Τεχνικά ζητήματα ΓΚΠΔ– Επισημάνσεις – Μελέτη περιπτώσεων

1. Ασφάλεια κατά την επεξεργασία προσωπικών δεδομένων

2. Προστασία ήδη από το σχεδιασμό και εξ ορισμού

3. Ειδικές απαιτήσεις από τη νομοθεσία για τις ηλεκτρονικές επικοινωνίες - cookies και συναφείς τεχνολογίες

ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Η ασφάλεια στο ΓΚΠΔ (2)

- **Άρθρο 32**: (…) ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση:
  - α) της **ψευδωνυμοποίησης** και της **κρυπτογράφησης** δεδομένων προσωπικού χαρακτήρα,
  - β) της δυνατότητας διασφάλισης του **απορρήτου**, της **ακεραιότητας**, της **διαθεσιμότητας** και της **αξιοπιστίας** των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση,
  - γ) της δυνατότητας **αποκατάστασης** της **διαθεσιμότητας** και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση συμβάντος ασφάλειας λόγω φυσικού ή τεχνικού λόγου,
  - δ) διαδικασίας για την τακτική δοκιμή, εκτίμηση και **αξιολόγηση** της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.
- Κατά την εκτίμηση του ενδεδειγμένου επιπέδου ασφάλειας λαμβάνονται ιδίως υπόψη οι κίνδυνοι που απορρέουν από την επεξεργασία (…)

Η ασφάλεια στο ΓΚΠΔ (1)

- **Άρθρο 24**: 1. Λαμβάνοντας υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας εφαρμόζει **κατάλληλα τεχνικά και οργανωτικά μέτρα** προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό. Τα εν λόγω μέτρα **επανεξετάζονται και επικαιροποιούνται** όταν κρίνεται απαραίτητο.

- 2. Όταν δικαιολογείται σε σχέση με τις δραστηριότητες επεξεργασίας, τα μέτρα που αναφέρονται στην παράγραφο 1 περιλαμβάνουν την **εφαρμογή κατάλληλων πολιτικών** για την προστασία των δεδομένων από τον υπεύθυνο επεξεργασίας

Στόχοι Ασφάλειας

- Εμπιστευτικότητα (confidentiality)
  - Οι πληροφορίες δεν πρέπει να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα
- Ακεραιότητα (integrity)
  - Οι πληροφορίες πρέπει να είναι ακέραιες, γνήσιες – όχι αλλοιωμένες/τροποποιημένες
    - Προσοχή: Δεν πρέπει να συγχέεται με την απαίτηση της ακρίβειας των δεδομένων
- Διαθεσιμότητα (availability)
  - Η εξασφάλιση ότι τα δεδομένα και οι συναφείς υπηρεσίες θα είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους
- Όταν η πληροφορία αφορά προσωπικά δεδομένα, οι ανωτέρω ορισμοί ισχύουν αντιστοίχως

Επιλογή κατάλληλων μέτρων ασφάλειας

- Προκύπτουν λαμβάνοντας υπόψη (πρβλ. αρ. 25):
  - τις τελευταίες εξελίξεις,
  - το κόστος εφαρμογής
  - τα χαρακτηριστικά της επεξεργασίας (φύση - πεδίο εφαρμογής - πλαίσιο – σκοποί)
- Κρίσιμος παράγοντας η σωστή αξιολόγηση των κινδύνων και των πιθανών συνεπειών
- Παραδείγματα λίστας επιλογής μέτρων μείωσης κινδύνων
  - ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security controls
  - ISO/IEC 27701 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management
  - ISO/IEC 29151 - Information technology — Security techniques — Code of practice for personally identifiable information protection
  - Εθνικά πρότυπα (NIST/SP 800-53), λίστες εποπτικών αρχών (CNIL - AGPD) ή άλλων οργανισμών

