ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

17η Ευρωπαϊκή Ημέρα Προστασίας Δεδομένων
Ενημερωτική Ημερίδα της Αρχής

Γενικός Κανονισμός και Προστασία Προσωπικών Δεδομένων: Από την Τυπική Συμμόρφωση στην Ουσιαστική Εφαρμογή

Καθηγητής Χρήστος Καλλονιάτης
Τμήμα Πολιτισμικής Τεχνολογίας και Επικοινωνίας, Πανεπιστήμιο Αιγαίου
Μέλος της Αρχής Προστασίας Δεδομένων

Καθηγητής Κωνσταντίνος Λαμπρινουδάκης
Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιώς
Μέλος της Αρχής Προστασίας Δεδομένων

ΓΚΠΔ: Βασικές Αρχές Συμμόρφωσης

1. **Νομιμότητα, αντικειμενικότητα, διαφάνεια**
   - **Νομιμότητα:** η επεξεργασία πρέπει να συμμορφώνεται με τις απαιτήσεις του Κανονισμού
   - **Αντικειμενικότητα:** τα υπό επεξεργασία δεδομένα πρέπει να αντιστοιχούν στην περιγραφή τους
   - **Διαφάνεια:** ενημέρωση του Υποκειμένου περί της επεξεργασίας των δεδομένων του
2. **Περιορισμός του σκοπού**
   - Τα προσωπικά δεδομένα πρέπει να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς
   - Τα προσωπικά δεδομένα πρέπει να χρησιμοποιούνται μόνο για τον σκοπό για τον οποίο συλλέχθηκαν, για τον οποίο το Υποκείμενο των Δεδομένων έδωσε τη συγκατάθεσή του
   - Περαιτέρω επεξεργασία απαιτεί εκ νέου λήψη της συγκατάθεσης

ΓΚΠΔ: Βασικές Αρχές Συμμόρφωσης

3. **Ελαχιστοποίηση των δεδομένων**

   Τα προσωπικά δεδομένα που έχουν συλλεχθεί πρέπει να είναι κατάλληλα, συναφή και να περιορίζονται στα απολύτως αναγκαία για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία

4. **Ακρίβεια**
   - Τα δεδομένα θα πρέπει «να είναι ακριβή και όταν είναι αναγκαίο, να επικαιροποιούνται»
   - Οι κάτοχοι των δεδομένων οφείλουν να σχεδιάσουν και να χρησιμοποιούν διαδικασίες επανελέγχου των δραστηριοτήτων διαχείρισης/αρχειοθέτησης των ΔΠΧ

ΓΚΠΔ: Βασικές Αρχές Συμμόρφωσης

5. **Περιορισμός της περιόδου αποθήκευσης**
   - Τα δεδομένα πρέπει να «διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα»
   - Τα δεδομένα τα οποία δεν χρειάζονται πια, πρέπει να διαγράφονται
6. **Ακεραιότητα και εμπιστευτικότητα**

   Τα δεδομένα πρέπει να «υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλειά τους, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων»

ΓΚΠΔ: Βασικές Αρχές Συμμόρφωσης

7. Εξυπηρέτηση των Δικαιωμάτων των Υποκειμένων των Δεδομένων

1. Το δικαίωμα ενημέρωσης του Υποκειμένου των Δεδομένων
2. Το δικαίωμα πρόσβασης του Υποκειμένου των Δεδομένων
3. Το δικαίωμα του Υποκειμένου των Δεδομένων στη διόρθωση των δεδομένων του
4. Το «δικαίωμα στη λήθη» του Υποκειμένου των Δεδομένων
5. Το δικαίωμα του Υποκειμένου των Δεδομένων στον περιορισμό της επεξεργασίας
6. Το δικαίωμα του Υποκειμένου των Δεδομένων στη φορητότητα των δεδομένων του
7. Το δικαίωμα της εναντίωσης
8. Το δικαίωμα της αντίρρησης στις περιπτώσεις profiling

Η Συμμόρφωση στην Πράξη…

1. Αρχεία Δραστηριοτήτων Επεξεργασίας
2. Υπεύθυνος Προστασίας Δεδομένων
3. Προστασία των δεδομένων ήδη από το σχεδιασμό & εξ ορισμού
4. Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων
5. Διαχείριση περιστατικών παραβίασης προσωπικών δεδομένων
6. Ασφάλεια Επεξεργασίας
7. Πολιτικές Προστασίας Δεδομένων

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Αρχεία Δραστηριοτήτων Επεξεργασίας

- Περιγραφή περιστατικών:
  - Περιπτώσεις που ο Υπεύθυνος/Εκτελών την επεξεργασία **δεν τηρούσε επικαιροποιημένα** τα αρχεία δραστηριοτήτων
  - Περιπτώσεις που ο Υπεύθυνος/Εκτελών την επεξεργασία **δημιούργησε τα αρχεία δραστηριοτήτων μετά τη διαδικασία ακρόασης του**
  - Αρχεία δραστηριοτήτων χρησιμοποιήθηκαν κατά την εξέταση υπόθεσης και διαπιστώθηκε **ανακολουθία μεταξύ ΥΕ/ΕΕ**
- Συμπέρασμα:
  - Τα αρχεία δραστηριοτήτων πρέπει να τηρούνται επικαιροποιημένα και να αποτυπώνουν ορθά τις σχέσεις μεταξύ Υπευθύνων και Εκτελούντων την Επεξεργασία

Υπεύθυνος Προστασίας Δεδομένων (1/2)

- Περιγραφή περιστατικών:
  - Κατά την εξέταση καταγγελιών διαπιστώθηκε:
    - **μη ορισμός** ΥΠΔ
    - **ελλιπής συνεργασία** του ΥΠΔ με τον υπεύθυνο επεξεργασίας για την επίτευξη της απαιτούμενης συμμόρφωσης
    - **αδυναμία του ΥΠΔ** (κυρίως σε υπευθύνους επεξεργασίας μεγάλου μεγέθους) να **συμμετέχει δεόντως και εγκαίρως** σε όλα τα ζητήματα που αφορούν την παρακολούθηση της συμμόρφωσης με τον ΓΚΠΔ και τον ν. 4624/2019 συμπεριλαμβανομένων της λογοδοσίας και των σχετικών (εσωτερικών) ελέγχων
    - ο ΥΠΔ **αναλαμβάνει εκτελεστικό ρόλο** (απάντηση σε έγγραφα της Αρχής από τον ΥΠΔ αντί του φορέα, άσκηση δικαιωμάτων μέσω του ΥΠΔ με απαντήσεις που δεν είναι αποδεκτές)
  - Ο ΥΠΔ **θεωρούσε ότι μπορεί να εκπροσωπήσει** τον υπεύθυνο επεξεργασίας
  - Ο ΥΠΔ **κατείχε παράλληλα ρόλο** που δεν ήταν ανεξάρτητος από τα καθήκοντα του

Υπεύθυνος Προστασίας Δεδομένων (2/2)

- Συμπέρασμα:
  - Παρ’ ότι προβλέπεται η δυνατότητα ορισμού ενός ΥΠΔ για περισσότερες δημόσιες αρχές ή φορείς, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία, πρέπει να διασφαλίζει ότι ένας μόνο υπεύθυνος προστασίας δεδομένων, συνεπικουρούμενος από ομάδα εφόσον απαιτείται, δύναται να επιτελεί αποτελεσματικά όλα τα καθήκοντά του για όλες τις δημόσιες αρχές και δημόσιους φορείς, στους οποίους έχει οριστεί
  - Ο ΥΠΔ πρέπει να ενεργεί ελεγκτικά/εποπτικά/καθοδηγητικά και όχι εκτελεστικά
  - Ο ΥΠΔ δεν μπορεί να εκπροσωπεί τον Υπεύθυνο Επεξεργασίας και δεν πρέπει να κατέχει άλλο ρόλο που συνδέεται με τα καθήκοντα του

