Privacy and data protection by design

Αθηνά Μπούρκα | ENISA

European Union Agency for Network and Information Security

Περιεχόμενα

Privacy and data protection by design

By design..

Άρθρο 25 ΓΚΠΔ (GDPR)
Σχεδιασμός που υλοποιεί τις αρχές προστασίας δεδομένων

Σχεδιασμός με βάσει την ιδιωτικότητα

- Ενσωμάτωση μέτρων προστασίας της ιδιωτικότητας σε συστήματα και εφαρμογές.
- Όχι μόνο τεχνική – διαδικασίες, οργανωτικά μέτρα, άνθρωποι: μια στρατηγική αλλαγή.
- Πρακτική εφαρμογή: εύκολες ‘νίκες’ και μεγάλες προκλήσεις.

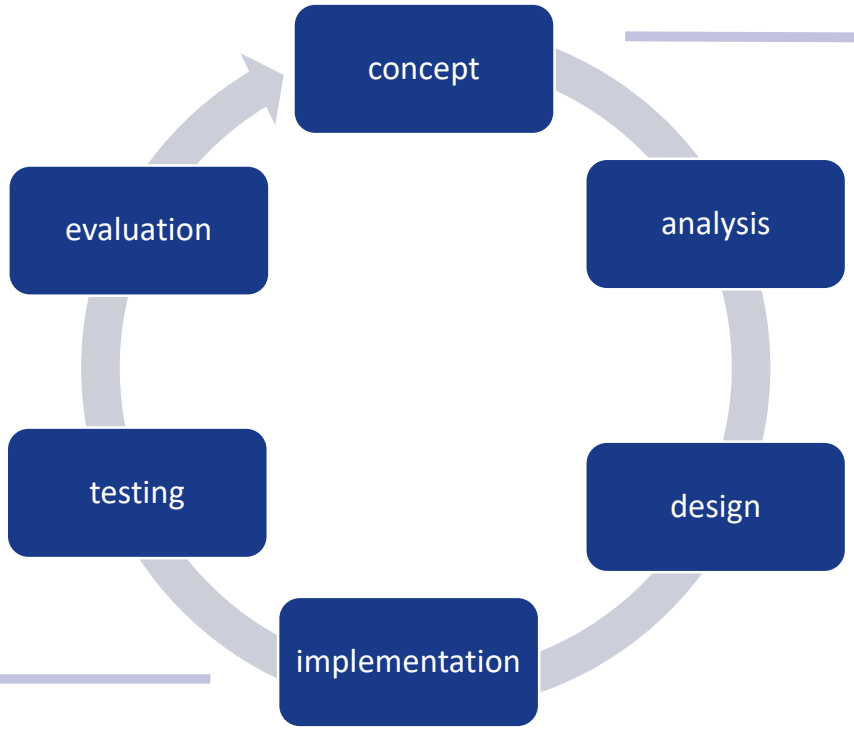
Think privacy – Design privacy

Άρθρο 25(1) ΓΚΠΔ – Προστασία των δεδομένων ήδη από το σχεδιασμό

«Λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων από την επεξεργασία, 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 δεδομένων, όπως η ελαχιστοποίηση δεδομένων, και η ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία κατά τρόπο ώστε να πληρούνται οι απαιτήσεις του παρόντος κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων».

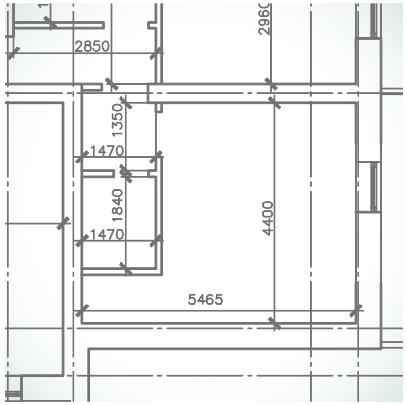
Τεχνολογία για την προστασία των δεδομένων

