Πανεπιστήμιο Θεσσαλίας
ΔΠΜΣ Σχολής Θετικών Επιστημών

Ψηφιακή Ασφάλεια και Ιδιωτικότητα

Προστασία προσωπικών δεδομένων: Νομικό πλαίσιο και νέες προκλήσεις

Δρ. Κωνσταντίνος Λιμνιώτης
E-mail: klimniotis at dpa.gr

Εισαγωγή

- Η συντριπτική πλειοψηφία των οργανισμών (δημόσιοι – ιδιωτικοί) επεξεργάζονται προσωπικά δεδομένα
  - Υπαλλήλων τους
  - Πελατών τους
- Ακόμα και μία απλή διαδικτυακή υπηρεσία επεξεργάζεται προσωπικά δεδομένα
  - Η IP διεύθυνση ενός υπολογιστή - που τηρείται κατά κανόνα στα αρχεία καταγραφής (log files) κάθε web server – θεωρείται και αυτή, όπως θα δούμε, προσωπικό δεδομένο!
- Η επεξεργασία προσωπικών δεδομένων συνεπάγεται πληθώρα νομικών υποχρεώσεων
  - Ακριβώς γιατί η προστασία προσωπικών δεδομένων είναι ένα θεμελιώδες ανθρώπινο δικαίωμα και πρέπει να είναι θωρακισμένη
- Κατά την ανάλυση επικινδυνότητας και διαχείριση κινδύνων, πρέπει να λαμβάνεται υπόψη και η σημασία της επεξεργασίας προσωπικών δεδομένων
  - Όχι μόνο από τη σκοπιά οικονομικών απωλειών και δυσφήμισης του οργανισμού, αλλά και από τη σκοπιά των νομικών υποχρεώσεων

Η έννοια της ιδιωτικότητας

- Ιδιωτικότητα (Privacy):
  - The ability of the individual to control the terms under which personal information is acquired and used. (Westin A..F., 1967)
  - A state or condition of limited access to a person, information about him, intimacies of personal identity (F. Schoeman, 1984)
  - The right to privacy is the right to be left alone (Brandeis, 1928)
  - Πλήθος άλλων ορισμών…..

- Με το θεσμικό πλαίσιο της προστασίας προσωπικών δεδομένων, τίθενται προϋποθέσεις νομιμότητας της επεξεργασίας προσωπικών δεδομένων, καθώς επίσης αναγνωρίζονται συναφή δικαιώματα και υποχρεώσεις, στο πλαίσιο προστασίας του θεμελιώδους αγαθού της ιδιωτικότητας.
  - Άρα, η προστασία προσωπικών δεδομένων είναι στενά συνυφασμένη με την ιδιωτικότητα
  - Η ακριβής σχέση τους θα συζητηθεί εκ νέου στη συνέχεια…

Ιστορικά στοιχεία

- **1950**: Η προστασία της ιδιωτικής ζωής αναγνωρίζεται ως δικαίωμα στην ΕΣΔΑ (Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου - άρθρο 8)
  - Παν πρόσωπον δικαιούται εις τον σεβασμόν της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του (…).

- **1981**: Συμβούλιο της Ευρώπης, Σύμβαση 108 για την Προστασία του Ατόμου από την Αυτοποιημένη Επεξεργασία Προσωπικών Δεδομένων
  - (…) Οι πληροφορίες προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική προέλευση, τα πολιτικά φρονήματα, τις θρησκευτικές ή άλλες πεποιθήσεις, όπως και οι πληροφορίες προσωπικού χαρακτήρα που σχετίζονται με την υγεία ή την σεξουαλική ζωή, δεν δύνανται να αποτελέσουν αντικείμενο αυτοματοποιημένης επεξεργασίας, εάν το εσωτερικό δίκαιο δεν προβλέπει κατάλληλες εγγυήσεις. Το αυτό ισχύει για τις πληροφορίες προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες (…)

Προστασία προσωπικών δεδομένων – Ευρωπαϊκή Νομοθεσία

- 1995: Οδηγία 95/46/ΕΚ για την προστασία των φυσικών προσώπων από την επεξεργασία των προσωπικών δεδομένων τους και την ελεύθερη διακίνηση των δεδομένων (Ευρωπαϊκό Συμβούλιο και Κοινοβούλιο).

- 2002: Οδηγία 2002/58/ΕΚ για την προστασία των φυσικών προσώπων από την επεξεργασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών (Ευρωπαϊκό Συμβούλιο και Κοινοβούλιο)
  - Ειδικότερη περίπτωση που αφορά τα δεδομένα στις τηλεπικοινωνιακές υπηρεσίες (π.χ. δεδομένα θέσης/κίνησης στην τηλεφωνία, cookies κτλ.)
  - 2009: Οδηγία 2009/136/ΕΚ που τροποποιεί την 2002/58/ΕΚ

- Μία Ευρωπαϊκή Οδηγία – όπως οι παραπάνω - πρέπει να ενσωματωθεί στην εθνική νομοθεσία κάθε Κράτους – Μέλους
  - Άρα, όλα τα Κράτη – Μέλη έχουν σχεδόν το ίδιο νομικό πλαίσιο, αφού το κάθε ένα έχει στην έννομη τάξη του ένα νόμο που βασίζεται στην ίδια Οδηγία
  - Υπάρχουν όμως πάντα μικρές διαφοροποιήσεις (η ίδια η Οδηγία αφήνει διάφορα θέματα ανοικτά στον εκάστοτε εθνικό νομοθέτη).

Προστασία προσωπικών δεδομένων – Εθνική νομοθεσία

- Οι ανωτέρω Οδηγίες έχουν ενσωματωθεί στην εθνική νομοθεσία των Κρατών-Μελών

- Στην Ελλάδα:
  - Νόμοι 2472/1997, 3471/2006, 4070/2012
  - Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (www.dpa.gr)

- 2001: Συνταγματική αναθεώρηση.
  - Άρθρο 9Α: 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.

- Νέος Κανονισμός της ΕΕ, που ενισχύει περαιτέρω την προστασία των προσωπικών δεδομένων, τίθεται σε εφαρμογή στις 25 Μαΐου 2018

Προσωπικά Δεδομένα

- Προσωπικά δεδομένα (ή Δεδομένα προσωπικού χαρακτήρα):
  - κάθε πληροφορία (άμεση ή έμμεση) που αναφέρεται σε φυσικό πρόσωπο και χαρακτηρίζει το υποκείμενο από φυσική, βιολογική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική άποψη (άρ. 2 του ν. 2472/1997)
  - Δεν λογίζονται ως προσωπικά δεδομένα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία

- Στην πράξη, προσωπικά δεδομένα είναι τα δεδομένα που αφορούν ένα πρόσωπο και συνδέονται με την ταυτότητά του, όπως για παράδειγμα:
  - το όνομά μας
  - η διεύθυνσή μας (ταχυδρομική αλλά και ηλεκτρονική – email),
  - το τηλέφωνό μας,
  - τα ενδιαφέροντά μας,
  - οι απόψεις μας,
  - η εικόνα μας (φωτογραφία/video)
  - …..
- Είναι όμως και πολλά περισσότερα, που ίσως δεν φανταζόμαστε
  - Το ψευδώνυμό μας (nickname) σε μία διαδικτυακή υπηρεσία, ακόμα και αν δεν παραπέμπει στο πραγματικό μας ονοματεπώνυμο
  - Η IP διεύθυνση του υπολογιστή μας από τον οποίο «σερφάρουμε»
- Με άλλα λόγια, κάθε δεδομένο από το οποίο υπάρχει πιθανότητα/περίπτωση να αναγνωριστούμε

Ευαίσθητα προσωπικά δεδομένα

- Κάποια προσωπικά δεδομένα χρήζουν ακόμα μεγαλύτερης προστασίας, γιατί εμπίπτουν στο σκληρό πυρήνα της ιδιωτικότητας

- Ευαίσθητα δεδομένα: τα δεδομένα που αφορούν σε
  - φυλετική ή εθνική προέλευση,
  - πολιτικά φρονήματα,
  - θρησκευτικές ή φιλοσοφικές πεποιθήσεις,
  - συμμετοχή σε συνδικαλιστική οργάνωση,
  - υγεία,
  - κοινωνική πρόνοια,
  - ερωτική ζωή,
  - ποινικές διώξεις ή καταδίκες,
  - στη συμμετοχή σε συναφείς με τα παραπάνω ενώσεις

Ανώνυμα δεδομένα

Τα ανώνυμα δεδομένα δεν θεωρούνται προσωπικά δεδομένα

- Οδηγία 95/46/ΕΚ: Οι αρχές της προστασίας δεν εφαρμόζονται σε δεδομένα που έχουν καταστεί ανώνυμα κατά τρόπο ώστε να μην μπορεί να εξακριβωθεί πλέον η ταυτότητα του προσώπου στο οποίο αναφέρονται

- Είναι εύκολος ο χαρακτηρισμός των δεδομένων ως ανώνυμων;
  - Οδηγία 95/46/ΕΚ: «Για να διαπιστωθεί αν η ταυτότητα ενός προσώπου μπορεί να εξακριβωθεί, πρέπει να λαμβάνεται υπόψη το σύνολο των μέσων που μπορούν ευλόγως να χρησιμοποιηθούν, είτε από τον υπεύθυνο της επεξεργασίας, είτε από τρίτο, για να εξακριβωθεί η ταυτότητα του εν λόγω προσώπου»

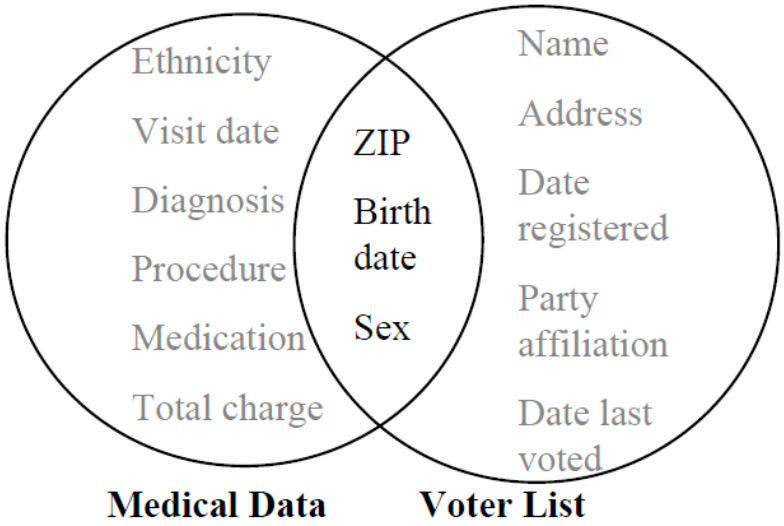
- Με άλλα λόγια, πρέπει να είναι πρακτικά απολύτως αδύνατον να ταυτοποιηθεί κάποιος (και όχι απλά να υπάρχει μικρή πιθανότητα ταυτοποίησης)

- Ερώτηση: Το αποτύπωμα, μέσω μίας hash function, ενός μοναδικού αναγνωριστικού ενός προσώπου (π.χ. Αριθμός ταυτότητας, Αριθμός Φορολογικού Μητρώου κτλ.) θα πρέπει να θεωρείται ανώνυμο δεδομένο;
  - Κάποιος μπορεί να ισχυριστεί «ναι», δεδομένου ότι η hash function είναι μη αναστρέψιμη
  - Δεδομένου ότι οι αλγόριθμοι υπολογισμού hash είναι γνωστοί και ότι υπάρχει επίσης δυνατότητα να γνωρίζουμε το αναγνωριστικό κάποιου, συμπεραίνουμε ότι υπάρχει περίπτωση να ταυτοποιηθεί κάποιος μέσω επαναϋπολογισμού του hash του αριθμού ταυτότητάς του – άρα, δεν μπορούν να θεωρηθούν ανώνυμα δεδομένα!!

Παράδειγμα «κακής» ανωνυμοποίησης

- [Sweeney, 2002]: Νοσοκομείο στην πολιτεία της Μασαχουσέτης δημοσιοποίησε, για ερευνητικούς σκοπούς, «ανώνυμη» λίστα ασθενών (φύλο/ημερομηνία γέννησης/ ΤΚ/ εθνικότητα και στοιχεία νοσηλείας).

- Ερευνητές συνέκριναν αυτή τη λίστα με τη δημόσια προσβάσιμη λίστα των ψηφοφόρων στην πολιτεία, όπου τα στοιχεία (φύλο/ημερομηνία γέννησης/ ΤΚ) ήταν κοινά



  - Για συγκεκριμένη ημ/νία γέννησης, έξι άτομα είχαν την ίδια, τρεις εξ αυτούς άντρες, μόνο ένας με τον ίδιο ταχυδρομικό κώδικα (ZIP code)
    - Αυτός ήταν ο (τότε) κυβερνήτης της Μασαχουσέτης
  - ΣΥΜΠΕΡΑΣΜΑ: Μη «βιαστούμε» να χαρακτηρίσουμε τα δεδομένα που επεξεργαζόμαστε ως ανώνυμα!!

