

The Greek Data Protection Act: The IT Professional's Perspective

Dimitris Gritzalis

June 2001

Δημερίδα για την “**Ασφάλεια στις Τεχνολογίες των Πληροφοριών**”

Λευκωσία, 15-16 Ιουνίου 2001



Ο Ελληνικός νόμος για την προστασία των προσωπικών δεδομένων

Η οπτική του ειδικού στην Ασφάλεια στην Πληροφορική και τις Επικοινωνίες

Δρ. Δημήτρης Γκρίτζαλης

Επ. Καθηγητής Ασφάλειας στην Πληροφορική και τις Επικοινωνίες
Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών

Μέλος της Αρχής Προστασίας Προσωπικών Δεδομένων της Ελλάδος



Μια διαπίστωση και ένας στόχος



Διαπίστωση

Η ενσωμάτωση της Πληροφορικής και των Τηλεπικοινωνιών στη σύγχρονη κοινωνικο-οικονομική πραγματικότητα δεν μπορεί και δεν πρέπει να θέτει σε κίνδυνο τις θεμελιώδεις **ατομικές ελευθερίες**.

Στόχος

Καθορισμός όρων και προϋποθέσεων θεμιτής επεξεργασίας **προσωπικών δεδομένων**, ώστε να προστατεύεται η προσωπική ζωή.



Ισχύον σχετικό θεσμικό πλαίσιο

◆ Νόμος 2472/1997:

Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα

Αρχή Προστασίας
Προσωπικών Δεδομένων



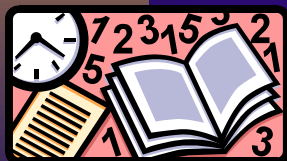
◆ Νόμος 2774/1999:

Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα



Προσωπικά και ευαίσθητα δεδομένα

- ◆ **Προσωπικά δεδομένα** είναι όσα αφορούν, άμεσα ή έμμεσα, φυσικά πρόσωπα.
- ◆ **Ευαίσθητα προσωπικά δεδομένα** είναι τα δεδομένα που αφορούν φυλετική ή εθνική προέλευση, πολιτικά φρονήματα, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, συμμετοχή σε ένωση, σωματείο και συνδικαλιστική οργάνωση, υγεία, κοινωνική πρόνοια, ερωτική ζωή, καθώς και ποινικές διώξεις ή καταδίκες.





Προϋποθέσεις θεμιτής επεξεργασίας : Ο Έλληνας και ο Κοινοτικός νομοθέτης

Τα προσωπικά δεδομένα για να τύχουν νόμιμης επεξεργασίας πρέπει:

Να συλλέγονται κατά τρόπο **θεμιτό και νόμιμο**, για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψη των σκοπών αυτών.

Να είναι **σαφή, πρόσφορα και όχι περισσότερα** από όσα κάθε φορά απαιτείται ενόψη των σκοπών της επεξεργασίας.

Να είναι **ακριβή** και να υποβάλλονται σε ενημέρωση.

Να διατηρούνται σε μορφή που επιτρέπει τον **προσδιορισμό της ταυτότητας** των υποκειμένων, **μόνο** κατά τη διάρκεια της περιόδου που απαιτείται για την **εκπλήρωση των σκοπών** της επεξεργασίας.





Προϋποθέσεις θεμιτής επεξεργασίας (συν.)

Για να υπάρχει νόμιμη επεξεργασία πρέπει:

Το υποκείμενο των δεδομένων να έχει δώσει τη **συγκατάθεσή** του (εξαίρεση (ε): “η επεξεργασία είναι απολύτως αναγκαία για την ικανοποίηση εννόμου συμφέροντος, ..., υπό τον όρο ότι τούτο υπερέχει προφανώς των συμφερόντων των θιγόμενων προσώπων και δεν θίγονται οι θεμελιώδεις ελευθερίες αυτών”).

Ο υπεύθυνος επεξεργασίας να έχει **γνωστοποιήσει** στην Αρχή τη σύσταση και λειτουργία του αρχείου ή την έναρξη της επεξεργασίας.

Η επεξεργασία ευαίσθητων δεδομένων επιτρέπεται **κατ’ εξαίρεση**, υπό προϋποθέσεις και ύστερα από **άδεια** της Αρχής.

Να τηρείται το **απόρρητο** και η **ασφάλεια** της επεξεργασίας.





Απόρρητο και ασφάλεια της επεξεργασίας

Για να διασφαλιστεί το απόρρητο και η ασφάλεια της επεξεργασίας πρέπει:

Η διεξαγωγή της επεξεργασίας να γίνεται από πρόσωπα με επαγγελματικά προσόντα που παρέχουν επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας.

