Ασφάλεια επεξεργασίας και Γνωστοποίηση Περιστατικών Παραβίασης Δεδομένων

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Γεώργιος Ρουσόπουλος

Δρ. Μηχ. Η/Υ & Πληροφορικής

Ε.Ε.Π. - Α.Π.Δ.Π.Χ.

grousopoulos at dpa.gr

Κωνσταντίνος Λιμνιώτης

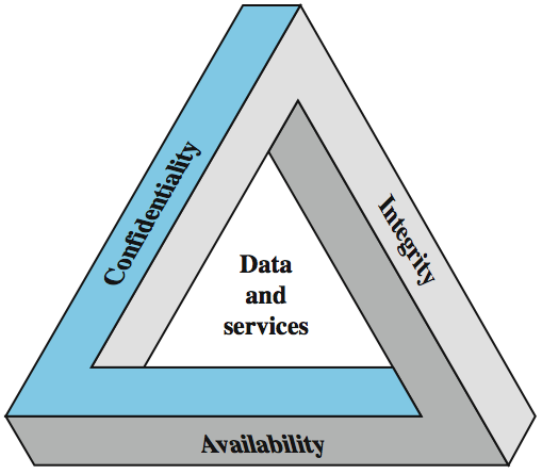
Δρ. Πληροφορικής και Τηλ/νιών

Ε.Ε.Π. - Α.Π.Δ.Π.Χ.

klimniotis at dpa.gr

Η έννοια της ασφάλειας

- Ασφάλεια δικτύων και πληροφοριών
  - Παραδοσιακά, ο όρος χρησιμοποιείται για να περιγράψει τη συλλογή εργαλείων/τεχνικών που αναπτύσσονται προκειμένου να επιτευχθούν οι εξής στόχοι:
    - **Εμπιστευτικότητα (Confidentiality),**
    - **Ακεραιότητα (Integrity)**
    - **Διαθεσιμότητα (Availability)**



- Τρίπτυχο **C.I.A.**

- Πλήγμα σε οποιοδήποτε από τα ανωτέρω, από τυχαία ή εσκεμμένη ενέργεια, συνιστά – γενικά – περιστατικό ασφάλειας

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Στόχοι Ασφάλειας

- Εμπιστευτικότητα (confidentiality)
  - Οι πληροφορίες δεν πρέπει να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα
- Ακεραιότητα (integrity)
  - Οι πληροφορίες πρέπει να είναι ακέραιες, γνήσιες – όχι αλλοιωμένες/τροποποιημένες
- Διαθεσιμότητα (availability)
  - Η εξασφάλιση ότι τα δεδομένα και οι συναφείς υπηρεσίες θα είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους
- Όταν η πληροφορία αφορά προσωπικά δεδομένα, οι ανωτέρω ορισμοί ισχύουν αντιστοίχως

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

Η ασφάλεια στο ΓΚΠΔ

- **Άρθρο 32**: (…) ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση:
  - α) της ψευδωνυμοποίησης και της κρυπτογράφησης δεδομένων προσωπικού χαρακτήρα,
  - β) της δυνατότητας διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση,
  - γ) της δυνατότητας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση συμβάντος ασφάλειας λόγω φυσικού ή τεχνικού λόγου,
  - δ) διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.
- Κατά την εκτίμηση του ενδεδειγμένου επιπέδου ασφάλειας λαμβάνονται ιδίως υπόψη οι κίνδυνοι που απορρέουν από την επεξεργασία (…)

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Τι νέο εισάγει ο ΓΚΔΠ ως προς την ασφάλεια;