Οργανωτικά & τεχνικά μέτρα ασφάλειας

- Οργανωτικά μέτρα ασφάλειας
  - Ορισμός υπευθύνου ασφαλείας με σαφείς αρμοδιότητες
  - Εκπαίδευση προσωπικού
  - Ορισμός διαδικασιών διαχείρισης περιστατικών
  - Σχέδιο επιχειρησιακής συνέχειας / αποκατάστασης από καταστροφές
  - Τακτικός έλεγχος/επικαιροποίηση αποτελεσματικότητας μέτρων
  - Θέματα που άπτονται εξωτερικών συνεργατών / προμηθευτών (εκτελούντες την επεξεργασία)
  - Μέτρα φυσικής ασφάλειας
  - κ.α.
- Τεχνικά μέτρα ασφάλειας
  - Μέτρα ασφάλειας βάσεων δεδομένων
    - κρυπτογράφηση/ψευδωνυμοποίηση, έλεγχος πρόσβασης (αυθεντικοποίηση χρηστών, τεχνικές πρόσβασης σε εξουσιοδοτημένους χρήστες, υλοποίηση αρχής «need-to-know» κτλ.
  - Μέτρα ασφάλειας επικοινωνιών
    - Κρυπτογράφηση, έλεγχος εισερχομένης κίνησης, χρήση εικονικού ιδιωτικού δικτύου κτλ.
  - Συστηματική και αυτοματοποιημένη λήψη αντιγράφων ασφάλειας
  - Αρχεία καταγραφής ενεργειών (log files)
  - Εργαλεία ανίχνευσης εισβολών
  - Διαμόρφωση περιβάλλοντος υπολογιστών
  - κ.α.

Εμπειρία παραλείψεων σε ζητήματα ασφάλειας σε διαδικτυακούς τόπους

- Μη εφαρμογή ενημερώσεων ασφαλείας σε online εφαρμογές (π.χ CMS)
- Απλοί κωδικοί πρόσβασης
- Απουσία αυθεντικοποίησης σε λογαριασμό χρήστη (είσοδος μόνο με URL)
- Εύκολη πρόσβαση σε λογαριασμό χρήστη από μια διαδοχική ηλεκτρονική διεύθυνση URL
- Έλλειψη κρυπτογράφησης
- Ευρετηρίαση δεδομένων σε μια μηχανή αναζήτησης

Προστασία δεδομένων ήδη από το σχεδιασμό και εξ ορισμού (αρ. 25)

- Προστασία **από το σχεδιασμό (by design)**:
  - Τεχνολογίες ιδιωτικότητας και προστασία προσωπικών δεδομένων **κατά το σχεδιασμό συστήματος/εφαρμογής.**
  - **Αποτελεσματικότητα μετρήσιμη**
  - **Ενσωμάτωση στην επεξεργασία**
  - Λαμβάνοντας υπόψη:
    - Τελευταίες εξελίξεις τεχνολογίας (state of the art)
    - Κόστος τεχνολογικών λύσεων - εφαρμογής μέτρων.
    - Φύση, πεδίο εφαρμογής, σκοποί επεξεργασίας.
    - Κίνδυνοι για τα δικαιώματα και τα τις ελευθερίες των υποκειμένων.

- Προστασία **εξ ορισμού (by default)**:
  - Οι προ-καθορισμένες/αρχικές ρυθμίσεις πρέπει να είναι **οι πιο φιλικές προς την προστασία δεδομένων.**
  - Εξ ορισμού, τα δεδομένα προσωπικού χαρακτήρα δεν καθίστανται προσβάσιμα χωρίς την παρέμβαση του φυσικού προσώπου σε αόριστο αριθμό φυσικών προσώπων.

Προστασία δεδομένων ήδη από το σχεδιασμό και εξ ορισμού (αρ. 25)

- **Ενδεικτικά στοιχεία**
  - Διαφάνεια
    - Σαφήνεια
    - Σημασιολογία
    - Προσβασιμότητα
    - Χρονισμός
    - Συνάφεια
    - Σχεδιασμός κατανοητός, οικουμενικός

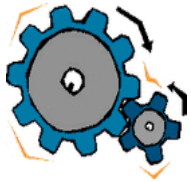
Προστασία δεδομένων ήδη από το σχεδιασμό και εξ ορισμού (αρ. 25)

- **Ενδεικτικά στοιχεία**
  - Ελαχιστοποίηση δεδομένων
    - Αποφυγή επεξεργασίας
    - Απόδειξη συνάφειας, σύνδεση με σκοπό
    - Χρήση συγκεντρωτικών δεδομένων
    - Ψευδωνυμοποίηση
    - Ανωνυμοποίηση
    - Διαγραφή
    - Κατάλληλη ροή δεδομένων
    - "state of the art" τεχνολογίες

Ψευδωνυμοποίηση

Αρχικά δεδομένα

Mary	Adams	Female	23
John	Brown	Male	26
Anna	Frank	Female	32
Tom	Hill	Male	42
.	.	.	.
.	.	.	.



