

# Data Protection Legislation and Direct Marketing

## The compliance challenge

1

Presenter: Hugh Jones

Sytorus Ltd.

# Key concept - What is privacy?

*"The right to be left alone ... the most comprehensive of rights, and the right most valued by civilized men."*

*Justice Louis Brandeis, U.S. Supreme Court, (Olmstead vs U.S., 1928)*

*"The right of the individual to be protected against intrusion into his personal life or affairs ... by direct physical means or by publication of information"*

*Calcutt Report on Privacy 1990*



# Why Data Protection?

‘Individuals must be able to enjoy the benefits of new technology, while at the same time remaining in control of their privacy.’

*Billy Hawkes*

*Data Protection Commissioner*

*02 July, 2011*



# The Data Protection Acts

Irish Data Protection Act 1988:

... to regulate in accordance with its provisions the collection, processing, keeping, use and disclosure of certain information relating to individuals that is processed automatically. [13th July, 1988]

Irish / UK Data Protection (Amendment) Act 1998 / 2003:

...the protection of individuals with regard to the processing of personal data and on the free movement of such data

EC (Privacy and Electronic Communications) Regulations, 2011

...applying to the processing of personal data in connection with the provision of publicly available electronic communications services, including networks supporting data collection and identification devices.



# The Golden Rule of Consent

- “Only market willing customers”
- “A clear indication of consent”
- Strong customer resistance to “junk mail” or “spam”
- Failure to respect consumer choice is against the law
- Criminal offence where electronic means are used
- If selling on-line, need privacy statement
- Cookie Regulations



# The Characters in the Acts

- Data Subject - An individual who is the subject of personal data
- Data Controller - A person who, either alone or with others, controls the contents and use of personal data
- Data Processor - A person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his employment

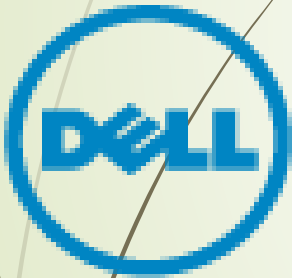


# Liability

- 29 (1) “where an offence under this Act has been committed by a body corporate and is proved to have been committed with the consent or connivance of or to be attributable to any neglect on the part of a person, being a director, manager, secretary or other officer of that body corporate, or a person who was purporting to act in any such capacity, that person, as well as the body corporate, shall be guilty of that offence and be liable to be proceeded against and punished accordingly”



# Brand Impact....



brasserie  
sixty6



TESCO CLUBCARD



# Irish Data Protection Legislation

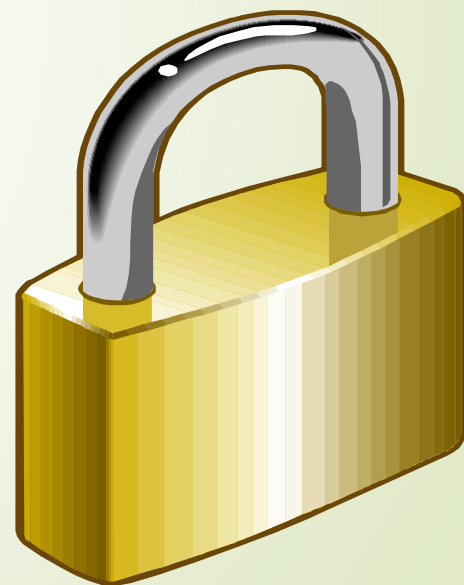
- Data Protection Act 1988
- Data Protection (Amendment) Act 2003
- EU Electronic Communications Regulations 2011



# The Data Controllers' Obligations

# The Data Protection Rules

- Fairly obtained
- Specified & lawful purpose
- Not Incompatible with purpose or purposes
- Safe and secure
- Accurate & up to date
- Adequate, relevant & not excessive
- Not kept for longer than is necessary
- Rights of access



# Fair Processing

- Effort go gain consent
  - Clear
  - Informed
  - Freely given, not conditional
  - Unambiguous
- Basis for gathering personal data
- Cookie Directive
  - Mechanism used
  - Appropriate notification
  - Assistance with disabling
  - Impact on user experience

# Specified Purpose(s)

13

Data should be used only for a specified and lawful purpose....

Case (2011):

- Telecoms service provider offers their subscriber database as a distribution list for third parties

DPC's Finding:

- Breach of the T+C's, "no scope to send direct marketing, unless there is prior consent"
- Law is extremely protective of subscribers against unsolicited electronic communications
- Not sufficient to have this in T+C's – must offer an 'opt in' tick box or similar – an active indication of consent



# Incompatible Processing

14

Processing of data should not be incompatible with the specific process or processes

Case (2008):

Mobile phone customers receiving unsolicited messages to their new mobile phones. Involved adult content.

DPC Finding:

- Marketing was unsolicited; processes not robust enough to determine whether recipient had given consent
- Company agreed to a €27,000 'donation' to dialysis unit of Crumlin C.H. and a refund of premium rate charges



# Safe and Secure

- Data Controller must prevent unlawful or unauthorised access
- Data Controller must inform the Commissioner of all breaches of personal data in relation to electronic communications
- No obligation to notify Commissioner as long as data/hardware is encrypted
- Data Controller must maintain a log of all data leaks/loss





# Safe and Secure

## Case (2009)

Company sends 1400 e-mails as part of a marketing campaign – no consent was sought, and recipients' addresses are legible in the .cc field

## DPC Finding

- New employee using an old database, lacking 'opt in' preferences
- No 'opt out' option was included in the e-mails
- Company agreed to engage a third-party service provider to manage future e-mail campaigns
- 1400 free passes to a social event; charitable donation of €500

# Accurate and Up-to-date

The data must be kept accurate, and where necessary, kept up-to-date

## Case (2009):

Mobile phone company fails to suppress customers' 'opt out' preference following an initial marketing campaign

DPC Finding:

- Suppression functionality in the firm's system was faulty
- Four-week lag from 'opt out' to actioning the preference
- E-learning and training for all staff re their obligations
- Apologies and €150 ex gratia payments to two recipients

# Adequate, Relevant and Not excessive

Processing of personal data should be adequate, relevant and not excessive in relation to the specified purpose(s)

Case (2011):

Company deploys 'persistent' cookies on user's computer without any reference or notification

DPC Finding:

- Users should be notified of any use of 'tracking' or 'persistent' cookies
- 'Session' cookies are permitted, where they are essential to the provision of the required service - e.g. Online 'shopping basket'

# Retention / Destruction

19

Personal data should only be held for as long as necessary

- Where a customer has failed to 'opt in' to marketing campaign, or
- Has not been contacted within a 12-month period to renew / re-affirm their consent
- Records should be removed from distribution database or blocked from future marketing campaigns



# “Rule 5 Campaign”

- A ‘work-around’ to re-vitalise legacy data
- Focus on data which falls outside the 12-month window
- Focus on data accuracy and completeness
- No sales activity!



# Where can we safely send data?

- Members of the EEA (28 EU + 3 EFTA)
- Safe Countries (10)
  - Switzerland, Jersey, Guernsey, Isle of Man, Argentina, Canada, Faroe Islands, Israel, Uruguay, New Zealand
- Safe Harbor
  - between EU countries and US companies
- Countries which meet 'Adequacy' requirements

# Compliance 'Toolkit'

- Thick Skin
- Objectivity
- Focus – a clear definition of role
- Awareness
- Training
- Outward Calm
- Courage
- Clarity of Purpose
- Patience
- Endurance



# Why should we comply with the Data Protection Acts?

- A legal obligation
- Makes good business sense (clean, accurate data)
- Encourages good decision-making
- Protects...
  - Professional reputation
  - Client trust
  - Perception of commercial brand
  - Credibility as a service provider

# Introducing Sytorus

- Sytorus is a Data Protection consultancy, based in Dublin
- We offer
  - Training
  - Advisory Services
  - Data Protection Assessments
  - Privacy Impact Assessments
  - Evaluation of IT capability
- Visit our website, [www.PrivacyEngine.io](http://www.PrivacyEngine.io),
- Avail of our **free, 30-day trial!**