- Εξειδίκευση, με πρόταση «ενδεδειγμένων» τεχνικών και οργανωτικών μέτρων:
  - Ψευδωνυμοποίηση και Κρυπτογράφηση
  - Διασφάλιση Απορρήτου, Ακεραιότητας, Διαθεσιμότητας και **Αξιοπιστίας**
  - Αποκατάσταση Διαθεσιμότητας και της πρόσβασης σε περίπτωση συμβάντος
  - Δοκιμή, εκτίμηση και διαρκής αξιολόγηση της αποτελεσματικότητας των μέτρων
- Προκύπτουν λαμβάνοντας υπόψη (πρβλ. αρ. 25):
  - τις τελευταίες εξελίξεις,
  - το κόστος εφαρμογής,
  - τα χαρακτηριστικά της επεξεργασίας (φύση - πεδίο εφαρμογής - πλαίσιο – σκοποί)
- Κρίσιμος παράγοντας η σωστή αξιολόγηση των κινδύνων και των πιθανών συνεπειών
- Χρήση εγκεκριμένου κώδικα δεοντολογίας ή μηχανισμού πιστοποίησης για την απόδειξη της συμμόρφωσης.....
- Διαδικασίες διαχείρισης περιστατικών παραβίασης.....

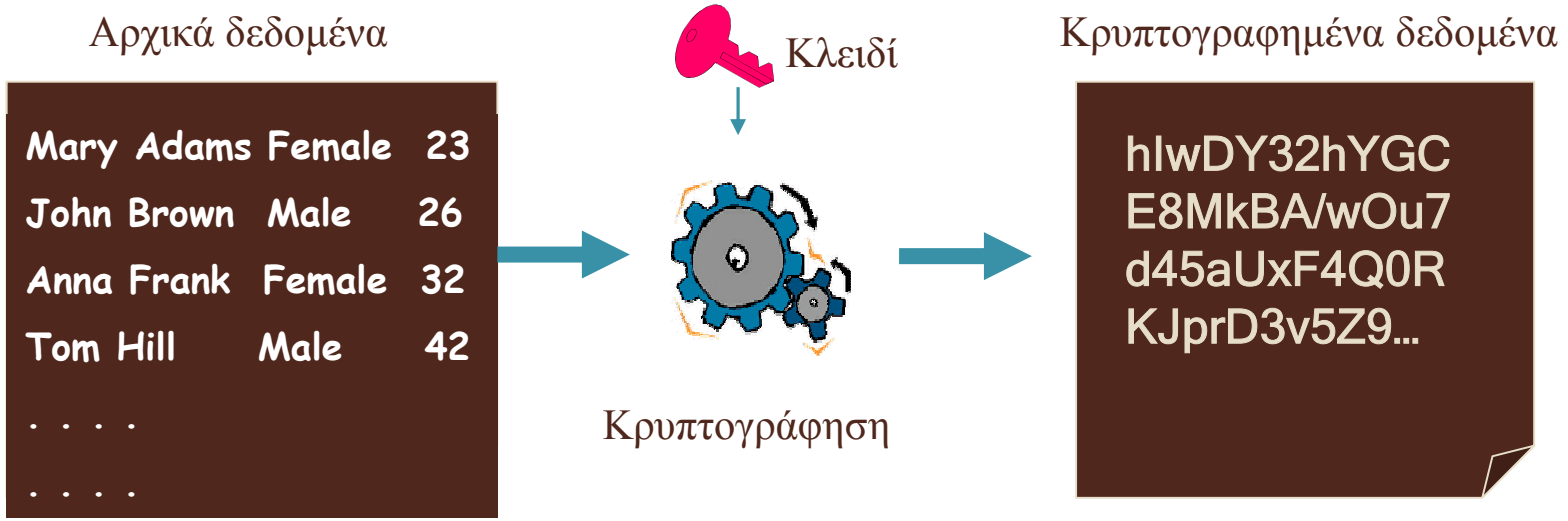
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Η κρυπτογράφηση ως μέσο ασφάλειας

- Τα δεδομένα μετασχηματίζονται σε ακατάληπτη μορφή με βάση κάποιον αλγόριθμο αλλά και με τη χρήση ενός μυστικού κλειδιού.
- Μόνο όποιος γνωρίζει το μυστικό κλειδί μπορεί να ανακτήσει τα αρχικά δεδομένα από τα κρυπτογραφημένα
  - Άρα, είναι αντιστρεπτή η διαδικασία (αποκρυπτογράφηση), αλλά μόνο από εξουσιοδοτημένους χρήστες, που γνωρίζουν το κλειδί αποκρυπτογράφησης
- Υπάρχουν γνωστοί αλγόριθμοι κρυπτογράφησης που θεωρούνται ασφαλείς, ως πρότυπα κρυπτογράφησης
  - Σε κάθε περίπτωση όμως, η ασφάλεια βασίζεται στη μυστικότητα του κλειδιού