Ψευδωνυμοποίηση

Ψευδωνυμοποιημένα δεδομένα

A	Female	23
B	Male	26
Γ	Female	32
Δ	Male	42
.	.	.
.	.	.

Η αντιστοίχιση «ονοματεπώνυμο – ψευδώνυμο» είναι αναφερόμενες στον ΓΚΠΔ *συμπληρωματικές πληροφορίες*

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

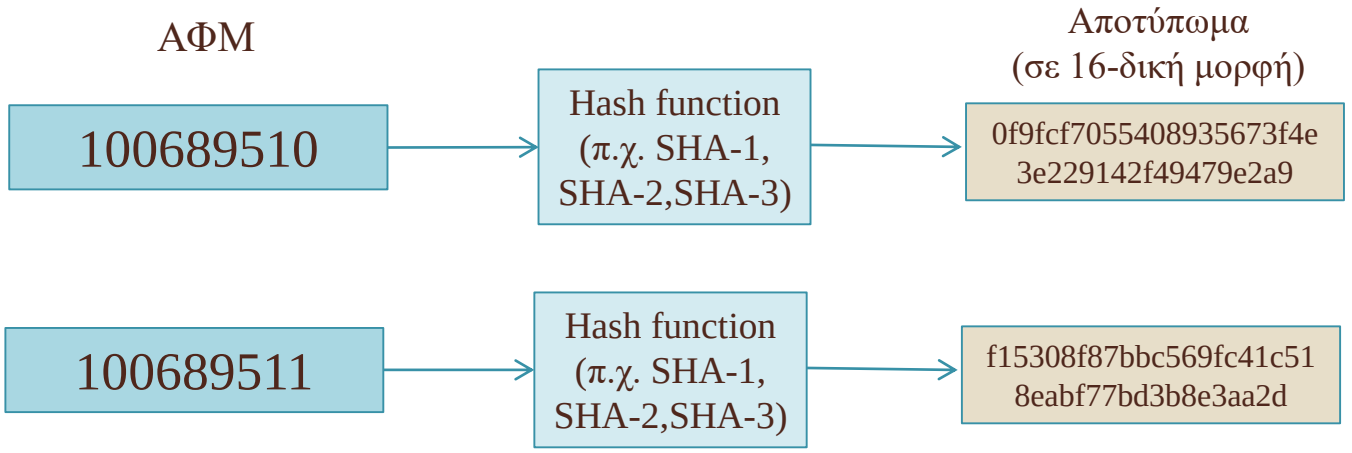
www.dpa.gr

Ψευδωνυμοποίηση vs ανωνυμοποίηση

Κάθε μετασχηματισμός ενός αναγνωριστικού σε μία νέα, ακατάληπτη μορφή, δεν πρέπει να θεωρείται ανωνυμοποίηση **αν υπάρχει περίπτωση, από την ακατάληπτη αυτή μορφή, να συμπεράνει/υπολογίσει κανείς την τιμή του αναγνωριστικού.**

- Παράδειγμα: Κρυπτογραφική συνάρτηση κατακερματισμού (hash function) είναι μη αναστρέψιμη.

- «ίδιο άτομο – ίδιο (ακατάληπτο) αναγνωριστικό»