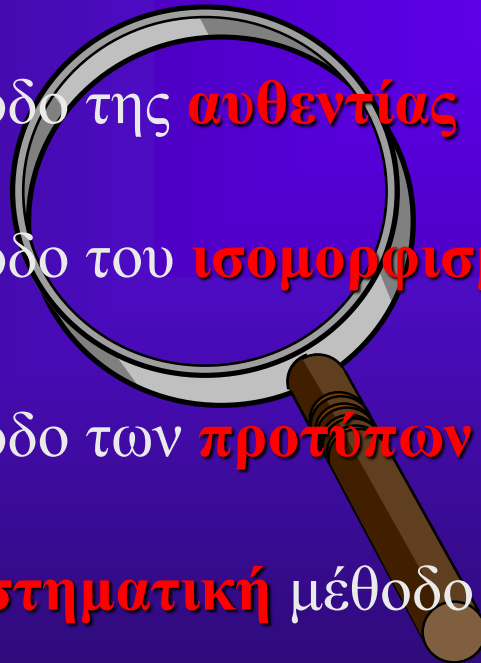
Να λαμβάνονται τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια και την προστασία των δεδομένων. Τα μέτρα αυτά πρέπει να εξασφαλίζουν επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων.

Όταν η επεξεργασία διεξάγεται από τρίτο, η ανάθεση πρέπει να γίνεται εγγράφως.

Πώς επιλέγονται τα μέτρα προστασίας;

Η επιλογή μπορεί να γίνει με τους εξής βασικούς τρόπους:

- ❑ Με τη μέθοδο της **αυθεντίας**
- ❑ Με τη μέθοδο του **ισομορφισμού**
- ❑ Με τη μέθοδο των **προτύπων**
- ❑ Με μια **συστηματική** μέθοδο



