



## **CASE STUDY:**

**Processing employees'  
biometric data (fingerprints)  
by a private company**



# National Supervisory Authority for Personal Data Processing

- Our DPA received a complaint from an employee that Company X processes employee personal data, including biometric data (fingerprints)
- The complainant stated that this type of data were collected in order to monitor employee access into the premises



# National Supervisory Authority for Personal Data Processing

- Investigation:
  - Company X has decided to monitor employee and visitor access into its premises
  - Means used: video surveillance system (156 video cameras), magnetic access cards, security guard and biometric (fingerprint) readers
  - Video images were stored for 30 days and deleted afterwards
  - The Log for card access kept for 60 days
  - The list of employees/magnetic cards was updated monthly



# National Supervisory Authority for Personal Data Processing

- Company X didn't notify this processing of personal data to the DPA
- The company claimed that it obtained the data subjects' consent
- DPA noticed that the employees could only agree to the processing of their personal information



# National Supervisory Authority for Personal Data Processing

- **Requirements imposed by Law no. 677/2001:**
  - Article 4 – personal data must be:
    - a) processed fairly and in accordance with the existing legal provisions
    - b) collected for specific, explicit and legitimate purposes
    - c) adequate, pertinent and non excessive in relation to the purpose
    - d) accurate and, if necessary, updated;
    - e) stored in such a manner that allows the identification of the data subject only for the time limit required to fulfill the purposes for which they are collected and later processed



# National Supervisory Authority for Personal Data Processing

## Requirements imposed by Law no. 677/2001:

- Article 5 – data subject's consent – general rule for processing personal data
- Article 7 para. 2 c) – data subject's consent required in order to process "special categories of data"
- Article 12 – data subject's right of information



# National Supervisory Authority for Personal Data Processing

## Decision no. 89/2006

- Article 1 para. 1 b) – processing biometric data may present special risks for the individual's rights and liberties
- Article 1 para. 2 – a preliminary control must be carried out by the DPA before the processing begins
- Article 2 data controllers must notify with 30 days in advance



# National Supervisory Authority for Personal Data Processing

## Order no. 52/2002 minimum security measures

Refers to the following issues:

- user authentication
- type of access
- collection of data
- safety copies
- computers and access terminals
- access log
- communication systems
- staff training
- computer usage
- printing personal data



# National Supervisory Authority for Personal Data Processing

- Actions taken by our DPA:
  - a decision was issued to temporarily suspend the processing of biometric data and
  - Company X was required to bring further justification in favor of continuing to process biometric data for the mentioned purpose (within 10 days)
  - a final Decision was issued ordering Company X to stop processing the biometric data of its employees and delete all such data it had stored



# National Supervisory Authority for Personal Data Processing

**Thank you for your attention!**

*international@dataprotection.ro / george.grigore@dataprotection.ro*

*Olari no. 32, 2<sup>nd</sup> district  
Bucharest, 024057  
Phone 252.55.99 Fax: 252.57.57  
www.dataprotection.ro*