Responding to Data Breaches

Robert Mourik
Director Regulatory Affairs Europe
23th October 2009

TELEFÓNICA, S.A.
Dirección Regulación Corporativa

Telefónica Markets

More than 260 million customers in 24 markets

Key Messages

1. Data protection is key to the success of ICT companies such as Telefónica.

1. Data protection issues are not black & white and require careful case by case assessment

2. Level playing field with all industry players required

ICT services produce vast quantities of personal data

65 billion **phone calls** per year

2 million **emails** per second

1 million **IM messages** per second

8 terabytes per second **traffic**

255 exabytes **magnetic storage**

1 million **voice queries** per hour

2 billion **location nodes** activated

600 billion **RFID tags** in use

Source: Kevin Kelly, December 2007

Telefónica's business depends on Customer Confidence

- Data Protection is key for Telefónica's brand reputation
  - Value of Telefónica brands: ~ $19 billion*
- Excellent Data Protection practices are standard practice
  - Business principles and training
  - Dedicated DP teams in each operating business
  - Company wide minimum standards
  - Internal and external audits
  - Security teams and research
- New business models rely more and more on the use of personal data (i.e. behavioural advertising)

* Source: Brand Finance, 2007

Data Breaches – our views and experience (1)

Cost of Data Breaches Difficult to Quantify

- Many tangible and intangible elements
- Main cost: reputational
- Engineering resources: opportunity costs
- Consequential procedural changes
- Outbound calls by Call centre (service level hit)
- Dealing with certain customers

Duration of Notification

- Each case is different
- Notify when extend, cause and solution are known
- “without undue delay” workable – tightening may be counterproductive
- Trust and open communication with the national authorities is important
- Critical: DP office that is trustworthy, level headed, in tune with industry & consumers

Data Breaches – our views and experience (2)

Reporting to consumers

- Telefónica has experience with reporting breaches to its customers. Need for careful analysis and it may not always be appropriate to notify*
- Notification requirement needs to be flexible enough to ensure that the downsides of notification can be avoided and that any regime is constructive and not counterproductive to the aim (enhance consumer trust).
- There are many scenarios in which poorly thought out (or poorly timed/ pre-emptive) notification can be counter productive
- Telefónica weary of blanket reporting requirement – each case is different and requires different approach.
- Close communication with Data Protection authorities.

* For example: alerting those that might exploit weaknesses, generating confusion and eliciting further abuse – many phishing emails in the banking sector use notice of 'technical issues' in an attempt to dupe customers.

Data Breaches – our views and experience (3)

- **Common reporting format?**
  - Could be very inflexible. Again, each incident is unique.
  - Keep it simple, don't create unnecessary red tape
  - Reporting to customers: operators know customers better, have communications experience. DPA can check script.

- **Increased auditing?**
  - Extensive existing audit requirements (internal, external, SOX)
  - Audits are very disruptive and costly
  - Existing relationship with DPA sufficient guarantee
  - Avoid red tape

Data Breaches – Call for Level Playing Field

- Current scope of application limited to electronic communication service providers: causes potential distortion of competition.
- Consumer trust and confidence is a crucial element in encouraging online trade: not just an issue for telco's!
- Other ICT players use more personal data.
- All companies subject to General Data protection Directive should have same requirements.