



Data Protection – the Governance Challenge

Billy Hawkes

Data Protection Commissioner

**Governance Forum, IPA
4 February , 2010**

**An Coimisinéir
Cosanta Sonraí**



**Data Protection
Commissioner**

Presentation Outline

- The Governance Challenge
- Data Protection – Legal Context
- Data Protection Commissioner
- Questions you should ask



Lots of Personal Data....

- Large, centralised Databases
- Legal Obligation to provide Personal Data to State
 - *Register of births, marriages, deaths*
 - *PPS: increased data sharing*
 - *Welfare, Revenue, Grant Schemes*
 - *Permits/Licenses , Planning*
- Data Mining/Sharing

Security breach Group set up to inquire into variant
raises concern Social and Family Affairs leaks data
about safety of to abuse Probe launched **to criminal**
leak to criminal **brother**

Data chiefs
launch probe { **Public's information will be**
safe, says data commissioner

Official gave private details
to media in new leak shock
Conroy: officers face action if data accessed without good reason

Department employee resigns after accessing records of 40 people **dog's**

leaked data Govt info **vow to stop**
your details

Six officials probed over leaks **g leaked**



Eurobarometer 2008

Individual (DS) Concern about Data Protection	EU Average %	Ireland %
Concerned	63.8	70.5
Not Concerned	34.8	28.2
Don't know / no answer	1.4	1.3



Strongly Disagree %
Slightly Disagree %
Neither %
Slightly Agree %
Strongly Agree %

Net Agree %
Don't Know %

Public sector organisation keep personal information held about you in a safe and secure manner



56 17

Private sector organisation keep personal information held about you in a safe and secure manner



52 16

Public sector organisation have controls in place to ensure that their employees cannot access your personal information inappropriately



51 18

Private sector organisation have controls in place to ensure that their employees cannot access your personal information inappropriately



49 18

Public Awareness Survey April 2008

An Coimisinéir
Cosanta Sonraí



Data Protection
Commissioner

Data Protection: a Governance Issue

- It matters to customers, clients, employees
- EU & National Data Protection Law
- Other Laws and Obligations
 - *Financial Regulator*
 - *Consumer Law*
 - *Official Secrets Act/Freedom of Information Act*
 - *Legal & Ethical confidentiality obligations*
- ***Are you satisfied that your Organisation is compliant with its obligations?***

An Coimisinéir
Cosanta Sonraí



Data Protection
Commissioner

Presentation Outline

- The Governance Challenge
- **Data Protection – Legal Context**
- Data Protection Commissioner
- Questions you should ask

An Coimisinéir
Cosanta Sonraí



Data Protection
Commissioner

Data Protection: a Human Right

- Part of Right to Personal Privacy
- Personal Privacy : necessary in a Democratic Society
- Not absolute: other necessary Rights on a Democratic Society (e.g. Freedom of Expression, Rights of Others)
- Limited Common Law recognition



Constitution of Ireland

- *Implicit* Right to Personal Privacy under Article 40.3.1 ... *The State guarantees in its laws to respect, and, as far as practicable, by its laws to defend and vindicate the personal rights of the citizens*
- Court Interpretation: *the right to privacy is one of the fundamental personal rights of the citizen which flow from the Christian and democratic nature of the State*

An Coimisinéir
Cosanta Sonraí



Data Protection
Commissioner



European Convention on Human Rights (ECHR)

- *Explicit* Right to Personal Privacy under Article 8 of 1950 *European Convention for the Protection of Human Rights & Fundamental Freedoms* (ECHR)
- Convention ratified by all 25 EU Member States and most other European countries (46 Council of Europe Members)
- ECHR now indirectly part of Irish law due to ECHR Act 2003

An Coimisinéir
Cosanta Sonraí



Data Protection
Commissioner

ECHR Article 8: Right to respect for Private and Family Life



- *(1) Everyone has the right to respect for his private and family life, his home and his correspondence.*
- *(2) There shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*
- [tension with Article 10: Freedom of Expression]



Lisbon Treaty

Article 16 Treaty on the Functioning of the Union

- *1. Everyone has the right to the protection of personal data concerning them.*
- *2. The **European Parliament and the Council**, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data.*
- *Compliance with these rules shall be subject to the control of independent authorities.*



EU Charter of Fundamental Rights: Article 8

- **Protection of personal data**
- *1. Everyone has the right to the protection of personal data concerning him or her.*
- *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
- *3. Compliance with these rules shall be subject to control by an independent authority.*



An Coimisinéir
Cosanta Sonraí



Data Protection
Commissioner



EU & Irish Legislation

- Data Protection Directive 95/46/EC
- Electronic Privacy Directive 2002/58/EC
- EUROPOL etc
- Police & Justice Decision 2008/977/JHA
- Data Protection Acts 1988 & 2003
- EC Electronic Privacy Regulations 2003 (SI 535/2003) **and 2008 (SI 526/2008)**
- Corresponding Acts
- (to be transposed)



The Data Protection Rules

1. Fair obtaining & processing
 - *Consent*
2. Specified purpose
3. No disclosure
 - *unless "compatible"*
4. Safe and secure
5. Accurate, up-to-date
6. Relevant, not excessive
7. Retention period
8. Right of access

