση της καταχώρισης της στην εφαρμογή της Διαύγειας.
- Ο ΑΔΑ παράγεται αλγοριθμικά με βάση:
 - την ημερομηνία καταχώρισης,
 - το φορέα και τον αύξοντα αριθμό πράξης του φορέα,
 - εγγράφεται αυτόματα σε κάθε σελίδα του εγγράφου που αναρτάται.
- Κάθε Απόφαση έχει μόνο έναν ΑΔΑ, ενώ όταν μια απόφαση για κάποιο λόγο ακυρώνεται ο ΑΔΑ της παραμένει ανενεργός