Βασικοί Ορισμοί

- Επεξεργασία δεδομένων (αυτοματοποιημένη ή μη): Κάθε εργασία, όπως συλλογή, καταχώριση, οργάνωση, αποθήκευση, τροποποίηση, εξαγωγή, ανάκτηση, αναζήτηση, χρήση, ανακοίνωση, διαβίβαση, διασύνδεση, δέσμευση, διαγραφή καταστροφή

- Υποκείμενο δεδομένων (data subject): το φυσικό πρόσωπο στο οποίο αφορούν τα δεδομένα

- Υπεύθυνος επεξεργασίας (data controller): το (φυσικό ή νομικό) πρόσωπο που καθορίζει το σκοπό και τον τρόπο επεξεργασίας

- Εκτελών την επεξεργασία (data processor): το (φυσικό ή νομικό) πρόσωπο που δρα για λογαριασμό του υπεύθυνου επεξεργασίας

Γίνεται συχνά επεξεργασία δεδομένων;

- Το 24ωρο ενός μαθητή… (από το site www.dpa.gr)

7:15	**Διαβάζεις το e-mail σου** – ο πάροχος ηλεκτρονικών επικοινωνιών καταγράφει την ώρα που μπήκες στο λογαριασμό σου, τον αποστολέα του μηνύματός σου, καθώς και την ώρα που σου έστειλε το μήνυμα.
7:30	**«Κατεβάζεις» ένα τραγούδι στο iPod** – η εταιρεία που σου πουλάει το τραγούδι καταγράφει το e-mail σου και τις μουσικές σου προτιμήσεις.
7:50	**Η μητέρα σου σε πάει με το αυτοκίνητο στο σχολείο** – το αυτοκίνητο διαθέτει συσκευή GPS που καταγράφει τη διαδρομή σας από το σπίτι στο σχολείο. Σε κάποια σημεία της διαδρομής υπάρχουν κάμερες ρύθμισης της κυκλοφορίας και ελέγχου παραβιάσεων του Κώδικα Οδικής Κυκλοφορίας.
10:10	**Μπαίνεις στην τάξη** – στο απουσιολόγιο του τμήματός σου καταγράφονται οι απόντες για κάθε διδακτική ώρα. Ο σχολικός σου φάκελος περιλαμβάνει τους βαθμούς και τις αξιολογήσεις που σε αφορούν.
12:00	**Ο κολλητός σου σε τραβάει μια φωτογραφία με το κινητό** – η φωτογραφία είναι αστεία και λέει πως μπορεί αργότερα να την ανεβάσει στο facebook.
15:00	**Σερφάρεις στο διαδίκτυο από το σπίτι** – ο browser που χρησιμοποιείς καταγράφει τις σελίδες που επισκέπτεσαι. Κάποιες σελίδες εγκαθιστούν στον υπολογιστή σου μικρά αρχεία (cookies) ώστε να μπορούν να σε αναγνωρίζουν όταν θα τις ξαναεπισκεπτείς.
15:15	**Κλικάρεις μια διαφήμιση που έχει ενδιαφέρον** – η διαφημιστική εταιρεία καταγράφει τις προτιμήσεις σου ώστε να μπορεί να σου στέλνει προσφορές για προϊόντα που σε ενδιαφέρουν.
15:30	**Στέλνεις μια ηλεκτρονική κάρτα σε έναν φίλο που έχει γενέθλια** – για την αποστολή της κάρτας πρέπει να συμπληρώσεις μια φόρμα με διάφορα προσωπικά σου στοιχεία και το email σου.
16:00	**Ψάχνεις στοιχεία για την έκθεση που πρέπει να παραδώσεις αύριο** – στο google καταγράφονται όλες οι αναζητήσεις που πραγματοποιείς, μαζί με την χρονική στιγμή της αναζήτησης και τη διεύθυνση δικτύου (IP) με την οποία ο υπολογιστής σου συνδέεται, μέσω του Παρόχου, στο διαδίκτυο.
18:00	**Πηγαίνεις στο γυμναστήριο** – στην είσοδο υπάρχει κάμερα που καταγράφει όσους μπαίνουν και βγαίνουν. Στην υποδοχή «περνάς» την κάρτα μέλους σου από το ειδικό μηχάνημα που την σκανάρει και εμφανίζει τα στοιχεία σου στην οθόνη.
19:00	**Ακούς τα φωνητικά σου μηνύματα στο κινητό** – το τηλέφωνο σου καταγράφει όλους όσους σε κάλεσαν, τους αριθμούς τηλεφώνου τους και τις ώρες κλήσης.
22:00	**Μπαίνεις στο Facebook** – διαβάζεις τι έκαναν σήμερα οι φίλοι σου και γράφεις τα δικά σου νέα. Βλέπεις ότι έχεις γίνει tagged στην σημερινή φωτογραφία που ήδη ανέβασε ο κολλητός σου και κάποιοι έχουν ήδη βάλει σχόλια. Αποδέχεσαι τα friend requests για δύο νέους φίλους, παρόλο που τον έναν δεν το ξέρεις πολύ καλά.

Παράδειγμα

- Η εταιρεία Α, για να προωθήσει τα προϊόντα της, αναθέτει σε μία εταιρεία πληροφορικής Β την ανάπτυξη σχετικής ιστοσελίδας.
- Δυνητικοί πελάτες της εταιρείας Α μπορούν να κάνουν εγγραφή (registration) στην ιστοσελίδα και να ενημερώνονται για νέα προϊόντα ή και να προβαίνουν σε αγορές μέσω Διαδικτύου
- Η πλήρης τεχνική υποστήριξη/συντήρηση της ιστοσελίδας γίνεται από την εταιρεία Β
- Για την περαίωση ηλεκτρονικών αγορών, η εταιρεία Α συνεργάζεται με την εταιρεία Γ η οποία είναι πιστοποιημένος (κατά το πρότυπο PCI/DSS) πάροχος υπηρεσιών ηλεκτρονικών πληρωμών - επεξεργάζεται δεδομένων πιστωτικών καρτών πελατών της Α προκειμένου να ολοκληρωθεί μία πληρωμή.
- Υπεύθυνος επεξεργασίας είναι η εταιρεία Α, ενώ οι εταιρείες Β και Γ είναι εκτελούσες την επεξεργασία
  - Οι πελάτες (χρήστες) είναι υποκείμενα των δεδομένων
- Υπεύθυνος έναντι του νόμου είναι κυρίως ο υπεύθυνος επεξεργασίας (ο οποίος υποχρεούται από το νόμο να επιλέγει κατάλληλους εκτελούντες)

Νομιμότητα Επεξεργασίας Προσωπικών Δεδομένων (άρ. 4 του ν. 2472/1997)

Βασικές αρχές που πρέπει να διέπουν κάθε επεξεργασία προσωπικών δεδομένων

- Αρχή της νομιμότητας (θεμιτή και νόμιμη συλλογή)
  - Τα δεδομένα να συλλέγονται για νόμιμο σκοπό και επίσης κάθε περαιτέρω επεξεργασία να είναι για νόμιμο σκοπό
- Αρχή του σκοπού (επεξεργασία για σαφή και προκαθορισμένο σκοπό)
  - Ο σκοπός πρέπει να είναι σαφής (όχι γενικόλογος) και προκαθορισμένος (να μην αλλάζει εκ των υστέρων)
- Αρχή της αναλογικότητας (συνάφεια, προσφορότητα, αναγκαιότητα των δεδομένων)
  - Δεν πρέπει να συλλέγονται περισσότερα δεδομένα από όσα χρειάζονται!!
- Αρχή της ακρίβειας των δεδομένων
  - Τα δεδομένα να αποτυπώνουν την πραγματικότητα
- Αρχή του καθορισμού της χρονικής διάρκειας της επεξεργασίας
  - τα δεδομένα τηρούνται μόνο για όσο χρόνο χρειάζεται για την επίτευξη του σκοπού της επεξεργασίας

Κάποια παραδείγματα

- Τα προσωπικά δεδομένα πρέπει να συλλέγονται με νόμιμο τρόπο και για νόμιμο σκοπό
  - Π.χ. για προωθητικές ενέργειες (διαφημιστικά sms/mail) πρέπει να λάβουμε με νόμιμο τρόπο τα στοιχεία επικοινωνίας
    - Η αυτοματοποιημένη αναζήτηση διευθύνσεων e-mail από internet, εν όψει του ανωτέρω σκοπού, δεν είναι νόμιμος τρόπος συλλογής
    - Η αγορά/πώληση λιστών για αυτόν το σκοπό δεν είναι νόμιμη
- Τα προσωπικά δεδομένα πρέπει να επεξεργάζονται για τον αρχικό (νόμιμο και σαφή) σκοπό που συνελέγησαν
  - Π.χ. δεδομένα πελατών που συνέλεξε μία επιχείρηση στο πλαίσιο των δραστηριοτήτων της δεν μπορεί να τα χορηγήσει/πουλήσει αλλού
- Αρχή της αναλογικότητας
  - Η επιχείρηση πρέπει να ζητά τα απολύτως απαραίτητα δεδομένα και όχι περισσότερα από τους πελάτες της

Η έννοια της συγκατάθεσης (άρ. 5 του ν. 2472/1997)

- Η επεξεργασία προσωπικών δεδομένων κάποιου επιτρέπεται μόνο όταν αυτός (υποκείμενο των δεδομένων) έχει δώσει τη συγκατάθεσή του (consent) (σαφής, ρητή και ειδική)
- Εξαιρέσεις:
  - Επεξεργασία αναγκαία στο πλαίσιο σύμβασης
  - Επεξεργασία που επιβάλλεται από νόμο (δηλ. ο υπεύθυνος επεξεργασίας υποχρεούται για αυτή βάσει νόμου)
  - Επεξεργασία αναγκαία για τη διαφύλαξη ζωτικών συμφερόντων του υποκειμένου των δεδομένων (π.χ. στο πλαίσιο έκτακτης ανάγκης)
  - Αναγκαία για την εκτέλεση έργου δημοσίου συμφέροντος
  - Απολύτως αναγκαία για την ικανοποίηση έννομου συμφέροντος του υπεύθυνου της επεξεργασίας ή τρίτου, στον οποίο ανακοινώνονται τα δεδομένα, το οποίο (συμφέρον) υπερέχει προφανώς των δικαιωμάτων και συμφερόντων του υποκειμένου
    - Π.χ. διαβίβαση δεδομένων για δικαστική χρήση ή διαβίβαση φακέλου επιτυχόντος σε διαγωνισμό σε συνυποψήφιό του που αμφισβητεί τη μοριοδότηση

Παραδείγματα ως προς τη συγκατάθεση

- Δεν επιτρέπεται να αναρτήσουμε φωτογραφίες ή video τρίτων προσώπων στο Διαδίκτυο χωρίς τη συγκατάθεσή τους
  - Υπάρχουν κάποιες εξαιρέσεις (π.χ. αν η σχετική ανάρτηση είναι περιορισμένη σε κλειστό κύκλο προσώπων, οπότε αυτή η επεξεργασία θα μπορούσε να θεωρηθεί ως οικιακή/προσωπική δραστηριότητα)

- Δεν επιτρέπεται να γίνεται αυτόματη αναγνώριση του προσώπου κάποιου ("tag") σε φωτογραφίες του που αναρτώνται στο Διαδίκτυο, χωρίς τη συγκατάθεσή του

- Μία ιστοσελίδα δεν επιτρέπεται να εγκαθιστά cookies στον υπολογιστή του χρήστη χωρίς τη ρητή συγκατάθεσή του
  - Ακόμα και αν το πρόγραμμα πλοήγησης (browser) είναι ρυθμισμένο έτσι ώστε να δέχεται cookies (που είναι και η τυπική περίπτωση), αυτό δεν θεωρείται ρητή συγκατάθεση!!
  - Μία γενική ενημέρωση (π.χ. με αναδυόμενο παράθυρο), χωρίς δυνατότητα μη αποδοχής των cookies, δεν θεωρείται λήψη συγκατάθεσης
    - Εξαίρεση αποτελούν κάποια cookies που είναι απαραίτητα για ένα session (π.χ. τα session cookie επιτρέπονται χωρίς συγκατάθεση)

Υποχρέωση γνωστοποίησης (άρ. 6 του ν. 2472/1997)

