Γενικός Κανονισμός Προστασίας Δεδομένων και συμμόρφωση
Μια νέα πρόκληση για τον δημόσιο και ιδιωτικό τομέα

Λίλιαν Μήτρου

Καθηγήτρια Πανεπιστημίου Αιγαίου – Δικηγόρος
Πρόεδρος της Νομοπαρασκευαστικής Επιτροπής για την προσαρμογή του εθνικού δικαίου στον Γενικό Κανονισμό Προστασίας Δεδομένων και την ενσωμάτωση της Οδηγίας ΕΕ/ 2016/680

L.mitrou@aegean.gr

Νέες απαιτήσεις- Νέα εργαλεία/ 1

- **Απλοποίηση των διαδικασιών και υποχρεώσεων**
  - Προσέγγιση με βάση τον κίνδυνο (risk based approach) ή πώς η ευελιξία συνδέεται με την ευθύνη
- **Αναδιοργάνωση των μηχανισμών συμμόρφωσης** -
  - **Λογοδοσία** (accountability): ευθύνη και απόδειξη της συμμόρφωσης
  - **Ενίσχυση «αυτοελέγχου»** με
    - Τήρηση **αρχείων επεξεργασιών**
    - **εκτίμηση κινδύνων κι επιπτώσεων**
    - κι εσωτερικούς μηχανισμούς όπως ο (εσωτερικός) **Υπεύθυνος Προστασίας Δεδομένων**

Νέες απαιτήσεις- Νέα εργαλεία/ 2

- Ενίσχυση **διαφάνειας**
- Κοινοποίηση **παραβίασης δεδομένων** – [data breach notification]
  - Ενίσχυση μέτρων – κουλτούρας ασφάλειας
  - Το διακύβευμα της φήμης
- **Αυστηρότερες κυρώσεις για μη συμμόρφωση**
  - Γενικοί όροι επιβολής προστίμων
  - *Δαμόκλειος σπάθη των προστίμων*
  - Αναφορά σε δυνατότητα κρατών μελών για νομοθετική πρόβλεψη κι επιβολή άλλων κυρώσεων – αποτελεσματικών, αναλογικών κι αποτρεπτικών

Νέες απαιτήσεις-Νέα εργαλεία/ 3

- **Ενίσχυση των δικαιωμάτων και των ενδίκων βοηθημάτων** των προσώπων
  - **Λήθη/Φορητότητα**
  - "actio popularis" – αναλογία με το δίκαιο καταναλωτή
  - **Εγγύτητα** αναφορικά με άσκηση ενδίκων μέσων – Εις ολόκληρον ευθύνη υπεύθυνου κι εκτελούντα επεξεργασία
- **Ενίσχυση του ρόλου και των μέσων των ανεξάρτητων αρχών**
- **Συντονισμός** των αρχών προστασίας δεδομένων κρατών μελών
  - One–stop–shop και Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Κανονισμός ή Κανονοδηγία;

- Παρά τον στόχο της ενιαίας ρύθμισης και της εξάλειψης των αποκλίσεων ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (2016/679/Ε) σε αρκετές ρυθμίσεις **προσομοιάζει με Οδηγία**.
- **Υβρίδιο;** Δεκάδες **«ρήτρες παρέκκλισης» (- ευελιξίας)** επιτρέπουν ή και επιβάλλουν τη **συμβολή του εθνικού νομοθέτη** στη ρύθμιση
- Ερμηνευτικό ζήτημα ως προς το περιεχόμενο των εθνικών κανόνων: **εξειδίκευση ή/και ενίσχυση της προστασίας**;
- **Γνώμονας και όριο είναι οι ρυθμίσεις του Κανονισμού**

Ο ρόλος του εθνικού νομοθέτη

- Δυνατότητα **διατήρησης ή θέσπισης ειδικών διατάξεων** για τον **περαιτέρω προσδιορισμό** της εφαρμογής των κανόνων αναφορικά με την επεξεργασία προσωπικών δεδομένων
  - προς συμμόρφωση με νομική υποχρέωση,
  - προς εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας.

- Περιθώρια χειρισμού στα κράτη μέλη, ώστε να **εξειδικεύσουν τους κανόνες** του, συμπεριλαμβανομένων αυτών που αφορούν την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα («ευαίσθητα δεδομένα»).

(Ορισμένα) ζητήματα προς ρύθμιση κι αντιμετώπιση/1

- Ειδικότερες ρυθμίσεις για τα **δεδομένα υγείας και τα γενετικά δεδομένα** (π.χ. ως προς τις προυποθέσεις επεξεργασίας τους από ασφαλιστικές ή φαρμακευτικές εταιρίες ή τα νοσοκομεία) ;
- Ειδικότερες ρυθμίσεις για τον **(εσωτερικό) υπεύθυνο προστασίας δεδομένων;**
  - Ο ορισμός ενός υπευθύνου προστασίας δεδομένων δεν είναι υποχρεωτικός σε όλες τις περιπτώσεις
  - Επέκταση της υποχρέωσης ; Ευχέρεια του εθνικού νομοθέτη
  - Εσωτερικός υπεύθυνος ως βέλτιστη πρακτική;
- (Ποινικές) Κυρώσεις σε εθνικό επίπεδο;

(Ορισμένα) ζητήματα προς ρύθμιση κι αντιμετώπιση/2

- **Πιστοποίηση συμμόρφωσης ως μηχανισμός αυτοελέγχου και στοιχείο λογοδοσίας**
  - Φορέας διαπίστευσης για τους μηχανισμούς/ οργανισμούς πιστοποίησης;
  - Αρχή Προστασίας Δεδομένων ή Εθνικό Σύστημα Διαπίστευσης (Ε.ΣΥ.Δ.)
- **Κώδικες δεοντολογίας**
  - Εξειδίκευση ρυθμίσεων σε συγκεκριμένα πεδία/ κλάδους οικονομίας
  - Στοιχείο λογοδοσίας
  - Μορφή συρρύθμισης – έγκριση Αρχής Προστασίας Προσωπικών Δεδομένων

(Ορισμένα) ζητήματα προς ρύθμιση κι αντιμετώπιση/3

- **Ειδικές ρυθμίσεις** για τις εργασιακές σχέσεις;
- Προστασία δεδομένων των εργαζομένων
  - Το ζήτημα της **συγκατάθεσης**
  - Ζητήματα ως προς **εύρος/σκοπούς επεξεργασίας**
  - **Επιτήρηση** ιδίως επικοινωνιών/χρήσης υποδομής
- Υποχρεωτική η **«πολιτική χρήσης επικοινωνιών, διαδικτύου, υποδομής»;**

Μία δύσκολη προσαρμογή;

- Η προσαρμογή αφορά **όλους τους «αποδέκτες»** των νέων ρυθμίσεων: τόσο τον νομοθέτη όσο και τους υπεύθυνους επεξεργασίας
- **Ευρύτατο πεδίο εφαρμογής** …..και οι δικαστικές αρχές
- Η συμμόρφωση αναφέρεται **στο πλαίσιο που θα προκύψει και από την εθνική νομοθεσία «προσαρμογής».**
- Απαιτείται μία **επισκόπηση της επεξεργασίας** ώστε να **προσδιοριστούν οι υποχρεώσεις και οι ενέργειες** που θα εξασφαλίσουν συμμόρφωση και μετάβαση στο νέο πλαίσιο
- **Αλλαγή αντίληψης και κουλτούρας** - Συνεργασία
- **Ενίσχυση του ρόλου της ΑΠΔΠΧ** αλλά και **αύξηση των απαιτήσεων**

Βήματα προς την εφαρμογή/1

- Ενημέρωση/ συνειδητοποίηση των απαιτήσεων και των αλλαγών που απαιτούνται
  - Σε ποιο επίπεδο;
  - Εντοπισμός «προβληματικών περιοχών»
- Λογοδοσία : πλαίσιο πολιτικών και διαδικασιών
  - Διαχειριστική/ Οργανωτική/ Τεχνική/ Νομική υποστήριξη της συμμόρφωσης
  - Έλεγχος συμμόρφωσης
  - Εκπαίδευση/ Ενημέρωση

Βήματα προς την εφαρμογή/2

- «Χαρτογράφηση» δεδομένων/ αρχείων/ βάσεων σε συσχετισμό με προσωπικά δεδομένα
- «Χαρτογράφηση» πληροφοριακών διαδικασιών και ροών
  - εντός οργανισμού (δεδομένα «συναλλασσομένων» και εργαζομένων)
  - ροών/διαβιβάσεων εκτός οργανισμού
- Εξέταση – χαρτογράφηση των πηγών άντλησης/προέλευσης των δεδομένων

Βήματα προς την εφαρμογή/3

- Data Protection by design : δεν αφορά μόνο τις τεχνολογίες υπό στενή έννοια αλλά και τον σχεδιασμό εφαρμογών, διαδικασιών, εργασιών με γνώμονα την προστασία δια/ εκ του σχεδιασμού
- Data Protection Impact Assessment : σχετίζεται αλλά δεν ταυτίζεται με την εκτίμηση κινδύνου
  - Πλαίσιο εκτίμησης επιπτώσεων το οποίο πρέπει να (συ)σχετίζεται με τη διαχείριση κινδύνων και εν γένει τις διαδικασίες διαχείρισης (project management) μέσα σέ έναν οργανισμό
  - Χρονικά προηγείται των άλλων βημάτων αλλά ταυτόχρονα συνιστά μία ….διαρκή διαδικασία.

Βήματα προς την εφαρμογή/4

- Έλεγχος συμβάσεων, όρων, διατυπώσεων σε έντυπα ενημέρωσης, γνωστοποίησης, συγκατάθεσης
- Έλεγχος / Εισαγωγή διαδικασιών χειρισμού αιτημάτων (πρόσβασης, διαγραφής κ.α)/ παραπόνων κλπ.
- Επανέλεγχος και επιβεβαίωση των βάσεων νομιμότητας

- **Μία ευκαιρία αξιολόγησης της ποσότητας, ποιότητας και αξίας των τηρουμένων δεδομένων**

Η 25η Μαΐου 2018 ....

δεν είναι το τέλος

αλλά

η αρχή της εφαρμογής του Κανονισμού

και της συμμόρφωσης

προς τις επιταγές του

Σας ευχαριστώ

για την προσοχή σας