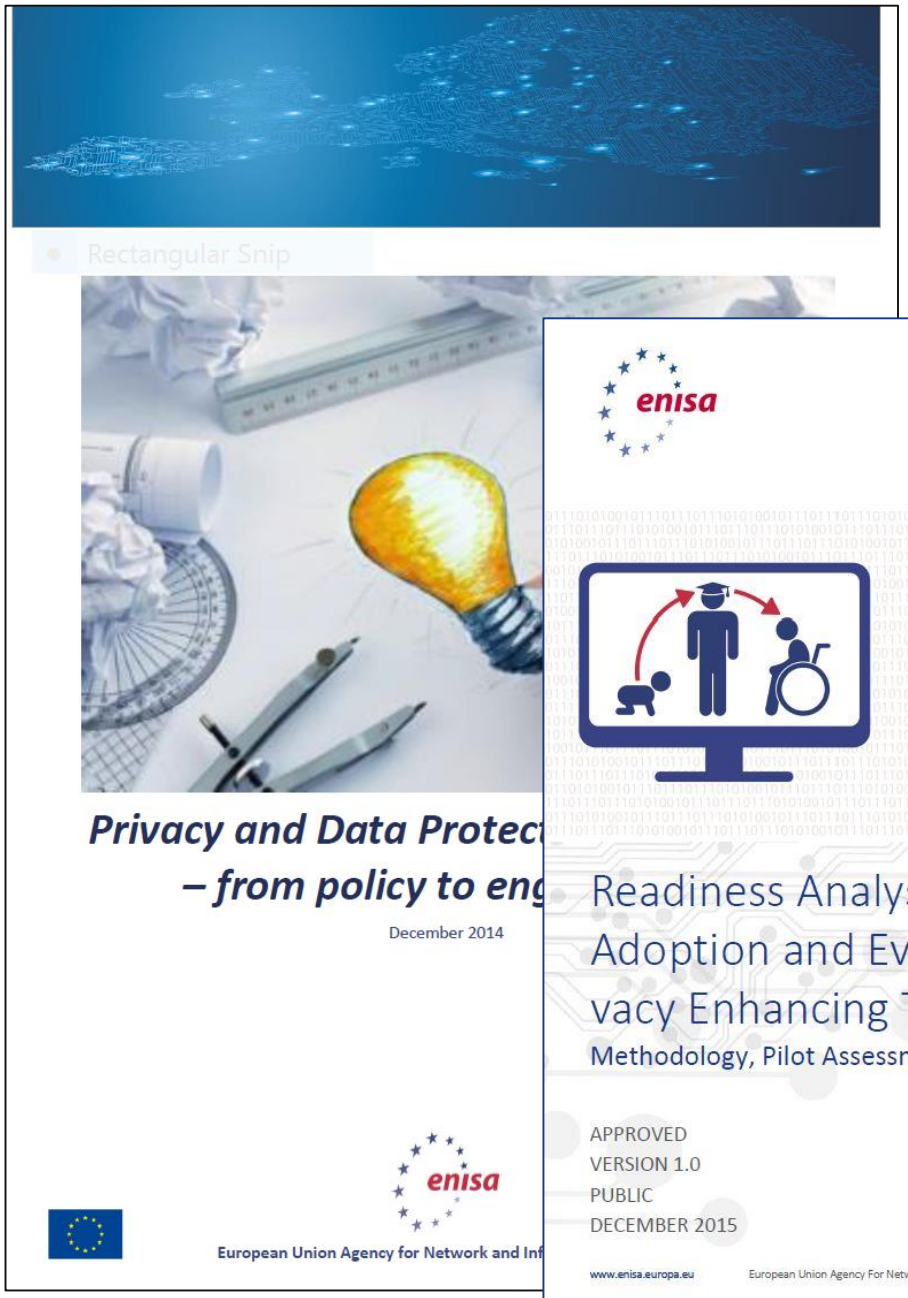
Πως μεταφράζονται οι νομικές απαιτήσεις σε τεχνικά μέτρα;