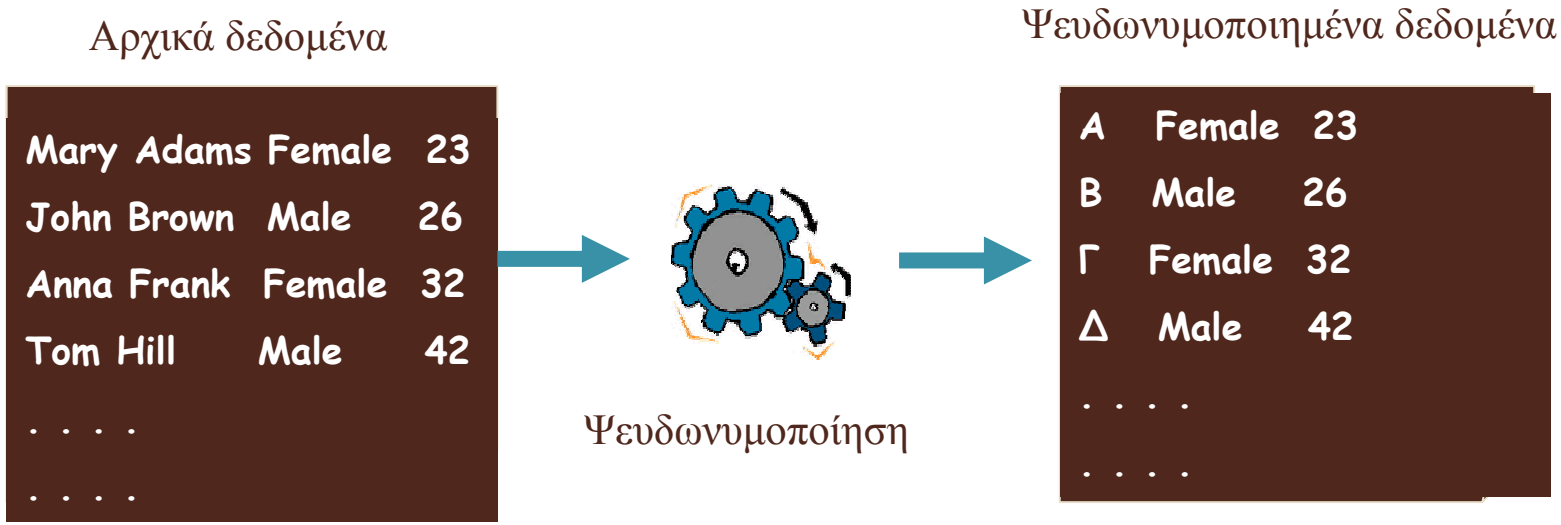


ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Η ψευδωνυμοποίηση ως μέσο ασφάλειας

- Στον ΓΚΠΔ η ψευδωνυμοποίηση ορίζεται ρητά:
  - *η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο*



Η αντιστοίχιση «ονοματεπώνυμο – ψευδώνυμο» είναι οι ως άνω αναφερόμενες *συμπληρωματικές πληροφορίες*

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Η ψευδωνυμοποίηση δεν είναι ανωνυμοποίηση !!!

- Στον ΓΚΠΔ αναφέρεται ρητώς ότι τα ψευδωνυμοποιημένα δεδομένα δεν πρέπει να θεωρούνται ανώνυμα
  - *Τα δεδομένα προσωπικού χαρακτήρα που έχουν υποστεί ψευδωνυμοποίηση, η οποία θα μπορούσε να αποδοθεί σε φυσικό πρόσωπο με τη χρήση συμπληρωματικών πληροφοριών, θα πρέπει να θεωρούνται πληροφορίες σχετικά με ταυτοποιήσιμο φυσικό πρόσωπο.*
- Άρα, η ψευδωνυμοποίηση δεν συνιστά ανωνυμοποίηση και, συνεπώς, στα ψευδωνυμοποιημένα δεδομένα έχει εφαρμογή ο ΓΚΠΔ, ως δεδομένα προσωπικού χαρακτήρα
- Ωστόσο, η ενδεχόμενη δυσκολία άρσης της ψευδωνυμοποίησης από κάποιον τρίτο μπορεί να συνιστά μία κατάλληλη εγγύηση για την προστασία των δεδομένων
  - Ο ΓΚΠΔ σαφώς προκρίνει τη χρήση της ψευδωνυμοποίησης για ως τεχνική που μπορεί να εξεταστεί η υιοθέτησή της για περαιτέρω διασφάλιση της ασφάλειας της επεξεργασίας και της προστασίας των θεμελιωδών δικαιωμάτων

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

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 (άρ. 33-34):

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

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

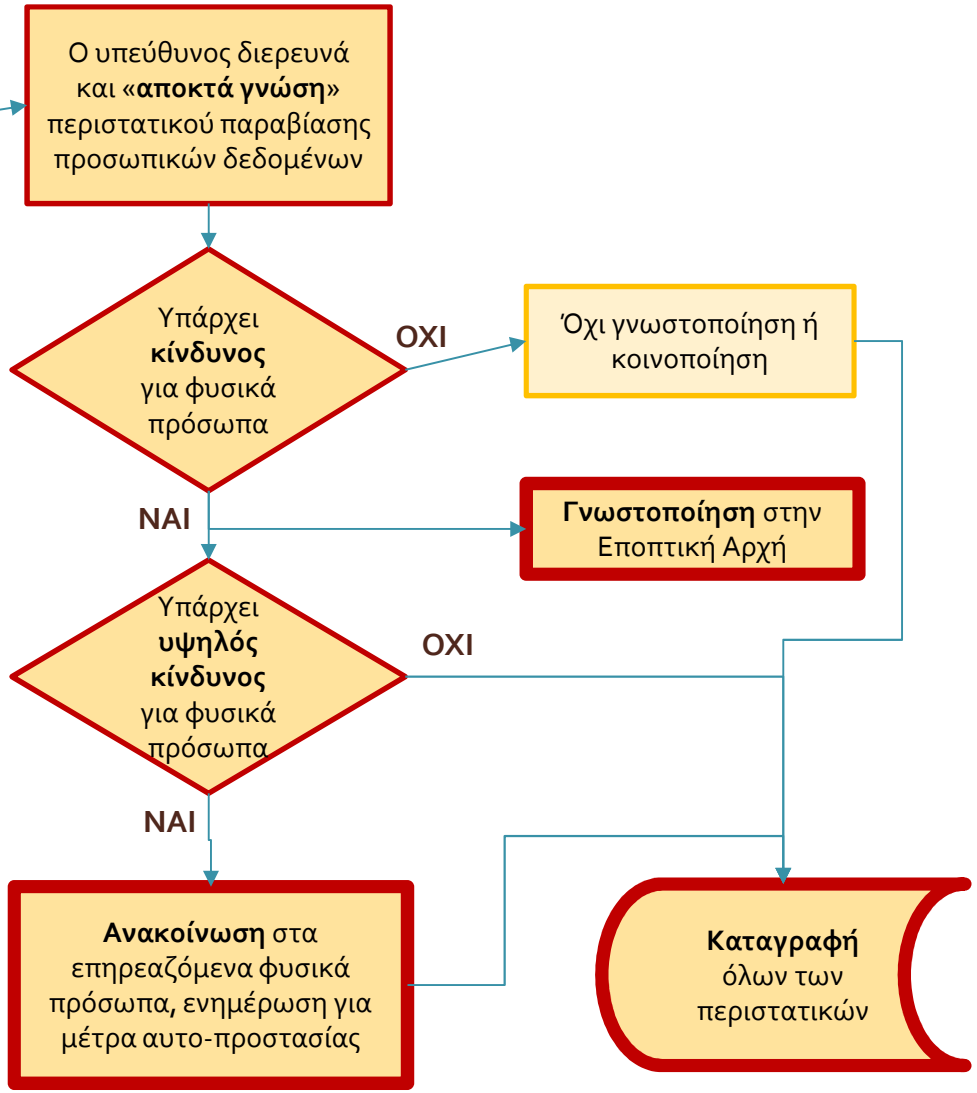
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Παραβίαση δεδομένων προσωπικού χαρακτήρα

Η διαδικασία

Ο υπεύθυνος **ανιχνεύει/ μαθαίνει** περιστατικό ασφάλειας



Ο.Ε. 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: <u>άμεση</u>, 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 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.

