Data Protection – What's In Store

Dean Murray, Partner

Overview of the Data Protection Act 1998

- In force since March 2000
- All personal data must be processed in accordance with 8 data protection principles
  - Fair and lawful processing
  - Processed for limited purposes
  - Adequate relevant and not excessive
  - Accurate and up to date
  - Not kept longer than necessary
  - Processed in accordance with data subject rights
  - Technical and organisational security
  - Not transferred outside EEA without adequate protection
- Failure to process properly can lead to enforcement action by ICO

The GDPR

- EU Regulation – will automatically become part of UK law on 25 May 2018

- Unclear how Brexit will affect application but:
  - Cannot ignore it in the hope Brexit will remove it;
  - Likely to be in place in very similar form post Brexit; and
  - If your data subject is in an EU country you will need to comply anyway.

- Need to consider how the changes will affect your use of data

Significant Changes Introduced by GDPR

- Consent will be more difficult to use
  - Clear affirmative action
  - Can be withdrawn
  - Can't be bundled into a larger document (eg terms and conditions)
- Higher Fines – up to €20 million or 4% of Group global turnover
- Mandatory notification of breaches within 72 hours
- Subject access requests must now be responded to within 30 days (rather than 40 as currently) and you can no longer charge for response
- Additional subject rights (eg right to be forgotten)

Data Protection

Elizabeth Denham :

"*…cyber security is not an IT issue, **it is a boardroom issue**. Companies must be diligent and vigilant. They must do this not only because they have a duty under the law, but because they have a duty to their customers.*"

Bought In Data

- Assist Law Limited buys in a database which the provider warrants is "opted in"
- Data gathered using tick boxes or statements that by providing details the person consented to receive marketing communications from third parties
- Calls were made to TPS numbers – they complained
- ICO found that the persons had not "opted in"
- ICO found that the company should have:
  - Required evidence of consent; and
  - Screened against the TPS
- Fine of £30,000

Data Breaches

- Talk Talk acquired Tiscali UK operations 2009
- Cyber attack on Tiscali database (SQL injection attack)
- Talk Talk unaware Tiscali webpages still live
- Attack accessed 156,959 customers. About 10% included bank account number and source code
- Database operated outdated software for which a fix was made available 3.5 years before the attack
- No proactive monitoring activities to prevent attack
- £400,000 fine
- £55-60m - estimated cost to Talk Talk.
  - Incident costs £40-45m
  - loss of £15m in trading revenue from loss of 101,000 customers

Any questions

Dean Murray

Partner | Commercial

E: dean.murray@wardhadaway.com

T: 0191 204 4201