IT & IT LAW

SDM 024

Personal Data

2017

Evangelia Vagena

Ph.D, DEA Droit et Informatique

Προσωπικά δεδομένα

Right to privacy-«Privacy is the right to be let alone»- προστασία ιδιωτικού βίου

≠

Right to data protection- προστασία προσωπικών δεδομένων

Ιστορικά…

- 1970 Ευρώπη
- Σουηδία 1973, Γερμανία 1976, Γαλλία 1978, Αγγλία 1983…Ελλάδα 1997
- «Ηλεκτρονικό φακέλωμα»
- Τεχνολογικές εξελίξεις – ευρεία επεξεργασία προσωπικών δεδομένων

Βασικό νομοθετικό πλαίσιο

- Ευρωπαϊκή νομοθεσία:
  - Οδηγία 95/46/ΕΚ
  - Οδηγία 2002/58/ΕΚ
  - Οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Μαρτίου 2006 για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών και για την τροποποίηση της Οδηγίας 2002/58/ΕΚ
  - ΑΠΟΦΑΣΗ ΠΛΑΙΣΙΟ 2008/977/ΔΕΥ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 27ης Νοεμβρίου 2008 για την προστασία των δεδομένων προσωπικού χαρακτήρα που τυγχάνουν επεξεργασίας στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις
  - Οδηγία 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009 , για τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ
- Σύνταγμα άρθρο 9^{A}:

  «Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει.»
- 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 (τροποποίησε τον ν. 2774/99)

Προσωπικά δεδομένα

= *κάθε* πληροφορία που αναφέρεται σε και περιγράφει ένα άτομο, όπως:

- στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση κλπ.), φυσικά χαρακτηριστικά,
- εκπαίδευση,
- εργασία (προϋπηρεσία, εργασιακή συμπεριφορά κλπ),
- οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά),
- ενδιαφέροντα, δραστηριότητες, συνήθειες.

✓Το άτομο στο οποίο αναφέρονται τα δεδομένα ονομάζεται *υποκείμενο των δεδομένων.*

Ευαίσθητα προσωπικά δεδομένα

= προσωπικά δεδομένα ενός ατόμου που αναφέρονται

- στη φυλετική ή εθνική του προέλευση,
- στα πολιτικά του φρονήματα,
- στις θρησκευτικές ή φιλοσοφικές του πεποιθήσεις,
- στη συμμετοχή του σε συνδικαλιστική οργάνωση,
- στην υγεία του,
- στην κοινωνική του πρόνοια,
- στην ερωτική του ζωή,
- τις ποινικές διώξεις και καταδίκες του, καθώς και
- στη συμμετοχή του σε συναφείς με τα ανωτέρω ενώσεις προσώπων.

Τα ευαίσθητα δεδομένα προστατεύονται από τον Νόμο με αυστηρότερες ρυθμίσεις από ότι τα απλά προσωπικά δεδομένα.

Επεξεργασία προσωπικών δεδομένων

= *κάθε εργασία* που πραγματοποιείται σε δεδομένα προσωπικού χαρακτήρα, όπως: συλλογή, καταχώριση, οργάνωση, διατήρηση ή αποθήκευση, τροποποίηση, εξαγωγή, χρήση, διαβίβαση, διάδοση, συσχέτιση ή συνδυασμός, διασύνδεση, δέσμευση, διαγραφή, καταστροφή.

Επιτρεπτή επεξεργασία προσωπικών δεδομένων

- Κανόνας: μόνο όταν το άτομο έχει δώσει τη ***συγκατάθεσή*** του

- Εξαιρέσεις: α. 5 ν. 2472/1997

Επιτρεπτή επεξεργασία προσωπικών δεδομένων χωρίς συγκατάθεση

α) Η επεξεργασία είναι αναγκαία για *την* ***εκτέλεση σύμβασης***, στην οποία συμβαλλόμενο μέρος είναι υποκείμενο δεδομένων ή για τη λήψη μέτρων κατόπιν αιτήσεως του υποκειμένου κατά το προσυμβατικό στάδιο.

β) Η επεξεργασία είναι αναγκαία για την *εκπλήρωση υποχρεώσεως* του υπεύθυνου επεξεργασίας, η ***οποία επιβάλλεται από το νόμο***.

γ) Η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου, εάν αυτό τελεί σε ***φυσική ή νομική αδυναμία*** να δώσει τη συγκατάθεσή του.

δ) Η επεξεργασία είναι αναγκαία για την εκτέλεση ***έργου δημόσιου συμφέροντος*** ή έργου που εμπίπτει στην άσκηση δημόσιας εξουσίας και εκτελείται από δημόσια αρχή ή έχει ανατεθεί από αυτή είτε στον υπεύθυνο επεξεργασίας είτε σε τρίτο, στον οποίο γνωστοποιούνται τα δεδομένα.

