



Data Protection- Implications for modern technology

Joe Meade

Data Protection Commissioner

HEAnet Annual Conference

November 11th, 2004



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

Presentation Outline

- **Offline v Online**
- **Background – Human Rights**
- **Data Protection Principles**
- **Rights of data subjects**
- **Role of the Data Protection Commissioner**
- **Technology issues**
- **When things go wrong**



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

Data Protection

WHAT IS IT

- Protection of personal privacy ...
- ... against threat of computer power
- ...by regulating computer use ...
- ... by giving people new rights
- ... *and now also extended to manual files*

WHY

- **Post-World War II emphasis on human rights**
- **George Orwell, “1984” (published in 1949)**
- **International Agreements on Human Rights**
- **Development of computer power**



Data Protection Commissioner

An Coimisinéir Cosanta Sonraí

Privacy: Legal development

- Constitution of Ireland (1937; case-law)
- Universal Declaration on Human Rights (1948)
- European Convention on Human Rights (1950)
- OECD guidelines 1980
- Convention 108 (Council of Europe, 1981)
- Data Protection Act, 1988
- EU Directives 95/46, 97/66 and 2002/58
- Charter of Fundamental Rights of the EU 2000
- Data Protection (Amendment) Act, 2003 and Sis
- European Convention on Human Rights Act 2003
- EU Constitution 2004



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

Key Concepts

- **Privacy is a human right**
- **Data Protection Laws are one method of protecting privacy rights**
- **Data Protection is **not** FOI**



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

Data Protection Acts, 1988 & 2003

The Acts create a balance environment:

RIGHTS

for

individuals

RESPONSIBILITIES

for

users of personal data



Data Protection Commissioner

An Coimisinéir Cosanta Sonraí

Definitions

- **Personal Data**
 - Data relating to a living individual identifiable from data in possession or likely to come into possession
- **Data**
 - Automated or manual data
- **Manual Data**
 - Structured by reference to individuals in a way that makes data readily accessible
 - Transition period to October, 2007 for some provisions



Data Protection Commissioner

An Coimisinéir Cosanta Sonraí

Definitions

- **Processing**
 - Virtually anything done with data.
 - Including just holding data
- **Data Subject**
 - an individual who is the subject of personal data
- **Data Controller**
 - a person who controls the contents and use of personal data
- **Data Processor**
 - A person who processes personal data on behalf



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

The Data Protection Rules.

1. Fair obtaining
 - 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. **Comply with access request**



Data Protection Commissioner

An Coimisinéir Cosanta Sonraí

Obtain & Process Fairly

- **Data controller must give full information about**
 - identity
 - purposes
 - disclosees
 - any other data necessary for “fairness”
- **Third party data controllers**
 - must contact data subject to provide these details
 - must give name of original data controller

One of these conditions required:

- Consent
- Legal obligation
- Contract with individual
- Necessary to protect vital interests
- Necessary for a public function (Justice)
- necessary for ‘legitimate interests’



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

Processing Sensitive Data

One of these additional conditions is required

- **Explicit consent**
- **Necessary under employment law**
- **To prevent injury or protect vital interests**
- **Process the data of members/clients of non-profit orgs.**
- **Legal advice**
- **For Medical Purposes**
- **Statutory function**



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

What are sensitive data?

- Physical or mental health
- Racial origin
- Political opinions
- Religious or other beliefs
- Sexual life
- Criminal convictions
- Alleged commission of offence**
- Trade Union membership**



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

Disclosing personal data

- not generally permitted – compatibility test
- section 8 – lifts the restrictions on disclosure:
 - **crime; tax; State security; international relations**
 - **required urgently to protect life and limb**
 - **required by law or court order**
 - **with consent of, or on behalf of, data subject**
- No general public interest test



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

Security Procedures

Security measures

- *Appropriate security measures*
 - **Appropriate to the harm that might result..**
 - **Appropriate to the nature of the data**
- *May have regard to cost of implementation*
- *May have regard to the current state of technology*
- *Staff must know and comply with measures*
- *Internal review of security measures-part of Internal Audit function ?*



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

Data Protection Training.

- **Obligation** on employer to ensure staff are aware of data protection obligations.
- **Policy.**
 - A Code of Practice.



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

Data Processors

Agents and sub-contractors

There must be a written contract in place

**Data Controller must take reasonable steps
to ensure compliance with security
measures**



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

Retention of data

- Legal obligations to hold data?
- Customer files
 - Do you need to hold **all** that data?
- Personnel files
 - Revenue requirement?
- Must have policy thought through
 - Defend retention as necessary for purpose.



