FBE Congress
Sessione Stage
The legal Profession and Data Protection
Wroclaw 22 September 2011

Security Measures and Data Protection
by
Francesco Tedeschi
The legal Profession and Data Protection

HARVARD

LAW REVIEW.

VOL. IV. DECEMBER 15, 1890. NO. 5.

THE RIGHT TO PRIVACY.

THAT the individual shall have full protection in person and
in property is a principle as old as the common law; but
it has been found necessary from time to time to define anew the
exact nature and extent of such protection. Political, social, and
economic changes entail the recognition of new rights, and the
common law, in its eternal youth, grows to meet the demands
of society. Thus, in very early times, the law gave a remedy only
for physical interference with life and property, for trespasses vi
et armis. Then the “right to life” served only to protect the
subject from battery in its various forms; liberty meant freedom
from actual restraint; and the right to property secured to the in-
dividual his lands and his cattle. Later, there came a recognition of
man’s spiritual nature, of his feelings and his intellect. Gradually
the scope of these legal rights broadened; and now the right to
life has come to mean the right to enjoy life,—the right to be let
alone; the right to liberty secures the exercise of extensive civil
privileges; and the term “property” has grown to comprise every
form of possession—intangible, as well as tangible.

Thus, with the recognition of the legal value of sensations, the
protection against actual bodily injury was extended to prohibit mere attempts to do such injury; that is, the putting another in
The legal Profession and Data Protection
The legal Profession and Data Protection

Sign Charter of fundamental rights of the European Union
The legal Profession and Data Protection

*Personal data*

any information relating to natural or legal persons, bodies or associations that are or can be identified, even indirectly, by reference to any other information including a personal identification number
The legal Profession and Data Protection

*Processing*

any operation, or set of operations, carried out with or without the help of electronic or automated means, concerning the collection, recording, organisation, keeping, interrogation, elaboration, modification, selection, retrieval, comparison, utilization, interconnection, blocking, communication, dissemination, erasure and destruction of data, whether the latter are contained or not in a data bank.
The legal Profession and Data Protection

Processing
The legal Profession and Data Protection

*Lawyer and data protection*

It’s necessary to change the operating *Weltanschauung* and direct management models of the work compatible with those generally accepted as virtuous.
The legal Profession and Data Protection

Security Policies and Security Plan

International Standards
The legal Profession and Data Protection

Security Policies and Security Plan

International Standards

BS 7799 Evolution

|----------|-----------------|-----------------|-----------------|---------|

UNE 71502
The legal Profession and Data Protection

Security Policies and Security Plan

ISMS Model

Definition of the high-level security policy

Validity of ISMS specification

Risk evaluation

Risk management

Choice controls to treat the risk

Operate controls to treat the risk

New processing or his modalities

New threats

New standards implementative
The legal Profession and Data Protection

Security Policies and Security Plan

PDCA Model

Plan (establish the ISMS)
Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization’s overall policies and objectives.

Do (implement and operate the ISMS)
Implement and operate the ISMS policy, controls, processes and procedures.

Check (monitor and review the ISMS)
Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.

Act (maintain and improve the ISMS)
Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.
The legal Profession and Data Protection

Security Policies and Security Plan

PDCA Model

Figure 1 — PDCA model applied to ISMS processes
The legal Profession and Data Protection

Security Measures: Steps Computer use

Computerised authentication

- Identifying code
- ID Verification code
The legal Profession and Data Protection

Security Measures: Steps Computer use

Computerised authentication

- Identifying code
- ID Verification code

→ User Id
→ Password
→ Device
→ Physical Feature
The legal Profession and Data Protection

Security Measures: Steps Computer use

Computerised authentication

Password

String of alphanumeric characters with sufficient minimum length (*reccomended 8*)

- Easy to remember
- Not based on anything somebody else could easily guess
- Not vulnerable to dictionary attacks
- Free of consecutive identical characters
- Easily indentified by the user
- Easily typed
The legal Profession and Data Protection

Security Measures: Steps Computer use

Computerised authentication
Device
Badge; magnetic card or radio apparatus
Risk:
Lost or duplication
The legal Profession and Data Protection

Security Measures: Steps Computer use

Computerised authentication

Physical Feature

Voice; sign; fingerprint; retina and other
The legal Profession and Data Protection
Security Measures: Steps Computer use

Computerised authentication

Identifying code  ID Verification code

authentication credentials

Removal

Not used  Job termination
The legal Profession and Data Protection
Security Measures: Steps Computer use

Authorisation profile

Who can do What
The legal Profession and Data Protection
Security Measures: Steps Computer use

Computer protection
Risk
Malware
The legal Profession and Data Protection

Security Measures: Computer protection

Types of Malware

Damage PC System

Damage Personal Data
The legal Profession and Data Protection

Security Measures: Computer protection

Malware direct to damage pc system

Virus  Worm  Trojan  DoS  Rootkit
The legal Profession and Data Protection

Security Measures: Computer protection

Malware direct to damage personal data

Spyware

Adware

Dialer
Malware and fake e-mail
The legal Profession and Data Protection

Security Measures: Computer protection

Malware and file sharing
The legal Profession and Data Protection

Security Measures: Computer protection

Software

Antivirus

Firewall
The legal Profession and Data Protection

Security Measures: Computer protection

New threat

Phishing
The legal Profession and Data Protection

Security Measures: Computer protection

Weak ring in the chain of computer security
The legal Profession and Data Protection

Security Measures: Computer protection

Computer Adage:

Real secure computer

Is PC off

Internet
The legal Profession and Data Protection

Security Measures: Computer protection

But the PC off is not real secure

Tempest attack
The legal Profession and Data Protection
Security Measures: Steps Computer use Protection personal data and work

Backup
The legal Profession and Data Protection

Security Measures

Processing Data without computer

a) regular update of the specifications concerning scope of the processing operations that may be performed by the individual entities in charge of the processing and/or by the individual organisational departments

b) implementing procedures such as to ensure safekeeping of records and documents committed to the entities in charge of the processing for the latter to discharge the relevant tasks

c) implementing procedures to keep certain records in restricted-access filing systems and regulating access mechanisms with a view to enabling identification of the entities in charge of the processing.
The legal Profession and Data Protection
Security Measures and risks quantization

- Evaluation impact and frequency of each type of risk
- Assignment a value to any risk
- Evaluation measures for the prevention of security risks

Find:
- measures which slow unwanted access (Penetration Time)
- measures that signal unwanted access (Detection Time)
- measures to facilitate early intervention (Intervention Time)

\[ PT >> DT + IT \]
The legal Profession and Data Protection

Data Protection and Data Transmission

Traditional mode for sending documents
The legal Profession and Data Protection

Data Protection and Data Transmission

Digital mode for sending documents
The legal Profession and Data Protection

Data Protection and Data Transmission

Secure mode for sending digital documents
The legal Profession and Data Protection
Security Measures and Data Protection

Conclusion

Communication from the European Commission of 31 May 2006:

➢ promote training programmes in the private sector to provide employees with the knowledge and skills necessary to implement security practices;

➢ promote diversity, openness, interoperability, usability and competition as key drivers for security, and to stimulate the deployment of security-enhancing products and services to combat ID theft and other privacy-intrusive attacks;
The legal Profession and Data Protection
Security Measures and Data Protection

Conclusion

Justice does not exist where there is no freedom

Luigi Einaudi
Wroclaw Regional Chambers of Legal Advisor

THANK YOU