Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
Λ. Κηφισίας 1-3, 11523 Αθήνα
http://www.dpa.gr

Τεχνολογίες και Διαδικασίες ως μέσα συμμόρφωσης με τον Γενικό Κανονισμό Προστασίας Δεδομένων

Βασίλης Ζορκάδης
zorkadis@dpa.gr

Εκδήλωση
Επετειακή Ημερίδα Αρχής Προστασίας Δεδομένων

Μέγαρο Μουσικής
Αθήνα, 22 Μαρτίου 2018

1. Εισαγωγή, η αρχή της λογοδοσίας (accountability principle)
2. Οι υποχρεώσεις υπευθύνων και εκτελούντων την επεξεργασία από τη σκοπιά τεχνολογιών και διαδικασιών
   - Προστασία δεδομένων εκ σχεδιασμού και εξ ορισμού
   - Εκτίμηση αντικτύπου στην προστασία δεδομένων και προηγούμενη διαβούλευση
   - Ασφάλεια δεδομένων
   - Γνωστοποίηση παραβίασης δεδομένων
   - Καταγραφή επεξεργασιών
   - Κώδικες δεοντολογίας και πιστοποίηση
3. Βασικές τεχνολογίες
4. Πρότυπα και μεθοδολογίες
5. Συμπεράσματα από τη σκοπιά των Εποπτικών αρχών

Αρχή της Λογοδοσίας (accountability principle)

- Η αρχή της λογοδοσίας: ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωσή του με όλες τις άλλες αρχές που διέπουν την επεξεργασία δεδομένων
- (οι άλλες αρχές επεξεργασίας: νομιμότητα, αντικειμενικότητα και διαφάνεια, περιορισμός σκοπού, ελαχιστοποίηση, ακρίβεια, χρόνος τήρησης, ακεραιότητα, εμπιστευτικότητα και διαθεσιμότητα δεδομένων)
- Διαχείριση κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων με την εφαρμογή κατάλληλων οργανωτικών και τεχνικών μέτρων
- Κατάλληλες πολιτικές προστασίας δεδομένων
- Εγκεκριμένοι κώδικες δεοντολογίας ή μηχανισμοί πιστοποίησης μπορούν να χρησιμοποιηθούν ως στοιχεία απόδειξης της συμμόρφωσης με τις προβλέψεις του Γενικού Κανονισμού

Προστασία δεδομένων εκ σχεδιασμού και εξ ορισμού

Προστασία εκ σχεδιασμού

- State of the art
- Κόστος, φύση και πεδίο εφαρμογής, σκοποί επεξεργασίας
- Κίνδυνοι για δικαιώματα και ελευθερίες
- Καθορισμός οργανωτικών και τεχνικών μέτρων κατά την ανάπτυξη και εφαρμογή κατά τη λειτουργία

Προστασία εξ ορισμού

- Αρχική ρύθμιση φιλική στην προστασία δεδομένων
- Π.χ. κλειστή πρόσβαση – σχήμα εξουσιοδοτήσεων

Εκτίμηση αντικτύπου από την επεξεργασία δεδομένων και προηγούμενη διαβούλευση

Για επεξεργασίες υψηλού κινδύνου, πριν την εφαρμογή τους, υποχρέωση εκτίμησης αντικτύπου

