TRAIN-GR-CY

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

Problem-based training activities on data protection reform

Περιστατικά παραβίασης προστασίας προσωπικών δεδομένων

1ο Εκπαιδευτικό Σεμινάριο για DPOs

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

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

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 ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Παραβίαση δεδομένων προσωπικού χαρακτήρα

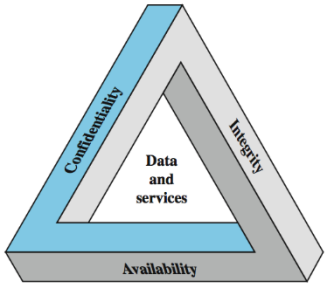
Τι εννοείται για το ΓΚΠΔ;

«Η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία»

- Ο ΓΚΠΔ εφαρμόζεται **μόνο όταν υπάρχουν προσωπικά δεδομένα**
- **Περιστατικά προστασίας δεδομένων ⊂ Περιστατικά ασφάλειας**

Τύποι περιστατικών παραβίασης προστασίας δεδομένων:

Παραβίαση: { **Εμπιστευτικότητας** / **Διαθεσιμότητας** / **Ακεραιότητας** } ή συνδυασμός



Καινοτομίες του ΓΚΠΔ:

- Καταγραφή όλων των περιστατικών
- Γνωστοποίηση όσων ενέχουν κίνδυνο στην Εποπτική Αρχή
- Ενημέρωση επηρεαζόμενων προσώπων για υψηλό κίνδυνο

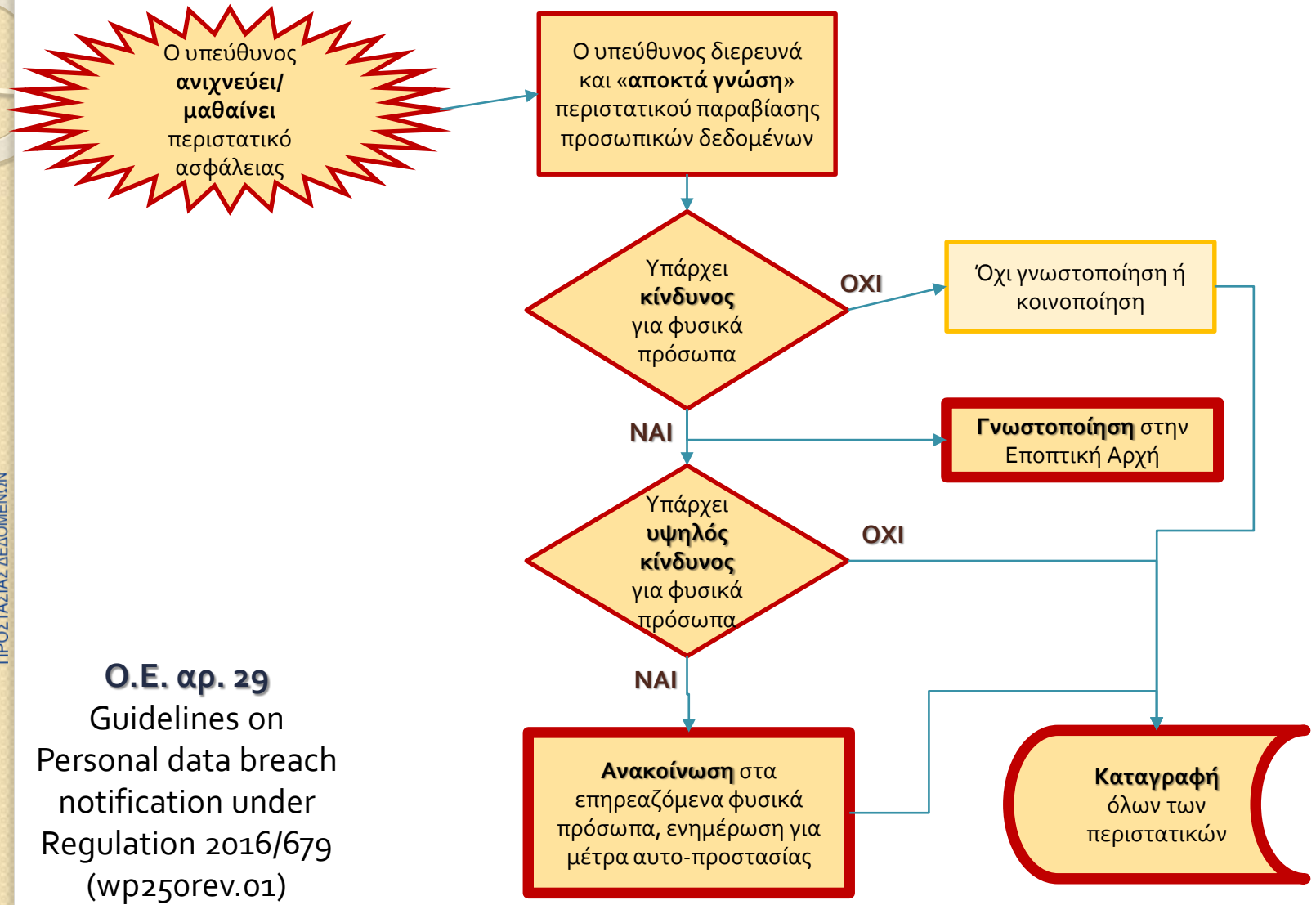
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Παραβίαση δεδομένων προσωπικού χαρακτήρα

