Legal use of personal data to fight telecom fraud

Dimitris Gritzalis

May 2001

Ημερίδα Ελληνικού Φορέα Αντιμετώπισης Τηλεπικοινωνιακής Απάτης (ΕΦΤΑ)
"Τηλεπικοινωνιακή Απάτη: Μέθοδοι - Πρόληψη - Προεκτάσεις"
Αθήνα, 26 Μάη 2001

Δυνατότητες θεμιτής αξιοποίησης προσωπικών δεδομένων για την αντιμετώπιση της τηλεπικοινωνιακής απάτης

Δρ. Δημήτρης Α. Γκρίτζαλης

Επίκουρος Καθηγητής Ασφάλειας στην Πληροφορική και τις Επικοινωνίες
Οικονομικό Πανεπιστήμιο Αθηνών

Αναπλ. Μέλος Αρχής Προστασίας Προσωπικών Δεδομένων

Ισχύον σχετικό θεσμικό πλαίσιο

- **Νόμος 2472/97**:

  Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα

- **Νόμος 2774/99**:

  Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα

Μια διαπίστωση και ένας στόχος

Διαπίστωση

Η τηλεπικοινωνιακή απάτη θα μπορούσε να αντιμετωπισθεί αποτελεσματικότερα αν - για το σκοπό αυτό - ήταν

- τεχνολογικά δυνατή και
- θεμιτή

η επεξεργασία (επιλεγμένων) προσωπικών δεδομένων.

Στόχος

Με ποιές προϋποθέσεις είναι θεμιτή η επεξεργασία προσωπικών δεδομένων;

Προϋποθέσεις θεμιτής επεξεργασίας

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 εν όψει των σκοπών αυτών.
- Να είναι σαφή, πρόσφορα και όχι περισσότερα από όσα κάθε φορά απαιτείται εν όψει 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 θιγομένων 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.
- Αν η επεξεργασία διεξάγεται από τρίτο, η ανάθεση πρέπει να γίνεται εγγράφως.

Πώς επιλέγονται τα μέτρα προστασίας;

Η επιλογή μπορεί να γίνει με τρεις - τουλάχιστον - τρόπους:

Με τη μέθοδο της **αυθεντίας**

Με τη μέθοδο του **ισομορφισμού**

Με εκπόνηση **μελέτης επικινδυνότητας**

Πώς επιλέγονται τα μέτρα προστασίας;

Η Μελέτη Επικινδυνότητας (Risk Analysis review) αποτελεί το **μόνο συστηματικό τρόπο** για την αποτίμηση της επικινδυνότητας μιας επεξεργασίας, ενώ **ικανοποιεί** και τις απαιτήσεις που θέτει το ισχύον θεσμικό πλαίσιο.

Αποτέλεσμα της μελέτης είναι ο **εντοπισμός και η αναλυτική περιγραφή όλων 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.

Σ υ μ π ε ρ α σ μ α τ ι κ ά

Για την αντιμετώπιση της τηλεπικοινωνιακής απάτης μπορεί να αξιοποιηθούν και προσωπικά δεδομένα, υπό την προϋπόθεση ότι:

Θα τηρηθούν οι όροι και οι προϋποθέσεις που θέτει η κείμενη νομοθεσία και θα δοθεί **εξαιρετική προσοχή** στην **προστασία** των προσωπικών δεδομένων που τυγχάνουν επεξεργασίας (δηλαδή πρέπει να υπάρξει συστηματική επιλογή και επιμελής υλοποίηση των τεχνικών και οργανωτικών μέτρων ασφαλείας)

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., Lambrinoudakis 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 Communica-tions 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.