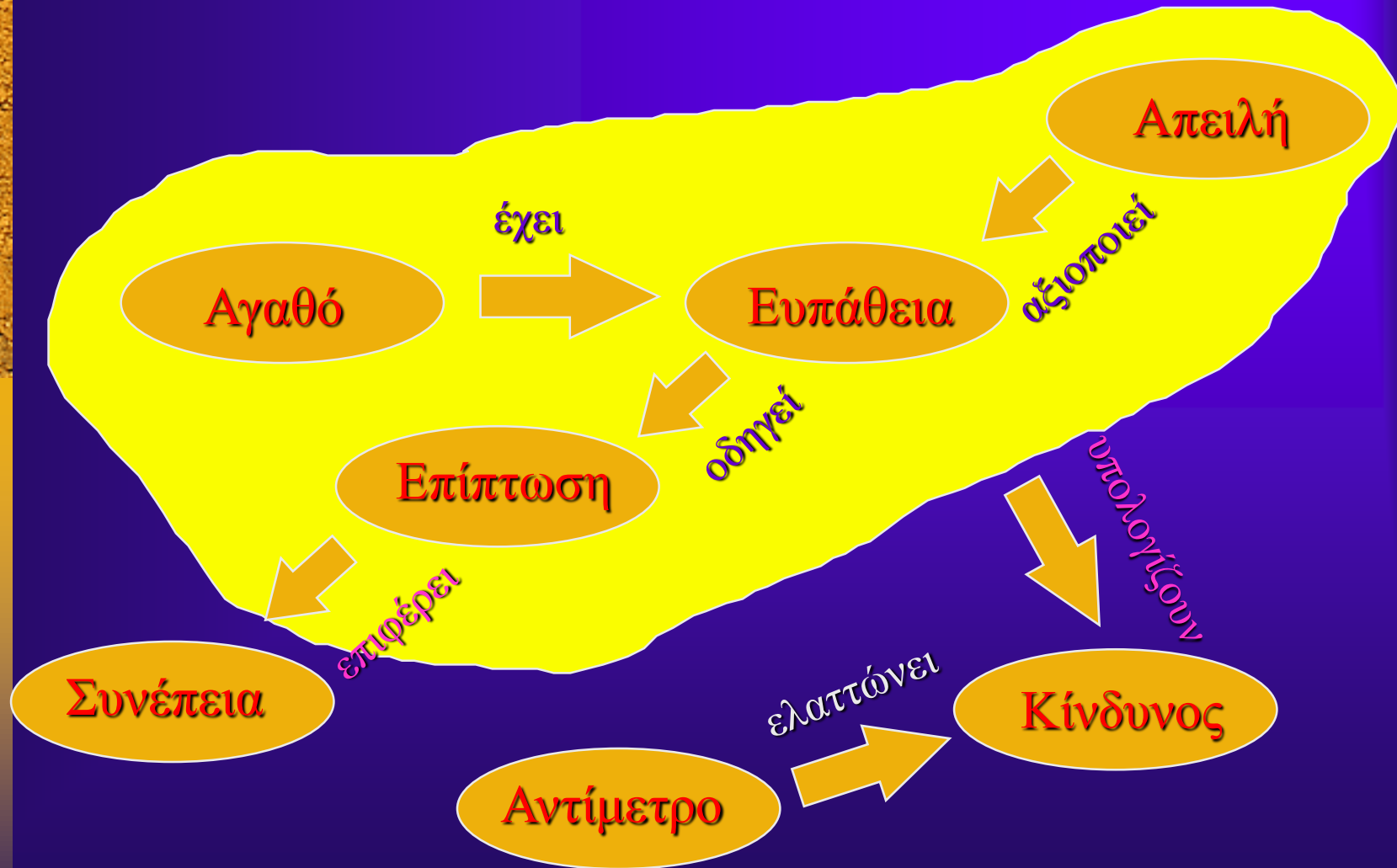


Συστηματική μέθοδος

Η χαρακτηριστική εκπρόσωπος αυτού του είδους είναι η μέθοδος που στηρίζεται στην εκπόνηση μελέτης επικινδυνότητας (risk analysis), η οποία:

- α) Αποτελεί **συστηματικό τρόπο** για την αποτίμηση της επικινδυνότητας μιας επεξεργασίας.
- β) **Ικανοποιεί πλήρως** τις προϋποθέσεις που θέτει το ισχύον θεσμικό πλαίσιο.

Η “λογική” της ανάλυσης επικινδυνότητας





Που καταλήγει η μελέτη επικινδυνότητας;

- ◆ Αποτέλεσμα της μελέτης αποτίμησης επικινδυνότητας είναι ο **εντοπισμός και η αναλυτική περιγραφή των οργανωτικών και τεχνικών μέτρων** που πρέπει να ληφθούν για να τηρηθεί το απόρρητο και η ασφάλεια μιας επεξεργασίας.
- ◆ Η λήψη των μέτρων αυτών **εξασφαλίζει επίπεδο προστασίας ανάλογο προς τους κινδύνους** που συνεπάγεται η επεξεργασία.



Συμπερασματικά

- ◆ Η προστασία της προσωπικής ζωής αποτελεί βασικό συστατικό του σύγχρονου **θεσμικού πλοστασίου** μιας δημοκρατικής κοινωνίας.
- ◆ Απαιτείται **διεπιστημονική συνεργασία** για την εφαρμογή του θεσμικού αυτού οπλοστασίου.
- ◆ Ο ρόλος των Πληροφορικών είναι κομβικός, ειδικά σε θέματα **ασφάλειας**.
- ◆ Οι παρεμβάσεις των Πληροφορικών πρέπει να αποβλέπουν σε **δόκιμες** και **αξιόπιστες τεχνικές λύσεις**.



References

1. Gritzalis D., "Enhancing security and supporting interoperability in healthcare information systems", *Medical Informatics*, Vol. 23, No. 4, pp. 309-324, 1998.
2. Gritzalis D., "A baseline security policy for distributed healthcare information systems", *Computers & Security*, Vol. 16, No. 8, pp. 709-719, 1997.
3. Gritzalis D., Kantzavelou I., Katsikas S., Patel A., "A classification of health information systems security flaws", *Proc. of the 11th International Information Security Conference*, pp. 453-464, Chapman & Hall, 1995.
4. Gritzalis D., Lambrinouidakis C., "A data protection scheme for a remote vital signs monitoring service", *Medical Informatics Journal*, Vol. 25, No. 2, pp. 207-224, 2000.
5. Gritzalis D., "Principles and requirements for a secure e-voting system", *Computers & Security*, Vol. 21, No. 6, pp. 539-556, 2002.
6. Iliadis J., Gritzalis D., Spinellis D., Preneel B., Katsikas S., "Evaluating certificate status information mechanisms", *Proc. of the 7th ACM Computer and Communications Security Conference*, pp. 1-9, ACM Press, 2000.
7. Katsikas S., Spyrou T., Gritzalis D., Darzentas J., "Model for network behaviour under viral attack", *Computer Communications*, Vol. 19, No. 2, pp. 124-132, 1996.
8. Pavlopoulos S., Gritzalis D., et al., "Vital signs monitoring from home with open systems", in *Proc. of the 16th International Congress for Medical Informatics*, pp. 1141-1145, IOS Press, 2000.
9. Spinellis D., Gritzalis D., " PANOPTIS: Intrusion detection using process accounting records", *Journal of Computer Security*, Vol. 10, No. 2, pp. 159-176, IOS Press, 2002.