**An Coimisinéir
Cosanta Sonraí**



**Data Protection
Commissioner**

Keep
accurate

Have a
retention
policy

**Inform and
get consent**

Justification
to process

Beginning
Getting the
Data

Middle
While you have
the data

End
Disposing of
data

**Specify
purpose**

**Only gather
what is
required**

Respond
to access
requests

Disclose
only if
compatible
or allowable
exception

Keep secure
and dispose
securely

**An Coimisinéir
Cosanta Sonraí**



**Data Protection
Commissioner**

**Keep
accurate**

Have a
retention
policy

Inform and
get consent

**Justification
to process**

Beginning
Getting the
Data

Middle
While you have
the data

End
Disposing of
data

Specify
purpose

Only gather
what is
required

**Respond
to access
requests**

**Disclose only
if compatible
or allowable
exception**

Keep secure
and dispose
securely

**An Coimisinéir
Cosanta Sonraí**



**Data Protection
Commissioner**

Keep
accurate

Inform and
get consent

Justification
to process

**Have a
retention
policy**

Beginning

Getting the
Data

Middle

While you have
the data

End

Disposing of
data

Specify
purpose

Only gather
what is
required

Respond
to access
requests

Disclose
only if
compatible
or allowable
exception

**Keep secure
and dispose
securely**



DP and FOI

- *A right conferred by the Data Protection Act shall not prejudice the exercise of a right conferred by the Freedom of Information Act 1997.*
- *The Commissioner and the Information Commissioner shall, in the performance of their functions, co-operate with and provide assistance to each other (DP Act 2003)*

An Coimisinéir
Cosanta Sonraí



Data Protection
Commissioner

Presentation Outline

- The Governance Challenge
- Data Protection – Legal Context
- **Data Protection Commissioner**
- Questions you should ask



Role of Data Protection Commissioner

(standard throughout EU)

- **Enforcer Role:** compliance by data controllers & processors
- **Ombudsman Role:** resolution of disputes between data subjects and data controllers or processors
- **Educational Role:** Promotes DP rights and good practice
- **Registration Authority:** obligation on major holders of personal data to be placed on public register



How does (Irish) DPC fulfill role?

- Investigations/Audits
 - *Arising from complaints*
 - *On own initiative*
- Maintains public register
- Codes of Practice
- Guidance booklets, website, presentations, advice, Annual Report



Complaints 2008

TYPE	%
Direct Marketing*	35
Access Rights	30
Disclosure	16
Accuracy	2
Other	17

- 1031 formal complaints
- 2009 900+
- Many more enquiries dealt with informally

* Mainly electronic (SMS etc)



Some Audit Targets

- Dept. Social & Family Affairs
- Local Authority
- Secondary School
- Revenue
- Semi State Body
- Motor Tax Office
- Borough Council
(Community CCTV)



Registration

- Register available to public - transparency
- Information on Register
 - *Purpose*
 - *Type of data*
 - *Transfers abroad*
 - *Disclosures*
- Required to register only if data processed automatically
- Offence to hold personal data if not registered



Who must Register?

- **Public sector bodies**
- Financial institutions
- Insurance companies
- Direct marketing
- Debt collection
- Credit referencing
- Internet access
- Telecommunications
- Health related
- Data Brokers
- Data Processors

**An Coimisinéir
Cosanta Sonraí**



**Data Protection
Commissioner**

Codes of Practice

- Garda Síochána (Police Force)
- Insurance Sector
- Injuries Board
- [Working on Banking Sector Code]
- Public Sector Bodies?



Powers of DPC

- Information notice (section 12)
- Enforcement notice (section 10)
- Compliance Audits (section 10)
- Powers of entry and inspection (section 24)
- Decision on complaints (section 10)
- Refusal to register (section 17)
- Prohibition of non-EEA transfers (section 11)
- Prosecute Offences (section 30)



General Approach of DPC

- Strong emphasis on Education
- Supportive of compliant data controllers
- Alert to issues arising from Complaints
 - *Emphasis on Right of Access*
 - *Addressing the “big picture”*
- Target problem data controllers
 - *Use full powers*
- Work with other Regulators



Offences and Penalties

- Failure to comply with a Notice
- Failure to register
- Failure to comply with terms of register entry
- Fine of up to €100,000
- Separate offences & penalties under Electronic Communications Regulations – increased 2008
 - *prosecutions going through the Courts*



Other Penalties

- Reputational damage – the most important penalty?
- Named in the DPC Annual Report
- Liability to civil suit for damages

An Coimisinéir
Cosanta Sonraí



Data Protection
Commissioner

Presentation Outline

- The Governance Challenge
- Data Protection – Legal Context
- Data Protection Commissioner
- **Questions you should ask**



Stocktaking

- Do we know what types of personal data we hold?
 - *Electronically (also CCTV images)*
 - *Paper*
- Can we justify:
 - *Why we collect it?*
 - *What it is used for?*
 - *Length of time we hold it?*
 - *Who has access to it?*
 - *Who it is disclosed to?*



General Policy

- Is the Organisation conscious of its data protection responsibilities?
- Do we have a Data Protection Policy approved at Board level? Who is responsible for its implementation?
- Has the Organisation thought through the implications of the policy for the types of personal data that it handles?
- Is there a system of regular reporting to the Board on implementation?



Data Security

- Do we have the necessary physical, IT and organisational measures to protect the security of the personal data entrusted to us?
- Access Controls
 - *Internal*
 - *External*
 - *Audit Trails*
 - *Portable Devices*
- Training
- Disposal



What if things go wrong ...

- Is there a clear plan on how to deal with a security breach?
- Does it provide for notification of the DPC and customers/clients?
 - *Anticipate legislation (Working Group examining issue)*
- Have you thought through what type of remedy customers/clients might expect?

**An Coimisinéir
Cosanta Sonraí**



**Data Protection
Commissioner**

Thank You!

Office of the Data Protection Commissioner

Canal House

Station Road

Portarlinton

Co Laois

Phone: LoCall 1890 252231

057 8684800

Fax: 057 8684757

Email: info@dataprotection.ie

Website: www.dataprotection.ie