Η διαδικασία



O.E. αρ. 29
Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01)

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

...η στιγμή που ο υπεύθυνος αποκτά γνώση του γεγονότος ...

- **Μη αντικειμενικός** ο ορισμός χρονικής στιγμής (εξαρτάται από τις συνθήκες)
- Έμφαση στις **άμεσες ενέργειες** για την εκτίμηση αν μια αναφορά περιστατικού είναι παραβίαση προσωπικών δεδομένων.
  - Ο χρόνος διερεύνησης δεν «προσμετράται», αρκεί να είναι άμεση η αντίδραση.
  - Σημαντικός βαθμός βεβαιότητας ότι συνέβη παραβίαση => ξεκινάει το "χρονόμετρο"

Σημεία προσοχής:

  - Εσωτερικές διαδικασίες διερεύνησης και χειρισμού περιστατικών,
  - Αναφορά των ευρημάτων στα κατάλληλα πρόσωπα εντός του υπεύθυνου επεξεργασίας
  - Διαδικασίες που καλύπτουν και τους εκτελούντες την επεξεργασία

- Αν ο εκτελών αντιληφθεί παραβίαση ενημερώνει τον υπεύθυνο αμελλητί!
  - Ο χρόνος μετράει για τον υπεύθυνο, από τη στιγμή που ενημερωθεί.
  - Ασφαλέστερο: άμεση, βασικού επιπέδου, ενημέρωση. Λεπτομέρειες σε 2η φάση.
  - Ο εκτελών μπορεί να γνωστοποιήσει ο ίδιος, μόνο αν αυτό προβλέπεται συμβατικά.
  - Αναθέσεις πολλών επιπέδων ενέχουν ιδιαίτερο κίνδυνο καθυστερημένων αντιδράσεων.

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

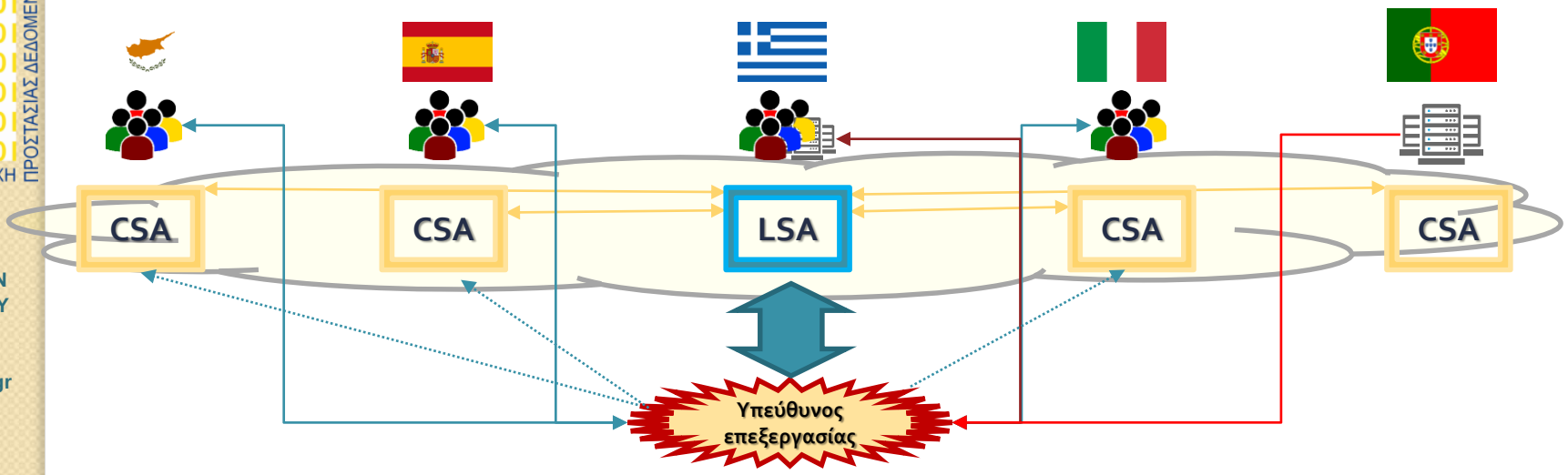
Πληροφορίες προς την Εποπτική Αρχή εντός 72 ωρών