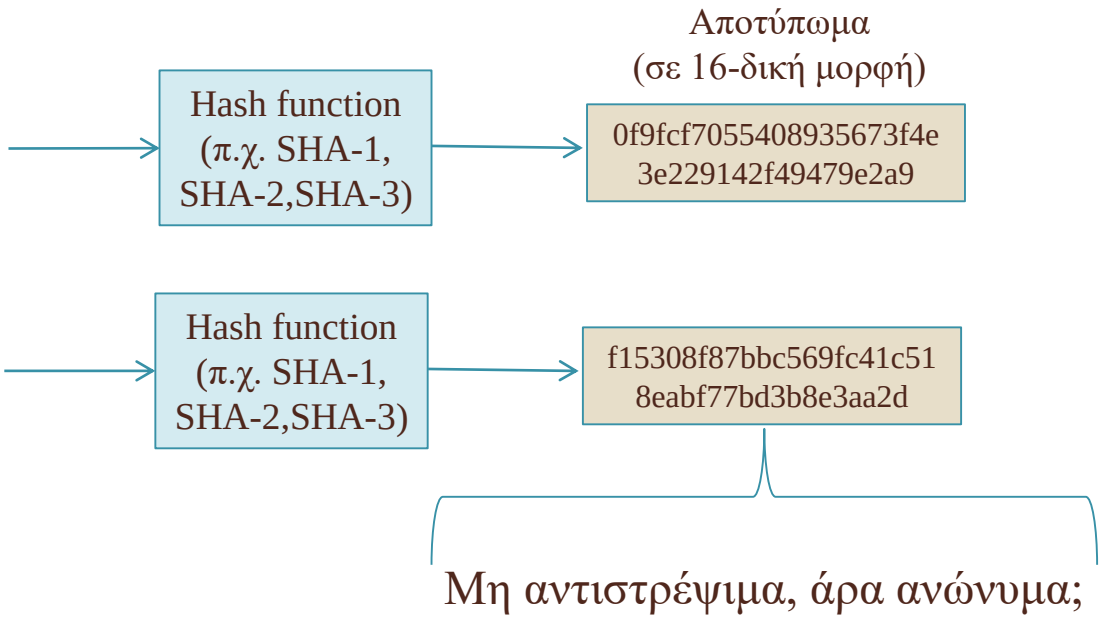
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ
www.dpa.gr

Ψευδωνυμοποίηση vs ανωνυμοποίηση

Κάθε μετασχηματισμός ενός αναγνωριστικού σε μία νέα, ακατάληπτη μορφή, δεν πρέπει να θεωρείται ανωνυμοποίηση **αν υπάρχει περίπτωση, από την ακατάληπτη αυτή μορφή, να συμπεράνει/υπολογίσει κανείς την τιμή του αναγνωριστικού.**

- Παράδειγμα: Κρυπτογραφική συνάρτηση κατακερματισμού (hash function) είναι μη αναστρέψιμη.

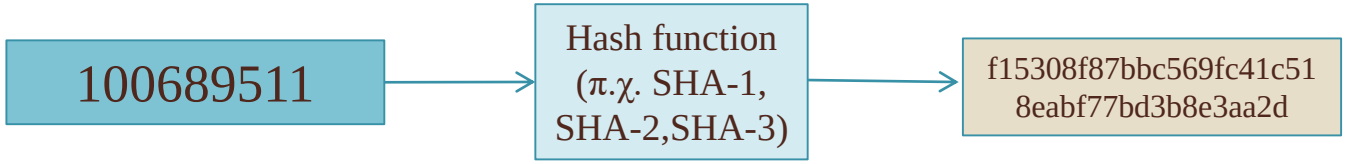
- «ίδιο άτομο – ίδιο (ακατάληπτο) αναγνωριστικό»



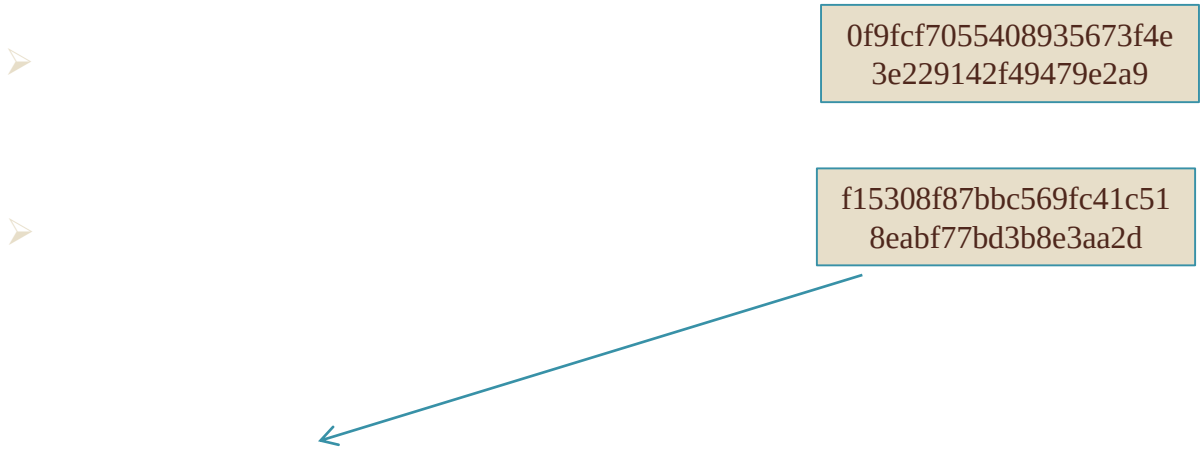
Ψευδωνυμοποίηση vs ανωνυμοποίηση

Μπορούμε να διαπιστώσουμε αν ο Α με ΑΦΜ 100689511 βρίσκεται στη λίστα;