- Ο υπεύθυνος επεξεργασίας, όταν επεξεργάζεται προσωπικά δεδομένα άλλων (όχι των εργαζομένων του), οφείλει να γνωστοποιεί αυτήν την επεξεργασία στην Αρχή Προστασίας Προσωπικών Δεδομένων
  - Ουσιαστικά, αναλόγως με το πού είναι η έδρα του υπεύθυνου επεξεργασίας, εφαρμόζεται το αντίστοιχο εθνικό Δίκαιο και, άρα, ο υπεύθυνος επεξεργασίας οφείλει να γνωστοποιεί την επεξεργασία στην οικεία αρχή Προστασίας Δεδομένων
  - Π.χ. η εταιρεία Facebook έχει, ως προς την Ευρωπαϊκή Ένωση, εγκατάσταση στην Ιρλανδία (και όχι στην Ελλάδα). Παρά το γεγονός ότι επεξεργάζεται και δεδομένα (μεταξύ άλλων) Ελλήνων, οφείλει να υποβάλει γνωστοποίηση στην ιρλανδική Αρχή Προστασίας Προσωπικών Δεδομένων
  - Αντίστροφα, μία επιχείρηση με έδρα στην Ελλάδα οφείλει να γνωστοποιήσει την επεξεργασία στην ελληνική Αρχή Προστασίας Δεδομένων, ακόμα και αν επεξεργάζεται και δεδομένα πολιτών άλλης χώρας
- Η υποχρέωση γνωστοποίησης βαρύνει τον υπεύθυνο επεξεργασίας και όχι τον εκτελούντα

Επεξεργασία ευαίσθητων δεδομένων (άρ. 7 του ν. 2472/1997)

- Απαγορεύεται η συλλογή και επεξεργασία ευαίσθητων δεδομένων
- Κατ' εξαίρεση επιτρέπεται, ύστερα από άδεια της Αρχής Προστασίας Προσωπικών Δεδομένων, εφόσον συντρέχει μία εκ των προϋποθέσεων:
  - Υπάρχει γραπτή συγκατάθεση του υποκειμένου των δεδομένων
  - Η επεξεργασία είναι απαραίτητη για τη διασφάλιση ζωτικού συμφέροντος του υποκειμένου των δεδομένων αν τελεί σε φυσική ή νομική αδυναμία να δώσει συγκατάθεση
  - Αφορά δεδομένα που δημοσιοποιεί το ίδιο το υποκείμενο ή είναι αναγκαία για άσκηση δικαιώματος ενώπιον δικαστηρίου
  - Η επεξεργασία αφορά θέματα υγείας και εκτελείται από πρόσωπο που ασχολείται κατ' επάγγελμα με υπηρεσίες παροχής υπηρεσιών υγείας
  - Η επεξεργασία εκτελείται από δημόσια αρχή (για σκοπούς που προσδιορίζονται ρητά στο συγκεκριμένο άρθρο)
  - Η επεξεργασία πραγματοποιείται για ερευνητικούς και επιστημονικούς σκοπούς
  - Αφορά δεδομένα δημοσίων προσώπων κατά την άσκηση του δημοσιογραφικού επαγγέλματος
- Στην άδεια που εκδίδει η εκάστοτε Αρχή Προστασίας Προσωπικών Δεδομένων, τίθενται συγκεκριμένοι όροι για την επεξεργασία

Διασυνοριακή ροή δεδομένων (άρ. 9 του ν. 2472/1997)

- Η διαβίβαση δεδομένων προσωπικού χαρακτήρα είναι ελεύθερη:
  - προς χώρες-μέλη της Ευρωπαϊκής Ένωσης
  - σε χώρες όπου η Ευρωπαϊκή Επιτροπή έχει κρίνει ότι παρέχεται επαρκές επίπεδο προστασίας (π.χ. Ελβετία)
- Σε διαφορετικές περιπτώσεις, χρειάζεται είτε άδεια της Αρχής είτε να παρέχεται ένα άλλο σύνολο διασφαλίσεων
  - Π.χ. για την περίπτωση διαβίβασης δεδομένων στις Η.Π.Α., μέχρι το 2015 θεωρούνταν ασφαλής η διαβίβαση σε εταιρείες που είχαν προσχωρήσει σε ένα συγκεκριμένο σύνολο κανόνων, με το όνομα «Ασφαλής Λιμένας» (Safe Harbor)
  - Η διαβίβαση δεδομένων σε εταιρεία που είχε προσχωρήσει στο Safe Harbor (διέθετε σχετική πιστοποίηση) ήταν ελεύθερη, με γνωστοποίηση της διαβίβασης στην οικεία Αρχή Προστασίας Δεδομένων
    - Αυτό όμως έχει πια αλλάξει….

Διασυνοριακή ροή δεδομένων (άρ. 9 του ν. 2472/1997)- συνέχεια

- Με την Απόφαση C-362/14 του ΔΕΕ (Δικαστηρίου Ευρωπαϊκής Ένωσης), η διαβίβαση προσωπικών δεδομένων πολιτών της ΕΕ σε εταιρεία της Αμερικής που έχει προσχωρήσει στον «Ασφαλή Λιμένα» δεν είναι ασφαλής
  - Η υπόθεση εκκίνησε με σχετική αγωγή του Maximillian Schrems, υπό το πρίσμα των αποκαλύψεων του Snowden για παρακολουθήσεις των Μυστικών Υπηρεσιών των ΗΠΑ
- Πλέον, από 01-08-2016, υπάρχει νέο σύνολο κανόνων – «Ασπίδα Ασφαλείας» (Privacy Shield) για διαβιβάσεις στις Η.Π.Α.
  - Η διαβίβαση είναι ελεύθερη, εφόσον η εταιρεία έχει λάβει αυτήν την πιστοποίηση
  - (βλ. https://www.privacyshield.gov/welcome για σχετικό υλικό, με λίστα και των εταιρειών που έχουν λάβει σχετική πιστοποίηση)

Tweet του Edward Snowden μετά την έκδοση της Απόφασης του ΔΕΕ
(πηγή: http://www.blogmedien.de/?p=1087)

Ασφάλεια της επεξεργασίας (άρ. 10 του ν. 2472/1997)

- Απόρρητο/ασφάλεια της επεξεργασίας
  - Η επεξεργασία δεδομένων είναι απόρρητη – διεξάγεται από πρόσωπα που τελούν υπό έλεγχο του υπεύθυνου ή του εκτελούντος την επεξεργασία
  - Για τη διεξαγωγή της επεξεργασίας ο υπεύθυνος επεξεργασίας οφείλει να επιλέγει πρόσωπα με αντίστοιχα επαγγελματικά προσόντα που παρέχουν επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου.
  - Ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει τεχνικά και οργανωτικά μέτρα για την προστασία από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση σε δεδομένα.
    - Τα μέτρα πρέπει να εξασφαλίζουν επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία
  - Τα ανωτέρω ισχύουν και για τον εκτελούντα την επεξεργασία
    - Η μοναδική περίπτωση όπου ο τρέχων νόμος αναγνωρίζει ρητές υποχρεώσεις και στον εκτελούντα την επεξεργασία (ο τομέας της ασφάλειας)
  - Η σχετική ανάθεση στον εκτελούντα πρέπει να γίνεται εγγράφως

Τα Δικαιώματά μας (άρ 11-13 του ν. 2472/1997)

- Υποχρέωση ενημέρωσης
  - Ο υπεύθυνος επεξεργασίας υποχρεούται να ενημερώνει το υποκείμενο των δεδομένων περί της ταυτότητάς του, του σκοπού και του είδους της επεξεργασίας και των δεδομένων, καθώς και των αποδεκτών αυτών
- Δικαίωμα πρόσβασης
  - Κάθε υποκείμενο των δεδομένων έχει δικαίωμα να γνωρίζει αν τα προσωπικά του δεδομένα αποτέλεσαν ή αποτελούν αντικείμενο επεξεργασίας (ποια δεδομένα, είδος επεξεργασίας, σκοπός κτλ.)
- Δικαίωμα αντίρρησης
  - Κάθε υποκείμενο των δεδομένων έχει δικαίωμα να προβάλλει οποτεδήποτε αντιρρήσεις για την επεξεργασία προσωπικών του δεδομένων

- Τα δικαιώματά μας ως πολίτες => υποχρεώσεις μας ως υπεύθυνοι επεξεργασίας
  - Οι υπεύθυνοι επεξεργασίας οφείλουν να παρέχουν ενημέρωση και να εξετάζουν/ικανοποιούν τα δικαιώματα πρόσβασης και αντίρρησης εντός 15 ημερών από την υποβολή τους

Η άσκηση των δικαιωμάτων στην πράξη

- Ο υπεύθυνος επεξεργασίας οφείλει πάντα να ενημερώνει τους χρήστες για την επεξεργασία των προσωπικών τους δεδομένων
  - Είδος δεδομένων, είδος επεξεργασίας, σκοπός, αποδέκτες
- Διαβάζουμε πάντα τους όρους χρήσης στα διάφορα sites
- Έχουμε το δικαίωμα να ρωτήσουμε ό,τι θέλουμε σχετικά με τα προσωπικά μας δεδομένα που υφίστανται επεξεργασία
  - Οφείλουμε, βάσει του νόμου, να λάβουμε σαφή απάντηση εντός 15 ημερών
- Έχουμε το δικαίωμα να ζητήσουμε διαγραφή προσωπικών μας δεδομένων
  - Με εξαίρεση ειδικές περιπτώσεις, ο υπεύθυνος επεξεργασίας οφείλει, βάσει νόμου, να το ικανοποιήσει εντός 15 ημερών

Προσωπικά δεδομένα και ιδιωτικότητα

- Επανερχόμαστε στο αρχικό ερώτημα: Ποια η σχέση προσωπικών δεδομένων και ιδιωτικότητας;
- Η προστασία προσωπικών δεδομένων είναι κατά μία έννοια ευρύτερη, διότι:
  - Καλύπτει κάθε είδους προσωπικά δεδομένα, όχι μόνο τα «σημαντικά»
    - Άλλωστε, ένα «μη σημαντικό» προσωπικό δεδομένο μπορεί, υπό συνθήκες να καταστεί σημαντικό
  - Καλύπτει και ένα είδος δικαιωμάτων και υποχρεώσεων (δικαίωμα πρόσβασης, υποχρέωση ενημέρωσης κτλ.)
- Είναι όμως ταυτόχρονα και ειδικότερη της ιδιωτικότητας, καθώς η τελευταία καλύπτει και θέματα όπως το δικαίωμα στη μοναξιά κτλ. (τα οποία δεν έχουν να κάνουν με προστασία προσωπικών δεδομένων)

Προσωπικά δεδομένα στις ηλεκτρονικές επικοινωνίες

- 2002: Οδηγία 2002/58/ΕΚ (e-Privacy Directive) για την προστασία των φυσικών προσώπων από την επεξεργασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών (Ευρωπαϊκό Συμβούλιο και Κοινοβούλιο)
  - Όλα τα κράτη μέλη έχουν ήδη συμμορφωθεί.
  - Στην Ελλάδα: Νόμος 3471/2006
  - 2009: Οδηγία 2009/136/ΕΚ που τροποποιεί την 2002/58/ΕΚ
    - Στην Ελλάδα: Νόμος 4070/2012

- Κατ' αναλογία με την Οδηγία 95/46/ΕΚ, η οποία αντικαθίσταται στις 25 Μαΐου 2018 από τον νέο Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων, είναι υπό διαμόρφωση νέος Κανονισμός στην ΕΕ (e-Privacy Regulation) για να αντικαταστήσει την Οδηγία 2002/58/ΕΚ

Προσωπικά δεδομένα στον τομέα ηλεκτρονικών επικοινωνιών

Ν. 3471/2006 και τροποποίησή του με το ν. 4070/2012

- Δεδομένα θέσης:
  - Δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών ή από υπηρεσία ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών.
- Δεδομένα κίνησης:
  - Δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μίας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσής της.
- Παραβίαση δεδομένων προσωπικού χαρακτήρα:
  - Παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη διάδοση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάσθηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατά οιονδήποτε άλλο τρόπο σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών

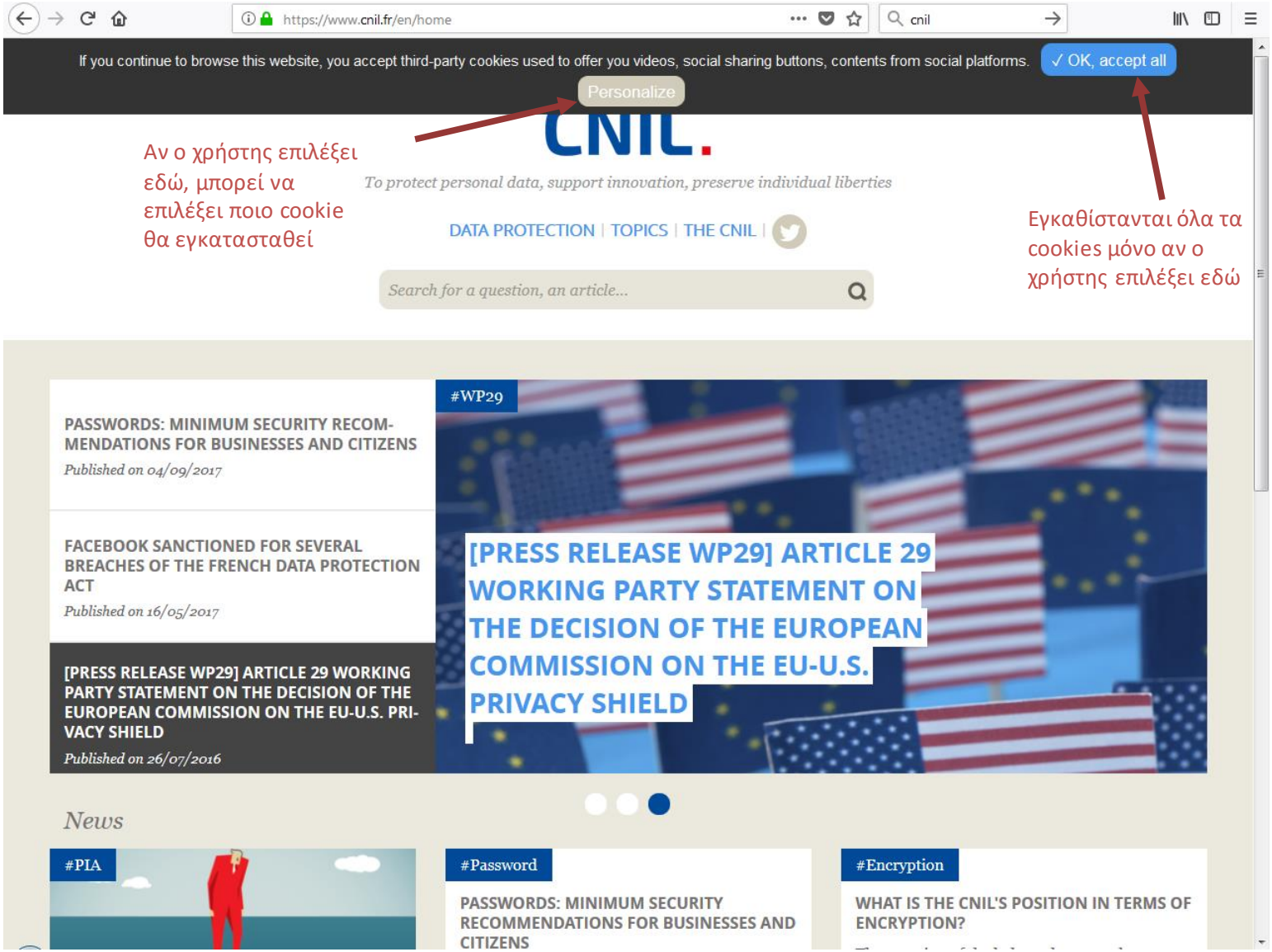
Προσωπικά δεδομένα στον τομέα ηλεκτρονικών επικοινωνιών

- Άρθρο 4 του ν. 3471/2006:
  - Οποιαδήποτε χρήση των υπηρεσιών ηλεκτρονικών επικοινωνιών που παρέχονται μέσω δημοσίου δικτύου επικοινωνιών, καθώς και των συναφών δεδομένων κίνησης και θέσης, προστατεύεται από το απόρρητο των επικοινωνιών
    - Η άρση αυτού επιτρέπεται μόνο υπό τους όρους και διαδικασίες που προβλέπονται από το άρθρο 19 Συντ.
  - Απαγορεύεται η ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των ηλεκτρονικών επικοινωνιών και των συναφών δεδομένων κίνησης και θέσης
  - Επιτρέπεται η καταγραφή συνδιαλέξεων και των συναφών δεδομένων κίνησης μόνο κατά τη διάρκεια νόμιμης επαγγελματικής πρακτικής
  - Η αποθήκευση πληροφοριών ή η απόκτηση πρόσβασης στον τερματικό εξοπλισμό χρήστη επιτρέπεται μόνο αν ο τελευταίος έχει δώσει τη συγκατάθεσή του μετά από σαφή και εκτενή ενημέρωση (όπως τροποποιήθηκε στο ν. 4070/2012)
    - Παράδειγμα: cookies

Η περίπτωση των cookies

- 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»)
- Ο πάροχος της υπηρεσίας (site) πρέπει να παρέχει ενημέρωση για αυτήν την εγκατάσταση των cookies
- Για άλλες περιπτώσεις cookies, πρέπει να υπάρχει ρητή συγκατάθεση του χρήστη
  - Π.χ. Cookies για έλεγχο επισκεψιμότητας site, cookies για σκοπό την προβολή (στοχευμένων ή μη) διαφημιστικών μηνυμάτων κτλ.
- 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



Αν ο χρήστης δεν κάνει καμία ενέργεια, δεν εγκαθίσταται κανένα cookie (περίπτωση «opt-in» συγκατάθεσης)

Δικαιώματα χρηστών - Μη ζητηθείσα επικοινωνία

- Άρθρο 11 του ν. 3471/2006
  - Η πραγματοποίηση μη ζητηθεισών επικοινωνιών με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας, χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών και για κάθε είδους διαφημιστικούς σκοπούς, επιτρέπεται μόνο αν ο συνδρομητής συγκατατεθεί εκ των προτέρων ρητώς (opt-in).
  - Δεν επιτρέπεται η πραγματοποίηση κλήσεων για τους ανωτέρω σκοπούς, εφόσον ο συνδρομητής έχει δηλώσει προς το φορέα της διαθέσιμης στο κοινό υπηρεσίας ότι δεν επιθυμεί γενικώς να δέχεται τέτοιες κλήσεις (opt-out) (όπως τροποποιήθηκε στο ν. 3917/2011)
  - Τα στοιχεία επαφής ηλεκτρονικού ταχυδρομείου που αποκτήθηκαν νομίμως, στο πλαίσιο της πώλησης προϊόντων ή υπηρεσιών ή άλλης συναλλαγής, μπορούν να χρησιμοποιούνται για την απευθείας προώθηση παρόμοιων προϊόντων ή υπηρεσιών του προμηθευτή, ακόμα και χωρίς την προηγούμενη συγκατάθεση (opt-out), υπό την προϋπόθεση ότι παρέχεται η δυνατότητα να αντιτάσσεται, με εύκολο και δωρεάν τρόπο, για μελλοντική επεξεργασία.

Ανεπιθύμητη αλληλογραφία - Spam

- Δεν επιτρέπεται να σας στείλει κάποιος διαφημιστικό e-mail χωρίς να έχετε δώσει τη συγκατάθεσή σας
  - Μόνη εξαίρεση είναι αν είχατε προηγούμενη συναλλακτική επαφή μαζί του
  - Και σε αυτήν την περίπτωση ωστόσο, πρέπει να σας παρέχει τη δυνατότητα να εκφράσετε με τρόπο εύκολο και δωρεάν την αντίθεσή σας
    - Π.χ. πατώντας σχετικό link….

- Προσοχή! Ακόμα και αν έχετε αναρτήσει την ηλεκτρονική σας διεύθυνση στο Internet (π.χ. σε κάποιο προσωπικό σας web site), οπότε και είναι δημόσια προσβάσιμη, πάλι δεν μπορεί κάποιος να τη χρησιμοποιήσει για να σας στείλει διαφημιστικό υλικό εάν δεν έχετε δώσει τη συγκατάθεσή σας!

Ηλεκτρονικές επικοινωνίες - Ασφάλεια επεξεργασίας και διαχείριση περιστατικών παραβίασης

- Άρθρο 12 του ν. 3471/2006 (όπως τροποποιήθηκε στο ν. 4070/2012)
  - Ο τηλεπικοινωνιακός πάροχος οφείλει να λαμβάνει τα κατάλληλα μέτρα για την ασφάλεια ώστε να εξασφαλίζει κατ' ελάχιστο τα εξής:
    - Πρόσβαση σε προσωπικά δεδομένα έχει μόνο εξουσιοδοτημένο προσωπικό για νομίμως εγκεκριμένους σκοπούς
    - Προστασία προσωπικών δεδομένων (από καταστροφή, απώλεια κτλ.)
    - Εφαρμογή πολιτικής ασφάλειας
  - Σε περίπτωσης παραβίασης προσωπικών δεδομένων, ο πάροχος γνωστοποιεί αμελλητί την παραβίαση στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και στην Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών
  - Όταν η παραβίαση ενδέχεται να έχει δυσμενείς επιπτώσεις στο συνδρομητή ή σε άλλο άτομο, ο πάροχος ενημερώνει αμελλητί και το θιγόμενο άτομο.
    - Η ενημέρωση δεν είναι αναγκαία αν έχει εφαρμόσει τα κατάλληλα τεχνολογικά μέτρα – ασφαλή κρυπτογράφηση των δεδομένων
  - Τήρηση αρχείου περιστατικών παραβίασης (με αναλυτική περιγραφή αυτών)

Για την ώρα, αυτήν την υποχρέωση την έχουν μόνο οι πάροχοι τηλεπικοινωνιακών υπηρεσιών (όχι οι άλλες κατηγορίες υπευθύνων επεξεργασίας)

Τι ισχύει σχετικά με περιστατικά παραβίασης προσωπικών δεδομένων;

- Παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή απώλεια, αλλοίωση, μη εξουσιοδοτημένη διάδοση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάσθηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατά οιονδήποτε άλλο τρόπο σε επεξεργασία
- Στην Ελλάδα: (μετά τον πρόσφατο νόμο 4070/2012): Ειδικά κριτήρια έχουν τεθεί στον τομέα των ηλεκτρονικών επικοινωνιών αναφορικά με περιστατικό παραβίασης προσωπικών δεδομένων
  - Σε περίπτωσης παραβίασης προσωπικών δεδομένων, ο πάροχος τηλεπικοινωνιακών υπηρεσιών γνωστοποιεί αμελλητί την παραβίαση στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και στην Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών
  - Όταν η παραβίαση ενδέχεται να έχει δυσμενείς επιπτώσεις στο συνδρομητή ή σε άλλο άτομο, ο πάροχος ενημερώνει αμελλητί και το θιγόμενο άτομο.
    - Η ενημέρωση δεν είναι αναγκαία αν έχει εφαρμόσει τα κατάλληλα τεχνολογικά μέτρα, όπως ασφαλή κρυπτογράφηση των δεδομένων
  - Τήρηση αρχείου περιστατικών παραβίασης (με αναλυτική περιγραφή αυτών)

Για την ώρα, αυτήν την υποχρέωση την έχουν μόνο οι πάροχοι τηλεπικοινωνιακών υπηρεσιών (όχι οι άλλες κατηγορίες υπευθύνων επεξεργασίας)

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

- Στην Ελλάδα: Ανεξάρτητη Αρχή κατοχυρωμένη και στο Σύνταγμα (9 Α και 101 Α)
- Αρμοδιότητες
  - Ελεγκτικές
    - Εξέταση προσφυγών/καταγγελιών
    - Διενέργεια διοικητικών ελέγχων
    - Χορήγηση αδειών επεξεργασίας ευαίσθητων προσωπικών δεδομένων
    - Εποπτεία Συστημάτων (Σένγκεν, VIS, Eurodac)
  - Ρυθμιστικές
    - Έκδοση κανονιστικών πράξεων/οδηγιών
    - Έκδοση γνωμοδοτήσεων για κάθε ρύθμιση που αφορά την επεξεργασία και προστασία προσωπικών δεδομένων
    - Έκδοση συστάσεων και υποδείξεων προς τους υπεύθυνους επεξεργασίας
    - Συνεργασία με τις αρχές άλλων κρατών μελών της ΕΕ

Ενδεικτικές αποφάσεις της ελληνικής Αρχής

- Υποθέσεις διαγραφής αποτελεσμάτων από τη μηχανή αναζήτησης Google (“δικαίωμα στη λήθη») – (Αποφάσεις 82, 83 και 84/2016)
- Περιστατικό διαρροής προσωπικών δεδομένων από σύστημα ηλεκτρονικών κρατήσεων ξενοδοχείου (Απόφαση 85/2015)
- Περιστατικό διαρροής προσωπικών δεδομένων από διαδικτυακή υπηρεσία φορέα ασφάλισης (Απόφαση 57/2014)
- Ασφάλεια του Συστήματος Ηλεκτρονικής Συνταγογράφησης (Απόφαση 138/2013)
- Επεξεργασία δεδομένων πιστωτικών καρτών για αγορές μέσω Διαδικτύου (Απόφαση 100/2013)
- Διαρροή δεδομένων φορολογουμένων – επιβολή προστίμου στη Γ.Γ.Π.Σ. (Απόφαση 98/2013)
- Υπόθεση διαρροής προσωπικών δεδομένων από το ελληνικό site της εταιρείας Sony Music (Απόφαση 59/2012))