WHAT

HOW




Rectangular Snip
Privacy and Data Protect
– from policy to eng
December 2014
European Union Agency for Network and Inf
y tools for the
C
gy for the evaluation of PETs for
rs
ency For Network And Information Security
Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies
Methodology, Pilot Assessment, and Continuity Plan
APPROVED
VERSION 1.0
PUBLIC
DECEMBER 2015
www.enisa.europa.eu
European Union Agency For Network And Information Security

Στρατηγικές σχεδιασμού με βάση την ιδιωτικότητα

Στρατηγικές σχεδιασμού με βάσει την ιδιωτικότητα & προστασία δεδομένων

	PRIVACY BY DESIGN STRATEGY	DESCRIPTION
1	Minimize	The amount of personal data should be restricted to the minimal amount possible (data minimization).
2	Hide	Personal data and their interrelations should be hidden from plain view.
3	Separate	Personal data should be processed in a distributed fashion, in separate compartments whenever possible.
4	Aggregate	Personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful.
5	Inform	Data subjects should be adequately informed whenever personal data is processed (transparency).
6	Control	Data subjects should be provided agency over the processing of their personal data.
7	Enforce	A privacy policy compatible with legal requirements should be in place and should be enforced.
8	Demonstrate	Data controller must be able to demonstrate compliance with privacy policy into force and any applicable legal requirements.

Στρατηγικές.. by design (1)

#1 Minimize

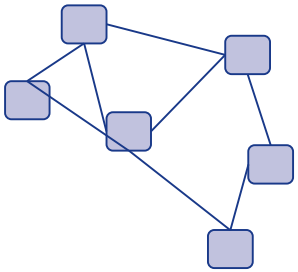
- **Αποκλεισμός (Exclude)**: αποφυγή επεξεργασίας δεδομένων.
- **Επιλογή (Select)**: επεξεργασία συγκεκριμένων δεδομένων.
- **Αφαίρεση (Strip)**: διαγραφή μέρους των δεδομένων.
- **Καταστροφή (Destroy)**: πλήρης διαγραφή των δεδομένων.

#2 Hide

- **Περιορισμός (Restrict)**: παρεμπόδιση πρόσβασης.
- **Ανάμειξη (Mix)**: επεξεργασία με τυχαίο τρόπο.
- **Σύγχυση (Obfuscate)**: παρεμπόδιση κατανόησης.
- **Αποσύνδεση (Dissociate)**: διαχωρισμός σε τμήματα.

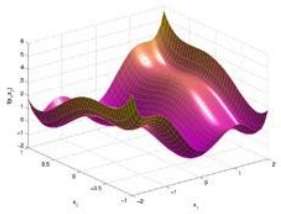
Στρατηγικές.. by design (2)

#3 Separate



- **Διανομή (Distribute)**: διαμερισμός δεδομένων.
- **Απομόνωση (Isolate)**: ανεξάρτητη επεξεργασία σε τμήματα.

#4 Aggregate



- **Σύνοψη (Summarise)**: επεξεργασία κοινών στοιχείων.
- **Συγκέντρωση (Group)**: επεξεργασία κοινών κατηγοριών.
- **Διατάραξη (Perturb)**: προσθήκη θορύβου, μείωση ακρίβειας.

Στρατηγικές.. by design (3)

#5 Inform

- **Παροχή (Supply)**: πολλαπλοί τρόποι ενημέρωσης.
- **Γνωστοποίηση (Notify)**: έγκαιρη ειδοποίηση για αλλαγές.
- **Επεξήγηση (Explain)**: παροχή εύληπτων λεπτομερειών.

#6 Control

- **Συγκατάθεση (Consent)**: ειδική και ελεύθερη συγκατάθεση.
- **Επιλογή (Choose)**: δυνατότητα επιλογής του χρήστη.
- **Επικαιροποίηση (Update)**: δυνατότητα τροποποίησης.
- **Ανάκληση (Retract)**: δυνατότητα διαγραφής δεδομένων.