1. 1) Υπολογίζουμε το αποτύπωμα του ΑΦΜ του Α



- 2) Ελέγχουμε αν το αποτύπωμα είναι στην «ανωνυμοποιημένη» λίστα



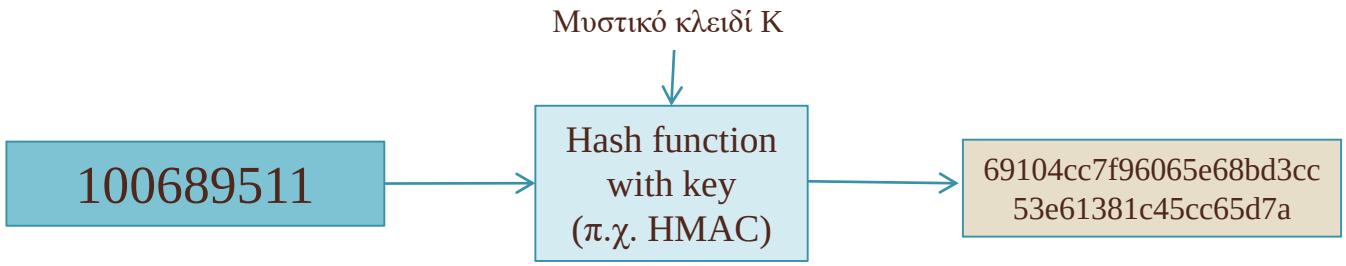
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Εναλλακτική προσέγγιση

Χρήση κρυπτογραφικής συνάρτησης με μυστικό κλειδί

Π.χ. υπολογισμός ενός Message Authentication Code (MAC)



- Ακολούθως, το μυστικό κλειδί πρέπει να καταστρέφεται
- Είναι «ισοδύναμο» με το να γίνεται μία τυχαία, μη αντιστρεπτή, αντιστοίχιση του μοναδικού αναγνωριστικού (ΑΦΜ) με μία συμβολοσειρά με χαρακτηριστικά τυχαιότητας

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Η «ευρεία» έννοια του αναγνωριστικού

- Εκτός από τα αναγνωριστικά (identifiers), υπάρχουν και τα οιονεί-αναγνωριστικά (quasi-identifiers), που συνδυαστικά δύνανται επίσης να οδηγήσουν σε ταυτοποίηση

- Η απλή απαλοιφή των αναγνωριστικών δεν διασφαλίζει εγγυημένα ανωνυμία

- Σύμφωνα έρευνα στις Η.Π.Α. 2002 , το 87% του πληθυσμού των Η.Π.Α. μπορεί να ταυτοποιηθεί από την τριπλέτα «Ταχ. Κώδικας - ημερομηνία γέννησης – φύλο»

- Πολλές «έξυπνες» εφαρμογές συλλέγουν το Google Advertising ID (GAID)
  - Ακόμα κι αν από μόνο του δεν αποκαλύπτει την ταυτότητα του χρήστη της συσκευής, μπορεί – έστω και υπό προϋποθέσεις – να οδηγήσει σε ταυτοποίηση του χρήστη
    - Π.χ. μπορεί να συλλεγεί και από εφαρμογές που συλλέγουν επίσης και κάποιο αναγνωριστικό του χρήστη (π.χ. e-mail)

Εφαρμογή τεχνικών ανωνυμοποίησης

Π.χ δεν δημοσιεύουμε επακριβώς την ηλικία, αλλά ένα εύρος ηλικιών (π.χ. 30-40)

- Με αυτόν τον τρόπο, η μονοσήμαντη συσχέτιση μίας καταχώρησης του «ανώνυμου» πίνακα με μία του «επώνυμου» καθίσταται πιο δύσκολη
- Είναι μία διαδικασία που πρέπει να γίνεται με προσοχή
  - Είναι πολύ πιθανό, ακόμα και με μία τέτοια τεχνική, πάλι να μην μπορεί να ειπωθεί με βεβαιότητα ότι έχει επιτευχθεί ανωνυμοποίηση,
  - Μπορεί ωστόσο να αντιμετωπίζει αποτελεσματικά τους κινδύνους
  - Η εξέταση της αποτελεσματικότητας αυτή μπορεί να γίνεται στο πλαίσιο μίας μελέτης αντικτύπου ως προς την προστασία προσωπικών δεδομένων