- α) **φύση της παραβίασης** δεδομένων προσωπικού χαρακτήρα,
  - κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων υποκειμένων των δεδομένων
  - κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων αρχείων
- β) όνομα και στοιχεία επικοινωνίας DPO ή άλλου σημείου **άμεσης επικοινωνίας**
- γ) **ενδεχόμενες συνέπειες** της παραβίασης
- δ) ληφθέντα ή προτεινόμενα προς λήψη **μέτρα** από τον υπεύθυνο επεξεργασίας
  - για την **αντιμετώπιση της παραβίασης** των δεδομένων προσωπικού χαρακτήρα
  - μέτρα για την **άμβλυνση ενδεχόμενων δυσμενών συνεπειών** της (όπου ενδείκνυται)
- Χρήσιμο είναι επίσης να προσδιορίζεται και τυχόν **εκτελών την επεξεργασία**
  - ιδίως επειδή μπορεί να υπάρχουν και άλλα ανάλογα περιστατικά.
- Υπέρβαση των 72 ωρών μόνο *με ειδική αιτιολόγηση της καθυστέρησης*.
- Στόχος της διάταξης: **οι πολίτες να είναι σε θέση να αντιμετωπίσουν τα αποτελέσματα της παραβίασης**
  - Η Εποπτική Αρχή ενημερώνεται για να επιβλέπει τις ενέργειες του υπεύθυνου
  - Σε σύνθετα περιστατικά η γνωστοποίηση μπορεί να γίνει σε φάσεις. Ο υπεύθυνος πρέπει όμως να μπορεί να αποδείξει την αναγκαιότητα της τμηματικής γνωστοποίησης.

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

Σε ποια Εποπτική Αρχή υποβάλλεται η γνωστοποίηση;

- Ως αρχή, η γνωστοποίηση γίνεται **σε μία Εποπτική Αρχή**, την «Επικεφαλής Εποπτική Αρχή» (LSA) όπως ορίζεται στο άρ. 56 του ΓΚΠΔ.
- Η **LSA** είναι ο **μοναδικός συνομιλητής** υπευθύνου ή εκτελούντος για διασυνοριακή πράξη επεξεργασίας
- Για τον ορισμό της LSA συμβουλευτείτε τη σχετική γνώμη του αρ. 29 (wp244)
  - Σε περίπτωση αμφιβολίας για την LSA, ενημέρωση, τουλάχιστον, της Αρχής του κράτους όπου έχει συμβεί το περιστατικό.
  - Σε κάθε περίπτωση, πρέπει να αναφέρονται οι επηρεαζόμενες χώρες (λόγω Φ.Π. ή εγκαταστάσεων)
  - Προληπτικά, μπορεί επίσης να γνωστοποιηθεί και σε Αρχές χωρών των οποίων οι πολίτες επηρεάζονται
  - Φόρμα/μέθοδος γνωστοποίησης μπορεί να διαφέρει ανά κράτος μέλος (με κοινά στοιχεία)



ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Πότε **δεν** απαιτείται γνωστοποίηση στην Εποπτική Αρχή;

- Παραβίαση δεδομένων προσωπικού χαρακτήρα που **δεν ενδέχεται** να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, δεν απαιτείται να γνωστοποιηθεί!