Ζητείται η γνώμη του υπευθύνου προστασίας δεδομένων

Εποπτική αρχή δημοσιοποιεί λίστα επεξεργασιών υψηλού κινδύνου

Διαβούλευση με την εποπτική αρχή αν παραμένει υψηλός κίνδυνος

Εκτίμηση αντικτύπου από την επεξεργασία δεδομένων και προηγούμενη διαβούλευση

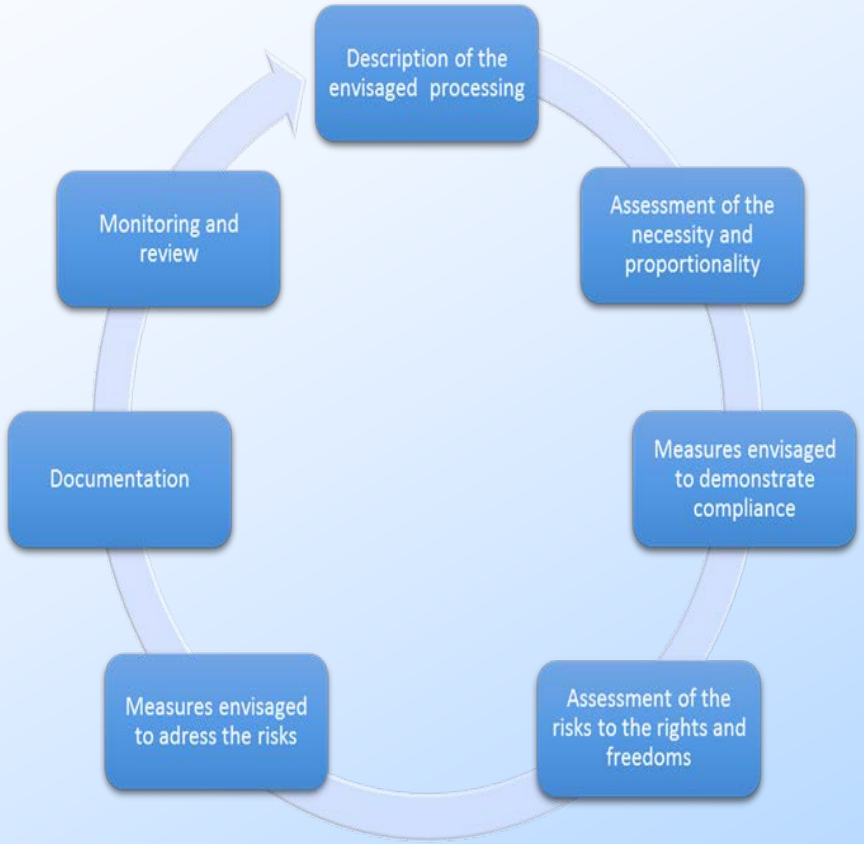
Ενδεικτικές επεξεργασίες υψηλού κινδύνου

- Συστηματική και εκτενής αξιολόγηση προσωπικών πτυχών – αυτοματοποιημένη λήψη αποφάσεων -δημιουργία προφίλ
- Ειδικές κατηγορίες δεδομένων – σε μεγάλη κλίμακα
- Παρακολούθηση δημοσίως προσβάσιμων χώρων – συστηματικά και σε μεγάλη κλίμακα

Κριτήρια κατευθυντηρίων γραμμών της ΟΕ29

- Αξιολόγηση – προφίλ-πρόβλεψη
- Αυτόματη λήψη αποφάσεων
- Συστηματική παρακολούθηση
- Ειδικές κατηγορίες δεδομένων
- Επεξεργασία ευρείας κλίμακας
  - Αριθμός φυσικών προσώπων
  - Όγκος δεδομένων,
  - Γεωγραφική κάλυψη
  - Χρόνος επεξεργασίας
- Συγχώνευση βάσεων δεδομένων
- Δεδομένα ευάλωτων προσώπων
- Νέες τεχνολογίες ή νέα χρήση, Διαβιβάσεις εκτός ΕΕ
- Επεξεργασία που μπορεί να εμποδίσει την άσκηση δικαιωμάτων ή λήψη υπηρεσιών

Εκτίμηση αντικτύπου από την επεξεργασία δεδομένων και προηγούμενη διαβούλευση



Μεθοδολογία (ISO, NIST, ENISA, εποπτικές αρχές)

Περιεχόμενα εκτίμησης

- Πράξεις επεξεργασίας, σκοποί, έννομο συμφέρον υπευθύνων επεξεργασίας.
- Εκτίμηση αναγκαιότητας και αναλογικότητας σε συνάρτηση με τους σκοπούς επεξεργασίας
- Εκτίμηση κινδύνων για τα δικαιώματα και ελευθερίες
- Μέτρα αντιμετώπισης κινδύνων
- Έλεγχος συμμόρφωσης και με κώδικες δεοντολογίας

Προηγούμενη διαβούλευση με την εποπτική αρχή

Επανεξέταση εκτίμησης και Δημοσίευση εκτίμησης

Εκτίμηση αντικτύπου από την επεξεργασία δεδομένων και προηγούμενη διαβούλευση

Εκτίμηση αναγκαιότητας και αναλογικότητας σε συνάρτηση με τους σκοπούς επεξεργασίας

- Νομιμότητα, αντικειμενικότητα και διαφάνεια της επεξεργασίας
- Περιορισμός του σκοπού
  - Συμβατοί οι σκοποί επιστημονικής, ιστορικής και στατιστικής έρευνας
- Περιορισμός χρόνου τήρησης
- Ελαχιστοποίηση και ακρίβεια δεδομένων
- Σεβασμός δικαιωμάτων
  - Ενημέρωσης, πρόσβασης, διόρθωσης, διαγραφής, φορητότητας δεδομένων κ.λπ.

Εκτίμηση κινδύνων για τα δικαιώματα και ελευθερίες

- Προέλευση, φύση, ιδιαιτερότητες και σοβαρότητα κινδύνων
- Οι κίνδυνοι παράνομης πρόσβασης, μη εξουσιοδοτημένης αλλαγής και απώλειας
- Ενδεχόμενες επιπτώσεις
- Απειλές που οδηγούν στους κινδύνους και πιθανότητες επέλευσης
- Εκτίμηση επιπτώσεων

Αντιμετώπιση κινδύνων, επιλογή και υλοποίηση μέτρων, περιοδική αναθεώρηση

Ασφάλεια επεξεργασίας

Κατάλληλο επίπεδο ασφάλειας

- Ψευδώνυμα, κρυπτογράφηση
- Διασφάλιση απορρήτου, ακεραιότητα, διαθεσιμότητα
- Αντιμετώπιση φυσικών ή τεχνικών συμβάντων
- Αξιολόγηση και αναθεώρηση μέτρων

Κατάλληλο επίπεδο-Αντιμετώπιση κινδύνων

Κώδικες δεοντολογίας και πιστοποίηση

Γνωστοποίηση παραβίασης δεδομένων

Υπεύθυνος επεξεργασίας

- Εντός 72 ωρών, γνωστοποίηση στην εποπτική αρχή – αιτιολόγηση για καθυστέρηση
- Εξαίρεση, ακίνδυνη για δικαιώματα και ελευθερίες φυσικών προσώπων

Εκτελών την επεξεργασία

- Μόλις αντιληφθεί

Γνωστοποίηση παραβίασης δεδομένων

Περιεχόμενα γνωστοποίησης

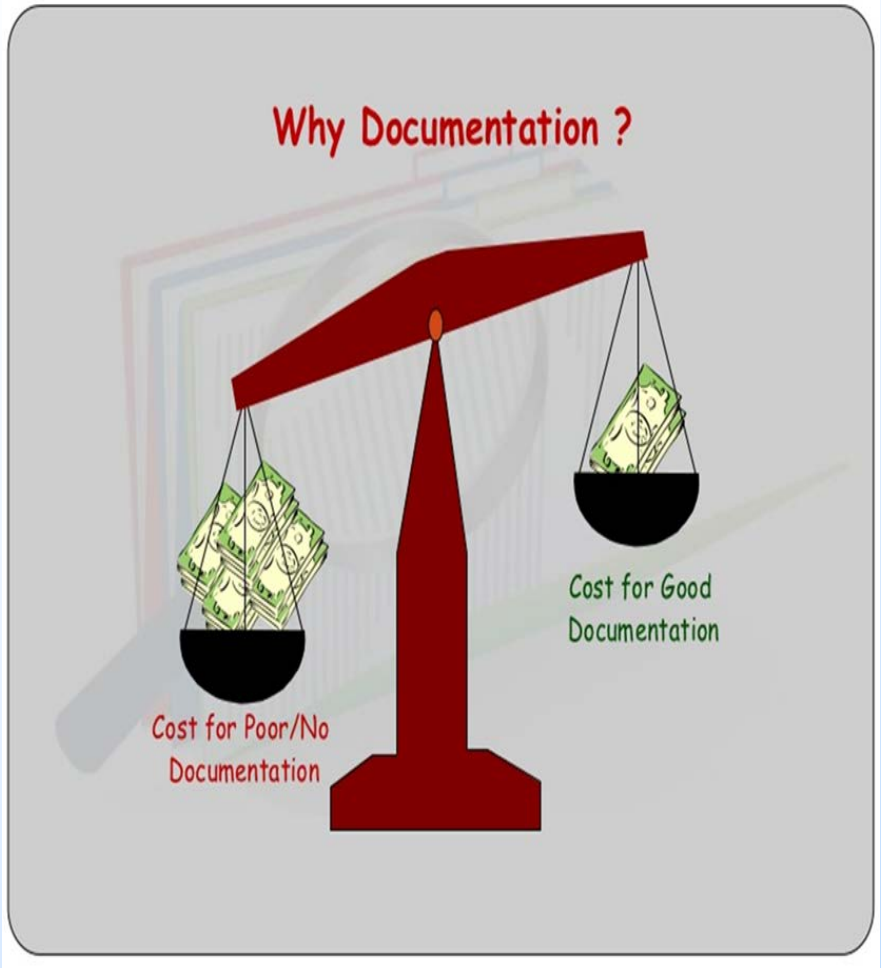
- Είδη δεδομένων και κατηγορίες υποκειμένων
- Όνομα και στοιχεία επικοινωνίας υπευθύνου προστασίας δεδομένων ή άλλου σημείου για περ. πληροφορίες
- Ενδεχόμενες συνέπειες
- Μέτρα αντιμετώπισης

Τεκμηρίωση

Ανακοίνωση στα υποκείμενα

- Υψηλός κίνδυνος για δικαιώματα και ελευθερίες
- Περιεχόμενα γνωστοποίησης
- Δεν απαιτείται ανακοίνωση, αν
  - Κατάλληλα μέτρα - κρυπτογράφηση
  - Εκ των υστέρων μέτρα που εξουδετερώνουν τους κινδύνους
  - Δυσανάλογη προσπάθεια – δημόσια ανακοίνωση
- Εποπτική αρχή μπορεί να ζητήσει να το πράξει

Καταγραφή επεξεργασιών



- Υπεύθυνος επεξεργασίας με >250 συνεργατών ή για επεξεργασίες υψηλού κινδύνου ή ειδικών κατηγοριών δεδομένων
- Για κάθε δραστηριότητα επεξεργασίας, τηρείται τεκμηρίωση με τα ακόλουθα στοιχεία:
  - Σκοποί επεξεργασίας
  - Δεδομένα και υποκείμενα
  - Αποδέκτες δεδομένων
  - Ενδεχόμενες διαβιβάσεις εκτός ΕΕ
  - Χρόνος τήρησης
  - Οργανωτικά και τεχνικά μέτρα προστασίας
- Παρόμοια υποχρέωση για τον εκτελούντα της επεξεργασία
- Κατόπιν αιτήματος, τίθεται στη διάθεση της εποπτικής αρχής

Κώδικες δεοντολογίας

Ενθαρρύνεται η εκπόνηση κωδίκων δεοντολογίας, ιδίως για πολύ μικρές, μικρές ή μεσαίες επιχειρήσεις

Εγκρίνεται από την εποπτική αρχή και δημοσιεύεται

Αν αφορά και άλλα κράτη μέλη, τότε η επάρκειά του κρίνεται από το ΕΣΠΔ και τίθεται σε ισχύ στην ΕΕ μετά από εκτελεστική πράξη της Επιτροπής

Παρακολούθηση τήρησης του κώδικα από τρίτους φορείς, διαπιστευμένους από την εποπτική αρχή. Η διαπίστευση μπορεί να ανακληθεί

Παραβίαση αρχών – κανόνων του κώδικα οδηγεί σε εξαίρεση του υπ. επεξεργασίας

Πιστοποίηση

- Ενθαρρύνεται η θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων, σφραγίδων και σημάτων
- Εφαρμογή από υπεύθυνους ή εκτελούντες την επεξεργασία
- Αποτελεί απόδειξη συμμόρφωσης με τον Γ. Κανονισμό, χωρίς όμως να περιορίζει τις υποχρεώσεις των υπευθύνων ή εκτελούντων την επεξεργασία
- Ούτε θίγονται οι αρμοδιότητες των εποπτικών αρχών
- Η πιστοποίηση γίνεται από φορέα πιστοποίησης ή την εποπτική αρχή
- Πιστοποίηση για μέγιστη περίοδο 3 ετών, δυνατότητα ανανέωσης, ανάκληση
- Μητρώο με μηχανισμούς πιστοποιήσεων, σφραγίδων και σημάτων τηρείται από το ΕΣΠΔ και είναι δημόσια προσβάσιμο

Διαπίστευση φορέων πιστοποίησης

- Κανονισμός (ΕΚ) αριθ. 765/200 και Πρότυπο EN-ISO/IEC 17065/2012
- Ειδικές απαιτήσεις-κριτήρια που ορίστηκαν από την εποπτική αρχή

Η Επιτροπή μπορεί να εκδίδει πράξεις σχετικά με τις απαιτήσεις που πρέπει να λαμβάνονται υπόψη από μηχανισμούς πιστοποίησης, καθώς και πράξεις σχετικά με τη θέσπιση τεχνικών προτύπων για μηχανισμούς πιστοποίησης, σφραγίδες και σήματα προστασίας δεδομένων, καθώς και μηχανισμούς για την προώθηση και την αναγνώριση των εν λόγω μηχανισμών πιστοποίησης, σφραγίδων και σημάτων

Βασικές Τεχνολογίες

- Κρυπτογραφικές τεχνικές
  - Καθιερωμένη κρυπτογραφία
    - Συμμετρική και ασύμμετρη κρυπτογραφία, ψηφιακές υπογραφές
  - Προηγμένη κρυπτογραφία
    - Τεχνικές μηδενικής γνώσης
    - Λειτουργική κρυπτογράφηση (identity-based, attribute-based)
    - Ομομορφική κρυπτογραφία
    - Ασφαλής πολυμερής υπολογισμός
  - Μετακβαντική κρυπτογραφία
- Ισχυρές (ψευδο-)τυχαίες ακολουθίες
- Συναρτήσεις κατακερματισμού ή (μονόδρομες συναρτήσεις)
- Μηχανισμοί ασφάλειας και προστασίας δεδομένων
- Ανωνυμοποίηση
  - K-anonymity, l-diversity, t-closeness
  - Διαφορική ιδιωτικότητα
- Ψευδωνυμοποίηση–Tokenization
- Blockchain

Πρότυπα και Μεθοδολογίες

- ISO/IEC 29134:2017, Information technology - Security techniques – Privacy impact assessment – Guidelines, Int. Organization for Standardization (ISO)
- ISO/IEC 29151, … — Code of practice for personally identifiable information protection
- ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO 31000
- NIST/SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations
- ENISA, κατευθυντήριες γραμμές ΟΕ29, εποπτικών αρχών Γαλλίας, Γερμανίας, Ηνωμένου Βασιλείου, Ισπανίας

ΣΥΜΠΕΡΑΣΜΑΤΑ από τη σκοπιά των ΕΠΟΠΤΙΚΩΝ ΑΡΧΩΝ

- Ιδιαίτερα απαιτητικές οι τεχνολογικές και διαδικαστικές πτυχές των υποχρεώσεων των υπευθύνων και εκτελούντων την επεξεργασία

- Κρίσιμης σημασίας να αποφύγει ο εθνικός νομοθέτης να επιβάλλει ως υποχρεωτική την προηγούμενη διαβούλευση με την εποπτική αρχή για σειρά επεξεργασιών ή ακόμη και αδειοδοτήσεις ή γνωστοποιήσεις πέραν αυτών που προβλέπει ήδη ο ΓΚΠΔ

- Η εποπτική αρχή μπορεί να είναι αποτελεσματική μόνο αν έχει διαχειρίσιμο όγκο εργασιών και τη δυνατότητα ιεράρχησης των εργασιών της

Ευχαριστώ πολύ για την προσοχή σας!

zorkadis@dpa.gr