Στρατηγικές.. by design (4)

#7 Enforce

- **Δημιουργία (Create)**: πολιτική προστασίας δεδομένων.
- **Διατήρηση (Maintain)**: επικαιροποίηση πολιτικής.
- **Υποστήριξη (Uphold)**: διασφάλιση υλοποίησης πολιτικής.

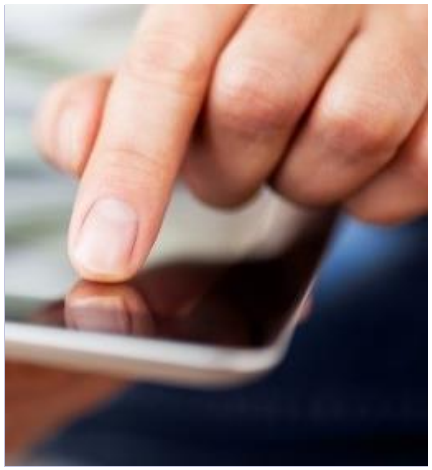
#8 Demonstrate

- **Καταγραφή (Log)**: καταγραφή ενεργειών.
- **Έλεγχος (Audit)**: έλεγχος, καταγραφή σημείων βελτίωσης.
- **Αναφορά (Report)**: ανάκληση και αναθεωρήσεις.

Τεχνολογίες ενίσχυσης της ιδιωτικότητας

Τεχνολογίες ενίσχυσης ιδιωτικότητας

PETs στην πράξη…?



Η κρυπτογρά-φηση είναι ακριβή ή δύσκολη

Τα δεδομένα είναι απαραίτητα για XYZ

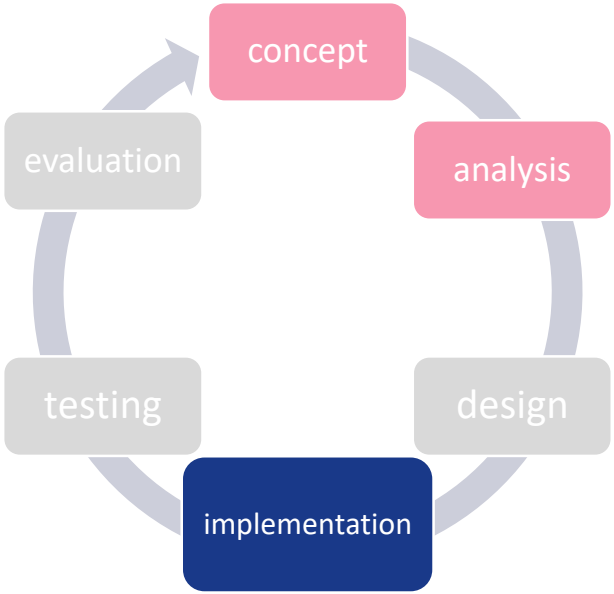
Η ομομορφική (homomorphic) κρυπτογρά-φηση θα λύσει όλα τα προβλήματα.

Ζήτησα συγκατά-θεση και τώρα μπορώ να κάνω ό,τι θέλω

Διέγραψα τα ονόματα και τα δεδομένα είναι ανώνυμα τώρα.

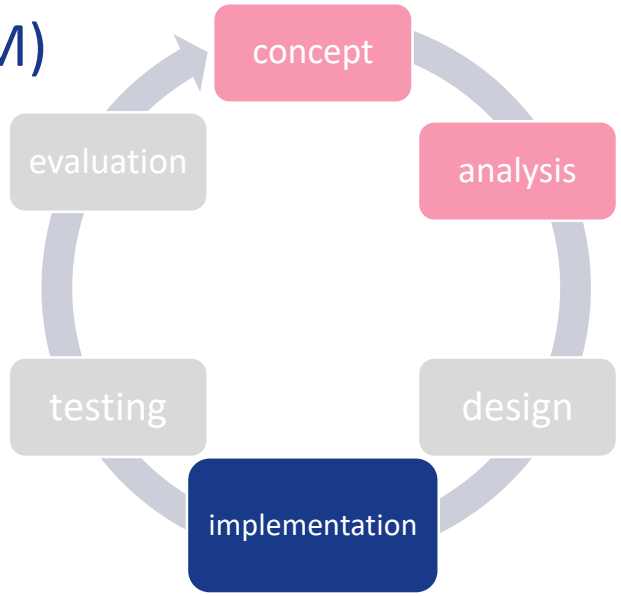
Τεχνολογίες (1)

