Γενικός Κανονισμός Προστασίας Δεδομένων
Υποχρεώσεις και συμμόρφωση

Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου
Καθηγήτρια, Πανεπιστήμιο Μακεδονίας
Διευθύντρια Διιδρυματικού Μεταπτυχιακού
«ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ»
www.mli.uom.gr, www.itlaw.uom.gr

ealex@uom.gr

ΙΔΙΩΤΙΚΟΤΗΤΑ

- Οι τεχνολογικές εξελίξεις επηρεάζουν το περιεχόμενο της έννοιας της ιδιωτικότητας

- Από το δικαίωμα στο ιδιωτικό απόρρητο και στην «απόλαυση της μοναξιάς» ……..
- ……στο δικαίωμα της πληροφοριακής ιδιωτικότητας, του πληροφοριακού αυτοκαθορισμού και της προστασίας των προσωπικών δεδομένων

ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ
Σύγκρουση δικαιωμάτων

- Δικαίωμα στα προσωπικά δεδομένα

versus

- Δικαίωμα στην πληροφόρηση
- Δικαίωμα στη δημόσια ασφάλεια
- Δικαίωμα στην ελευθερία της έκφρασης, του λόγου και του τύπου
- Δικαίωμα στη διαφάνεια
- Δικαίωμα στην επικοινωνία
- Δικαίωμα στην επιστημονική έρευνα
- Δικαίωμα στην ελευθερία των τεχνών και των επιστημών
- Δικαίωμα στη διανοητική ιδιοκτησία

ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ
Personal data
Έννοια

- Προσωπικό δεδομένο είναι *οποιαδήποτε* **πληροφορία** για *συγκεκριμένο* ζων φυσικό πρόσωπο

- Υποκείμενο δεδομένων data subject
- Υπεύθυνος επεξεργασίας controller
- Εκτελών την επεξεργασία processor
- Αποδέκτης δεδομένων recipient
- Υπεύθυνος προστασίας δεδομένων data protection officer DPO

ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ
Ελληνική νομική ρύθμιση

- Σύνταγμα (9^{A})
- Ειδική νομοθεσία (ν. 2472/1997, 3471/2006)
- Γενική ρύθμιση προστασίας της προσωπικότητας

ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ Ευρωπαϊκή νομική ρύθμιση

- Άρθρο 16 ΣΛΕΕ «Κάθε πρόσωπο έχει δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα που το αφορούν».
- Οδηγία 95/46/Ε.Κ. του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24.10.1995 (L 281,31) «Για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας προσωπικών δεδομένων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών»
- Ο Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, άρθρο 8
- Κανονισμός (ΕΚ) αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 18ης Δεκεμβρίου 2000 σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών, ΕΕ 2001 L 8

ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ Ευρωπαϊκή νομική ρύθμιση

- Η Οδηγία 2002/58/Ε.Κ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12.7.2002 (ΕΕ L 201) σχετικά με την επεξεργασία των προσωπικών δεδομένων και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)

- Τροποποιήσεις της άνω Οδηγίας από την καταργηθείσα (2014) Οδηγία 2006/24 και την Οδηγία 2009/136

- Κανονισμός 611/2013 της Ευρωπαϊκής Επιτροπής της 24ης Ιουνίου 2013 σχετικά με τα εφαρμοστέα μέτρα για την κοινοποίηση παραβιάσεων προσωπικών δεδομένων βάσει της Οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, ΕΕ L 173 της 26.6.2013

ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ Ευρωπαϊκή νομική ρύθμιση

- Κανονισμός 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων), ΕΕ L 119 της 4.5.2016

- Οδηγία 2016/680 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαισίου 2008/977/ΔΕΥ του Συμβουλίου, ΕΕ L 119 της 4.5.2016

- Οδηγία (ΕΕ) 2016/681 σχετικά με τη χρήση των δεδομένων που περιέχονται στις καταστάσεις ονομάτων επιβατών (PNR) για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων, ΕΕ L 119 της 4.5.2016

