



Πανεπιστήμιο Αιγαίου

Προστασία Προσωπικών Δεδομένων

Αρχές – Νόμιμες Βάσεις

Λίλιαν Μήτρου (L.Mitrou@aegean.gr)

Αναπληρώτρια Καθηγήτρια

Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών
Συστημάτων



Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο



ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης



ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Άδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.



Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Αιγαίου**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.



Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο



ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης



Η νομοθετική προστασία σε διεθνές επίπεδο

- ✦ Διασυνοριακή ροή ως χαρακτηριστικό των νέων τεχνολογικών, οικονομικών και γεωπολιτικών εξελίξεων
- ✦ Παγκοσμιοποίηση της πληροφορίας και των δραστηριοτήτων που σχετίζονται με τη χρήση και διαχείρισή της
- ✦ Ως προς την προστασία προσωπικών δεδομένων οι πρώτες διεθνείς/υπερεθνικές κανονιστικές αντιδράσεις καταγράφονται σε σχετικά πρώιμο στάδιο

Διεθνή και Υπερεθνικά κανονιστικά κείμενα.

- ✦ Διεθνείς Συμβάσεις – Συμβούλιο της Ευρώπης
 - Σύμβαση της Ρώμης (1950) για την προστασία των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών (ΕΔΔΑ)
 - Σύμβαση 108/28.1.1981 για την προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα
- ✦ Υπερεθνικό Δίκαιο – Ευρωπαϊκή Ένωση
 - Οδηγία 95/46/ΕΚ για την προστασία του ατόμου έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών
 - Οδηγία 2002/58/ΕΚ (που αντικατέστησε την 97/66/ΕΚ) για την προστασία της ιδιωτικότητας στις ηλεκτρονικές επικοινωνίες

ΟΟΣΑ: Κατευθυντήριες Αρχές(1980)

Πρόκειται για κείμενο μη δεσμευτικού χαρακτήρα (soft law)

- ✦ Αρχή της περιορισμένης συγκέντρωσης και συλλογής δεδομένων (collection limitation principle)
- ✦ Αρχή της ποιότητας των δεδομένων (data quality principle)
- ✦ Αρχή του προσδιορισμένου σκοπού (purpose specification principle)
- ✦ Αρχή της περιορισμένης χρήσης των προσωπικών δεδομένων (use limitation principle)
- ✦ Αρχή μέτρων ασφαλείας των προσωπικών δεδομένων (Security Safeguards Principle)
- ✦ Αρχή της διαφάνειας (openness principle)
- ✦ Αρχή της συμμετοχής του ατόμου (individual participation principle)
- ✦ Αρχή της ευθύνης (accountability principle)

Κοινοτική πρωτοβουλία: Οδηγία 95/46/ΕΚ

- ☛ Το ενδιαφέρον της ΕΚ προσανατολιζόταν πρωτίστως στην ενίσχυση της αγοράς και της ροής της πληροφορίας (“laissez innover”).
- ☛ Δραστηριοποίηση της Κοινότητας
 - Προφανής αύξηση της διασυνοριακής ροής προσωπικών δεδομένων μεταξύ των κρατών-μελών
 - Συνειδητοποίηση της σημασίας ασφάλειας δικαίου και της προστασίας προσωπικών δεδομένων για την απελευθέρωση και την εξέλιξη της αγοράς των ΤΠΕ και των υπηρεσιών επεξεργασίας
 - Αλλαγή της στάσης σε σχέση με την προστασία ατομικών δικαιωμάτων

Σκοποί της Κοινοτικής Οδηγίας

- ✦ Σκοπός της Κοινοτικής Οδηγίας
 - Προστασία των ατομικών δικαιωμάτων και ελευθεριών και ιδίως του ιδιωτικού βίου
 - Ελεύθερη κυκλοφορία των προσωπικών δεδομένων
- ✦ Η Οδηγία αποσκοπούσε στην εναρμόνιση των εθνικών νομοθεσιών σε ένα όσο το δυνατό υψηλότερο επίπεδο προστασίας
- ✦ Η Οδηγία αναγνωρίζει την ευχέρεια για τη διαρκή βελτίωση της προστασίας δεδομένων, έστω και εάν αυτό οδηγήσει σε αποκλίσεις

Βασικές συνιστώσες της κοινοτικής νομοθεσίας

- Συγκροτημένος συνδυασμός διαφορετικών κανονιστικών μοντέλων και όχι ανανέωση ρυθμιστικών εργαλείων
- Βασικές επιλογές του κοινοτικού νομοθέτη
 - Οριοθέτηση νομιμότητας επεξεργασίας
 - Ποιοτικά χαρακτηριστικά δεδομένων και αρχή του σκοπού
 - Ειδικές κατηγορίες δεδομένων
 - Αρχή της διαφάνειας (έναντι υποκειμένου/αρχής ελέγχου)
 - Θεσμικός έλεγχος
 - Αυτορρύθμιση

Εθνικό κανονιστικό πλαίσιο

- ✦ Σύνταγμα (άρθρο 9Α)
- ✦ Νόμος 2472/97 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα
- ✦ Νόμος 3471/06 για την προστασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών (αντικατέστησε τον ν. 2774/99)

Η σημασία της ένταξης του δικαιώματος στο Σύνταγμα

- ✦ Δέσμευση από Συνθήκες και Κοινοτική νομοθεσία
- ✦ Η συμβολική σημασία
- ✦ Η σημασία της συνταγματικής θωράκισης για την εφαρμογή του κανονιστικού πλαισίου

Προστασία προσωπικών δεδομένων

- Δίκαιο προστασίας προσωπικών δεδομένων: εάν και υπό ποιες προϋποθέσεις είναι νόμιμη η επεξεργασία προσωπικών δεδομένων, δηλ. των πληροφοριών που αναφέρονται/ σχετίζονται με ένα άτομο
- Σύνολο κανόνων, προϋποθέσεων, όρων, εξουσιών και απαγορεύσεων αλλά και από ρυθμίσεις σχετικές με διαδικασίες, θεσμικούς ελέγχους, εγγυήσεις και αντίβαρα των περιορισμών των δικαιωμάτων των προσώπων

Προστασία προσωπικών δεδομένων

- Δίκαιο προστασίας προσωπικών δεδομένων: εάν και υπό ποιες προϋποθέσεις είναι νόμιμη η επεξεργασία προσωπικών δεδομένων, δηλ. των πληροφοριών που αναφέρονται/ σχετίζονται με ένα άτομο
- Σύνολο κανόνων, προϋποθέσεων, όρων, εξουσιών και απαγορεύσεων αλλά και από ρυθμίσεις σχετικές με διαδικασίες, θεσμικούς ελέγχους, εγγυήσεις και αντίβαρα των περιορισμών των δικαιωμάτων των προσώπων

Νόμος 2472/97

Αντικείμενο και σκοπός

- ✦ Μεταφορά των ρυθμίσεων της Οδηγίας 95/46 στην ελληνική έννομη τάξη με αποκλίσεις προς την κατεύθυνση της μείζονος προστασίας
- ✦ Αντικείμενο του νόμου είναι η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα
- ✦ Σκοπός του νόμου είναι η προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής

Βασικά χαρακτηριστικά του Ν. 2472/97

- ✦ Δημόσιο και ιδιώτες ως ισοδύναμες πηγές διακινδύνευσης για τα δικαιώματα – Ενιαίοι κανόνες
- ✦ Ηλεκτρονική και «παραδοσιακή» επεξεργασία : Ενιαίοι κανόνες
- ✦ Ενισχυμένος ρόλος για την ανεξάρτητη Αρχή

Δεδομένα προσωπικού χαρακτήρα/1

- Δεδομένα προσωπικού χαρακτήρα είναι κάθε πληροφορία που αναφέρεται στο “υποκείμενο των δεδομένων”
- Υποκείμενο δεδομένων
 - Κάθε Φυσικό Πρόσωπο – η ταυτότητα του οποίου είναι προσδιορισμένη ή μπορεί να προσδιοριστεί βάσει ενδεικτικά απαριθμούμενων χαρακτηριστικών –στοιχείων (φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική υπόσταση)
- Δεν λογίζονται ως δεδομένα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιοριστούν τα υποκείμενα

Δεδομένα προσωπικού χαρακτήρα/2

Περιγραφικά

Αξιολογικά

Σχέσεις προς πρόσωπα/πράγματα

Συμπεριλαμβάνονται

- δεδομένα ήχου-εικόνας

- Βιομετρικά δεδομένα : βιολογικά/συμπεριφορικά

- Στοιχεία ψηφιακής ταυτότητας

Επεξεργασία

- ✚ Τεχνολογικά ουδέτερος ορισμός
- ✚ Κάθε εργασία – Ενδεικτική απαρίθμηση στο νόμο
 - Από τη Συλλογή έως την Καταστροφή
 - Ανωνυμοποίηση / Ψευδωνυμοποίηση ως μορφές επεξεργασίας
 - Ειδικά ρυθμισμένες μορφές : Διασύνδεση αρχείων (συσχέτιση /συνδυασμός δεδομένων περισσοτέρων αρχειων)
- ✚ Με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων
- ✚ Που εφαρμόζεται σε δεδομένα

Αρχείο

κάθε σύνολο δεδομένων που

- αποτελεί αντικείμενο επεξεργασίας
- είναι διαρθρωμένο
- είναι προσιτό με συγκεκριμένα κριτήρια

•τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχείο

Υπεύθυνος κι Εκτελών

- ✦ Υπεύθυνος επεξεργασίας: οποιοσδήποτε καθορίζει τον σκοπό και τον τρόπο της επεξεργασίας.
 - Ευθύνη για εφαρμογή νόμου – κυρώσεις
 - Οδηγίες σε εκτελούντα
- ✦ Εκτελών την επεξεργασία: οποιοσδήποτε επεξεργάζεται δεδομένα για λογαριασμό του υπεύθυνου επεξεργασίας.
 - Ευθύνη για εφαρμογή νόμου μέσω τήρησης οδηγιών υπεύθυνου/ ασφάλεια – εμπιστευτικότητα

Η νομιμότητα της επεξεργασίας

- ✦ Κάθε επεξεργασία συνιστά επέμβαση σε θεμελιώδη δικαιώματα
- ✦ Η επεξεργασία είναι νόμιμη μόνο εφόσον θεμελιώνεται στις περιπτώσεις που ο νόμος ορίζει δεσμευτικά και περιοριστικά ως βάσεις νομιμότητάς της

Βάσεις νομιμότητας επεξεργασίας (άρθρο 5)

- ✦ Συγκατάθεση ως κανόνας
- ✦ Εκτέλεση σύμβασης στην οποία το υποκείμενο είναι συμβαλλόμενο μέρος
- ✦ Εκπλήρωση υποχρέωσης του υπευθύνου επεξεργασίας από το νόμο
- ✦ Διαφύλαξη ζωτικού συμφέροντος του υποκειμένου εφόσον συντρέχει νομική ή φυσική αδυναμία για έγκυρη συγκατάθεση
- ✦ Εκτέλεση έργου δημόσιου συμφέροντος ή έργου που εμπίπτει στην άσκηση δημόσιας εξουσίας
- ✦ Ικανοποίηση εννόμου συμφέροντος υπεύθυνου επεξεργασίας – τρίτου εφόσον
 - Αυτό υπερέχει προφανώς των δικαιωμάτων του υποκειμένου
 - Η επεξεργασία είναι απολύτως αναγκαία για την εκπλήρωσή του

Η έννοια της συγκατάθεσης (2 ια)