1. Authentication
   - Client-server, end-to-end
2. Attributed Based Credentials (ABCs)
3. Encryption
   - Client-server, end-to-end
   - Key rotation & forward secrecy
4. Storage privacy
   - Local encrypted storage
   - Encrypted search
5. Anonymous communication
   - Proxies & VPNs
   - Onion routing



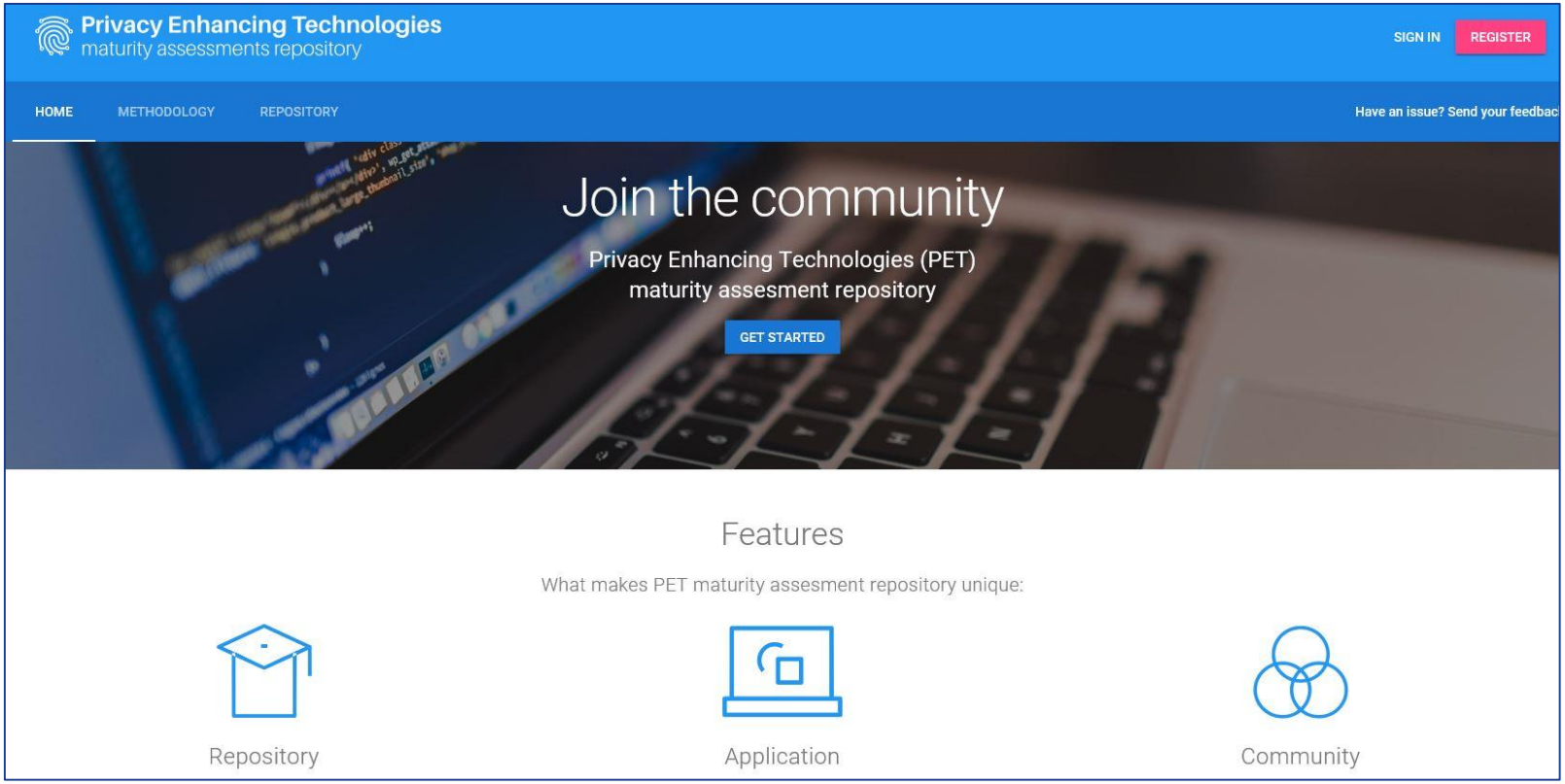
Τεχνολογίες (2)

6. Database Privacy
   - Statistical Disclosure Control (SDC)
   - Privacy Preserving Data Mining (PPDM)
   - Privacy Information Retrieval (PIM)
7. Privacy preserving computations
   - Homomorphic encryption
   - Secure multi-party computation
8. Transparency & control mechanisms
   - Privacy policies, privacy icons
   - Privacy preferences & sticky policies
   - Personal Data Clouds (PDC)



Ποιο είναι το βέλτιστο εργαλείο?

Προς την ανάπτυξη μίας κοινόχρηστης βάσης τεχνολογιών (PETs repository)



Privacy and data protection by default

Ιδιωτικότητα εξ ορισμού (privacy by default)

Εξ ορισμού (default): προκαθορισμένη τιμή ή επιλογή σε ένα σύστημα όταν η τιμή/επιλογή δεν έχουν καθοριστεί ειδικότερα από τον χρήστη.

Ιδιωτικότητα εξ ορισμού (privacy by default): η τιμή ή επιλογή καθορίζεται έτσι ώστε να εξασφαλίζει εξ ορισμού την ιδιωτικότητα.

Άρθρο 25(2) ΓΚΠΔ - προστασία δεδομένων εξ ορισμού

Ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέσα για να εξασφαλίσει ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας. Αυτή η υποχρέωση ισχύει για το εύρος των δεδομένων προσωπικού χαρακτήρα που συλλέγονται, τον βαθμό της επεξεργασίας τους, την περίοδο αποθήκευσης και την προσβασιμότητά τους. Ειδικότερα, τα εν λόγω μέτρα διασφαλίζουν ότι, εξ ορισμού, τα δεδομένα προσωπικού χαρακτήρα δεν καθίστανται προσβάσιμα χωρίς την παρέμβαση του φυσικού προσώπου σε αόριστο αριθμό φυσικών προσώπων».

Βασικές αρχές για ‘privacy defaults’

- Ελαχιστοποίηση των δεδομένων
- Περιορισμός του βαθμού της επεξεργασίας
- Ελαχιστοποίηση της αποθήκευσης των δεδομένων
- Περιορισμός της προσβασιμότητας των δεδομένων

Έρευνα Norwegian Consumer Council: Deceived by design..

‘By design & by default’– στην πράξη

- Οι υπεύθυνοι επεξεργασίας δεν ελέγχουν πάντα τον σχεδιασμό.
- Οι μεθοδολογίες σχεδιασμού δεν ακολουθούν πάντα τον τρόπο που λειτουργεί το οικοσύστημα.
- Οι απαιτήσεις ασφαλείας δεν καλύπτουν όλες τις πτυχές της ιδιωτικότητας.
- Σχεδιασμός και χρηστικότητα (usability).
- Ανάγκη για έρευνα και κατευθυντήριες γραμμές.

“

Design is not just what it looks like and feels like. Design is how it works.

Steve Jobs

”

Ευχαριστώ για την προσοχή σας!

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu