

IRISH DATA PROTECTION LEGISLATION 1988, 2003 AND 2011

THE COMPLIANCE CHALLENGE FOR THE DATA PROTECTION OFFICER

Presenter: Hugh Jones
Irish Computer Society

AIMS, OBJECTIVES

- ◉ AIM - To understand the relevance of the Irish Data Protection legislation in Ireland for Direct Marketing
- ◉ OBJECTIVES - To facilitate that learners:
- ◉ Cover the core concepts of Irish Data Protection legislation
- ◉ Review the provisions of the July 2011 legislation
- ◉ Understand how the new legislation is being interpreted
- ◉ Look at recent case studies to illustrate these points

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

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]

Data Protection (Amendment) Act 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 Irish customer resistance to “junk mail” or “spam”
- ◉ Failure to respect consumer choice is against the law
- ◉ Criminal offence where electronic means 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

DATA PROTECTION OFFICER

- ◉ Not yet a mandatory role
- ◉ Proposed for organisations > 250 staff
- ◉ Unclear definition of responsibilities
- ◉ Not necessarily a permanent staff member
- ◉ Important point of reference within company
- ◉ Responsive to DP queries
- ◉ Obligations to Register, Notify
- ◉ Obligation to respond to Notices
- ◉ Obligation not to impede Appointed Officers

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”

In the headlines....

**Insurance Company Staff caught
spying on Celebrities' Records**

Protecting privacy - A victory for us all

PlayStation Users on high alert after hacking

40% of tech firms view
potential staff on Web

**Telecoms companies plead
guilty to data protection offences**

**PlayStation fans hit by Credit
Card hacker**

**Celebs in Insurance
Spy Probe**

Sony Hackers Hit Up
To 250,000 Irish
Users in Data Theft

**Top telecoms firms fined for
cold calling customers**

Customer "harassed" by 225 calls from UPC

Insurers to discuss Code after
Report identifies breaches of data
law

Telecom companies plead
guilty in unsolicited calls case

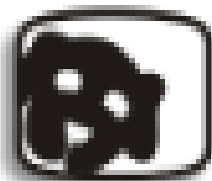
Telecom firms prosecuted for sales methods

Details of online Sony video game players stolen

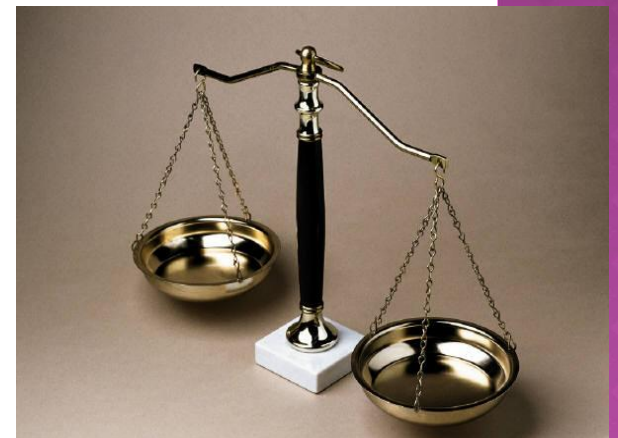
Brand Impact....



brasserie
sixty6



THE DATA CONTROLLERS' OBLIGATIONS



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



FAIRLY OBTAINED

- Obtaining

- Fair Processing Notice

- Processing

- Lawful Processing Conditions 2(a)

- Sensitive Processing

- Lawful Processing Conditions 2(b)

FAIRLY NOTIFIED

Data Controller shall make readily available:

- ◉ The identity of the Data Controller
- ◉ The Identity of Nominated Representative (if applicable)
- ◉ The purpose or purposes of processing
- ◉ With whom the data will be shared,
- ◉ Any secondary purposes and
- ◉ Any other information in order to make the processing fair

FAIRLY PROCESSED (I) - NOTIFICATION

- ◉ Subject should be clearly informed in advance of marketing
- ◉ Marketing messages should include identification of the sender
- ◉ Must include contact details at which the sender can be reached
- ◉ Marketing material must include the option to 'opt out'
- ◉ No calls to a mobile without the subscriber's prior, clear consent
- ◉ No mailing without first checking the National Directory data-base

FAIRLY PROCESSED (II) WE ASSUMED YOU'D BE INTERESTED...

- ◉ Where contact details have been obtained through sale of product or service, this information can only be used further where:
 - The product being marketed is similar to the product or service sold to the customer at the time the contact details were obtained; and
 - At the time of collection, the customer had the option to 'opt out'; and
 - Each subsequent marketing campaign offers the customer the option to 'opt out';

FAIRLY PROCESSED (III) USE IT OR LOSE IT....

- The contact details must have been gathered in the previous 12 months;
- If more than 12 months old, the customer must have received a marketing approach in the previous 12 months to which they did not object or after which they did not choose to 'opt out';
- Where no previous sale or service has been conducted, the Customer must first 'opt in' before being contacted

SPECIFIED PURPOSE(S)

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

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
- ◉ Network subscribers must be notified of any risk of a breach of their Data Protection rights
- ◉ Data Controller must inform the DP 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

Personal data should only be held for as long as necessary

- ◉ Call traffic details should only be held for as long as necessary to:
 - Process invoices
 - Complete interconnect services
 - Resolve billing queries or disputes
- ◉ 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 data-base or blocked from future marketing campaigns

WHERE CAN WE SAFELY SEND DATA?

- Members of the EEA (27 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

DPO 'TOOLKIT'

- ◉ Thick Skin
- ◉ Objectivity
- ◉ Focus - a clear definition of role
- ◉ Competence
- ◉ Qualification
- ◉ Outward Calm
- ◉ Courage
- ◉ Clarify of Purpose
- ◉ Patience
- ◉ Endurance

WHY SHOULD YOU COMPLY WITH THE DATA PROTECTION ACT?

- ◉ A Legal Requirement
- ◉ Makes good business sense
- ◉ Encourages good information handling
- ◉ Protects reputation, trust and brand

QUESTIONS