Ισχύον νομικό καθεστώς για γενική προστασία προσωπικών δεδομένων (μέχρι 24/5/2018)

- Οδηγία 95/46 της Ε.Ε.
- Ν. 2472/1997

Ο ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (εφαρμογή από 25/5/2018)

Θεσπίζει κανόνες που αφορούν:

την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των προσωπικών τους δεδομένων

την ελεύθερη κυκλοφορία των προσωπικών δεδομένων

Έχει χαρακτηριστικά Οδηγίας
(συμπληρωματικός εθνικός νόμος)

Καινοτομίες Κανονισμού

- η εισαγωγή νέων δικαιωμάτων του υποκειμένου (δικαίωμα διαγραφής /δικαίωμα στη λήθη, στη φορητότητα)
- η προσθήκη νέων αρχών επεξεργασίας (της διαφάνειας, της λογοδοσίας, της ακεραιότητας και εμπιστευτικότητας)
- οι ενισχυμένες υποχρεώσεις του υπευθύνου επεξεργασίας (λογοδοσία, γνωστοποίηση παραβιάσεων προσωπικών δεδομένων στην Εποπτική Αρχή και στο υποκείμενο, προστασία των δεδομένων ήδη από το σχεδιασμό της επεξεργασίας και εξ ορισμού:privacy by design/privacy by default, εκτίμηση αντικτύπου όταν η επεξεργασία ενέχει σοβαρούς κινδύνους για τα προσωπικά δεδομένα)

Καινοτομίες Κανονισμού

- η αύξηση των υποχρεώσεων του εκτελούντος την επεξεργασία
- ο θεσμός του υπευθύνου προστασίας δεδομένων
- οι ειδικές προστατευτικές ρυθμίσεις για τα προσωπικά δεδομένα των παιδιών
- η ρητή δυνατότητα ανάκλησης της συγκατάθεσης του υποκειμένου
- η απάλειψη της γενικής υποχρέωσης δήλωσης της επεξεργασίας στην Εποπτική Αρχή ή λήψη της σχετικής άδειας

Καινοτομίες Κανονισμού

- Το Ευρωπαϊκό Συμβούλιο Προστασίας δεδομένων
- Ο μηχανισμός συνεκτικότητας
- Η ενθάρρυνση για θέσπιση μηχανισμών πιστοποίησης
- Η αυστηροποίηση των κυρώσεων (πρόστιμα μέχρι 20.000.000 ευρώ ή 4% του ετήσιου τζίρου, αποζημίωση. Οι ποινικές κυρώσεις ορίζονται από τα κράτη-μέλη)

Βασικές υποχρεώσεις υπευθύνου επεξεργασίας

- Ασφάλεια επεξεργασίας
- Τήρηση των αρχών επεξεργασίας (νομιμότητας, αναλογικότητας, ακρίβειας, καθορισμένου χρόνου επεξεργασίας, **λογοδοσίας, ακεραιότητας και εμπιστευτικότητας, διαφάνειας**)
- Λήψη συγκατάθεσης του υποκειμένου
- Ικανοποίηση των δικαιωμάτων του υποκειμένου (κύρια δικαιώματα:ενημέρωσης, πρόσβασης, εναντίωσης)
- Γνωστοποίηση/λήψη άδειας από την ΑΠΔΠΧ (παύει η γενική αυτή υποχρέωση με τον Κανονισμό)

Συμμόρφωση = Λογοδοσία

- **<u>ΣΥΜΜΟΡΦΩΣΗ με τον Κανονισμό ΣΗΜΑΙΝΕΙ:</u>**
  επίδειξη και **απόδειξη** συμμόρφωσης (λογοδοσία)
  ελευθερία ως προς τα μέσα, που *επανεξετάζονται* και *επικαιροποιούνται*

- **<u>Πρόσθετες υποχρεώσεις συμμόρφωσης σύμφωνα με τον Κανονισμό:</u>**
  -Εφαρμογή τεχνολογιών προστασίας της ιδιωτικότητας
  Privacy by design / by default (K25)
  -Τήρηση αρχείων επεξεργασίας (K30)
  -Υποχρεώσεις κοινοποίησης παραβιάσεων (K 33,34)
  -Εκτίμηση αντικτύπου της επεξεργασίας στα δεδομένα (K35)
  -Ορισμός υπευθύνου προστασίας δεδομένων, DPO (K37-39)
  Ενθάρρυνση για:
  Κώδικες δεοντολογίας και μηχανισμούς πιστοποίησης (K40-43)

Μέτρα συμμόρφωσης

Κατάλογος μέτρων συμμόρφωσης (ενδεικτικός, Γνώμη 3/2010 ομαδας 29)

- θέσπιση εσωτερικών διαδικασιών *πριν* την έναρξη της επεξεργασίας
- γραπτές πολιτικές προστασίας δεδομένων, διαθέσιμες στα υποκείμενα
- χαρτογράφηση διαδικασιών επεξεργασίας δεδομένων
- διορισμός υπευθύνου προστασίας δεδομένων+άλλων προσώπων
- εκπαίδευση υπαλλήλων, ιδίως των επικεφαλής ανθρώπινων πόρων τμημάτων πληροφορικής, ανάπτυξης, λοιπών υπηρεσιακών μονάδων
- διαφανείς διαδικασίες για αιτήματα πρόσβασης, διόρθωσης, διαγραφής
- εγκαθίδρυση εσωτερικού μηχανισμού χειρισμού καταγγελιών
- εσωτερικές διαδικασίες διαχείρισης+αναφοράς παραβιάσεων ασφάλειας
- αξιολόγηση του αντικτύπου στην ιδιωτική ζωή σε ειδικές περιπτώσεις
- διαδικασίες επαλήθευσης (εσωτερικός-εξωτερικός έλεγχος)

Ορισμός υπευθύνου προστασίας δεδομένων (DPO, άρθρο 37Κ)

Υποχρεωτικός ορισμός ***από*** τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία όταν:

- η επεξεργασία διενεργείται από ***δημόσια αρχή ή φορέα***, εκτός από δικαστήρια που ενεργούν στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας
- οι ***βασικές*** δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες, λόγω της φύσης, του πεδίου εφαρμογής και/ή των σκοπών τους, απαιτούν ***τακτική και συστηματική παρακολούθηση*** των υποκειμένων των δεδομένων *σε μεγάλη κλίμακα*
- οι ***βασικές*** δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν ***μεγάλης κλίμακας επεξεργασία ευαίσθητων δεδομένων***
- Το δίκαιο της Ε.Ε. ή των κρατών μελών μπορεί να επιβάλει τον ορισμό υπευθύνου προστασίας δεδομένων και σε άλλες περιπτώσεις

Προσόντα του DPO

Ο υπεύθυνος προστασίας δεδομένων διορίζεται βάσει **επαγγελματικών προσόντων** και ιδίως

- βάσει της ***εμπειρογνωσίας*** του στον τομέα του δικαίου και των πρακτικών προστασίας δεδομένων, σε εθνικό και ευρωπαϊκό επίπεδο (εξυπακούεται η άριστη γνώση του ΓΚΠΔ). Χρήσιμη η καλή γνώση του οργανισμού, διοικητικών κανόνων και διαδικασιών, των διενεργούμενων πράξεων , των συστημάτων πληροφορικής και των αναγκών του υπευθύνου επεξεργασίας σε ασφάλεια και προστασία δεδομένων.
- βάσει της ***ικανότητας εκπλήρωσης των καθηκόντων*** του

Η θέση του DPO (άρθρο 38Κ)

- Ο DPO **είτε** ανήκει στο προσωπικό του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία **είτε** ασκεί τα καθήκοντά με σύμβαση παροχής υπηρεσιών. Αποτελεσματική η λειτουργία ομάδας. Ο DPO λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο του οργανισμού.
- Συμμετέχει σε όλα τα ζητήματα προστασίας δεδομένων –εκτίμηση αντικτύπου
- Διαθέτει απαραίτητους πόρους και πρόσβαση σε δεδομένα και επεξεργασίες
- Δεν λαμβάνει εντολές/δεν απολύεται ούτε υφίσταται κυρώσεις επειδή επιτέλεσε τα καθήκοντά του. Τα υποκείμενα των δεδομένων μπορούν να επικοινωνούν με τον DPO για κάθε ζήτημα σχετικό με την επεξεργασία των δεδομένων τους/ την άσκηση των δικαιωμάτων τους
- Δεσμεύεται από την τήρηση του απορρήτου ή της εμπιστευτικότητας
- Μπορεί να έχει και άλλα καθήκοντα και υποχρεώσεις, που όμως δεν συνεπάγονται σύγκρουση συμφερόντων.
- Τα στοιχεία επικοινωνίας του DPO δημοσιοποιούνται και ανακοινώνονται στις οικείες εποπτικές αρχές

Ενδεικτικά καθήκοντα του DPO

- ενημερώνει και συμβουλεύει για τις υποχρεώσεις τους τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους υπαλλήλους που επεξεργάζονται δεδομένα
- παρακολουθεί τη **συμμόρφωση** με τον Κανονισμό, τη λοιπή νομοθεσία για την προστασία δεδομένων και με τις πολιτικές του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία (π.χ. ανάθεση αρμοδιοτήτων, ευαισθητοποίηση και κατάρτιση των υπαλλήλων που επεξεργάζονται δεδομένα, σχετικοί έλεγχοι)
- παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και παρακολουθεί την υλοποίησή της
- συνεργάζεται με την εποπτική Αρχή
- ενεργεί ως σημείο επικοινωνίας για την εποπτική Αρχή πχ κατά τη διαβούλευση για εκτίμηση αντικτύπου

Συνέπειες μη συμμόρφωσης

- Διορθωτικές εξουσίες Εποπτικής Αρχής
- Διοικητικά πρόστιμα
- Αποζημιωτική ευθύνη
- Ποινική ευθύνη

Διορθωτικές εξουσίες Εποπτικής Αρχής

- **προειδοποιήσεις** στον υπεύθυνο επεξεργασίας ή στον εκτελούντα την επεξεργασία ότι η σκοπούμενη επεξεργασία είναι πιθανόν να παραβαίνει τον Κανονισμό
- **επιπλήξεις** στον υπεύθυνο επεξεργασίας ή στον εκτελούντα την επεξεργασία όταν έχουν παραβεί τον Κανονισμό
- **εντολή** στον υπεύθυνο επεξεργασίας ή στον εκτελούντα την επεξεργασία να συμμορφώνεται προς τα αιτήματα του υποκειμένου ή να καθιστά την επεξεργασία σύμφωνη με τον Κανονισμό με συγκεκριμένο τρόπο και εντός ορισμένης προθεσμίας ή να ανακοινώνει την παραβίαση δεδομένων στο υποκείμενο ή να διορθώνει/διαγράφει δεδομένα ή να αναστέλλει τη διαβίβαση σε τρίτη χώρα
- επιβολή **περιορισμού/απαγόρευσης** της επεξεργασίας
- **απόσυρση πιστοποίησης** ή διαταγή προς οργανισμό πιστοποίησης να αποσύρει ένα πιστοποιητικό ή να μην εκδώσει πιστοποίηση
- **διοικητικό πρόστιμο** επιπλέον ή αντί των παραπάνω μέτρων

Διοικητικά πρόστιμα

(αποτελεσματικά, αναλογικά και αποτρεπτικά)

Σταθμιστικοί παράγοντες

- η φύση, η βαρύτητα και η διάρκεια της παράβασης, (αριθμός των υποκειμένων που έθιξε η παράβαση και βαθμός ζημίας τους)
- ο δόλος ή η αμέλεια του υπευθύνου/ενέργειες μετριασμού της ζημίας
- ο βαθμός ευθύνης του υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία, βάσει των λαμβανομένων τεχνικών/οργανωτικών μέτρων
- προηγούμενες παραβάσεις
- ο βαθμός συνεργασίας με την αρχή ελέγχου για την επανόρθωση της παράβασης και τον περιορισμό των δυσμενών επιπτώσεών της
- οι κατηγορίες δεδομένων που επηρεάζει η παράβαση
- ο τρόπος με τον οποίο η εποπτική αρχή πληροφορήθηκε την παράβαση, π.χ. εάν ο υπεύθυνος κοινοποίησε την παράβαση)
- εάν διατάχθηκε προηγουμένως η λήψη διορθωτικών μέτρων για το ίδιο αντικείμενο, ή συμμόρφωση με αυτά
- κάθε άλλο επιβαρυντικό ή ελαφρυντικό στοιχείο π.χ. τα οικονομικά οφέλη που αποκομίστηκαν ή ζημίες που αποφεύχθηκαν

Ύψος προστίμων

- **Έως 10 000 000 EUR ή, σε περίπτωση επιχειρήσεων, έως το 2 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών** του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο (παραβάσεις που αφορούν ανηλίκους, τήρηση αρχείων επεξεργασίας, διαδικασία ανάθεσης σε εκτελούντα την επεξεργασία, ζητήματα ασφάλειας, κοινοποίηση παραβιάσεων, υποχρεώσεις του φορέα πιστοποίησης κ.ά.)
- **Έως 20 000 000 EUR ή, σε περίπτωση επιχειρήσεων, έως το 4 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών** του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο (μη εφαρμογή βασικών αρχών επεξεργασίας, μη λήψη συγκατάθεσης, μη ικανοποίηση δικαιωμάτων του υποκειμένου, παράνομη διαβίβαση δεδομένων σε τρίτη χώρα ή σε διεθνή οργανισμό, μη συμμόρφωση προς εντολή της εποπτικής αρχής κ.ά.)

Αστική ευθύνη
(Αποζημίωση για υλική ή μη υλική ζημία)

- Κάθε υπεύθυνος επεξεργασίας είναι υπεύθυνος για τη ζημία που προκάλεσε
- Ο εκτελών την επεξεργασία ευθύνεται μόνο εφόσον δεν ανταποκρίθηκε στις υποχρεώσεις του Κανονισμού για τους εκτελούντες την επεξεργασία ή υπερέβη ή ενήργησε αντίθετα προς τις νόμιμες εντολές του υπευθύνου επεξεργασίας
- Ευθύνη εις ολόκληρον των υπευθύνων προς αποζημίωση
- Ο υπεύθυνος προς αποζημίωση απαλλάσσεται εάν αποδεικνύει ότι δεν φέρει καμία ευθύνη για το γενεσιουργό γεγονός της ζημίας

Εφαρμοστικά ζητήματα Κανονισμού

Αντιμετώπιση με τη συμβολή

- των εθνικών νόμων
- της Ομάδας του άρθρου 29 (Συμβούλιο Προστασίας Δεδομένων)
- των Αρχών Προστασίας Προσωπικών Δεδομένων (Εποπτικών Αρχών)
- συνεργατική προσέγγιση και ανταλλαγή πληροφοριών μεταξύ των υπηρεσιών επιβολής του νόμου, των δικαστικών αρχών, της βιομηχανίας των ΤΠΕ, συλλογικοτήτων χρηστών διαδικτύου

Ευχαριστώ για την προσοχή σας.

Καθηγήτρια Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου
Διευθύντρια Μεταπτυχιακού «ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ»
Πανεπιστήμιο Μακεδονίας- Τμ. Εφ. Πληροφορικής
www.itlaw.uom.gr , www.mli.uom.gr
ealex@uom.gr