Πότε «δεν ενδέχεται να προκληθεί κίνδυνος;»

Και οι 3 παράμετροι της ασφάλειας πρέπει να ικανοποιούνται:

- **Απόρρητο**: Τα προσωπικά δεδομένα να έχουν καταστεί ακατάληπτα σε τρίτους
  - κρυπτογράφηση - tokenization
- **Διαθεσιμότητα**: Υπάρχει αντίγραφο ασφαλείας - η υπηρεσία επαναλειτουργεί σε εύλογο χρόνο
- **Ακεραιότητα**: Δεν έχουν αλλοιωθεί δεδομένα

Προσοχή: Αν στο μέλλον υπάρξει αλλαγή στο "state of the art" ίσως τότε απαιτηθεί γνωστοποίηση!

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Πληροφορίες προς τα υποκείμενα - Ανακοίνωση

- *Όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να θέσει σε **υψηλό κίνδυνο** τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας ανακοινώνει **αμελλητί** την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων.*
- Υποχρέωση ενημέρωσης μόνο για τα **υψηλού κινδύνου** περιστατικά
  - ενώ στην Αρχή γνωστοποιούνται όλα όσα ενέχουν κίνδυνο
- **Αμελλητί**: Στόχος η προστασία των υποκειμένων με μέτρα που αυτά θα λάβουν.
  - **Αμελλητί < 72 ωρών!!!**
  - Μπορεί να καθυστερήσει αν υπάρχει ανάγκη αντιμετώπισης άλλων κινδύνων (π.χ. να διορθωθεί πρώτα το πρόβλημα που προκάλεσε το περιστατικό ή να γίνει, άμεσα, διερεύνηση από αρχή επιβολής του νόμου)
- Οι πληροφορίες είναι πρακτικά οι ίδιες με της γνωστοποίησης στην Εποπτική Αρχή.
  - Έμφαση στις συστάσεις προς τα ενδιαφερόμενα φυσικά πρόσωπα για τον μετριασμό δυνητικών δυσμενών συνεπειών

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Επικοινωνία με τα υποκείμενα των δεδομένων

- **Ατομική επικοινωνία**, ειδικά για την παραβίαση
  - Ειδική, όχι ως τμήμα άλλης ενημέρωσης
  - Επιλογή του(ων) μέσου(ων) **με μεγιστοποίηση της πιθανότητας** λήψης της ενημέρωσης (email, SMS, Instant messages, banners, ταχυδρομείο, ανακοινώσεις σε ΜΜΕ κλπ).
  - Κατανοητή και ξεκάθαρη, στη γλώσσα των υποκειμένων (ή τουλάχιστον στην ίδια γλώσσα με τη συλλογή)
  - Συμβουλευτείτε και WP260 – «Guidelines on transparency under Regulation 2016/679»
- Συνεργασία με Αρχή για την επιλογή του κατάλληλου μέσου.

Πότε δεν απαιτείται ανακοίνωση στα υποκείμενα;

- Όταν δεν απαιτείται και η γνωστοποίηση στην Αρχή
  - Ακατάληπτα δεδομένα, μικρός κίνδυνος
- Ο υπεύθυνος επεξεργασίας έλαβε μέτρα αμέσως μετά το περιστατικό και **δεν είναι πλέον πιθανό** να προκύψει υψηλός κίνδυνος
- Όταν η ατομική ενημέρωση προϋποθέτει δυσανάλογες προσπάθειες.
  - Τότε απαιτείται δημόσια ανακοίνωση ή παρόμοιο μέτρο
- Η Αρχή μπορεί να διατάξει να γίνει η επικοινωνία
  - Έχει τον τελευταίο λόγο για την αξιολόγηση του υψηλού κινδύνου.

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Αξιολόγηση κινδύνων

Πότε έχουμε Υψηλό Κίνδυνο;

- Διαφορές με την DPIA:
  - Δεν υφίσταται πλέον *πιθανότητα επέλευσης* ενός κινδύνου για την επεξεργασία, αλλά **βεβαιότητα**.
  - Υπάρχει **πιθανότητα υλοποίησης** ενός κινδύνου για τα υποκείμενα των δεδομένων!