Ενδεικτικές γνωμοδοτήσεις της ελληνικής Αρχής

- Ηλεκτρονικό εισιτήριο σε ΜΜΜ (Γνωμοδοτήσεις 1/2017 και 4/2017)
- Λειτουργία συστήματος ηλεκτρονικού φακέλου υγείας (Γνωμοδότηση 2/2015)
- Διαβατήρια: μεταγραφή του ονόματος με λατινικούς χαρακτήρες (Γνωμοδότηση 1/2013)
- Ηλεκτρονική κάρτα αποδείξεων / φοροκάρτα (Γνωμοδότηση 4/2010)
- Ανάρτηση νόμων, κανονιστικών και ατομικών πράξεων στο διαδίκτυο – Πρόγραμμα «Διαύγεια» (Γνωμοδότηση 1/2010)

Ενδεικτικές οδηγίες της ελληνικής Αρχής

- Ηλεκτρονική συγκατάθεση (Οδηγία 2/2011)
- Χρήση συστημάτων βιντεοεπιτήρησης για την προστασία προσώπων και αγαθών (Οδηγία 1/2011)
- Επεξεργασία προσωπικών δεδομένων για το σκοπό της πολιτικής επικοινωνίας (Οδηγία 1/2010)
- Ασφαλής καταστροφή προσωπικών δεδομένων μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού επεξεργασίας (Οδηγία 1/2005).
- Επεξεργασία προσωπικών δεδομένων των εργαζομένων (Οδηγία 115/2001)

Ευρωπαϊκό επίπεδο – Ομάδα Εργασίας του άρθρου 29

- Συστάθηκε με την Οδηγία 95/46/ΕΚ (στο άρ. 29 αυτής)
- Εκδίδει γνώμες σχετικά με διάφορα ζητήματα που άπτονται της προστασίας προσωπικών δεδομένων
- Αποτελείται από εκπροσώπους των Αρχών Προστασίας Δεδομένων όλων των Κρατών Μελών
- Ενδεικτικές γνώμες της Ο.Ε. 29:
  - Υπηρεσίες κοινωνικής δικτύωσης (5/2009)
  - Πλαίσιο εκπόνησης εκτιμήσεων των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων για τις εφαρμογές RFID (9/2011)
  - Βέλτιστες πρακτικές για τη διαφήμιση βάσει συμπεριφοράς (behavioral advertising) (16/2011)
  - Επεξεργασία προσωπικών δεδομένων με σύγχρονες βιομετρικές τεχνολογίες (3/2012 και η συναφής 2/2012)
  - Προστασία προσωπικών δεδομένων στο υπολογιστικό νέφος (cloud computing) (4/2012)
  - Εφαρμογές σε «έξυπνες» συσκευές (2/2013)
  - Τεχνικές ανωνυμοποίησης (5/2014)
  - Πρόσφατες εξελίξεις στο Internet of Things (8/2014)

Στο προσεχές μέλλον…

- Νέος Κανονισμός (ΕΕ) 679/2016 του Ευρωπαϊκού Κοινοβουλίου σε θέματα προστασίας των ατόμων για την επεξεργασία προσωπικών δεδομένων = General Data Protection Regulation (GDPR) (αντικατάσταση της Οδηγίας 95/46/ΕΚ)
  - Ενίσχυση της προστασίας προσωπικών δεδομένων
  - Εναρμόνιση βασικών κανόνων
    - Οι ίδιοι κανόνες θα ισχύουν σε όλα τα Κράτη Μέλη
  - Άμεση εφαρμογή σε όλα τα Κράτη Μέλη από τις 25 Μαΐου 2018
  - Νέες υποχρεώσεις για τους υπευθύνους επεξεργασίας
  - Ενίσχυση των δικαιωμάτων των πολιτών

- Ο GDPR αναμένεται να επιφέρει πολλές αλλαγές στη λειτουργία οργανισμών, που ήδη έχουν ξεκινήσει διαδικασίες για να είναι πλήρως συμμορφούμενοι με αυτόν

Τι συνεπάγεται ο GDPR;

- Δεν χρειάζεται εθνική νομοθεσία – θα έχει άμεση εφαρμογή
  - Άρα: μεγαλύτερος βαθμός εναρμόνισης μεταξύ των Κρατών Μελών (αφού με την Οδηγία 95/46/ΕΚ υπήρχε δυνατότητα διαφοροποίησης σε διάφορα σημεία της νομοθεσίας για το Κράτος Μέλος)
  - Έχει επίδραση και σε περιπτώσεις επεξεργασίας προσωπικών δεδομένων και εκτός Ευρωπαϊκής Ένωσης
    - Ο παρών κανονισμός εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των δραστηριοτήτων μιας εγκατάστασης ενός υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση, ανεξάρτητα από το κατά πόσο η επεξεργασία πραγματοποιείται εντός της Ένωσης.
    - Ο παρών κανονισμός εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα για τα οποία τα υποκείμενα που βρίσκονται στην Ένωση από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία ο οποίος δεν είναι εγκατεστημένος στην Ένωση, εάν οι δραστηριότητες επεξεργασίας σχετίζονται με:
      - την προσφορά αγαθών ή υπηρεσιών προς τα εν λόγω υποκείμενα των δεδομένων που βρίσκονται στην Ένωση, ανεξαρτήτως εάν απαιτείται πληρωμή από τα υποκείμενα των δεδομένων, ή
      - την παρακολούθηση της συμπεριφοράς τους, στον βαθμό που η συμπεριφορά αυτή λαμβάνει χώρα εντός της Ένωσης.
  - Άρα: εφαρμόζονται οι κανόνες προστασίας προσωπικών δεδομένων ακόμα και αν ο υπεύθυνος επεξεργασίας δεν έχει εγκατάσταση στην Ευρωπαϊκή Ένωση (κάτι που δεν ισχύει σήμερα)

Κυρώσεις

- Η Οδηγία 95/46/ΕΚ δεν «επέβαλλε» τις κυρώσεις που μπορούν να επιβληθούν (π.χ. ύψη προστίμου) για παραβιάσεις προσωπικών δεδομένων – εναπόκεινται στο κάθε Κράτος Μέλος
  - Στην Ελλάδα, το μέγιστο δυνατό ύψος προστίμου που προβλέπεται στο ν. 2472/1997 είναι 150.000 €
- Με τον GDPR τα πρόστιμα που δύνανται να επιβληθούν για παραβάσεις προβλέπονται πλέον στον Κανονισμό (αρ. 83) και όχι στην εκάστοτε εθνική νομοθεσία
  - Τίθενται σαφή κριτήρια αξιολόγησης του «μεγέθους» της παράβασης (φύση, βαρύτητα και η διάρκεια της παράβασης, ο δόλος ή η αμέλεια που την προκάλεσαν, οι ενέργειες του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασίας για να μετριάσει τη ζημία, τυχόν σχετικές προηγούμενες παραβάσεις κτλ.)
  - Οι παραβάσεις επισύρουν διοικητικά πρόστιμα έως 10.000.000 € ή, σε περίπτωση επιχειρήσεων, έως το 2 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο
- Στον GDPR ισχύουν για τον εκτελούντα της επεξεργασία «περίπου οι ίδιες» υποχρεώσεις με τον υπεύθυνο επεξεργασίας (όχι μόνο για την ασφάλεια της επεξεργασίας)
  - Άρα, υπάρχει πλέον δυνατότητα επιβολής προστίμου από την οικεία Αρχή Προστασίας Δεδομένων και σε εκτελούντα την επεξεργασία

Ανώνυμα και ψευδωνυμοποιημένα δεδομένα

Κανονισμός (ΕΕ) 2016/679 (GDPR)

- Οι αρχές της προστασίας δεν θα πρέπει να εφαρμόζονται σε ανώνυμες πληροφορίες, δηλ. πληροφορίες που δεν σχετίζονται προς ταυτοποιημένο ή ταυτοποιήσιμο πρόσωπο ή σε δεδομένα που έχουν καταστεί ανώνυμα κατά τρόπο ώστε η ταυτότητα του υποκειμένου να μην μπορεί να εξακριβωθεί

- Τα δεδομένα προσωπικού χαρακτήρα που έχουν υποστεί ψευδωνυμοποίηση, η οποία θα μπορούσε να αποδοθεί σε φυσικό πρόσωπο με τη χρήση συμπληρωματικών πληροφοριών, θα πρέπει να θεωρούνται πληροφορίες σχετικά με ταυτοποιήσιμο φυσικό πρόσωπο.

- Για να κριθεί κατά πόσον ένα φυσικό πρόσωπο είναι ταυτοποιήσιμο, θα πρέπει να λαμβάνονται υπόψη όλα τα μέσα τα οποία είναι ευλόγως πιθανό ότι θα χρησιμοποιηθούν, όπως για παράδειγμα ο διαχωρισμός του (singling out), είτε από τον υπεύθυνο επεξεργασίας είτε από τρίτο για την άμεση ή έμμεση εξακρίβωση της ταυτότητας του φυσικού προσώπου.

- Για να διαπιστωθεί κατά πόσον κάποια μέσα είναι ευλόγως πιθανό ότι θα χρησιμοποιηθούν για την εξακρίβωση της ταυτότητας του φυσικού προσώπου, θα πρέπει να λαμβάνονται υπόψη όλοι οι αντικειμενικοί παράγοντες, όπως τα έξοδα και ο χρόνος που απαιτούνται για την ταυτοποίηση, λαμβανομένων υπόψη της τεχνολογίας που είναι διαθέσιμη κατά τον χρόνο της επεξεργασίας και των εξελίξεων της τεχνολογίας.

Η έννοια της ψευδωνυμοποίησης

- Ο GDPR ορίζει σαφώς την έννοια της ψευδωνυμοποίησης:
  - η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο
- Ο GDPR ορίζει σαφώς ότι η ψευδωνυμοποίηση δεν είναι ανωνυμοποίηση και, άρα, τα ψευδωνυμοποιημένα δεδομένα πρέπει να θεωρούνται προσωπικά δεδομένα.
- Ο GDPR «προκρίνει» την ψευδωνυμοποίηση ως μέτρο ασφάλειας που πρέπει να ληφθεί υπόψη κατά τη σχεδίαση των χαρακτηριστικών της επεξεργασίας

Νέα στοιχεία του GDPR – Ευαίσθητα δεδομένα

- Τα ευαίσθητα δεδομένα («προσωπικά δεδομένα ειδικών κατηγοριών») (special categories of personal data) περιγράφονται στο άρθρο 9
- Σε αυτά υπάγονται και κάποιες νέες κατηγορίες δεδομένων, οι οποίες δεν είχαν χαρακτηριστεί ως ευαίσθητα στην Οδηγία 95/46/ΕΚ

1. Τα γενετικά δεδομένα
   - τα δεδομένα προσωπικού χαρακτήρα που αφορούν τα γενετικά χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν, όπως προκύπτουν, ιδίως, από ανάλυση βιολογικού δείγματος του εν λόγω φυσικού προσώπου και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με την φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου (άρθρο 4)
     - Π.χ. δεδομένα που προκύπτουν από ανάλυση DNA, RNA κτλ.
2. Τα βιομετρικά δεδομένα
   - δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα (άρθρο 4)

- Τόσο για τα γενετικά, όσο και για τα βιομετρικά δεδομένα, αλλά και για τα δεδομένα υγείας, ο GDPR αφήνει στα κράτη Μέλη περιθώρια να θέσουν και άλλους περιορισμούς - πέραν των όσων αναφέρει ο GDPR - για την επεξεργασία τους

Νέα στοιχεία του GDPR – Συγκατάθεση ανηλίκων

- Στον GDPR τίθενται σαφείς προϋποθέσεις για τη συγκατάθεση παιδιού σε σχέση με τις υπηρεσίες της κοινωνίας των πληροφοριών
- Εφόσον η νομιμότητα της επεξεργασία προσωπικών δεδομένων βασίζεται στη συγκατάθεση του χρήστη, τότε αν πρόκειται για συγκατάθεση παιδιού θα πρέπει αυτό να είναι τουλάχιστον 16 χρονών (άρ. 8 του GDPR).
  - Εάν το παιδί είναι ηλικίας κάτω των 16 ετών, η επεξεργασία αυτή είναι σύννομη μόνο εάν και στον βαθμό που η εν λόγω συγκατάθεση παρέχεται ή εγκρίνεται από το πρόσωπο που έχει τη γονική μέριμνα του παιδιού
  - Ο υπεύθυνος επεξεργασίας οφείλει να καταβάλλει εύλογες προσπάθειες για να επαληθεύσει στις περιπτώσεις αυτές ότι η συγκατάθεση παρέχεται ή εγκρίνεται από το πρόσωπο που έχει τη γονική μέριμνα του παιδιού, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία.
- Τα κράτη μέλη δύνανται να προβλέπουν διά νόμου μικρότερη ηλικία, υπό την προϋπόθεση ότι η εν λόγω μικρότερη ηλικία δεν είναι κάτω από τα 13 έτη.