ε) Η επεξεργασία είναι απολύτως αναγκαία για την ***ικανοποίηση του έννομου συμφέροντος*** που επιδιώκει ο υπεύθυνος επεξεργασίας ή ο τρίτος ή οι τρίτοι στους οποίους ανακοινώνονται τα δεδομένα και υπό τον όρο ότι τούτο υπερέχει προφανώς των δικαιωμάτων και συμφερόντων των προσώπων στα οποία αναφέρονται τα δεδομένα και δεν θίγονται οι θεμελιώδεις ελευθερίες αυτών.

Επιτρεπτή επεξεργασία *ευαίσθητων* προσωπικών δεδομένων

Μετά από **άδεια** της Αρχής Προστασίας Προσωπικών Δεδομένων

α) Το υποκείμενο έδωσε τη ***γραπτή συγκατάθεσή*** του εκτός εάν η συγκατάθεση έχει αποσπασθεί με τρόπο που αντίκειται στο νόμο ή τα χρηστά ήθη ή νόμος ορίζει ότι η συγκατάθεση δεν αίρει την απαγόρευση.

β) Η επεξεργασία είναι αναγκαία για τη ***διαφύλαξη ζωτικού συμφέροντος*** του υποκειμένου ή προβλεπόμενου από το νόμο συμφέροντος τρίτου, εάν το υποκείμενο τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του.

γ) Η επεξεργασία αφορά δεδομένα που ***δημοσιοποιεί το ίδιο το υποκείμενο ή είναι αναγκαία για την αναγνώριση, άσκηση ή υπεράσπιση δικαιώματος*** ενώπιον δικαστηρίου ή πειθαρχικού οργάνου.

δ) Η επεξεργασία αφορά θέματα υγείας και εκτελείται από πρόσωπο που ασχολείται ***κατ' επάγγελμα με την παροχή υπηρεσιών υγείας*** και υπόκειται σε καθήκον εχεμύθειας ή σε συναφείς κώδικες δεοντολογίας, υπό τον όρο ότι η επεξεργασία είναι απαραίτητη για την ιατρική πρόληψη, διάγνωση, περίθαλψη ή τη διαχείριση υπηρεσιών υγείας.

ε) Η επεξεργασία εκτελείται από ***Δημόσια Αρχή*** και είναι αναγκαία είτε αα) για λόγους εθνικής ασφάλειας είτε ββ) για την εξυπηρέτηση των αναγκών εγκληματολογικής ή σωφρονιστικής πολιτικής και αφορά τη διακρίβωση εγκλημάτων, ποινικές καταδίκες ή μέτρα ασφαλείας είτε γγ) για λόγους προστασίας της δημόσιας υγείας είτε δδ) για την άσκηση δημόσιου φορολογικού ελέγχου ή δημόσιου ελέγχου κοινωνικών παροχών.

στ) Η επεξεργασία πραγματοποιείται για ***ερευνητικούς και επιστημονικούς*** αποκλειστικά σκοπούς και υπό τον όρο ότι τηρείται η ***ανωνυμία*** και λαμβάνονται όλα τα απαραίτητα μέτρα για την προστασία των δικαιωμάτων των προσώπων στα οποία αναφέρονται.

ζ) Η επεξεργασία αφορά δεδομένα ***δημοσίων προσώπων,*** εφόσον αυτά συνδέονται με την άσκηση δημοσίου λειτουργήματος ή τη διαχείριση συμφερόντων τρίτων, και πραγματοποιείται αποκλειστικά για την άσκηση του ***δημοσιογραφικού επαγγέλματος***. Η άδεια της αρχής χορηγείται μόνο εφόσον η επεξεργασία είναι απολύτως αναγκαία για την εξασφάλιση του δικαιώματος πληροφόρησης επί θεμάτων δημοσίου ενδιαφέροντος καθώς και στο πλαίσιο καλλιτεχνικής έκφρασης και εφόσον δεν παραβιάζεται καθ' οιονδήποτε τρόπο το δικαίωμα προστασίας της ιδιωτικής και οικογενειακής ζωής.