- ✦ Ελευθερία συγκατάθεσης
- ✦ Ρητή, ειδική και σαφής δήλωση
- ✦ Εν πλήρη επιγνώσει
- ✦ Ενημερωμένη (informed consent)
- ✦ Ελεύθερα ανακλητή χωρίς αναδρομικό αποτέλεσμα

Ειδική προστασία για τα ευαίσθητα δεδομένα (άρθρο 7)

✦ Ειδικές κανονιστικές προϋποθέσεις

- Έγγραφη συγκατάθεση του ατόμου το οποίο αφορούν τα δεδομένα
- Ρητές εξαιρέσεις για ειδικές κατηγορίες δεδομένων και ειδικές κατηγορίες επεξεργασιών με κριτήριο το δημόσιο συμφέρον ή τα δικαιώματα άλλων προσώπων που πρέπει να εκπληρωθούν

✦ Οργανωτικές εγγυήσεις

- Άδεια της Αρχής Προστασίας Προσωπικών Δεδομένων
- Η υποχρέωση λήψης αδείας συντρέχει σωρευτικά με την πλήρωση των ειδικών κανονιστικών προϋποθέσεων

Εξαιρέσεις από γνωστοποίηση/άδεια (άρθρο 7 Α)

- ✦ Απαλλαγή από υποχρέωση γνωστοποίησης/ λήψης προηγούμενης άδειας
- ✦ Συνήθης χαρακτήρας αρχείων και απροσδιόριστα μεγάλος αριθμός
 - Αρχεία εργαζομένων / αρχεία πελατών προμηθευτών
 - Αρχεία μελών κομμάτων, ενώσεων, συλλόγων κ.α
- ✦ Δέσμευση των υπεύθυνων επεξεργασίας από υποχρεώσεις απορρήτου
 - Γιατροί (όχι νοσοκομεία/ ιατρικά κέντρα/ κλινικές κ.α)
 - Δικηγόροι
 - Συμβολαιογράφοι

Διασύνδεση αρχείων (άρθρο 8)

- ✦ Δυνατότητα συσχέτισης των δεδομένων ενός αρχείου με τα δεδομένα άλλου αρχείου/αρχείων
- ✦ Προηγούμενη άδεια στην περίπτωση που ένα τουλάχιστον αρχείο περιέχει ευαίσθητα δεδομένα ή πρόκειται να γίνει χρήση «ενιαίου κωδικού αριθμού»
- ✦ ΑΦΜ ως ενιαίος κωδικός αριθμός

Διασυνοριακή ροή (άρθρο 9)

- ✦ Ευρωπαϊκή Ένωση: ενιαίος χώρος κυκλοφορίας και προστασίας προσωπικών δεδομένων – σκοπός εναρμόνισης
- ✦ Κράτη με ικανοποιητικό επίπεδο προστασίας
 - Διαπίστωση ικανοποιητικού επιπέδου από Αρχή Προστασίας Προσωπικών Δεδομένων
 - Αποφάσεις της Ευρωπαϊκής Ένωσης
 - Safe Harbour Principles
- ✦ Κράτη χωρίς ικανοποιητικό επίπεδο επεξεργασίας
 - Κατ' εξαίρεση άδεια της Αρχής εφόσον συντρέχουν οι προβλεπόμενες στο νόμο προϋποθέσεις



● Ασφάλεια ως παράμετρος της προστασίας δικαιωμάτων

- ✦ Προστασία απορρήτου / εμπιστευτικότητα
- ✦ Υποχρέωση λήψης τεχνικών και οργανωτικών μέτρων
- ✦ Επίπεδο ασφάλειας ανάλογο προς το είδος και την ένταση των κινδύνων και το είδος των δεδομένων που υπόκεινται σε επεξεργασία
- ✦ Τόσο κατά τη φάση σχεδιασμού του πληροφοριακού συστήματος/συστήματος επεξεργασίας όσο κατά την επεξεργασία



Η προσέγγιση της Αρχής Προστασίας Προσωπικών Δεδομένων

- ✦ Σχέδιο/Μέτρα ασφάλειας (άρθρο 10 ν. 2472/97) ως στοιχείο γνωστοποίησης και βασική προϋπόθεση για την αδειοδότηση επεξεργασιών και αρχείων (άρθρο 6 § 2 η ν. 2472/97)
- ✦ Σχέδιο Ασφάλειας-Πολιτική Ασφάλειας
- ✦ Επιβολή κυρώσεων για μη τήρηση μέτρων ασφάλειας κατά την καταστροφή – Οδηγία Αρχής
- ✦ Επιβολή κυρώσεων για παραβίαση απορρήτου και μέτρων ασφάλειας (Υπουργείο Δικαιοσύνης)

Ποιοτικά χαρακτηριστικά Γενικές αρχές

- ✱ Αρχή της νομιμότητας
- ✱ Αρχή της θεμιτής και νόμιμης συλλογής
- ✱ Αρχή του σκοπού
- ✱ Αρχή της αναλογικότητας
- ✱ Αρχή της ορθότητας των δεδομένων
- ✱ Αρχή της χρονικά πεπερασμένης διάρκειας τήρησης
- ✱ Αρχή της διαφάνειας
- ✱ Αρχή του ελέγχου
- ✱ Αρχή της ασφάλειας

Αρχή του σκοπού (άρθρο 4)

- ✦ Επεξεργασία προσωπικών δεδομένων
 - Για καθορισμένους, σαφείς και νόμιμους σκοπούς
 - Απαγόρευση χρήσης για ασύμβατους σκοπούς
 - Απαγόρευση δευτερεύουσας χρήσης
- ✦ Αρχή σκοπού vs. Πολυλειτουργικότητα
- ✦ Η ασυμφωνία/ασυμβατότητα με τον αρχικό σκοπό κρίνεται
 - σε συνδυασμό με το σκοπό που έχει καταστεί γνωστός στο υποκείμενο
 - σε συνδυασμό με τις συνέπειες που έχει η περαιτέρω χρήση για το υποκείμενο

Αρχή της αναλογικότητας (άρθρο 4)

- ✦ Τα προσωπικά δεδομένα που υπόκεινται σε επεξεργασία πρέπει να είναι
 - Συναφή
 - Πρόσφορα – κατάλληλα
 - Όχι περισσότερα από όσα χρειάζονται ενόψει των σκοπών της επεξεργασίας
 - Μέτρο της αναλογικότητας είναι ο σκοπός, που καθορίζει όχι μόνο τη νομιμότητα του «εάν» αλλά και το «σε ποια έκταση»

Αρχές της ορθότητας και της χρονικά πεπερασμένης διάρκειας τήρησης (άρθρο 4)

- ☛ Τα δεδομένα πρέπει να είναι ακριβή και να υποβάλλονται σε ενημέρωση
 - Αποφυγή δυσμενών συνεπειών για τα υποκείμενα από ανακριβή στοιχεία
- ☛ Διατήρηση μόνο για το διάστημα που απαιτείται για την επίτευξη του σκοπού
 - Μετά την πάροδο αυτού του διαστήματος υποχρέωση του υπεύθυνου επεξεργασίας να προβεί σε διαγραφή/καταστροφή
 - Απόκλιση από την υποχρέωση με απόφαση της Αρχής Προστασίας Προσωπικών Δεδομένων

Αρχή της διαφάνειας και του ελέγχου

- ☛ Διαφάνεια έναντι του υποκειμένου των δεδομένων
 - Δικαιώματα των προσώπων
- ☛ Διαφάνεια έναντι της αρχής ελέγχου
 - Συστήματα γνωστοποίησης
 - Εναλλακτικές μορφές/διαδικασίες διαφάνειας
 - Εξαιρέσεις από τις υποχρεώσεις γνωστοποίησης και άδειας