Cookies και συναφείς τεχνολογίες

- Άρθρο 4 παρ. 5 του ν.3471/2006

- Η αποθήκευση πληροφοριών ή η απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη επιτρέπεται μόνο με συγκατάθεση κατόπιν σαφούς ενημέρωσής του .
  - Κατ' εξαίρεση επιτρέπεται, χωρίς συγκατάθεση αλλά πάντα με ενημέρωση, η αποθήκευση ή απόκτηση πρόσβασης αν είναι απαραίτητη για τη διαβίβαση μίας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή για παροχή υπηρεσίας της κοινωνίας της πληροφορίας, την οποία έχει ζητήσει ρητά ο χρήστης.
- Τα **cookies** εμπίπτουν σε αυτήν την περίπτωση
- Αν το πρόγραμμα πλοήγησης (φυλλομετρητής) του χρήστη έχει ρυθμιστεί ώστε να αποδέχεται όλα τα **cookies**, αυτό δεν μπορεί να εκληφθεί ως ειδική συγκατάθεση

Cookies και συναφείς τεχνολογίες
Άρθρο 4 παρ. 5 του ν.3471/2006

- Επιτρέπεται η εγκατάσταση **cookies** στον τερματικό εξοπλισμό του χρήστη (π.χ. υπολογιστή), χωρίς τη συγκατάθεσή του, μόνο αν αυτά είναι απολύτως απαραίτητα για την παροχή της υπηρεσίας
  - Π.χ. **Session cookies**, για να μας «αναγνωρίζει» η υπηρεσία εφόσον έχουμε συνδεθεί και πραγματοποιούμε ηλεκτρονικές αγορές (π.χ. τοποθέτηση σε «καλάθι αγορών»)

- Για άλλες περιπτώσεις **cookies**, πρέπει να υπάρχει ρητή συγκατάθεση του χρήστη
  - Π.χ. **Cookies** για έλεγχο επισκεψιμότητας του **site**, **cookies** για σκοπό την προβολή (στοχευμένων ή μη) διαφημιστικών μηνυμάτων κτλ.

Στοιχεία της έγκυρης συγκατάθεσης

Ελεύθερη

- Το υποκείμενο είναι σε θέση να **αρνηθεί** ή να **αποσύρει** τη συγκατάθεσή του **χωρίς να ζημιωθεί**

Συγκεκριμένη

- Προσδιορισμός του σκοπού
- Διαφορετική συγκατάθεση για διαφορετικούς σκοπούς

Εν πλήρη επιγνώσει

- Επαρκής ενημέρωση

Θετική Δήλωση Συναίνεσης

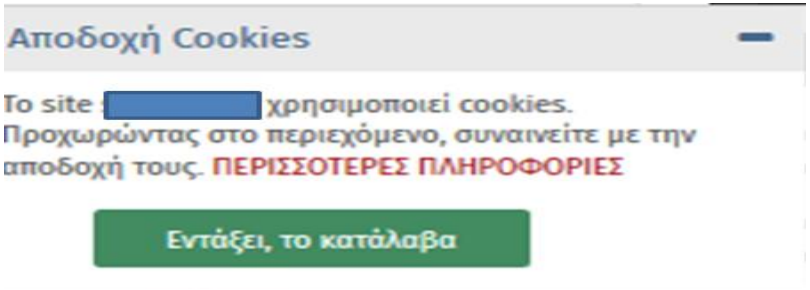
- Δήλωση ή σαφής θετική ενέργεια
- Σιωπηρή αποδοχή δεν νοείται ως συγκατάθεση
- Προ-τσεκαρισμένα κουτιά δεν αποτελούν έγκυρη μέθοδο
- Opt-out κουτιά δεν αποτελούν έγκυρη μέθοδο

Δυνατότητα ανάκλησης

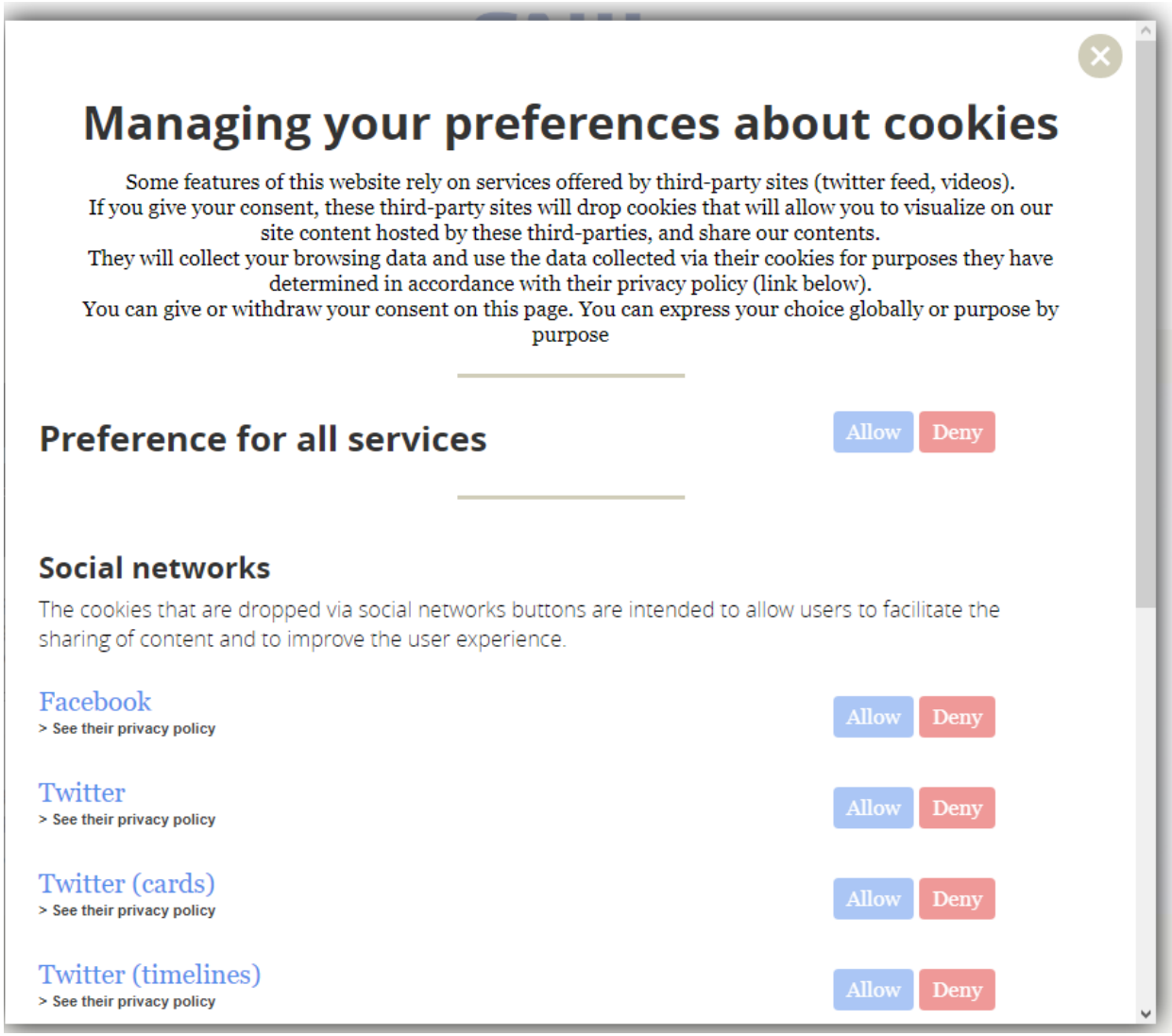
Cookies και συναφείς τεχνολογίες

- Η συγκατάθεση πρέπει να ληφθεί με σαφή ενέργεια του χρήστη (σαφής, ρητή και ειδική συγκατάθεση)
  - Να επιλέξει κατάλληλο κουμπί επιλογής ότι συναινεί, από όπου πρέπει να είναι σαφές ότι ενημερώνεται επαρκώς για το τι σημαίνει η επιλογή του

- Δεν θεωρείται σαφής, ρητή και ειδική συγκατάθεση του χρήστη αν απλά συνεχίζει να πλοηγείται αφού πρώτα ενημερώνεται (π.χ. με pop-up «παράθυρο») για την ύπαρξη των cookies



Παράδειγμα: το site της γαλλικής Αρχής Προστασίας Δεδομένων



Ευχαριστούμε για την προσοχή σας

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr