TRAIN-GR-CY

REC-DATA-2016/REC-DATA-2016-01

Problem-based training activities on data protection reform

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

1ο Εκπαιδευτικό Σεμινάριο για DPOs

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Centre for European Constitutional Law
Themistokles and Dimitris Tsatsos Foundation

University of Cyprus

Hellenic Republic
National and Kapodistrian University of Athens
Est. 1837

TRAIN-GR-CY

REC-DATA-2016/REC-DATA-2016-01

Πηγή χρηματοδότησης: European Commission, Rights, Equality and Citizenship Programme

Αριθμός συμβολαίου: 769169

Εταίροι:

Κέντρο Ευρωπαϊκού Συνταγματικού Δικαίου - Ίδρυμα Θεμιστοκλή και Δημήτρη Τσάτσου, συντονιστής,

Ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα,

Γραφείο Επιτρόπου προστασίας Δεδομένων Προσωπικού Χαρακτήρα της Κύπρου,

Πανεπιστήμιο Κύπρου και Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών

Ποσό χρηματοδότησης: 303.086,17 Ευρώ

Διάρκεια: 1/1/2018 – 31/1/2020 (24 μήνες)

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

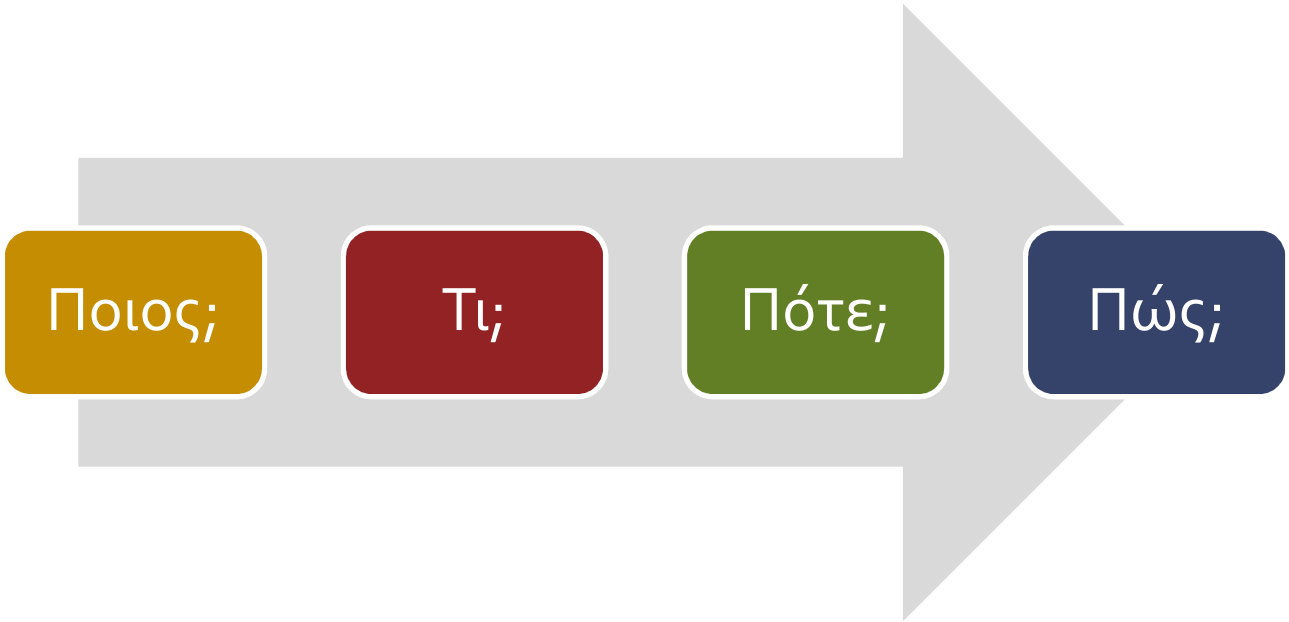
www.dpa.gr

Centre for European Constitutional Law
Themistokles and Dimitris Tsatsos Foundation

University of Cyprus

Hellenic Republic
National and Kapodistrian University of Athens
EST. 1837

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων



ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

Ποιος;

- Νομική υποχρέωση μόνο για τον υπεύθυνο επεξεργασίας
- Ο υπεύθυνος επεξεργασίας οφείλει, «όποτε ενδείκνυται», να «ζητεί τη γνώμη των υποκειμένων των δεδομένων ή των εκπροσώπων τους»
- Άλλοι ειδικοί ρόλοι και αρμοδιότητες , ανάλογα με την εσωτερική πολιτική, τις διαδικασίες και τους κανόνες
- Ο εκτελών συνδράμει στην διενέργεια της εκτίμησης
- Ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη του υπευθύνου προστασίας δεδομένων (ΥΠΔ)

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

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

Τι;

- Εργαλείο ελέγχου **&** απόδειξης συμμόρφωσης με ΓΚΠΔ
- Εργαλείο εντοπισμού - ανάλυσης κινδύνων για τα υποκείμενα κατά τη χρήση τεχνολογίας ή συστήματος από έναν οργανισμό στους διάφορους ρόλους των υποκειμένων (ως πολίτες, πελάτες, ασθενείς κ.λ.π)
- Με βάση την ανάλυση των αποτελεσμάτων, επιλογή και εφαρμογή των κατάλληλων μέτρων που αποκαθιστούν (**remedy**) τους κινδύνους.
- Η έννοια της εκτίμησης αντικτύπου στην ιδιωτικότητα υπάρχει πριν από τον ΓΚΠΔ (π.χ WP29, UK, CNIL, ISO / IEC 29134 , εκτός Ε.Ε, μεθοδολογίες, εργαλεία).

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

Περιεχόμενο ΕΑΠΔ στον ΓΚΠΔ

Τι;

- Συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας (+νομική βάση)
- Εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας
- Εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων
- Τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων

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

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

Τι;

Προσέγγιση με βάση τον Κίνδυνο

- Information Management System - προσωπικά δεδομένα

Διαχείριση Κινδύνων Προσωπικών Δεδομένων διαφέρει από "κλασική" Διαχείριση Κινδύνων Ασφαλείας

- Κίνδυνοι για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, όχι μόνο για τον υπεύθυνο επεξεργασίας
- Τυχόν δευτερεύουσες δυσμενείς επιπτώσεις
- Αποδεκτός κίνδυνος
- Τα τεχνικά και οργανωτικά μέτρα διαφέρουν από τα κλασικά μέτρα ασφάλειας.

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

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

Στόχοι προστασίας

Τι;

- Εμπιστευτικότητα
- Ακεραιότητα
- Διαθεσιμότητα

- Διαφάνεια
- Μη συνδεσιμότητα Unlinkability
- Δυνατότητα επέμβασης Intervenability

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

Τι;

- Αντιμετώπιση κινδύνων
  - Μείωση
  - Διατήρηση
  - Αποφυγή
  - Μετάθεση
- Επιλογή μέτρων μείωσης κινδύνων
  - ISO/IEC 27002
  - ISO/IEC 29151
  - Εθνικά πρότυπα, λίστες εποπτικών αρχών ή άλλων οργανισμών
- Πλάνο υλοποίησης μέτρων
- Παρακολούθηση και αναθεώρηση

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

Πότε;

- Πριν από την έναρξη της επεξεργασίας
- Σε υφιστάμενες πράξεις επεξεργασίας που ενδέχεται να επιφέρουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων και στις οποίες έχει επέλθει μεταβολή των κινδύνων, λαμβανομένης υπόψη της φύσης, του πεδίου εφαρμογής, του πλαισίου και των σκοπών της επεξεργασίας.
- Δεν απαιτείται ΕΑΠΔ σε πράξεις επεξεργασίας που έχουν ελεγχθεί από εποπτική αρχή και υλοποιούνται χωρίς καμία μεταβολή από τον προηγούμενο έλεγχο.
- Η ΕΑΠΔ αποτελεί διαρκή διαδικασία και όχι πράξη που διενεργείται άπαξ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

Πότε;

- Υποχρεωτικό όταν "*...ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων*"
  - 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
- Οι Αρχές ορίζουν καταλόγους με επεξεργασίες που απαιτείται ΕΑΠΔ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

Πότε;

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
- Επεξεργασία που μπορεί να εμποδίσει την άσκηση δικαιωμάτων ή λήψη υπηρεσιών

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Παραδείγματα επεξεργασιών με απαίτηση ΕΑΠΔ

Πότε;

- Γενετικών και δεδομένων υγείας
- Παρακολούθηση της κυκλοφορίας και με ευφυή συστήματα αυτόματης αναγνώρισης αριθμών κυκλοφορίας
- Συστηματική παρακολούθηση δραστηριοτήτων εργαζομένων
- Προφίλ από Κοινωνικά Δίκτυα
- Αξιολόγηση πιστοληπτικής ικανότητας
- Αρχειοθέτηση ψευδωνυμοποιημένων ευαίσθητων δεδομένων ευάλωτων ατόμων από ερευνητικά έργα ή κλινικές δοκιμές

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων – κατάλογος Ελλάδα

Πότε;

- *1η κατηγορία*: με βάση τα είδη και τους σκοπούς επεξεργασίας
- *2η κατηγορία:* με βάση το είδος των δεδομένων και/ή τις κατηγορίες των υποκειμένων
- *3η κατηγορία:* με βάση τα πρόσθετα χαρακτηριστικά και/ή τα χρησιμοποιούμενα μέσα της επεξεργασίας
- Υποχρεωτική
  - όταν πληρείται τουλάχιστον ένα από τα κριτήρια της 1ης ή της 2ης κατηγορίας.
  - όταν συντρέχει ένα τουλάχιστον κριτήριο ως προς την 3η κατηγορία και η επεξεργασία αφορά είδη και σκοπούς επεξεργασίας της 1ης κατηγορίας, ή/και είδη δεδομένων ή/και κατηγορίες υποκειμένων της 2ης κατηγορίας.

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων – κατάλογος Ελλάδα - υγεία

Πότε;

<u>1η κατηγορία</u>:

*... 1.1 Συστηματική αξιολόγηση, βαθμολόγηση, πρόβλεψη, πρόγνωση και κατάρτιση προφίλ, ιδίως πτυχών που αφορούν την οικονομική κατάσταση, την **υγεία**, τις προσωπικές προτιμήσεις ή ενδιαφέροντα, την αξιοπιστία ή τη συμπεριφορά, τη θέση ή τις κινήσεις ή την πιστοληπτική ικανότητα των υποκειμένων των δεδομένων. Π.χ εταιρεία βιοτεχνολογίας παρέχει απευθείας στους καταναλωτές γενετικές δοκιμές για να εκτιμήσει και να προβλέψει τους κινδύνους νόσου/υγείας.*

*... 1.6 Μεγάλης κλίμακας συστηματική επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν **την υγεία και τη δημόσια υγεία** για σκοπούς δημοσίου συμφέροντος, όπως η εισαγωγή και χρήση συστημάτων ηλεκτρονικής συνταγογράφησης και η εισαγωγή και χρήση ηλεκτρονικού φακέλου ή ηλεκτρονικής κάρτας υγείας.*

<u>2η κατηγορία:</u>

*... 2.1 Μεγάλης κλίμακας επεξεργασία των **ειδικών κατηγοριών δεδομένων** (περιλαμβανομένων των γενετικών και των βιομετρικών με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου) που αναφέρονται στο άρθρο 9 παρ. 1 και των δεδομένων που αναφέρονται στο άρθρο 10 του ΓΚΠΔ.*

<u>3η κατηγορία:</u>

*... 3.1 Καινοτόμος χρήση ή **εφαρμογή νέων τεχνολογιών ή οργανωτικών λύσεων**, οι οποίες μπορεί να περιλαμβάνουν νέες μορφές συλλογής και χρήσης δεδομένων, με ενδεχόμενο υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων ...*

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

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

Πώς;

Βήμα 1
- Ορισμός ομάδας έργου
- Εκτίμηση ανάγκης για διενέργεια ΕΑΠΔ - Τεκμηρίωση

Βήμα 2
- Επιλογή μεθοδολογίας
- Διεξαγωγή – καθορισμός μέτρων
- Δέσμευση συνεισφορά εμπλεκομένων

Βήμα 3
- Παρακολούθηση υλοποίησης μέτρων
- Διαβούλευση με Αρχή

Βήμα 4
- Τεκμηρίωση
- Δημοσίευση

Βήμα 5
- Έλεγχος
- Ανασκόπηση

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Διαβούλευση με Αρχή μετά το ΕΑΠΔ

- Εάν δεν έχουν προσδιοριστεί επαρκή μέτρα για τη μείωση των κινδύνων σε αποδεκτό επίπεδο (δηλαδή οι υπολειπόμενοι κίνδυνοι παραμένουν υψηλοί)
- Η Αρχή παρέχει γραπτώς συμβουλές εντός προθεσμίας μέχρι οκτώ εβδομάδων από την παραλαβή του αιτήματος διαβούλευσης

(δυνατότητα παράτασης προθεσμίας κατά έξι εβδομάδες, λόγω της πολυπλοκότητας που χαρακτηρίζει τη σχεδιαζόμενη επεξεργασία με ενημέρωση ενδιαφερομένων. Οι προθεσμίες μπορούν να αναστέλλονται έως η Αρχή λάβει τις πληροφορίες που ζήτησε για τους σκοπούς της διαβούλευσης).

Σχέση ΕΑΠΔ με υποχρέωση Γνωστοποίησης Περιστατικών Παραβίασης Δεδομένων

- Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων παρέχει τεκμηρίωση/καθοδήγηση σε περίπτωση περιστατικού παραβίασης

  - Απόφαση για τη γνωστοποίηση ή μη στην Αρχή
  - Απόφαση για ενημέρωση υποκειμένων
  - Εφαρμογή κατάλληλων μέτρων ασφάλειας

TRAIN-GR-CY

REC-DATA-2016/REC-DATA-2016-01

Problem-based training activities on data protection reform

Ευχαριστούμε για την προσοχή σας

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Centre for European Constitutional Law
Themistokles and Dimitris Tsatsos Foundation

University of Cyprus

Hellenic Republic
National and Kapodistrian University of Athens
EST. 1837