Νέα στοιχεία του GDPR – Δικαίωμα στη λήθη

- Άρθρο 17: Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση και ο υπεύθυνος επεξεργασίας υποχρεούται να τα διαγράψει χωρίς αδικαιολόγητη καθυστέρηση (εφόσον πληρούται σύνολο προϋποθέσεων)

- Όταν ο υπεύθυνος επεξεργασίας έχει δημοσιοποιήσει δεδομένα προσωπικού χαρακτήρα και υποχρεούται να τα διαγράψει, τότε, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία και το κόστος εφαρμογής, εφαρμόζει εύλογα μέτρα, συμπεριλαμβανομένων των τεχνικών μέτρων, για να ενημερώσει τους λοιπούς υπευθύνους επεξεργασίας των παραπάνω δεδομένων ότι το υποκείμενο των δεδομένων ζήτησε τη διαγραφή και από αυτούς τους υπευθύνους επεξεργασίας των τυχόν συνδέσμων προς τα δεδομένα αυτά ή αντιγράφων ή αναπαραγωγών των εν λόγω δεδομένων προσωπικού χαρακτήρα.

- => Με άλλα λόγια, αν ένας οργανισμός έχει δημοσιοποιήσει (νομίμως) προσωπικά δεδομένα και το υποκείμενο των δεδομένων ασκεί σε αυτόν το δικαίωμα στη λήθη, τότε ο οργανισμός οφείλει να φροντίσει να ενημερώσει όσους αναπαρήγαγαν τη δημοσιοποίηση/ανάρτηση ότι πρέπει επίσης να τα διαγράψουν

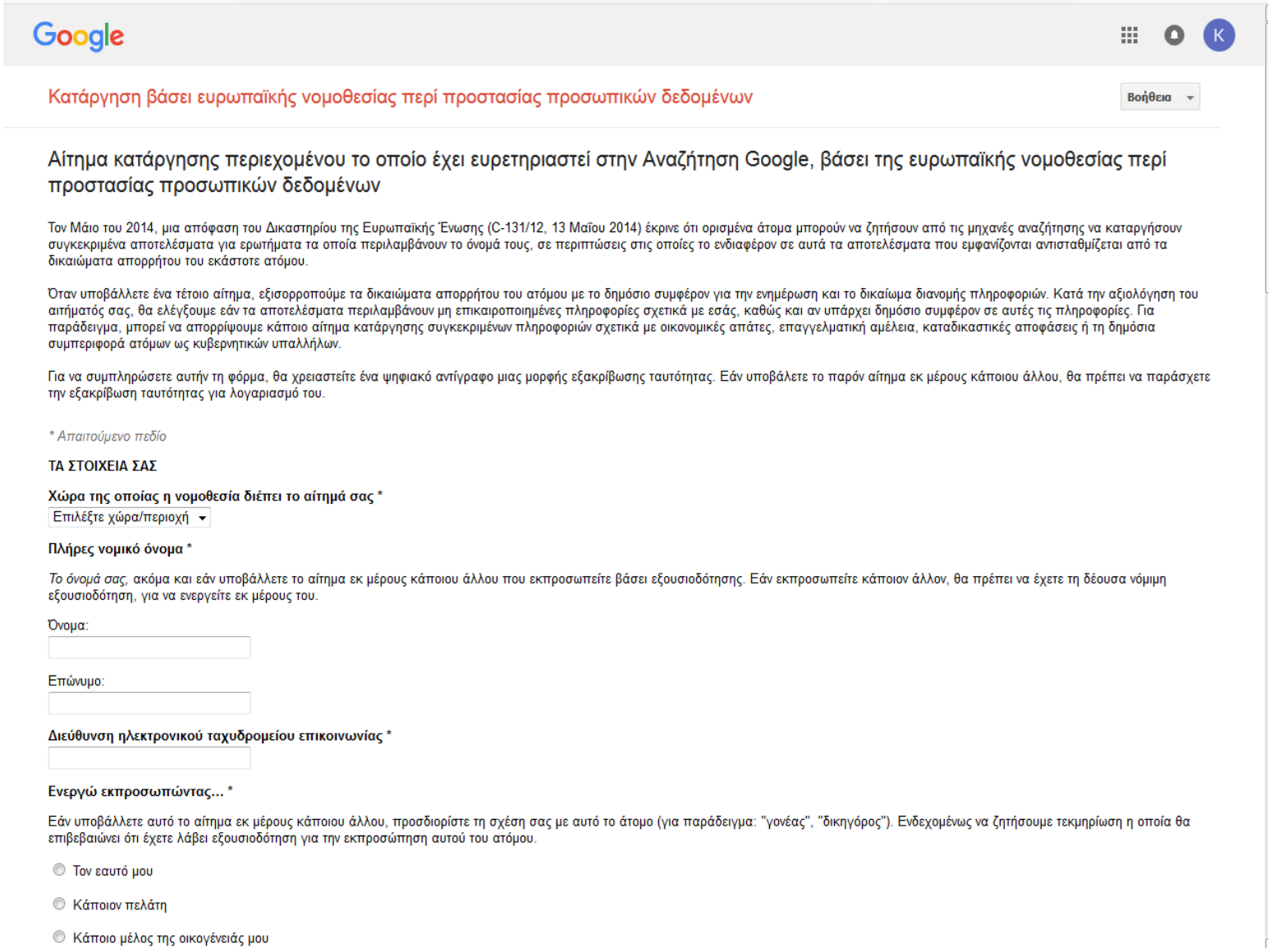
Νέα στοιχεία του GDPR – Δικαίωμα στη λήθη (2)

- Με άλλα λόγια, ο GDPR ενισχύει το δικαίωμα των πολιτών να ζητήσουν διαγραφή των δεδομένων τους, ιδίως δε σε περιπτώσεις αναρτήσεων / δημοσιοποιήσεων
  - Προβλέπονται ωστόσο στο άρθρο 17 και κάποιες εξαιρέσεις για τις οποίες ο υπεύθυνος επεξεργασίας δεν υποχρεούται να ικανοποιήσει το δικαίωμα στη λήθη (π.χ. για σκοπούς δημοσιοποίησης για το δημόσιο συμφέρον)
- Είναι πιο ισχυρό από το δικαίωμα αντίρρησης που ισχύει σήμερα (και το οποίο παραμένει και με τον GDPR)
- Το δικαίωμα στη λήθη θέτει λοιπόν νέες υποχρεώσεις σε συγκεκριμένες κατηγορίες υπευθύνων επεξεργασίας

Δικαίωμα στη λήθη σήμερα

- Δικαστήριο Ευρωπαϊκής Ένωσης – 2014
  - Υπόθεση Costeja:
    - Όταν, κατόπιν αναζήτησης που έχει πραγματοποιηθεί με βάση το ονοματεπώνυμο ενός προσώπου, εμφανίζεται στον κατάλογο αποτελεσμάτων σύνδεσμος προς ιστοσελίδα που περιέχει πληροφορίες για το εν λόγω πρόσωπο, αυτό μπορεί να αποτανθεί απευθείας στον φορέα εκμετάλλευσης της μηχανής αναζήτησης ή, εφόσον ο τελευταίος δεν ανταποκριθεί στην αίτηση του προαναφερθέντος προσώπου, στις αρμόδιες αρχές προστασίας δεδομένων προκειμένου να επιτύχει, υπό ορισμένες προϋποθέσεις, τη διαγραφή του επίμαχου συνδέσμου από τον κατάλογο αποτελεσμάτων
  - Όποιος επιθυμεί, ζητάει από μια μηχανή αναζήτησης να μην συμπεριλαμβάνει στα αποτελέσματα που επιστρέφει έγγραφές που αφορούν το συγκεκριμένο πρόσωπο
  - Η μηχανή αναζήτησης εξετάζει και είτε κάνει δεκτό το αίτημα είτε αιτιολογεί την άρνησή της
    - Εάν αρνηθεί, υπάρχει δικαίωμα προσφυγής στην οικεία Αρχή Προστασίας Δεδομένων
    - Πλήθος κριτηρίων εξετάζονται ως προς το αν πρέπει πράγματι να υπάρξει διαγραφή
  - Πολλά θέματα ακόμη ανοικτά:
    - Π.χ. εξαίρεση από τα αποτελέσματα της μηχανής google.gr συνεπάγεται αυτόματη εξαίρεση και από τη μηχανή google.com ?

Υπηρεσία «δικαιώματος στη λήθη» της Goole



Google

Κατάργηση βάσει ευρωπαϊκής νομοθεσίας περί προστασίας προσωπικών δεδομένων

Βοήθεια

Αίτημα κατάργησης περιεχομένου το οποίο έχει ευρετηριαστεί στην Αναζήτηση Google, βάσει της ευρωπαϊκής νομοθεσίας περί προστασίας προσωπικών δεδομένων

Τον Μάιο του 2014, μια απόφαση του Δικαστηρίου της Ευρωπαϊκής Ένωσης (C-131/12, 13 Μαΐου 2014) έκρινε ότι ορισμένα άτομα μπορούν να ζητήσουν από τις μηχανές αναζήτησης να καταργήσουν συγκεκριμένα αποτελέσματα για ερωτήματα τα οποία περιλαμβάνουν το όνομά τους, σε περιπτώσεις στις οποίες το ενδιαφέρον σε αυτά τα αποτελέσματα που εμφανίζονται αντισταθμίζεται από τα δικαιώματα απορρήτου του εκάστοτε ατόμου.

Όταν υποβάλλετε ένα τέτοιο αίτημα, εξισορροπούμε τα δικαιώματα απορρήτου του ατόμου με το δημόσιο συμφέρον για την ενημέρωση και το δικαίωμα διανομής πληροφοριών. Κατά την αξιολόγηση του αιτήματός σας, θα ελέγξουμε εάν τα αποτελέσματα περιλαμβάνουν μη επικαιροποιημένες πληροφορίες σχετικά με εσάς, καθώς και αν υπάρχει δημόσιο συμφέρον σε αυτές τις πληροφορίες. Για παράδειγμα, μπορεί να απορρίψουμε κάποιο αίτημα κατάργησης συγκεκριμένων πληροφοριών σχετικά με οικονομικές απάτες, επαγγελματική αμέλεια, καταδικαστικές αποφάσεις ή τη δημόσια συμπεριφορά ατόμων ως κυβερνητικών υπαλλήλων.

Για να συμπληρώσετε αυτήν τη φόρμα, θα χρειαστείτε ένα ψηφιακό αντίγραφο μιας μορφής εξακρίβωσης ταυτότητας. Εάν υποβάλετε το παρόν αίτημα εκ μέρους κάποιου άλλου, θα πρέπει να παράσχετε την εξακρίβωση ταυτότητας για λογαριασμό του.

** Απαιτούμενο πεδίο*

ΤΑ ΣΤΟΙΧΕΙΑ ΣΑΣ

Χώρα της οποίας η νομοθεσία διέπει το αίτημά σας *

Επιλέξτε χώρα/περιοχή

Πλήρες νομικό όνομα *

Το όνομά σας, ακόμα και εάν υποβάλλετε το αίτημα εκ μέρους κάποιου άλλου που εκπροσωπείτε βάσει εξουσιοδότησης. Εάν εκπροσωπείτε κάποιον άλλον, θα πρέπει να έχετε τη δέουσα νόμιμη εξουσιοδότηση, για να ενεργείτε εκ μέρους του.

Όνομα:

Επώνυμο:

Διεύθυνση ηλεκτρονικού ταχυδρομείου επικοινωνίας *

Ενεργώ εκπροσωπώντας... *

Εάν υποβάλλετε αυτό το αίτημα εκ μέρους κάποιου άλλου, προσδιορίστε τη σχέση σας με αυτό το άτομο (για παράδειγμα: "γονέας", "δικηγόρος"). Ενδεχομένως να ζητήσουμε τεκμηρίωση η οποία θα επιβεβαιώνει ότι έχετε λάβει εξουσιοδότηση για την εκπροσώπηση αυτού του ατόμου.