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

Rights of Individuals

- o To have data processed in accordance with principles
- o To get a copy of personal information
- o To correct information if it is wrong
- o To opt out of direct marketing
- o To complain to the Data Protection Commissioner



**Data Protection
Commissioner**

An Coimisinéir Cosanta Sonraí

Access Request

- **Rights granted to individuals are a means of giving them control over how their data are processed – transparency**
- **Applies to all manual and electronic records in existence at the time of receipt of an access request – regardless of when the record was created.**



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

Exemptions

- **Expression of an opinion exempt from an access request if the expression of an **opinion was given in confidence or under the understanding it would be treated as confidential.****
 - **Data relating to a criminal investigation**
 - **Data relating to a claim of liability**
 - **Data covered by legal privilege**
 - **Certain research data**
 - **Back-up data**
 - **Disproportionate effort**



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

Right to correct/erase/block

- **Data Subject makes a written request**
- **Personal data must be:**
 - **Corrected, if inaccurate; or**
 - **Deleted, if should not be held.**
- **Data Controller has 40 days to respond**
- **Notify those who got wrong information**



Data Protection Commissioner

An Coimisinéir Cosanta Sonraí

Role of the Commissioner

- **Upholds rights of individuals**
- **Enforces obligations of data controllers**
- **Investigates complaints**
- **Maintains public register**
- **European functions**



Data Protection Commissioner

An Coimisinéir Cosanta Sonraí

Commissioner's Powers

- Information notice (section 12)
 - Enforcement notice (section 10)
 - Prohibition notice (section 11)
 - Powers of entry and inspection (section 24)
 - “authorised officers”
 - Decision on complaints (section 10)
 - Refusal to register (section 17)
 - Initiate prosecutions (section 30)
- Codes of Practice
 - Encouraged/Produced by DPC
 - Audit (PROACTIVE)
 - Investigation to ensure compliance and identify contravention
 - Name & Shame
 - Annual Report absolutely privileged



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

Offences and Penalties

- Civil Liability
- Failure to comply with a Notice
- Failure to register
- Failure to comply with terms of register entry
- Fine of up to €100,000 and €3000 for each spam sent
 - **Court may order erasure of data**



Data Protection Commissioner

An Coimisinéir Cosanta Sonraí

Technology Issues

- **Surveillance in the workplace**
 - E-mail/Web-browsing/CCTV/Phone
- **Biometrics**
 - Authentication
- **Security**
 - Wireless LAN/
Encryption of e-mails
- **Internet processing**
 - Jurisdictional problems
- **SPAM**
 - E-mail/
SMS/Facsimile
- **Terminology**
 - Technologically neutral



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

Workplace surveillance

- **Acceptance that employees have a right to privacy – even in the workplace.**
- **This right must be balanced with employer's legitimate interests.**



**Data Protection
Commissioner**

An Coimisinéir Cosanta Sonraí

Limitation of Privacy Right

- Can an employer have a policy which prohibits personal use of equipment?
 - **Yes but...**
- Where no policy exists, can a default policy be decided upon?
 - **Yes, reasonable expectation to privacy.**



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

Balance

EMPLOYERS INTEREST

- Interest in profitable use of resources.
- Interest in preventing damage to equipment.
- Monitoring as legal requirement.

PROPORTIONATE

Any limitation of the employees' right to privacy should be **proportionate** to the likely damage to the employer's legitimate interests.



**Data Protection
Commissioner**

An Coimisinéir Cosanta Sonraí

Monitoring

- **E-mail monitoring.**
- **Web-browsing monitoring / profiling.**
- **Phone monitoring.**
- **CCTV monitoring.**



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

Policy

- **Before any monitoring takes place, employees should be notified of nature, extent and its purpose.**
- **Ideally, a policy **should** be available.** *Not restrictive but focus on prevention and education*



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

E-mails

- **Automatic screening software**
 - Prevent virus damage
 - Prevent large files slowing system
- **Log created**
 - Used to flag abuses
- **Inspection of e-mail content**
 - In context of an investigation



**Data Protection
Commissioner**

An Coimisinéir Cosanta Sonraí

Web-browsing

- Automatic blocking.
- Log of sites visited.
 - Generate report listing excessive use.
- Identification of sites.
 - Specific investigation.
- Profiling?



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

Phone Monitoring.

- **Listening to calls.**
- **Recording calls.**
- **Logging traffic data.**
 - **Produce report of excessive use.**
 - **Identify numbers in context of investigation.**



**Data Protection
Commissioner**

An Coimisinéir Cosanta Sonraí

CCTV Monitoring

- **Areas under surveillance.**
- **Purpose(s) of surveillance.**
- **Active monitoring –v- recording.**
- **Covert –exceptional (Gardai)**



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

Biometrics

- Ideally used to confirm person present is the same person as on ID card
- Discourage creation of centralised databases, **though favoured by State agencies**
- Avoid secondary uses: an access control system should not be used as a time management system.



Data Protection Commissioner

An Coimisinéir Cosanta Sonraí

Security

- **Is a DP requirement**
- **Technology offers many solutions**
- **Human factor is commonest failing (poor training / awareness)**
- **Access controls**
 - Who; where; when?
Profile
- **Network vulnerability – distance working**
- **Wireless LAN**
- **Home pc**
- **Audit Log**
 - Existence acts as a discouragement



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

Internet Processing

- **Jurisdictional problems**
- **Where is server located?**
- **From where is data controlled?**
- **Are users aware of location of server and lack of protection?**
- **Transfer of data provisions**
- **Restriction of use of cookies (SI 535/2003)**



**Data Protection
Commissioner**

An Coimisinéir Cosanta Sonraí

SPAM

- **Technology has offered marketers new low cost media**
- **E-communications more intrusive than direct mail**
- **E-Communications Directive 2002/58/EC**
- **Cookies**
- **Automated diallers**



**Data Protection
Commissioner**

An Coimisinéir Cosanta Sonraí

Marketing

- Phone and email direct marketing
 - *Adhere to opt-out registers for phone calls/ NDD soon*
 - “**Opt-in**” for unsolicited e-mails (“spam”)
 - Similar products and opt out option in future emails
 - **Identity** of email sender clear
- Automated phone diallers, fax machines etc for direct marketing
 - *Prior consent needed for personal calls*
 - *Opt out for business calls*



Data Protection Commissioner

An Coimisinéir Cosanta Sonraí

Combating SPAM

- **OK if sourced within EU**
 - Not all States have transposed Directive
- **Identifying spammers**
 - IP address most useful
 - Phone numbers blocked between Telcos
- **Filtering by ISP / Telco?**
 - Cannot be automatic; may only be done with consent of subscriber
 - Area under review



**Data Protection
Commissioner**

An Coimisinéir Cosanta Sonraí

Law enforcement

- **Traffic Data Retention Bill**
 - Easy with Telco data; difficult with internet traffic especially with floating IP addresses.
 - Retention period is under review as it raises certain concerns
- **US Federal authorities only want a service to be offered if it can be tapped.**



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

Concerns

Communications Traffic data can or could be used

- as a source of great assistance to marketers including telcos and ISPs to profile your habits
- to monitor your movements by reference to location of call as an information source and /or to snoop on you if necessary
- to make wrong assumptions about your personal behavior and to blackmail you perhaps-hackers, security of ISP/telco
- as a means of surveillance on every citizen just in case they did wrong .Unlike other forms of personal data traffic data can reveal very easily who you are communicating with and where you are in your normal private life even when there is no criminal activity of any sort contemplated or being carried out by you



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

Terminology

- Use of technologically neutral terminology in DP Acts prevents them from going out of date. Allows flexibility in interpretation.
- Issue raised might not obviously appear in legislation.



Data Protection

Commissioner

An Coimisinéir Cosanta Sonraí

Technology : an aid to privacy

- Privacy statements-real and adhered to
- Automatic restrictions at point of collection
 - Limit fields on on-line forms
- Automatic review
 - Review retention period and cull data
 - **PETS v PITS**
- Access controls
 - Access on a need to know basis



**Data Protection
Commissioner**

An Coimisinéir Cosanta Sonraí

Other aids to privacy

- **Audit logs**
 - **If people know they can be traced, will be careful about what they do**
 - **Human factor: sharing of passwords e.g PULSE**
 - **Use of biometrics to confirm user**



Data Protection Commissioner

An Coimisinéir Cosanta Sonraí

What to do

- Internal review
- **Senior management role**
- Corrective action
- Education and awareness
- Competitive advantage
- Dangers and costs/ public shame/business failure



Data Protection Commissioner

An Coimisinéir Cosanta Sonraí

Past Cases of Concern

- Work assessment
- Headhunting
- Medical records
- Photographs on school websites and permission
- Asylum seekers web data
- Local authority web data
- PPSN overall
-



Data Protection Commissioner

An Coimisinéir Cosanta Sonraí

Conclusion

- **Respect for privacy is an essential factor in the acceptance and development of e-commerce.**
- Just because something is technically feasible does not mean that its good or correct for society overall
 - Move with care and caution
- **Whilst tempted by the prizes offered by new technology, the public's rights must be respected by all concerns.**
- **Risk management is important**
- **Offline=Online**



More information

*Office of the Data Protection Commissioner, Block 6,
Floor 3, Irish Life Centre, Lr. Abbey St. Dublin*

Phone 0035318748544, fax0035318745405

info@dataprotection.ie

www.dataprotection.ie