Προστασία των δεδομένων ήδη από το σχεδιασμό & εξ ορισμού

- Περιγραφή περιστατικών:
  - Περιπτώσεις όπου ο υπεύθυνος επεξεργασίας προβαίνει σε διαγραφή δεδομένων (μετά από άσκηση δικαιώματος από το ΥΔ ή καταγγελία), αλλά στη συνέχεια προκύπτει ότι **τα δεδομένα συνεχίζουν να υφίστανται και να αξιοποιούνται** από το ΠΣ (έλλειψη διαδικασιών εξασφάλισης διαγραφής και προστασίας των δικαιωμάτων των υποκειμένων)
  - Μη τήρηση **της αρχής του περιορισμού της περιόδου αποθήκευσης** λόγω μη εφαρμογής των κατάλληλων τεχνικών και οργανωτικών μέτρων
- Συμπέρασμα:
  - ο υπεύθυνος επεξεργασίας, λαμβάνοντας υπόψη τις τεχνολογικές λύσεις, το κόστος, τους σκοπούς της επεξεργασίας, και τους κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων από την επεξεργασία, εφαρμόζει τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα.

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων (1/2)

- Περιγραφή περιστατικών:
  - Περιπτώσεις που ο υπεύθυνος επεξεργασίας, ενώ όφειλε (υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων), **δεν είχε εκπονήσει ΕΑΠΔ** (για παράδειγμα σύστημα βιντεοεπιτήρησης σε χώρο εργασίας)
  - Περιπτώσεις **πλημμελούς διεξαγωγής της ΕΑΠΔ** (για παράδειγμα απουσία εκτίμησης της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας, ελλιπής/λανθασμένη εκτίμηση των κινδύνων, ελλιπής/ λανθασμένη επιλογή μέτρων αντιμετώπισης)
  - Περιπτώσεις που κατά την εκπόνηση της ΕΑΠΔ ο υπεύθυνος επεξεργασίας δεν **ζήτησε τη γνώμη των υποκειμένων** των δεδομένων (πρόβλεψη άρθρου 35, παρ. 9) ή των εκπροσώπων τους για τη σχεδιαζόμενη επεξεργασία
  - Περιπτώσεις αιτημάτων διαβούλευσης με την Αρχή όταν ο υπεύθυνος επεξεργασίας **λανθασμένα καταλήγει ότι ο κίνδυνος δεν είναι δυνατόν να μετριαστεί** με εύλογα μέτρα όσον αφορά τη διαθέσιμη τεχνολογία και το κόστος εφαρμογής

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων (2/2)

- Συμπέρασμα:
  - Η ΕΑΠΔ αποτελεί σημαντικό εργαλείο πλήρωσης της υποχρέωσης λογοδοσίας που βαρύνει τον υπεύθυνο επεξεργασίας αφενός να λαμβάνει τα αναγκαία μέτρα προκειμένου να συμμορφώνεται προς τις απαιτήσεις του ΓΚΠΔ, αφετέρου, να αποδεικνύει ανά πάσα στιγμή την ανωτέρω συμμόρφωσή του, καθώς τον συνδράμει στην διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων και στην λήψη αποφάσεων για την επεξεργασία
  - Σύμφωνα με τις κατευθυντήριες γραμμές του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων οι κίνδυνοι για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων πρωτίστως αφορούν την προστασία των δεδομένων και της ιδιωτικής ζωής, αλλά και θεμελιώδη δικαιώματα, όπως την ελευθερία του λόγου, την ελευθερία της σκέψης, την ελευθερία κυκλοφορίας, την απαγόρευση των διακρίσεων, το δικαίωμα στην ελευθερία, την ελευθερία συνειδήσεως και θρησκείας

Διαχείριση Περιστατικών Παραβίασης Προσωπικών Δεδομένων

- Περιγραφή περιστατικών:
  - Πλήθος περιπτώσεων που ο υπεύθυνος επεξεργασίας παρά το ότι είχε διαπιστώσει παραβίαση προσωπικών δεδομένων (διαθεσιμότητα/απώλεια, διαρροή, μη εξουσιοδοτημένη πρόσβαση) **δεν προέβη σε γνωστοποίηση** στην Αρχή και **σε ενημέρωση των υποκειμένων των δεδομένων** (σε περιπτώσεις που ήταν απαραίτητο)
- Συμπέρασμα:
  - Ο υπεύθυνος επεξεργασίας θα πρέπει να έχει διαδικασίες και προκαθορισμένους ρόλους ώστε να εντοπίζει, να αξιολογεί και να λαμβάνει τα απαραίτητα μέτρα για τη διαχείριση πιθανών περιστατικών παραβίασης, συμπεριλαμβανομένων των υποχρεώσεων του για γνωστοποίηση του περιστατικού.

Ασφάλεια Επεξεργασίας (1/2)

- Περιγραφή περιστατικών:
  - Περιπτώσεις που **δεν έχουν ληφθεί τα κατάλληλα τεχνικά και οργανωτικά μέτρα**, πλήττοντας το απόρρητο/εμπιστευτικότητα των δεδομένων (μη εξουσιοδοτημένη πρόσβαση σε αρχεία, αποστολή εγγράφων σε φάκελο με παράθυρο/θυρίδα απ' όπου γινόταν ορατά προσωπικά δεδομένα κ.λπ.)
  - Περιπτώσεις **απώλειας της διαθεσιμότητας δεδομένων** λόγω της μη λήψης κατάλληλων τεχνικών και οργανωτικών μέτρων (ιατρικά δεδομένα, γνωματεύσεις)
  - Περιπτώσεις κατά τις οποίες πολίτες που χρησιμοποιούσαν συγκεκριμένες υπηρεσίες **αποκτούσαν πρόσβαση σε δεδομένα** (συμπεριλαμβανομένων δεδομένων ειδικών κατηγοριών) **άλλων πολιτών**
  - Περιπτώσεις **ελλιπών μέτρων ασφαλείας** (σε συνδυασμό με πλημμελή διεξαγωγή της εκτίμησης αντικτύπου), πλημμελούς υλοποίησης της διαδικασίας ανωνυμοποίησης και διαρροής κωδικών πρόσβασης που οδήγησαν σε παραβίαση-διαρροή προσωπικών δεδομένων
  - Περιπτώσεις **ελλιπών μέτρων ασφαλείας ή λανθασμένων ενεργειών χρηστών** που οδήγησαν στην εγκατάσταση κακόβουλου λογισμικού

Ασφάλεια Επεξεργασίας (2/2)

- Συμπέρασμα:
  - ο υπεύθυνος επεξεργασίας, οφείλει να λαμβάνει όλα τα κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το ανάλογο επίπεδο ασφάλειας έναντι των κινδύνων και συγκεκριμένα να διασφαλίζει το απόρρητο, την ακεραιότητα και τη διαθεσιμότητα της επεξεργασίας και των υπηρεσιών. Ενδεικτικά μέτρα που πρέπει να λαμβάνονται υπόψη:
    - κρυπτογράφηση, ψευδονυμοποίηση
    - διαβαθμισμένη πρόσβαση και επιλογή κατάλληλου μηχανισμού ελέγχου πρόσβασης
    - τήρηση logs, τήρηση αντιγράφων ασφαλείας,
    - ενεργοποίηση τείχους προστασίας στον υπολογιστή
    - ασφαλή απομακρυσμένη σύνδεση μόνο μέσω VPN
  - Συνεχής εκπαίδευση / ενημέρωση των χρηστών για πιθανούς κινδύνους (π.χ. Social Engineering) και τρόπους αντιμετώπισης των

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

17η Ευρωπαϊκή Ημέρα Προστασίας Δεδομένων
Ενημερωτική Ημερίδα της Αρχής

Σας ευχαριστούμε για την προσοχή σας