Πανεπιστήμιο Αιγαίου

Ειδικά θέματα Δικαίου της Πληροφορίας

Privacy by Design-Privacy by Default
Η τεχνολογική διάσταση της προστασίας προσωπικών δεδομένων

Λίλιαν Μήτρου (L.Mitrou@aegean.gr)

Αναπληρώτρια Καθηγήτρια

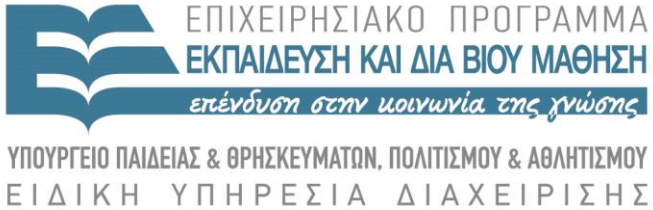
Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων

Άδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Αιγαίου**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.



Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Διάγραμμα

- Τεχνολογίες Ενίσχυσης Ιδιωτικότητας (PETs)
- Privacy by design
- Privacy by default
- Οι επιλογές του Σχεδίου Κανονισμού
- Privacy by design/by default στο ελληνικό δίκαιο
- Κριτικές παρατηρήσεις

Η ανεπάρκεια του δικαίου

- Ανεπάρκεια των παραδοσιακών εργαλείων του δικαίου να εξυφάνουν ένα αποτελεσματικό δίχτυ προστασίας
- Προστασία δια της τεχνολογίας
- Συμπλήρωμα/υποκατάστατο των νομικών κανόνων

Τεχνολογίες Ενίσχυσης Ιδιωτικότητας

- Ήδη από τη δεκαετία ’90 υπογραμμιζόταν η ανάγκη υιοθέτησης Τεχνολογιών Ενίσχυσης Ιδιωτικότητας
- ΤΠΕ που ενισχύουν την προστασία της ιδιωτικότητας
  - μηδενίζοντας ή μειώνοντας τη
  - μη αναγκαία αποκάλυψη, συλλογή, τήρηση, διαμοιρασμό των προσωπικών δεδομένων,
  - χωρίς να απομειώνεται η λειτουργικότητα των πληροφοριακών συστημάτων
- anonymizers, συστήματα διαχείρισης ταυτότητας, οι λεγόμενοι privacy proxies, μηχανισμοί κρυπτογράφησης φίλτρα (encryption mechanisms), φίλτρα κλπ
- Ανεπάρκεια διείσδυσης των PETs στην αγορά

Privacy by Design

- Φιλοσοφία της ένταξης της ιδιωτικότητας στα χαρακτηριστικά (specifications) διάφορων τεχνολογιών και αφορά
- Σχεδιασμό, λειτουργία και διαχείριση των τεχνολογιών επεξεργασίας πληροφορίας αλλά και των πληροφοριακών συστημάτων
- Προληπτικός χαρακτήρας
- Αρχιτεκτονική και σχεδιασμός συστημάτων αλλά και επιχειρησιακών διαδικασιών/πρακτικών
- Για όλον τον κύκλο ζωής

Privacy by Default

- Τεχνολογικές ρυθμίσεις και την αρχιτεκτονική των πλατφόρμων που ευνοούν, αν δεν προδιαγράφουν, την διάδοση και τον διαμοιρασμό προσωπικών πληροφοριών, χωρίς απαραίτητα αυτό να συνιστά και συνειδητή επιλογή του «χρήστη»
- Προεπιλεγμένες ρυθμίσεις ως αντιστροφή του κανόνα προστασίας
- Πρδγμ: visibility του profile ή του status ενός προσώπου στα ψηφιακά κοινωνικά δίκτυα
- Η έννοια της προστασίας της πληροφορικής ιδιωτικότητας ως κανόνας (by default) αποσκοπεί να προστατεύσει τα άτομα ακριβώς όταν τίθεται ζήτημα ελλείμματος κατανόησης των κινδύνων ή απώλειας του ελέγχου επί των ιδίων πληροφοριών

Η Οδηγία 95/46/ΕΚ και η λήψη τεχνικών μέτρων ως μείζων παρέμβαση

- Ιδίως η προστασία της ιδιωτικότητας μέσω της καθιέρωσης της privacy by default αντιμετωπίστηκε από την Ευρωπαϊκή Επιτροπή ως μία από τις μείζονος χαρακτήρα παρεμβάσεις
- Charismatic EU Regulator Seeks Privacy by Design!!!!
- Άρθρο 17 της Οδηγίας 95/46/ΕΚ (άρθρο 10 του Ν. 2472/97) προβλέπει – ως νομική και όχι απλά ως δεοντολογική υποχρέωση – τη λήψη των κατάλληλων τεχνικών και οργανωτικών μέτρων για την προστασία προσωπικών δεδομένων
- Προοίμιο (46): η προστασία δεδομένων απαιτεί τη λήψη κατάλληλων τεχνικών μέτρων και οργάνωση κατά τη στιγμή τόσο του σχεδιασμού των τεχνικών επεξεργασίας όσο και της εκτέλεσης της επεξεργασίας

Η ολιστική προσέγγιση της τεχνολογικής προστασίας

- Εισαγωγή των αρχών της προστασίας δεδομένων by design και by default
- Καταγραφή των πράξεων επεξεργασίας
- Εισαγωγή της κοινοποίησης των παραβιάσεων ασφάλειας (Data breach notification)
- Αποτίμηση των επιπτώσεων στην Ιδιωτικότητα/ προστασία δεδομένων που επιφέρει κάθε σχεδιαζόμενη επεξεργασία (Privacy Impact Assessment)

Privacy by design (Άρθρο 23 παρ. 1)

- Τόσο κατά το στάδιο του προσδιορισμού των μέσων της επεξεργασίας όσο και κατά την επεξεργασία καθεαυτή
- ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει
- τα κατάλληλα τεχνικά και οργανωτικά μέτρα και διαδικασίες κατά τρόπο ώστε
- η επεξεργασία να συνάδει προς/ανταποκρίνεται στις απαιτήσεις του Κανονισμού και να διασφαλίζει την προστασία των δικαιωμάτων του υποκειμένου των δεδομένων
- λαμβάνοντας υπόψη το επίπεδο της τεχνικής (state of the art) καθώς και το κόστος εφαρμογής

Privacy by default (Άρθρο 23 παρ. 2)

- *Υποχρέωση του Υπευθύνου Επεξεργασίας*
- *να εφαρμόσει μηχανισμούς ώστε να διασφαλίσει by default ότι*
- *θα υποβάλλονται σε επεξεργασία μόνο τα δεδομένα που είναι αναγκαία για κάθε επιμέρους ειδικό σκοπό επεξεργασίας*
- *Θα πρέπει να διασφαλίζεται (τεχνικά;) ότι τα δεδομένα δεν θα συλλέγονται και δεν θα τηρούνται πέραν του ελάχιστου αναγκαίου για τους σκοπούς της επεξεργασίας*
- *Η αρχή της ελαχιστοποίησης των υπό επεξεργασία δεδομένων αναφέρεται τόσο στον όγκο των δεδομένων όσο και στη διάρκεια τήρησης αυτών*
- *Υποχρέωση να εξασφαλίζεται ότι by default τα δεδομένα δεν θα είναι προσβάσιμα σε έναν αόριστο αριθμό προσώπων (κοινωνικά δίκτυα)*

Αξιολόγηση πρότασης

- Η προτεινόμενη ρύθμιση για προστασία δεδομένων by design δεν προσθέτει κάτι ουσιαστικό στις ήδη ισχύουσες και καθιερωμένες εκδηλώσεις της αρχής της αναλογικότητας, πλην της αναφοράς ότι αυτές θα πρέπει να ληφθούν υπόψη ήδη κατά τον σχεδιασμό (Επίτροπος για την Προστασία Προσωπικών Δεδομένων)
- Κρίσιμα στοιχεία : η διασφάλιση περιορισμού της χρήσης με κριτήριο τον σκοπό και την απαγόρευση περαιτέρω χρήσης των προσωπικών δεδομένων για ασύμβατους σκοπούς και η διασφάλιση διαφάνειας και ελεγξιμότητας

Τεχνική (περαιτέρω) νομοθεσία;

- Εξουσιοδότηση για έκδοση πράξεων που θα εξειδικεύουν τα περαιτέρω κριτήρια και τις απαιτήσεις για τα κατάλληλα μέτρα και μηχανισμούς, ιδίως για τις απαιτήσεις για προστασία δεδομένων by design που είναι εφαρμοστέοι σε διάφορους τομείς, προϊόντα και υπηρεσίες (παρ. 3)
- Ευχέρεια ως προς την εισαγωγή τεχνικών προδιαγραφών για τις απαιτήσεις που αφορούν την προστασία δεδομένων by design και by default (παρ. 4)
- Είναι αναγκαία/ σκόπιμη/χρήσιμη η κανονιστική εξουσιοδότηση για ζητήματα τεχνικού χαρακτήρα και είναι το κατάλληλο όργανο;
- Η Ομάδα 29 (Μάρτιος 2012) θεωρούσε ότι η Επιτροπή θα έπρεπε κατά τον προσδιορισμό των τεχνικών προδιαγραφών να συμβουλεύεται το European Data Protection Board
- Η Ομάδα 29, (στην γνωμοδότησή του Οκτωβρίου 2012) δεν αξιολογεί θετικά την ανάθεση αυτής της κανονιστικής εξειδίκευσης στην Επιτροπή, καθώς κρίνει ότι οι υποχρεώσεις που έχει ο υπεύθυνος επεξεργασίας είναι επαρκώς διευκρινισμένες και η ανταπόκρισή του σε αυτές θα πρέπει να κριθεί σε μία κατά περίπτωση βάση, λαμβανομένης υπόψη και της αρχής της λογοδοσίας που καθιερώνει το άρθρο 22 του Σχεδίου Κανονισμού