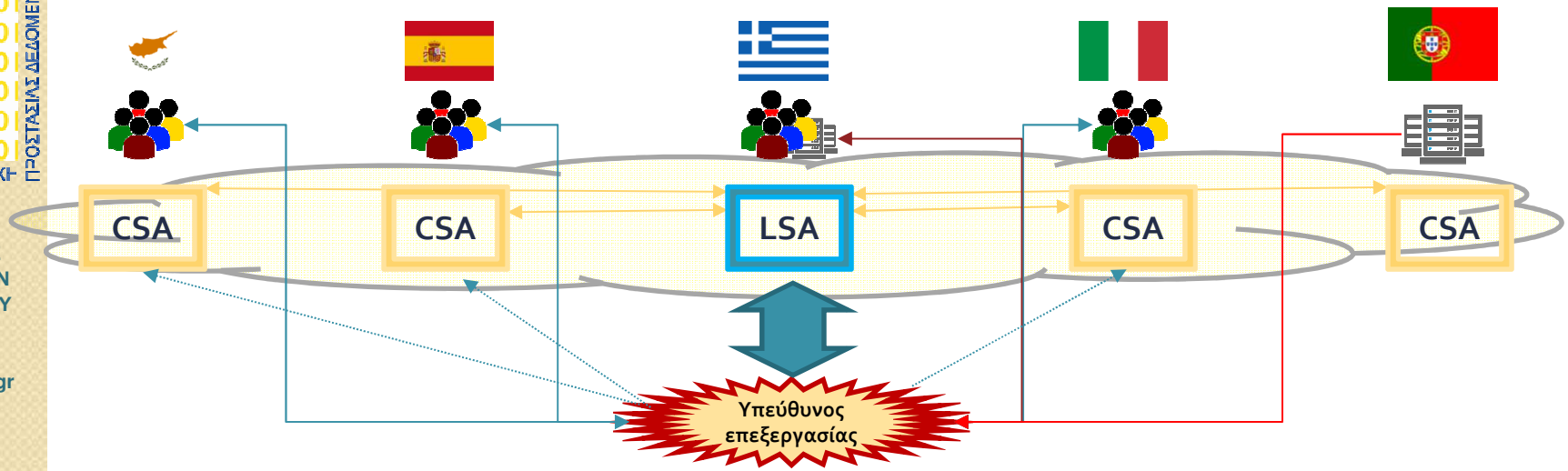
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

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

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
  - Π.χ. με ασφαλή κρυπτογράφηση, χωρίς διαρροή του μυστικού κλειδιού
- **Διαθεσιμότητα**: Υπάρχει αντίγραφο ασφαλείας - η υπηρεσία επαναλειτουργεί σε εύλογο χρόνο
- **Ακεραιότητα**: Δεν έχουν αλλοιωθεί δεδομένα – υπάρχει αντίγραφο ασφαλείας που επαναφέρει σε εύλογο χρόνο τα δεδομένα σε ακέραια μορφή

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 (κρυπτογραφημένα) 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 εκτίμηση αντικτύπου:
  - Δεν υφίσταται πλέον *πιθανότητα επέλευσης* ενός κινδύνου για την επεξεργασία, αλλά **βεβαιότητα**.

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

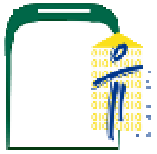
- Υποχρέωση τήρησης **εσωτερικού μητρώου περιστατικών παραβίασης**, ανεξάρτητα αν πρέπει να γνωστοποιούνται στην Αρχή.
- Το αρχείο αυτό χρησιμοποιείται, μεταξύ άλλων, **για να επιδειχθεί η συμμόρφωση** σε τυχόν έλεγχο της Αρχής.
  - Άρα, πρέπει να καταγράφονται και τα στοιχεία που αποδεικνύουν τη συμμόρφωση (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.