ΑΡΧΕΣ ΠΟΥ ΔΙΕΠΟΥΝ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ

- Αρχή της νομιμότητας της επεξεργασίας
- Αρχή της θεμιτής και νόμιμης συλλογής
- Αρχή του σκοπού
- Αρχή της αναλογικότητας/ ή συνάφειας
- Αρχή της ορθότητας των δεδομένων
- Αρχή της χρονικά πεπερασμένης διάρκειας τήρησης
- Αρχή του απορρήτου
- Αρχή της ασφάλειας

Αρχή της νομιμότητας της επεξεργασίας

- Επεξεργασία σύμφωνα με τις προϋποθέσεις που θέτει η νομοθεσία προστασίας των προσωπικών δεδομένων

- Επεξεργασία που να αποσκοπεί στους σκοπούς για τους οποίους επιτρέπεται να γίνεται νόμιμα

Αρχή της θεμιτής και νόμιμης συλλογής

Νόμιμη = να μην παραβιάζεται καμία διάταξη νόμου και να τηρούνται:

- Ενημέρωση υποκειμένου
- Συγκατάθεση υποκειμένου
- Προηγούμενη γνωστοποίηση στην ΑΠΔΠΧ
- Προηγούμενη άδεια για ευαίσθητα δεδομένα
- Γνωστοποίηση και για διασύνδεση αρχείων
- Διασφάλιση ίσου επιπέδου προστασίας αν υπάρχει διαβίβαση σε χώρες εκτός ΕΕ
- Απόρρητη και ασφαλής συλλογή δεδομένων

❖ Πρώτα εξετάζεται αν είναι νόμιμη κι έπειτα αν είναι θεμιτή, με βάση ηθικά κριτήρια δηλαδή.

➢ Παράδειγμα **αθέμιτης**: συλλογή δεδομένων σε μαιευτήρια από λεχώνες που μόλις γέννησαν (ΑΠΔΠΧ 523/2000

Αρχή του σκοπού

- Επεξεργασία προσωπικών δεδομένων
  - Για καθορισμένους, σαφείς και νόμιμους σκοπούς (δεν μπορεί οι σκοποί να είναι μελλοντικοί και άδηλοι π.χ. Profiling για σκοπούς marketing)
  - Απαγόρευση χρήσης για ασύμβατους σκοπούς
  - Απαγόρευση δευτερεύουσας χρήσης

  π.χ απόφαση ΑΠΔΠΧ 19/2002 απαγόρευση data mining

- 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/ ή συνάφειας

- Τα δεδομένα να είναι συναφή, πρόσφορα και όχι περισσότερα από όσα απαιτείται για την επίτευξη του σκοπού της επεξεργασίας.

π.χ απόφαση ΑΠΔΠΧ 51/2004 φωτοτυπία εκκαθαριστικού εφορίας ως αποδεικτικού ΑΦΜ παρέχει περισσότερα στοιχεία από όσα απαιτείται για την έκδοση παραστατικού πληρωμής (διαβατηρίων ανυπότακτων εξωτερικού)

Αρχή της ορθότητας των δεδομένων

- Να είναι ακριβή, να ανταποκρίνονται στην πραγματικότητα
- Να υπόκεινται σε επικαιροποίηση

✓ Βλ. οδηγία ΑΠΔΠΧ 2/2003 για τον τρόπο μεταγγραφής με λατινικά στοιχεία των ονομάτων στα δελτία ταυτότητας και τα διαβατήρια

✓ Βλ. πολλές αποφάσεις ΑΠΔΠΧ για τη βάση δεδομένων του ΤΕΙΡΕΣΙΑ

Αρχή της χρονικά πεπερασμένης διάρκειας τήρησης

- Η διάρκεια τήρησης των δεδομένων ορίζεται από την Αρχή Προστασίας Προσωπικών Δεδομένων
- Τα δεδομένα τηρούνται όσο χρόνο απαιτεί η επεξεργασία τους για το διάστημα που απαιτείται για την επίτευξη του σκοπού
- Μετά την πάροδο του παραπάνω χρόνου τα δεδομένα καταστρέφονται με ευθύνη του υπεύθυνου επεξεργασίας
- Τα δεδομένα τηρούνται και μετά τον παραπάνω χρόνο με απόφαση της Αρχής Προστασίας Προσωπικών Δεδομένων για σκοπούς *ιστορικούς, επιστημονικούς ή στατιστικούς*

Αρχή του απορρήτου

- Επεξεργασία μόνο από τον υπεύθυνο επεξεργασίας ή τον εκτελών αυτήν και κατ’ εντολή τους

- Απόρρητο ηλεκτρονικών επικοινωνιών

(βλ. αναλυτικά διαφάνειες για απόρρητο)

Αρχή της ασφάλειας

«Ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει τα κατάλληλα ***οργανωτικά και τεχνικά μέτρα*** για την ασφάλεια των δεδομένων και την προστασία τους από **τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση** και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Αυτά τα μέτρα πρέπει να εξασφαλίζουν επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας. Με την επιφύλαξη άλλων διατάξεων, η Αρχή παρέχει οδηγίες ή εκδίδει κανονιστικές πράξεις σύμφωνα με το άρθρο 19 παρ. 1 ι' για τη ρύθμιση θεμάτων σχετικά με τον βαθμό ασφαλείας των δεδομένων και των υπολογιστικών και επικοινωνιακών υποδομών, τα μέτρα ασφάλειας που είναι αναγκαίο να λαμβάνονται για κάθε κατηγορία και επεξεργασία δεδομένων, καθώς και *για τη χρήση τεχνολογιών ενίσχυσης της ιδιωτικότητας.»*

ΥΠΟΧΡΕΩΣΗ ΓΝΩΣΤΟΠΟΙΗΣΗΣ ΑΡΧΕΙΟΥ

Κάθε υπεύθυνος επεξεργασίας οφείλει να γνωστοποιεί στην Αρχή την επεξεργασία προσωπικών δεδομένων που πραγματοποιεί, εκτός αν εμπίπτει σε μία από τις περιπτώσεις του αρ. 7Α του Ν. 2472/1997.

ΕΞΑΙΡΕΣΗ ΑΠΟ ΥΠΟΧΡΕΩΣΗ ΓΝΩΣΤΟΠΟΙΗΣΗΣ ΑΡΧΕΙΟΥ

- 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

ΕΞΑΙΡΕΣΗ ΑΠΟ ΥΠΟΧΡΕΩΣΗ ΓΝΩΣΤΟΠΟΙΗΣΗΣ ΑΡΧΕΙΟΥ

α) Όταν η επεξεργασία πραγματοποιείται αποκλειστικά για σκοπούς που συνδέονται άμεσα με ***σχέση εργασίας ή έργου*** ή με παροχή υπηρεσιών στο δημόσιο τομέα και είναι αναγκαία για την εκπλήρωση υποχρέωσης που επιβάλλει ο νόμος ή για την εκτέλεση των υποχρεώσεων από τις παραπάνω σχέσεις και το υποκείμενο έχει προηγουμένως ενημερωθεί.

β) Όταν η επεξεργασία αφορά ***πελάτες ή προμηθευτές***, εφόσον τα δεδομένα δεν διαβιβάζονται ούτε κοινοποιούνται σε τρίτους. [..]Δεν απαλλάσσονται από την υποχρέωση γνωστοποίησης οι ασφαλιστικές εταιρείες για όλους τους κλάδους ασφάλισης, οι φαρμακευτικές εταιρείες, οι εταιρείες εμπορίας πληροφοριών και τα χρηματοπιστωτικά νομικά πρόσωπα, όπως οι τράπεζες και οι εταιρείες έκδοσης πιστωτικών καρτών.

γ) Όταν η επεξεργασία γίνεται από ***σωματεία, εταιρείες, ενώσεις προσώπων και πολιτικά κόμματα*** και αφορά δεδομένα των μελών ή εταιρειών τους, εφόσον αυτοί έχουν δώσει την συγκατάθεσή τους και τα δεδομένα δεν διαβιβάζονται ούτε κοινοποιούνται σε τρίτους. […]

δ) Όταν η επεξεργασία αφορά ***δεδομένα υγείας και γίνεται από ιατρούς*** ή άλλα πρόσωπα που παρέχουν υπηρεσίες υγείας, εφόσον ο υπεύθυνος επεξεργασίας δεσμεύεται από το ιατρικό απόρρητο ή άλλο απόρρητο που προβλέπει νόμος ή κώδικας δεοντολογίας και τα δεδομένα δεν διαβιβάζονται ούτε κοινοποιούνται σε τρίτους.[..] Δεν εμπίπτουν στην απαλλαγή της παρούσας διάταξης τα νομικά πρόσωπα ή οργανισμοί που παρέχουν υπηρεσίες υγείας, όπως κλινικές, νοσοκομεία, κέντρα αποθεραπείας και αποτοξίνωσης, ασφαλιστικά ταμεία και ασφαλιστικές εταιρείες, καθώς και οι υπεύθυνοι επεξεργασίας δεδομένων προσωπικού χαρακτήρα όταν η επεξεργασία διεξάγεται στο πλαίσιο προγραμμάτων τηλεϊατρικής ή παροχής ιατρικών υπηρεσιών μέσω δικτύου.

ε) Όταν η επεξεργασία γίνεται από ***δικηγόρους, συμβολαιογράφους, άμισθους υποθηκοφύλακες και δικαστικούς επιμελητές*** ή εταιρείες των προσώπων αυτών και αφορά στην παροχή νομικών υπηρεσιών προς πελάτες τους, εφόσον ο υπεύθυνος επεξεργασίας και τα μέλη των εταιρειών δεσμεύονται από υποχρέωση απορρήτου που προβλέπει νόμος και τα δεδομένα δεν διαβιβάζονται ούτε κοινοποιούνται σε τρίτους, εκτός από τις περιπτώσεις που αυτό είναι αναγκαίο και συνδέεται άμεσα με την εκπλήρωση εντολής του πελάτη.

στ) Όταν η επεξεργασία γίνεται από ***δικαστικές αρχές ή υπηρεσίες […]*** στο πλαίσιο απονομής της δικαιοσύνης ή για την εξυπηρέτηση των αναγκών της λειτουργίας τους.*

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»*

**αριθμός με τον οποίο καθίσταται ευχερής ο μονοσήμαντος προσδιορισμός της ταυτότητας ενός προσώπου όπως αριθμός δελτίου ταυτότητας, κοινωνικής ασφάλισης, φορολογικού μητρώου.*

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
  - ΗΠΑ δεν έχουν αντίστοιχη νομοθεσία αλλά «Safe Harbour Principles", αρχές ασφαλούς λιμένα για την προστασία της ασφαλούς ζωής- ειδική συμφωνία με ΕΕ για διαβίβαση δεδομένων για ΗΠΑ βλ. http://www.export.gov/safeharbor/eu/eg_main_018365.asp

- Κράτη χωρίς ικανοποιητικό επίπεδο επεξεργασίας
  - Κατ' εξαίρεση άδεια της Αρχής εφόσον συντρέχουν οι προβλεπόμενες στο νόμο προϋποθέσεις

Δικαιώματα των υποκειμένων

- Υποχρέωση /δικαίωμα ενημέρωσης
- Δικαίωμα πρόσβασης (αίτηση, χρηματικό ποσό)
- Δικαίωμα αντίρρησης (αίτημα, απάντηση σε 15 μέρες)
- Δικαίωμα επικαιροποίησης, διόρθωσης, διαγραφής
- Δικαίωμα εξαίρεσης από επεξεργασία για λόγους προώθησης προϊόντων και υπηρεσιών ή παροχής υπηρεσιών εξ αποστάσεως (Robinson lists)

Δικαίωμα πρόσβασης (άρθρο 12)

- Δικαίωμα λήψης πληροφοριών για το γεγονός της επεξεργασίας και για σκοπούς, εξέλιξη και λογική επεξεργασίας
- Καταβολή χρηματικού ποσού για άσκηση δικαιώματος (απόφαση αρχής)
- Προσφυγή στην Αρχή σε περίπτωση μη απάντησης/μη ικανοποιητικής απάντησης
- Εξαίρεση (με απόφαση Αρχής) σε περίπτωση επεξεργασίας για σκοπούς εθνικής ασφάλειας/διακρίβωσης ιδιαίτερα σοβαρών εγκλημάτων

ΥΠΟΧΡΕΩΣΗ ISPs ΓΙΑ ΔΙΑΤΗΡΗΣΗ ΔΕΔΟΜΕΝΩΝ

Ν. 3917/2011 *«Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών* ***ηλεκτρονικών επικοινωνιών*** *ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις.»*

ΥΠΟΧΡΕΩΣΗ ISPs ΓΙΑ ΔΙΑΤΗΡΗΣΗ ΔΕΔΟΜΕΝΩΝ

- «Κατά παρέκκλιση των σχετικών διατάξεων του ν. 3471/ 2006»(Α.3 ΠΑΡ.1)
- « Οι πάροχοι διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιου δικτύου επικοινωνιών ***υποχρεούνται να διατηρούν τα δεδομένα*** του άρθρου 5 που παράγονται ή υποβάλλονται σε επεξεργασία από αυτούς, προκειμένου τα δεδομένα αυτά να καθίστανται διαθέσιμα στις αρμόδιες αρχές για τη διακρίβωση ***ιδιαίτερα σοβαρών εγκλημάτων***, όπως αυτά ορίζονται στο άρθρο 4 του ν. 2225/1994 (ΦΕΚ 121 Α')».

- Για ένα χρόνο από τη στιγμή της επικοινωνίας (α.6)

- Επιπλέον υποχρεώσεις για την «ασφάλεια & την ακεραιότητα των δεδομένων»
  - Τα δεδομένα να είναι ίδιας ποιότητας και να έχουν την ίδια προστασία και ασφάλεια που παρέχει το δίκτυο
  - Να λαμβάνονται οργανωτικά & τεχνικά μέτρα προστασίας των δεδομένων
  - Να έχει πρόσβαση μόνο ειδικά εξουσιοδοτημένο προσωπικό
  - Να καταστρέφονται στο τέλος του χρονικού διαστήματος διατήρησης
  - Να υπάρχει ειδικό σχέδιο πολιτικής ασφαλείας
  - Να διατηρούνται σε μορφή που να επιτρέπει την ηλεκτρονική επεξεργασία τους & να διαβιβάζονται εντός 5 ημερών από το αίτημα της αρχής.

ΥΠΟΧΡΕΩΣΗ ISPs ΓΙΑ ΔΙΑΤΗΡΗΣΗ ΔΕΔΟΜΕΝΩΝ- ΕΙΔΟΣ ΔΕΔΟΜΕΝΩΝ

1) Δεδομένα αναγκαία για την ανίχνευση και τον προσδιορισμό της ***πηγής της επικοινωνίας***:[…]

β. όσον αφορά την πρόσβαση στο διαδίκτυο και τις υπηρεσίες ηλεκτρονικού ταχυδρομείου και τηλεφωνίας μέσω διαδικτύου:

αα) ο αποδοθείς κωδικός ταυτότητας χρήστη, ββ) ο κωδικός ταυτότητας χρήστη και ο τηλεφωνικός αριθμός που δίνονται σε κάθε επικοινωνία που εισέρχεται στο δημόσιο τηλεφωνικό δίκτυο, γγ) το ονοματεπώνυμο και η διεύθυνση του συνδρομητή ή εγγεγραμμένου χρήστη στον οποίο είχε αποδοθεί κατά το χρόνο επικοινωνίας διεύθυνση IP (πρωτοκόλλου διαδικτύου), κωδικός ταυτότητας χρήστη ή αριθμός τηλεφώνου

2) δεδομένα αναγκαία για τον προσδιορισμό ***του προορισμού της επικοινωνίας***:[…]

β. όσον αφορά την πρόσβαση στο διαδίκτυο και τις υπηρεσίες ηλεκτρονικού ταχυδρομείου και τηλεφωνίας μέσω διαδικτύου:

αα) η ημερομηνία και η ώρα σύνδεσης και αποσύνδεσης με το διαδίκτυο με βάση συγκεκριμένη ωριαία ζώνη, καθώς και η διεύθυνση πρωτοκόλλου του διαδικτύου (IP), είτε δυναμική είτε στατική, που απέδωσε στην επικοινωνία ο πάροχος υπηρεσιών πρόσβασης στο διαδίκτυο, καθώς και ο κωδικός ταυτότητας χρήστη του συνδρομητή ή εγγεγραμμένου χρήστη, ββ) η ημερομηνία και η ώρα σύνδεσης και αποσύνδεσης με την υπηρεσία ηλεκτρονικού ταχυδρομείου ή τηλεφωνίας μέσω διαδικτύου, με βάση συγκεκριμένη ωριαία ζώνη·

3) δεδομένα αναγκαία για τον προσδιορισμό της ***ημερομηνίας, ώρας και διάρκειας της επικοινωνίας***:[…]

β. όσον αφορά την πρόσβαση στο διαδίκτυο και τις υπηρεσίες ηλεκτρονικού ταχυδρομείου και τηλεφωνίας μέσω διαδικτύου:

αα) η ημερομηνία και η ώρα σύνδεσης και αποσύνδεσης με το διαδίκτυο με βάση συγκεκριμένη ωριαία ζώνη, καθώς και η διεύθυνση πρωτοκόλλου του διαδικτύου (IP), είτε δυναμική είτε στατική, που απέδωσε στην επικοινωνία ο πάροχος υπηρεσιών πρόσβασης στο διαδίκτυο, καθώς και ο κωδικός ταυτότητας χρήστη του συνδρομητή ή εγγεγραμμένου χρήστη, ββ) η ημερομηνία και η ώρα σύνδεσης και αποσύνδεσης με την υπηρεσία ηλεκτρονικού ταχυδρομείου ή τηλεφωνίας μέσω διαδικτύου, με βάση συγκεκριμένη ωριαία ζώνη·

4) δεδομένα αναγκαία για τον ***προσδιορισμό του είδους*** της επικοινωνίας:

β. όσον αφορά τις υπηρεσίες ηλεκτρονικού ταχυδρομείου και τηλεφωνίας μέσω διαδικτύου: η χρησιμοποιηθείσα διαδικτυακή υπηρεσία·

5) δεδομένα αναγκαία για τον ***προσδιορισμό του εξοπλισμού επικοινωνίας*** των χρηστών ή του φερομένου ως εξοπλισμού επικοινωνίας τους:[..]

γ. όσον αφορά την πρόσβαση στο διαδίκτυο και τις υπηρεσίες ηλεκτρονικού ταχυδρομείου και τηλεφωνίας μέσω διαδικτύου:

αα) ο τηλεφωνικός αριθμός καλούντος για την πρόσβαση μέσω τηλεφώνου, ββ) η ψηφιακή συνδρομητική γραμμή (DSL) ή άλλη απόληξη της πηγής της επικοινωνίας·

Cookies – opt out σύστημα

(Α.4 παρ. 5 ν.3471/2006 όπως τροποποιήθηκε με α.170 ν.4070/2012)

«Η αποθήκευση πληροφοριών ή η απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη επιτρέπεται μόνο αν ο συγκεκριμένος συνδρομητής ή χρήστης ***έχει δώσει τη συγκατάθεση του*** μετά από σαφή και εκτενή ενημέρωση κατά την παρ. 1 του άρθρου 11 του ν. 2472/1997. όπως ισχύει. Η συγκατάθεση του συνδρομητή ή χρήστη μπορεί να δίδεται μέσω *κατάλληλων ρυθμίσεων στο φυλλομετρητή* ιστού ή μέσω άλλης εφαρμογής. Τα παραπάνω δεν εμποδίζουν την οποιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η *διενέργεια της διαβίβασης μίας επικοινωνίας* μέσω δικτύου ηλεκτρονικών επικοινωνιών ή η οποία είναι αναγκαία για την παροχή υπηρεσίας της κοινωνίας της πληροφορίας, την οποία έχει ζητήσει ρητά ο χρήστης ή ο συνδρομητής. Με πράξη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.) ορίζονται ειδικότερα οι τρόποι παροχής πληροφοριών και δήλωσης της συγκατάθεσης.»

Συνεπώς αφορά:

- ✓ cookies που χρησιμοποιούνται για διαδικτυακή διαφήμιση (online advertising), είτε αυτά εγκαθίστανται από τον ίδιο τον πάροχο της ιστοσελίδας, είτε από τρίτα διαφημιστικά δίκτυα μέσω του επισκεπτόμενου site.
- ✓ cookies που εγκαθίστανται με σκοπό την στατιστική ανάλυση (web analytics), ακόμη και αν αυτά αφορούν απλώς την στατιστική ανάλυση της επισκεψιμότητας μιας ιστοσελίδας.
- ✓ Δεν χρειάζεται συγκατάθεση για cookies που εξυπηρετούν λειτουργικές ανάγκες της ιστοσελίδας και είναι απαραίτητα για την εμφάνισή της και την αποτελεσματική λειτουργία της στον υπολογιστή του καταναλωτή (functional cookies).

Δεδομένα κίνησης και θέσης σε ηλεκτρονικές επικοινωνίες (ν.3471/2006)

- «**δεδομένα κίνησης**»: τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μίας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσης της. Στα δεδομένα κίνησης μπορεί να περιλαμβάνονται, μεταξύ άλλων, ο *αριθμός, η διεύθυνση, η ταυτότητα της σύνδεσης ή του τερματικού εξοπλισμού του συνδρομητή ή και χρήστη, οι κωδικοί πρόσβασης, τα δεδομένα θέσης, η ημερομηνία και ώρα έναρξης και λήξης και η διάρκεια της επικοινωνίας, ο όγκος των διαβιβασθέντων δεδομένων, πληροφορίες σχετικά με το πρωτόκολλο, τη μορφοποίηση, τη δρομολόγηση της* επικοινωνίας καθώς και το δίκτυο από το οποίο προέρχεται ή στο οποίο καταλήγει η επικοινωνία.
- «**δεδομένα θέσης**»: τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών ή από μια υπηρεσία ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη *γεωγραφική θέση* του τερματικού εξοπλισμού του χρήστη μια διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών.»
- Κανόνας: **απαγόρευση επεξεργασίας** εκτός αν δοθεί συγκατάθεση χρήστη (opt in σύστημα)
- Τα δεδομένα θέσης μπορεί να τύχουν επεξεργασίας σε περιπτώσεις έκτακτης ανάγκης για να εντοπισθεί ο καλών από τις διωκτικές αρχές/ υπηρεσίες πρώτων βοηθειών και πυρόσβεσης

Επιπλέον δικαιώματα χρήστη σχετικά με την επεξεργασία των δεδομένων του στις ηλεκτρονικές επικοινωνίες (ν.3471/2006)

- Να μη λαμβάνει αναλυτικούς λογαριασμούς
- Να διαγράφονται εφόσον το ζητήσει ο χρήστης τα τελευταία 3 ψηφία αριθμών ή συνδέσεων
- Να εμποδίζει την αποκάλυψη της ταυτότητας και της αναγνώρισης της καλούσας και συνδεδεμένης γραμμής
- Να εμποδίζει τις αυτόματα προωθούμενες κλήσεις από τρίτους στην συσκευή του
- Δικαίωμα αντίρρησης για καταλόγους συνδρομητών
- Οι «μη αιτηθείσες ηλεκτρονικές επικοινωνίες» (spam) επιτρέπονται μόνο εφόσον ο χρήστης έχει δώσει τη συγκατάθεση του (opt in σύστημα)

Αρχή Προστασίας Προσωπικών Δεδομένων (ΑΠΔΠΧ)

- Ανεξάρτητος μηχανισμός ελέγχου
- Ανεξάρτητη αρχή κατοχυρωμένη στο Σύνταγμα (9 Α και 101 Α) – Απαγόρευση ιεραρχικού –πολιτικού ελέγχου
- Επιλογή Προέδρου και έξι μελών από το Κοινοβούλιο (ομοφωνία ή πλειοψηφία 4/5)
- Προσωπική/λειτουργική ανεξαρτησία
- Ασυμβίβαστα/κωλύματα
- Αντίστοιχες:
  - UK: Information Commissioner's Office http://ico.org.uk/
  - France: La Commission nationale de l'informatique et des libertés (CNIL)

Αρμοδιότητες Αρχής

- Ελεγκτικές αρμοδιότητες (αυτεπαγγέλτως/κατόπιν καταγγελίας)
- Αποφασιστικές αρμοδιότητες παρέμβασης (άδειες κλπ.)
- Κανονιστικές αρμοδιότητες (Οδηγίες, κανονιστικές πράξεις για ρύθμιση ειδικών θεμάτων)
- Γνωμοδοτικές αρμοδιότητες
- Κυρωτικές αρμοδιότητες

ΑΠΔΠΧ- επίκαιρη δραστηριότητα (κυβερνοεπιθέσεις)

Η ΑΠΔΠΧ συμμετείχε το Νοέμβριο του 2013 στην άσκηση κυβερνοάμυνας του ΝΑΤΟ CYBER COALITION 2013, που πραγματοποιήθηκε στην Ελλάδα υπό την αιγίδα του ΓΕΕΘΑ, και κατά την οποία δοκιμάστηκαν

α) η ικανότητα της χώρας να αντιμετωπίσει περιστατικά κυβερνοεπιθέσεων και

β) η ετοιμότητα της χώρας να συνδράμει διεθνείς φορείς σε περιπτώσεις κυβερνοεπίθεσης.

Η Αρχή συμμετείχε στην άσκηση τόσο σε διαδικαστικό επίπεδο, παρέχοντας συμβουλές σε θέματα που άπτονται των αρμοδιοτήτων της, όσο και τεχνικά, συμβάλλοντας στην επίλυση/αντιμετώπιση των εξετασθέντων περιστατικών κυβερνοεπίθεσης. Η συμμετοχή της Αρχής σε τέτοιου τύπου ασκήσεις βοηθάει τους φορείς που θα ενεργοποιηθούν σε περίπτωση πραγματικού περιστατικού κυβερνοεπίθεσης να γνωρίζουν τις ενέργειες στις οποίες πρέπει να προβούν προκειμένου να αποφύγουν ενδεχόμενη παραβίαση των ν. 2472/1997 και 3471/2006 κατά τη διάρκεια της διερεύνησης του περιστατικού.

Πηγή:
http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/NEWSMAIN/INFORMATIONAL/JAN2014.PDF

Κυρώσεις

- Διοικητικές κυρώσεις (άρθρο 21)
  - Προειδοποίηση/ Πρόστιμο/ Προσωρινή-Οριστική ανάκληση άδειας/ Καταστροφή αρχείου
- Αστική ευθύνη (άρθρο 23)
  - Υποχρέωση αποζημίωσης/χρηματικής ικανοποίησης σε περίπτωση περιουσιακής/ ηθικής βλάβης
- Ποινικές κυρώσεις (άρθρο 22)
  - Ευρεία «ποινικοποίηση» των παραβάσεων του νόμου
  - Άρθρο 22 παρ. 4: ποινική ευθύνη για παράβαση υποχρεώσεων ασφάλειας (τυχαία/σκόπιμη απώλεια, καταστροφή, μη εξουσιοδοτημένη πρόσβαση, αποκάλυψη κ.α)

Περισσότερες πληροφορίες:

- ΑΠΔΠΧ www.dpa.gr

- http://ec.europa.eu/justice/data-protection/law/index_en.htm

- Ευρωπαίος Επόπτης προστασίας δεδομένων
  EDPS- European Data Protection Supervisor

https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS

- Ομάδα Εργασίας άρθρου 29:

The **Article 29 Data Protection Working Party** was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the **protection of individuals** with regard to the processing of personal data and on the **free movement** of such data. It has advisory status and acts independently.

http://ec.europa.eu/justice/data-protection/article-29/index_en.htm