Παράγοντες

Τύπος παραβίασης
απόρρητο, διαθεσιμότητα, ακεραιότητα

Σοβαρότητα των επιπτώσεων στα υποκείμενα
Υποκλοπή ταυτότητας, Απάτη, Διακρίσεις, Φυσικοί κίνδυνοι, Ψυχολογική πίεση, Διαπόμπευση, Βλάβη στη φήμη, Άρνηση κρίσιμης υπηρεσίας. Ποια η σχέση Υπεύθυνου – «Αποδέκτη» δεδομένων;

Φύση και ποσότητα των δεδομένων
Ευαίσθητα/απλά; Μπορεί να χρησιμοποιηθούν για υποκλοπή ταυτότητας; Αποκαλύπτουν πληροφορίες που μπορεί να δημιουργήσουν «πρόβλημα» στα υποκείμενα

Ευκολία προσωποποίησης /αναγνώρισης
άμεση ή έμμεση αναγνώριση; Ψευδωνυμοποίηση

Κατηγορίες /ειδικά χαρακτηριστικά των υποκειμένων
παιδιά, ευάλωτες ομάδες, κτλ.

Ειδικά χαρακτηριστικά του υπευθύνου επεξεργασίας
Κυρίως αντικείμενο εργασιών (π.χ. Ιατρικό κέντρο)

Αριθμός υποκειμένων (;)
…χωρίς να σημαίνει ότι οι επιπτώσεις σε ένα και μόνο υποκείμενο δεν μπορεί να είναι σοβαρές.

Η ΟΕ του αρ. 29 παραπέμπει ως συμβουλή για τη μεθοδολογία αξιολόγησης κινδύνων στα κείμενα του ENISA

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Τεκμηρίωση – καταγραφή περιστατικών

- Αρ. 33 παρ. 5 (εφαρμογή αρχής της λογοδοσίας)

Ο υπεύθυνος επεξεργασίας τεκμηριώνει κάθε παραβίαση δεδομένων προσωπικού χαρακτήρα, που συνίστανται στα πραγματικά περιστατικά που αφορούν την παραβίαση δεδομένων προσωπικού χαρακτήρα, τις συνέπειες και τα ληφθέντα διορθωτικά μέτρα. Η εν λόγω τεκμηρίωση επιτρέπει στην εποπτική αρχή να επαληθεύει τη συμμόρφωση προς το παρόν άρθρο

- Υποχρέωση τήρησης **εσωτερικού μητρώου περιστατικών παραβίασης**, ανεξάρτητα αν πρέπει να γνωστοποιούνται στην Αρχή.
- Το αρχείο αυτό χρησιμοποιείται, μεταξύ άλλων, **για να επιδειχθεί η συμμόρφωση** σε τυχόν έλεγχο της Αρχής.
  - Άρα, πρέπει να καταγράφονται και τα στοιχεία που αποδεικνύουν τη συμμόρφωση (π.χ. οι εκτιμήσεις κινδύνου που οδήγησαν στην απόφαση να μη γνωστοποιηθεί το περιστατικό)
- Οι υπεύθυνοι οφείλουν να διερευνούν κάθε περιστατικό, χωρίς να επιβαρύνουν τις Εποπτικές Αρχές με πληροφορίες για τα περιστατικά που θεωρούν μικρής επικινδυνότητας.

Διαδικασία χειρισμού περιστατικών παραβίασης

1. **Προετοιμασία** για την αντιμετώπιση των περιστατικών
   - Προετοιμασία πολιτικής χειρισμού περιστατικών
   - Καθορισμός ομάδας χειρισμού περιστατικών
2. **Αναγνώριση** και αναφορά των περιστατικών
3. **Αξιολόγηση** των περιστατικών, απόφαση για τον τρόπο αντιμετώπισής τους
   - Π.χ. επιδιόρθωση για λόγους επιχειρησιακής συνέχεια ή δικανική συλλογή δεδομένων (**forensics**) ακόμα κι αν καθυστερήσει η λειτουργία της επιχείρησης;
4. **Αντιμετώπιση** των περιστατικών
   - Περιορισμός
   - Διερεύνηση
   - Επίλυση προβλημάτων
5. **Απόκτηση γνώσης** από τα περιστατικά
   - Όχι μόνο να βρεθεί πως θα μπορούσε να είχε αποφευχθεί το περιστατικό
   - Επικέντρωση και σε αλλαγή και βελτίωση των διαδικασιών

Χρήσιμα πρότυπα:

ISO/IEC 27035-1,2:2016 (Information technology -- Security techniques -- Information security incident management -- Part 1: Principles of incident management, Part 2: Guidelines to plan and prepare for incident response)

NIST 800-61 rev.2 Computer Security Incident Handling Guide

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

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 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