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Παραδείγματα εφαρμογής



Το backup αρχείων με προσωπικά δεδομένα αποθηκεύεται κρυπτογραφημένα, με ισχυρό αλγόριθμο κρυπτογράφησης, σε ένα DVD. Γίνεται κλοπή και το CD λείπει. Το μυστικό κλειδί δεν διέρρευσε	ΟΧΙ	ΟΧΙ
Μετά από «κυβερνοεπίθεση» hackers εξάγουν προσωπικά δεδομένα από ένα ιστότοπο που λειτουργεί με https	ΝΑΙ	ΠΟΛΥ ΠΙΘΑΝΟ
Μετά από σύντομη διακοπή ρεύματος παρατηρείται βλάβη στο τηλεφωνικό κέντρο. Οι πολίτες δεν μπορούν να ασκήσουν τα δικαιώματά τους	ΟΧΙ	ΟΧΙ
Ransomware προσβάλει Η/Υ κρυπτογραφώντας αρχεία με προσωπικά δεδομένα. Για τα αρχεία αυτά δεν υπάρχουν πρόσφατα backup. Η έρευνα δείχνει ότι αυτή ήταν η μόνη κακόβουλη ενέργεια	ΝΑΙ	ΑΝΑΛΟΓΑ...
Πολίτης τηλεφωνεί ενημερώνοντας ότι έλαβε επιστολή που προοριζόταν για άλλο παραλήπτη, από λάθος στη διεύθυνση. Το περιεχόμενο της επιστολής περιέχει οικονομικά στοιχεία.	ΝΑΙ	ΜΟΝΟ ΕΝΑΣ
Οι ηλεκτρονικοί φάκελοι ενός νοσοκομείου παραμένουν χωρίς πρόσβαση για 30 ώρες, λόγω τεχνικού προβλήματος	ΝΑΙ	ΝΑΙ
Από λάθος, αρχείο με προσωπικά δεδομένα 500 πολιτών στέλνεται σε λίστα ηλεκτρονικού ταχυδρομείου με 300 παραλήπτες	ΝΑΙ	ΑΝΑΛΟΓΑ...

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Η νέα διάταξη σε εφαρμογή από τις 25/5/2018

- Οι υπεύθυνοι που θα κληθούν να αντιμετωπίσουν περιστατικά πρέπει να καταλήγουν **γρήγορα**, *με ικανοποιητικό βαθμό βεβαιότητας*, αν οφείλουν να γνωστοποιήσουν.
  - Απαιτείται άμεσα τροποποίηση των εσωτερικών διαδικασιών χειρισμού περιστατικών
  - Απαιτούνται κατάλληλα μέτρα (logging) για τη διαπίστωση των επηρεαζομένων Φ.Π.
  - Απαιτούνται έτοιμες «προεκτιμήσεις» επικινδυνότητας – Η εκτίμηση αντικτύπου (DPIA) είναι πολύ χρήσιμη
- Σχέση **Υπεύθυνου Επεξεργασίας** – **Εκτελούντος την Επεξεργασία**:
  - Στενότερη και ταχύτερη συνεργασία
  - Οι εκτελούντες οφείλουν να λάβουν μέτρα και για τη δική τους προστασία (όχι μόνο μέτρα ασφάλειας και εσωτερικές διαδικασίες, αλλά και συμβατικές προβλέψεις από βλάβη της φήμης τους)
- Επανέλεγχος των παλαιότερων περιστατικών
  - Αν αλλάξει το «state of the art» ενδέχεται να προκύψει υποχρέωση γνωστοποίησης
- Οι υπεύθυνοι οφείλουν να παρακολουθούν λίστες με ευπάθειες
- Οφείλουν να παρακολουθούν «ύποπτες» κινήσεις στα συστήματά τους (π.χ. «περιέργως» αυξημένη κίνηση δικτύου, «ύποπτα» αρχεία κτλ.)

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Ευχαριστούμε για την προσοχή σας

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr