



# Preventing data loss – the legal impact of data loss

## Stewart Room

Partner, Privacy and Information Law Group

President, National Association of Data Protection Officers

+44 (0)20 7861 4000

[stewart.room@ffw.com](mailto:stewart.room@ffw.com)

March 2008



## Learning aims

- Identifying the legal framework for personal data.
- Identifying the consequences of data loss.
- Practical experiences of handling data loss cases.



# The legal framework for personal data (1)

## Security principles

Data Protection Directive 1995 - EU	Data Protection Act 1998 – UK	Data Protection Act 1998 - Ireland
Article 17	Seventh data protection principle	Section 2(1)(d) & 2C
<p>Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.</p> <p>Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.</p>	<p><b>Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.</b></p> <p>Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to—</p> <p>(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and</p> <p>(b) the nature of the data to be protected.</p>	<p>appropriate security measures shall be taken against unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.</p> <p>In determining appropriate security measures for the purposes of section 2(1)(d) of this Act, in particular ..., where the processing involves the transmission of data over a network, a data controller—</p> <p>(a) may have regard to the state of technological development and the cost of implementing the measures, and</p> <p>(b) shall ensure that the measures provide a level of security appropriate to—</p> <p>(i) the harm that might result from unauthorised or unlawful processing, accidental or unlawful destruction or accidental loss of, or damage to, the data concerned, and</p> <p>(ii) the nature of the data concerned.</p>



# The legal framework for personal data (2)

## Meaning of personal data

Data Protection Directive 1995 - EU	Data Protection Act 1998 – UK	Data Protection Act 1998 - Ireland
Article 2	Section 1	Section 1
<p>'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;</p>	<p>"personal data" means data which relate to a living individual who can be identified—</p> <p>(a) from those data, or</p> <p>(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,</p> <p>and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;</p>	<p>"personal data" means data relating to a living individual who can be identified either from the data or from the data in conjunction with other information in the possession of the data controller;</p>



# The legal framework for personal data (3)

## Consequences

Data Protection Directive 1995 - EU	Data Protection Act 1998 – UK	Data Protection Act 1998 - Ireland
Articles 23 & 24	Sections 13, 40 & 47	Sections 7 & 10
<p><b>Article 23 Liability</b> Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions ... is entitled to receive compensation from the controller for the damage suffered.</p> <p><b>Article 24 Sanctions</b> The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.</p>	<p><b>Section 13 Compensation</b> (1) An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation ... (2) An individual who suffers distress ... is entitled to compensation from the data controller for that distress if— (a) the individual also suffers damage by reason of the contravention ...</p> <p><b>Section 40 Enforcement notices</b> If the Commissioner is satisfied that a data controller has contravened or is contravening any of the data protection principles, the Commissioner may serve him with a notice (in this Act referred to as “an enforcement notice”) ...</p> <p><b>Section 47 Offences</b> A person who fails to comply with an enforcement notice, an information notice or a special information notice is guilty of an offence.</p>	<p><b>Section 7 Duty of care</b> For the purposes of the law of torts and to the extent that that law does not so provide, a person, being a data controller or a data processor, shall, so far as regards ... his dealing with such data, owe a duty of care to the data subject concerned</p> <p><b>Section 10 Enforcement</b> If the Commissioner is of opinion that a person has contravened or is contravening a provision of this Act ... the Commissioner may, by notice in writing (referred to in this Act as an enforcement notice) served on the person, require him to take such steps as are specified in the notice within such time as may be so specified to comply with the provision concerned</p> <p>A person who, without reasonable excuse, fails or refuses to comply with a requirement specified in an enforcement notice shall be guilty of an offence.</p>



# Where are data protection laws heading?

- Introduction of reporting of security breaches legislation?
  - See European Commission's proposal for a new Directive for the electronic communications sector (November 2007).
  - See the US example.
  - See Australian Privacy Commissioner's proposal (January 2008).
- Promotion of "Privacy Enhancing Technologies" (PETs).
  - See European Commission's PETs Communication (May 2007).
  - See UK Information Commissioner's laptop encryption policy (December 2007).
- Introduction of new criminal offences for data mishandling?
  - See UK Information Commissioner's submissions to House of Commons (December 2007).
- Wider sectoral legislation?
  - See FSA's fines of Nationwide (£980K, February 2007) and Norwich Union (£1.26m).



## Related consequences (non-dp)

- Brand and reputational damage.
- Other regulatory infringement.
- Breach of confidence.
- Breach of contract.
- Crimes.
  - UK = section 55 DPA, Fraud Act 2006 etc.
  - Ireland = section 21 DPA (unauthorised disclosure by data processor), section 22 (disclosure of data obtained without authority).



## Case study (1)

- Financial services institution.
- Break-in at premises.
- Disk arrays stolen.
- 370,000 data subjects affected.
- Reporting to police, ICO, FSA.
- Notifications to data subjects.
- Website, call-centre, CRA service.



## Case study (2)

- Retailer.
- Break-in at data processor's office.
- Laptop stolen.
- 26,000 data subjects.
- Reporting to police, ICO.
- Notifications to data subjects.
- Website, call-centre, CRA service.
- **Enforcement notice.**



## Any questions?

[stewart.room@ffw.com](mailto:stewart.room@ffw.com)

+44 (0)20 7861 4850

[www.dpalaw.info](http://www.dpalaw.info)