- Τον εαυτό μου
- Κάποιον πελάτη
- Κάποιο μέλος της οικογένειάς μου

Νέα στοιχεία του GDPR – Φορητότητα των δεδομένων

- Άρθρο 20: Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει να λάβει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν (και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας) σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο (για να μπορεί να τα μεταφέρει εύκολα αλλού), καθώς και το δικαίωμα να διαβιβάσει τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας χωρίς αντίρρηση από τον αρχικό υπεύθυνο επεξεργασίας.
- Μπορεί επίσης να ζητήσει την απευθείας διαβίβαση των δεδομένων προσωπικού χαρακτήρα από έναν υπεύθυνο επεξεργασίας σε άλλον, σε περίπτωση που αυτό είναι τεχνικά εφικτό.
  - Εισάγει νέες υποχρεώσεις στους υπεύθυνους επεξεργασίας να «μεταφέρουν» δεδομένα πελατών/χρηστών τους σε άλλον υπεύθυνο επεξεργασίας, εφόσον ο πελάτης/χρήστης (υποκείμενο των δεδομένων) το ζητήσει
  - Παράδειγμα περίπτωσης: Μεταφορά ηλεκτρονικού ταχυδρομείου σε άλλον πάροχο υπηρεσίας ηλεκτρονικού ταχυδρομείου

GDPR – Δημιουργία προφίλ χρηστών

- Άρθρο 22: Το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υφίστανται τα δεδομένα του αυτοματοποιημένη επεξεργασία (συμπεριλαμβανομένης της κατάρτισης προφίλ) για το σκοπό της λήψης αποφάσεων οι οποίες παράγουν έννομα αποτελέσματα που το αφορούν ή το επηρεάζουν σημαντικά με παρόμοιο τρόπο
- Τέτοιες αυτοματοποιημένες επεξεργασίες, στις οποίες αναφέρεται το εν λόγω άρθρο, μπορούν να είναι εκείνες με σκοπό την αξιολόγηση προσωπικών πτυχών σχετικά με ένα φυσικό πρόσωπο, ιδίως την ανάλυση ή την πρόβλεψη πτυχών που αφορούν τις προσωπικές προτιμήσεις ή συμφέροντα, την αξιοπιστία ή τη συμπεριφορά, τη θέση ή κινήσεις του κ.α. (βλ. και Σκέψη 71 στο Προοίμιο του GDPR).
- Η επεξεργασία προσωπικών δεδομένων προσώπων που βρίσκονται στην Ένωση από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία μη εγκατεστημένο στην Ένωση διέπεται από τον GDPR, εφόσον αφορά την παρακολούθηση της συμπεριφοράς των εν λόγω προσώπων.
  - Η διαμόρφωση προφίλ χρηστών μέσω Διαδικτύου, με σκοπό να ληφθούν αποφάσεις που το αφορούν ή να αναλυθούν ή να προβλεφθούν οι προσωπικές προτιμήσεις, οι συμπεριφορές και οι νοοτροπίες του, εμπίπτει σε αυτήν την περίπτωση (Σκέψη 24 στο Προοίμιο του GDPR)

Νέα στοιχεία του GDPR – Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού

- Άρθρο 25 παρ 1: (…) Ο υπεύθυνος επεξεργασίας εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων (όπως η ελαχιστοποίηση των δεδομένων) και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία κατά τρόπο ώστε να πληρούνται οι απαιτήσεις του GDPR και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων.
  - Με άλλα λόγια, ο υπεύθυνος επεξεργασίας θα πρέπει να μπορεί να αποδείξει ότι για την επεξεργασία προσωπικών δεδομένων που πραγματοποιεί εφαρμόζει μέτρα, π.χ. προσαρμοσμένα στην αρχή της αναλογικότητας (ώστε η επεξεργασία να είναι η ελάχιστη δυνατή), τα οποία μέτρα έχουν καθοριστεί ήδη κατά το σχεδιασμό της επεξεργασίας (Προστασία των δεδομένων ήδη από το σχεδιασμό - data protection by design)
- Αποτελεί σημαντική νέα υποχρέωση του υπεύθυνου επεξεργασίας, αφού υποχρεούται εξ αρχής να λαμβάνει μέριμνα για την ιδιωτικότητα και την προστασία των δεδομένων
  - Κάτι που πολλές φορές, δυστυχώς, δεν συμβαίνει σήμερα, αφού πολλά πληροφοριακά συστήματα αναπτύσσονται με μόνο σχεδιαστικό κριτήριο την εξυπηρέτηση του επιδιωκόμενου σκοπού – και ίσως και τη μείωση κόστους ή/και απλοποίηση υλοποίησης – και σε τελευταίο στάδιο γίνεται έλεγχος για το αν πρέπει να γίνει κάποια «διόρθωση» ως προς την ιδιωτικότητα

Νέα στοιχεία του GDPR – Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού (*συνέχεια*)

- Άρθρο 25 παρ. 2: 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 (…) Ειδικότερα, τα εν λόγω μέτρα διασφαλίζουν ότι, εξ ορισμού, τα δεδομένα προσωπικού χαρακτήρα δεν καθίστανται προσβάσιμα σε τρίτους χωρίς την παρέμβαση του υποκειμένου των δεδομένων.
  - Με άλλα λόγια, ο υπεύθυνος επεξεργασίας θα πρέπει να μπορεί να αποδείξει ότι για την επεξεργασία προσωπικών δεδομένων που πραγματοποιεί η προκαθορισμένη ρύθμιση είναι η πιο φιλική προς την ιδιωτικότητα (Προστασία των δεδομένων εξ ορισμού - data protection by default)
  - Για παράδειγμα, ένας πάροχος υπηρεσιών κοινωνικής δικτύωσης πρέπει να έχει προκαθορισμένες (default) ρυθμίσεις για τους χρήστες του εκείνες που είναι πιο φιλικές προς την ιδιωτικότητα!

Νέα στοιχεία του GDPR – Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού (*συνέχεια*)

- Άρθρο 25 παρ. 3: Εγκεκριμένος μηχανισμός πιστοποίησης μπορεί να χρησιμοποιηθεί ως στοιχείο που αποδεικνύει τη συμμόρφωση με τις απαιτήσεις data protection by design και data protection by default
  - Άρα, παρέχεται η δυνατότητα πιστοποίησης του οργανισμού ως προς το ότι ικανοποιεί τις ανωτέρω αρχές (κατ' αναλογία με την πιστοποίηση κατά ISO)
  - Η πιστοποίηση είναι εθελοντική και όχι υποχρεωτική
  - Ο μηχανισμός πιστοποίησης πρέπει να έχει τα χαρακτηριστικά εκείνα που προδιαγράφονται στο άρ. 42 του GDPR
  - Ύπαρξη φορέων πιστοποίησης (άρ. 43 του GDPR)

Νέα στοιχεία του GDPR – Data Protection Impact Assessment

- Άρθρο 35: Όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους.

- Συνεπώς, σε κρίσιμες επεξεργασίες, πρέπει να διενεργείται αρχικά μία μελέτη επιπτώσεων (αντικτύπου) ως προς την προστασία προσωπικών δεδομένων (Data Protection Impact Assessment - DPIA).
- => Σημαντική νέα υποχρέωση των υπεύθυνων επεξεργασίας, αφού θα πρέπει να εκπονήσουν και να τη διαθέτουν, εφόσον τους ζητηθεί, μια DPIA

- Ποιες περιπτώσεις επεξεργασίας είναι κρίσιμες;

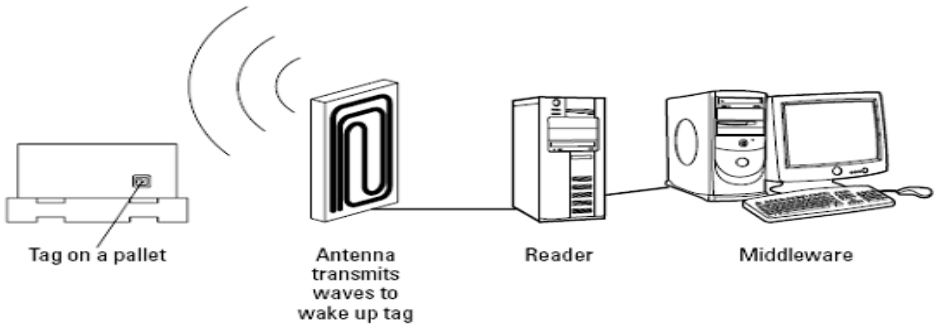
Νέα στοιχεία του GDPR – Data Protection Impact Assessment (συνέχεια)

- Η εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων απαιτείται ιδίως στην περίπτωση:
  - συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο,
  - επεξεργασίας μεγάλης κλίμακας των δεδομένων ειδικών κατηγοριών που αναφέρονται στο άρθρο 9 παράγραφος 1 ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10
  - συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα
- Άρα, για τέτοιου τύπου επεξεργασίες, θα πρέπει να εκπονείται υποχρεωτικά μία DPIA
- Άρ. 36: Ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη της οικείας Αρχής Προστασίας Προσωπικών Δεδομένων πριν από την επεξεργασία, όταν η εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων υποδεικνύει ότι η επεξεργασία θα προκαλούσε υψηλό κίνδυνο ελλείψει μέτρων μετριασμού της επικινδυνότητας
- => Άρα, σε εξαιρετικές περιπτώσεις, ο υπεύθυνος οφείλει να διαβουλευτεί με την Αρχή Προστασίας Προσωπικών Δεδομένων

Παράδειγμα εκπόνησης DPIA

- Ήδη οι Αρχές Προστασίας Δεδομένων, πριν θεσμοθετηθεί ο GDPR, βάσει της εθνικής τους νομοθεσίας (που με τη σειρά τους βασίζονται στην Οδηγία 95/46/ΕΚ) προέτρεπαν – ή και υποχρέωναν – εκπόνηση DPIA σε ειδικές περιπτώσεις
  - Ο GDPR τώρα τη θέτει ως υποχρεωτική
- Παράδειγμα: Η Ομάδα Εργασίας (Ο.Ε.) του άρ. 29 έχει προδιαγράψει από το 2011 ένα πλαίσιο εκπόνησης DPIA για RFID εφαρμογές που επεξεργάζονται προσωπικά δεδομένα
  - Βλ. *cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf*
- Η εκπόνηση DPIA ουσιαστικά είναι μία μελέτη επικινδυνότητας ως προς την προστασία προσωπικών δεδομένων

Τεχνολογίες RFID – Εκπόνηση DPIA



- 2009: Σύσταση της ΕΕ για την εφαρμογή αρχών προστασίας της ιδιωτικής ζωής και των δεδομένων στις RFID εφαρμογές (τεχνολογία αναγνώρισης μέσω ραδιοσυχνοτήτων).
- 2011: Εκπρόσωποι του κλάδου υπέβαλαν, προς έγκριση, τελικό αναθεωρημένο Πλαίσιο για την εκτίμηση των επιπτώσεων στην ιδιωτικότητα από τις RFID εφαρμογές
  - Το πλαίσιο εγκρίθηκε από την Ομάδα Εργασίας του Άρθρου 29 για την προστασία των δεδομένων (Γνώμη 9/2011 – Ο.Ε. 29)
  - Υποχρέωση εκπόνησης DPIA οποτεδήποτε η RFID εφαρμογή επεξεργάζεται καθ' οιονδήποτε τρόπο προσωπικά δεδομένα ή τα δεδομένα της μπορούν να διασυνδεθούν με προσωπικά δεδομένα
- Το Πλαίσιο αποτελεί βασικό οδηγό:
  - Αποτυπώνονται κίνδυνοι που ανακύπτουν ως προς την παραβίαση της ιδιωτικότητας, οι οποίοι πρέπει να λαμβάνονται υπόψη κατά την κατάρτιση μίας DPIA
  - Καταγράφονται μέτρα για την αντιμετώπιση των ανωτέρω κινδύνων

Νέα στοιχεία του GDPR – Περιστατικά παραβίασης δεδομένων

- Άρθρο 33: Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας γνωστοποιεί αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή (…), στην οποία θα αναφέρονται κατ' ελάχιστο:
  - η φύση της παραβίασης (συμπεριλαμβανομένων κατηγοριών και του κατά προσέγγιση πλήθους ατόμων που επηρεάζονται)
  - Όνομα και στοιχεία υπεύθυνου επικοινωνίας για περισσότερες πληροφορίες
  - Ενδεχόμενες επιπτώσεις
  - Ληφθέντα ή προτεινόμενα προς λήψη μέτρα για την αντιμετώπιση του περιστατικού
- Άρθρο 34: Όταν η παραβίαση ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων που παραβιάστηκαν, ο υπεύθυνος επεξεργασίας ανακοινώνει αμελλητί την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων.
  - Εκτός εάν τα δεδομένα που διέρρευσαν είναι ακατάληπτα (κρυπτογραφημένα) ή λήφθηκαν μέτρα που διασφαλίζουν ότι δεν είναι πιθανό να επέλθει ο ανωτέρω κίνδυνος ή αν η ενημέρωση προϋποθέτει δυσανάλογες προσπάθειες (οπότε θα πρέπει να υπάρξει δημόσια ανακοίνωση)
- Άρα, θεσπίζονται ρητές υποχρεώσεις για διαχείριση περιστατικών παραβίασης προσωπικών δεδομένων, για όλους τους υπεύθυνους επεξεργασίας
  - Τέτοιες υποχρεώσεις αυτή τη στιγμή, με την τρέχουσα νομοθεσία, ισχύουν μόνο για τους παρόχους τηλεπικοινωνιακών υπηρεσιών

Νέα στοιχεία του GDPR – Data Protection Officer

- Άρθρο 37: Ο υπεύθυνος και ο εκτελών την επεξεργασία ορίζουν υπεύθυνο προστασίας προσωπικού δεδομένα (data protection officer) σε κάθε περίπτωση όπου:
  - η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα, εκτός από δικαστήρια που ενεργούν στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας,
  - οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες, λόγω της φύσης, του πεδίου εφαρμογής και/ή των σκοπών τους, απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα,
  - οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα κατά το άρθρο 9 και δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα (…)
- Άρα, όλοι οι φορείς που δραστηριοποιούνται στους ανωτέρω τομείς υποχρεούνται στο να έχουν ένα άτομο αρμόδιο για θέματα προστασίας προσωπικών δεδομένων (Data Protection Officer – DPO)
  - Ο ρόλος αυτός κατά κανόνα δίνεται σε άτομα με ειδικές γνώσεις σε θέματα προστασίας δεδομένων, είτε νομικούς είτε επιστήμονες πληροφορικής
  - Μπορεί να είναι και εξωτερικός συνεργάτης

Data Protection Officer – Καθήκοντα και αρμοδιότητες

- Άρθρο 39: Ο DPO έχει τουλάχιστον τα εξής καθήκοντα:
  - ενημερώνει και συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους υπαλλήλους που επεξεργάζονται τις υποχρεώσεις τους που απορρέουν από τον παρόντα κανονισμό και από άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων,
  - παρακολουθεί τη συμμόρφωση με τον παρόντα κανονισμό, με άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων και με τις πολιτικές του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της ανάθεσης αρμοδιοτήτων, της ευαισθητοποίησης και της κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας, και των σχετικών ελέγχων,
  - παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και παρακολουθεί την υλοποίησή της
  - συνεργάζεται με την εποπτική αρχή
- Κατά την εκτέλεση των καθηκόντων του, λαμβάνει δεόντως υπόψη τον κίνδυνο που συνδέεται με τις πράξεις επεξεργασίας, συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας.
- Τα στοιχεία επικοινωνίας του DPO ανακοινώνονται στην οικεία Αρχή Προστασίας Δεδομένων, αλλά και στα υποκείμενα των δεδομένων! (βλ. άρ. 13 του GDPR, για τις πληροφορίες που περιέχει η ενημέρωση που οφείλει να παρέχει ο υπεύθυνος επεξεργασίας στα υποκείμενα των δεδομένων)

GDPR – Ασφάλεια επεξεργασίας

- Άρθρο 29: (…) 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, ιδίως από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας δημοσιοποίηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία

GDPR – Ασφάλεια επεξεργασίας (*συνέχεια*)

- Στον GDPR γίνεται ρητή αναφορά σε ψευδωνυμοποίηση και κρυπτογράφηση ως μέτρα ασφάλειας που πρέπει να εξεταστεί η υλοποίησή τους – δηλαδή «προτρέπει» στο να εξετάζονται τεχνικές ψευδωνυμοποίησης και ανωνυμοποίησης
  - Προσοχή: ας ανακαλέσουμε ότι η ψευδωνυμοποίηση ορίζεται ρητώς στον GDPR (δεν υπήρχε ισοδύναμος ορισμός στην 95/46/ΕΚ), με ειδική αναφορά στο ότι η ψευδωνυμοποίηση δεν συνιστά ανωνυμοποίηση!

- Η τήρηση εγκεκριμένου κώδικα δεοντολογίας (βλ. άρ. 40 του GDPR) ή εγκεκριμένου μηχανισμού πιστοποίησης (βλ. άρ 42 του GDPR) δύναται να χρησιμοποιηθεί ως στοιχείο για την απόδειξη της συμμόρφωσης με τις απαιτήσεις ασφάλειας του άρ. 31 του GDPR
  - Άρα, οι υπεύθυνοι επεξεργασίας δύνανται να λάβουν πιστοποίηση για την ασφάλειά τους από εγκεκριμένο φορέα, η οποία θα καταδεικνύει συμμόρφωση με τις απαιτήσεις του GDPR

GDPR – Υποβολή καταγγελίας στην εποπτική Αρχή

- Άρθρο 77: Κάθε υποκείμενο των δεδομένων έχει το δικαίωμα να υποβάλει καταγγελία σε εποπτική Αρχή (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα), ιδίως στο Κράτος-Μέλος στο οποίο έχει τη συνήθη διαμονή του ή τον τόπο εργασίας ή τον τόπο της εικαζόμενης παράβασης.
  - Διαφοροποίηση σε σχέση με την υπάρχουσα κατάσταση, όπου αρμόδια Αρχή για εξέταση καταγγελίας είναι εκείνη στην οποία έχει έδρα (εγκατάσταση) ο υπεύθυνος επεξεργασίας
- Πρόβλεψη για εκπροσώπηση υποκειμένων από οργανώσεις
  - Μη κερδοσκοπικό φορέα, οργάνωση ή ένωση (…) που διαθέτει καταστατικούς σκοπούς γενικού συμφέροντος και δραστηριοποιείται στον τομέα της προστασίας των δικαιωμάτων και των ελευθεριών των υποκειμένων των δεδομένων σε σχέση με την προστασία των δεδομένων τους προσωπικού χαρακτήρα – αρ. 80.

Συνεκτική εφαρμογή στην Ε.Ε.

- Οι εποπτικές αρχές οφείλουν να συνεργάζονται μεταξύ τους στην εξέταση υποθέσεων, στο πλαίσιο της συνεκτικής εφαρμογής του Κανονισμού (άρ. 51, αλλά και Τμήμα VII του GDPR).
  - Λειτουργία «Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων»
    - Αντικαθιστά την τωρινή Ο.Ε. του Άρ. 29
  - Κοινή αντιμετώπιση υποθέσεων που αφορούν σε πολλά κράτη μέλη, υπό το συντονισμό της «Επικεφαλούς Εποπτικής Αρχής» (συνήθως στη χώρα εγκατάστασης υπευθύνου)
  - Στόχος να μην επιβάλλονται από τα Κράτη Μέλη διαφορετικής βαρύτητας κυρώσεις για αντίστοιχες παραβάσεις
  - Αρχή Κράτους Μέλους στο οποίο ο υπεύθυνος ή κάποιος εκτελών την επεξεργασία έχει εγκατάσταση ή κράτους στο οποίο βρίσκεται σημαντικός αριθμός υποκειμένων των δεδομένων που επηρεάζεται , *δικαιούται* να συμμετέχει σε εξέταση υπόθεσης. Στόχος η συναίνεση στην απόφαση.
    - Σε περίπτωση διαφωνίας των Αρχών, ενεργοποίηση μηχανισμού συνεκτικότητας με στενά χρονικά πλαίσια.
  - Παροχή πληροφοριών από άλλες Αρχές (εθελοντικά)
  - Αμοιβαία συνδρομή (υποχρεωτικά) μεταξύ αρχών για τη συνεκτική εφαρμογή του κανονισμού
  - Κοινές επιχειρήσεις αρχών ελέγχου

… και πολλές αλλαγές ακόμη

- Τα ανωτέρω προσδιορίζουν ένα υποσύνολο μόνο από τις βασικές αλλαγές που επιφέρει ο GPDR
  - Υπάρχουν και άλλα πολλά νέα στοιχεία
- Η συμμόρφωση ενός οργανισμού (είτε του Δημόσιου Τομέα είτε του Ιδιωτικού) αποτελεί μία μεγάλη πρόκληση

- Για τα προσωπικά δεδομένα στις ηλεκτρονικές επικοινωνίες;
  - Και η Οδηγία 2002/52/ΕΚ επίκειται να αντικατασταθεί από νέο Κανονισμό, εναρμονισμένο με τις απαιτήσεις του GDPR
  - Θα καλύπτει όχι μόνο παρόχους τηλεπικοινωνιακών υπηρεσιών αλλά κάθε πάροχο αντίστοιχων υπηρεσίων (π.χ. VoIP τηλεφωνία κτλ.)

Κάποιες αλλαγές που επιφέρει ο GDPR

1 Δεδομένα που τα μεταφέρεις !

Μπορώ να πάρω πίσω τα δεδομένα που έδωσα σε έναν οργανισμό ή διαδικτυακή υπηρεσία και να τα μεταφέρω σε άλλους (κοινωνικά δίκτυα, παρόχους υπηρεσιών διαδικτύου κ.λπ.).

2 Μεγαλύτερη διαφάνεια

Γνωρίζω περισσότερα για την τύχη των δεδομένων μου και έτσι είναι πιο εύκολο να ασκήσω τα δικαιώματά μου.

3 Προστασία ανηλίκων

Οι διαδικτυακές υπηρεσίες πρέπει να λάβουν τη συγκατάθεση των γονέων πριν καταχωρίσουν οποιονδήποτε ανήλικο κάτω των 16, αν αυτό προβλέπεται στην εθνική νομοθεσία.

4 Υπηρεσία μίας στάσης

Σε περίπτωση προβλημάτων με τον τρόπο που χρησιμοποιούνται τα δεδομένα μου, μπορώ να επικοινωνήσω με την αρχή προστασίας δεδομένων της χώρας μου, ανεξάρτητα από το πού βρίσκεται ο οργανισμός που τα επεξεργάζεται.

5 Μεγαλύτερες κυρώσεις

Όταν παραβιάζονται τα προσωπικά δεδομένα, μπορεί να επιβληθεί στον υπόλογο οργανισμό πρόστιμο μέχρι 20.000.000€ ή 4% του ετήσιου παγκόσμιου κύκλου εργασιών του.

6 Δικαίωμα στη λήθη

Μπορώ να ζητήσω από μηχανές αναζήτησης να αφαιρέσουν από τα αποτελέσματά τους μια ιστοσελίδα με αρνητικό αντίκτυπο στην ιδιωτικότητά μου ή να ζητήσω από ένα δικτυακό τόπο να απαλείψει μια πληροφορία, υπό συγκεκριμένες προϋποθέσεις.

Illustration: Martin Vidberg

Χρήσιμες συνδέσεις

- Ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (www.dpa.gr)
- Κυπριακό Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (http://www.dataprotection.gov.cy)
- European Data Protection Supervisor (http://www.edps.europa.eu/EDPSWEB/)
- ENISA (http://www.enisa.europa.eu/)
- Ομάδα Εργασίας του Άρθρου 29 (http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm)
  - Περιέχει, μεταξύ άλλων, και όλες τις Γνώμες (Opinions)

Το νέο νομικό πλαίσιο

- General Data Protection Regulation:

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

- Η ελληνική έκδοση: http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&qid=1489137922233&from=en

- Σχετικές πληροφορίες και υλικό και στο:

http://ec.europa.eu/justice/data-protection/reform/index_en.htm

- Το προτεινόμενο σχέδιο του νέου Κανονισμού για την αντικατάσταση της e-Privacy Directive (τελευταία έκδοση: Ιαν. 2017)

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN

Ειδικότερες συνδέσεις

Κατευθυντήριες γραμμές της Ο.Ε. του Άρ. 29:

1. για τους DPOs:
   http://ec.europa.eu/newsroom/document.cfm?doc_id=44100

2. Για το δικαίωμα στη φορητότητα των δεδομένων:
   http://ec.europa.eu/newsroom/document.cfm?doc_id=44099

3. Για την υποχρέωση εκπόνησης DPIA:
   http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

4. Για την κοινοποίηση περιστατικών παραβίασης δεδομένων:
   http://ec.europa.eu/newsroom/document.cfm?doc_id=47741

If you reveal your secrets to the wind, you should not blame the wind for revealing them to the trees.

Kahlil Gibran