Υποχρεώσεις υπεύθυνου επεξεργασίας

- Οι υποχρεώσεις απευθύνονται και αφορούν σε υπεύθυνους επεξεργασίας ενώ οι ρυθμίσεις προσχεδιάζονται από αυτούς που αναπτύσσουν τεχνολογία
- Ομάδα 29: να καταστεί η αρχή της privacy by design υποχρεωτική/δεσμευτική για «σχεδιαστές και κατασκευαστές τεχνολογίας καθώς και για υπεύθυνους επεξεργασίας που έχουν να αποφασίσουν για την απόκτηση και χρήση ΤΠΕ
- Αναμφίβολα θα υπάρξει επιρροή στη σχετική αγορά

Privacy by design/by default στο ελληνικό δίκαιο

- Η αρχή της privacy by design αποτυπώνεται, έστω και με έμφαση στην ελαχιστοποίηση των προς επεξεργασία δεδομένων, ήδη στη ρύθμιση του ν. 2774/99 για την προστασία προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα
- Σύμφωνα με το άρθρο 4 παρ. 5 (που αντιστοιχεί στο άρθρο 5 παρ. 5 του ισχύοντος ν. 3471/06), «ο σχεδιασμός και η επιλογή των τεχνικών μέσων, καθώς και ο εξοπλισμός για την παροχή διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών πρέπει να γίνεται με κριτήριο και σκοπό την επεξεργασία όσο το δυνατόν λιγότερων δεδομένων προσωπικού χαρακτήρα»
- Αντίστοιχη ρύθμιση περιλαμβάνει ο ν. 3979/2011 για την ηλεκτρονική διακυβέρνηση που προβλέπει συγκεκριμένα ότι ο σχεδιασμός, η διαμόρφωση και η προμήθεια πληροφοριακών συστημάτων και υπηρεσιών ηλεκτρονικής διακυβέρνησης πρέπει να γίνεται, λαμβάνοντας υπόψη το δικαίωμα προστασίας των προσωπικών δεδομένων και την ανάγκη διαμόρφωσης των συστημάτων και υπηρεσιών κατά τρόπο ώστε να διασφαλίζεται η επεξεργασία όσο το δυνατόν λιγότερων δεδομένων προσωπικού χαρακτήρα

Τα όρια της παρέμβασης/1

- Επικρίσεις από παρόχους υπηρεσιών: σύγκρουση συμφερόντων μεταξύ της αξίωσης για ιδιωτικότητα και της αξιοποίησης της προσωπικής πληροφορίας ως εν τέλει συναλλακτικού αγαθού
- «Η αρχή της privacy by design είναι ευπρόσδεκτη αλλά η συνοδεύουσα αρχή της Privacy by default δεν λαμβάνει υπόψη το ήθος του διαμοιρασμού (ethos sharing) δεδομένων που συνιστά ακριβώς τη βάση των υπηρεσιών κοινωνικής δικτύωσης» και (παρακάτω) .. «την ειδική φύση της κοινωνικής δικτύωσης καθώς ο πιο συχνός λόγος για τον οποίο οι άνθρωποι σχετίζονται (με το Facebook) είναι για να μοιραστούν (πληροφορία) και να συνδεθούν με άλλους». (Lobbying Document του Facebook)

Τα όρια της παρέμβασης/2

- Σκεπτικισμός από τους εκπροσώπους των λεγόμενων computer ethics
  - Η προδιαγεγραμμένη προστασία δια της τεχνολογίας εγείρει ζητήματα ως προς τον σεβασμό της αυτονομίας του «χρήστη» εφόσον η συμπεριφορά του ενδέχεται να προσδιορίζεται από την αρχιτεκτονική και τον σχεδιασμό του συστήματος αντί για τις ατομικές επιλογές (τεχνολογικός πατερναλισμός)
  - Όμως (οι συνήθεις) προεπιλογές που δεν ευνοούν την ιδιωτικότητα καθοδηγούν, αν δεν χειραγωγούν επίσης τουλάχιστον τον μέσο χρήστη
- Προστασία ή «ενδυνάμωση του χρήστη»;

Τα όρια της παρέμβασης/3

- Κρισιμότερο είναι το ερώτημα ποιες ακριβώς κανονιστικές αρχές και επιλογές καλείται να ενσωματώσει η τεχνολογία;
- Η τεχνολογία περισσότερο δρομολογεί παρά αποτυπώνει κανονιστικές επιλογές του νομοθέτη
- Ζητήματα ισχύος του δικαίου και νομιμοποίησης
- Η ενσωμάτωση του δικαίου στην τεχνολογία είναι μία ευσεβής πλην όμως δυσχερώς εκπληρούμενη προσδοκία