

Data Protection Update



Calum Murray, Susannah Sheppard and Chris Middleton
Corporate Counsel Forum - 11 February 2010

Upcoming Events

CCF Spring Programme:

- [25 February 2010](#) - *BSkyB v EDS: don't write cheques your delivery team can't cash*
 - [25 March 2010](#) - Corporate deals in the UK and Europe: working with the differences
 - [21 April 2010](#) - Head in the Clouds or Blue sky thinking... is Cloudsourcing the 'new black' or 'so last year'?
 - [20 May 2010](#) - Open source software: towards governance in the organisation
-
- Book a place at any future session online at - www.kemplittle.com/forthcoming-events.html
 - Also invite you to suggest any topics you would like to hear about for Summer/Autumn 2010 sessions which we are planning...

Today's agenda

- Housekeeping
- Key developments over the past year - [Calum Murray](#)
- Specific issue: use of online personal data - [Susannah Sheppard](#)
- Short coffee break
- Current data protection issues in HR - [Chris Middleton](#)
- Questions

Key developments over the past year



Calum Murray, Partner, Commercial Technology
Corporate Counsel Forum - 11 February 2010

Key developments over the past year

- General news
- Expanded enforcement powers of Information Commissioner's Office (ICO)
- Impact of EU Telecoms Directives reforms

General news

- Standard for Data Protection:

- [May 2009](#)

- BSI British Standards – first standard on [personal information management](#)

- [BS 10012](#) - aims:

- establish best practice

- assist with data protection law compliance

- Guides on: risk assessment, retention, disposal and disclosure of data and training

- Fees for notification:

- From [1 October 2009](#)

- [New two-tiered](#) structure under the Data Protection Act 1998 (“DPA”)

- Key factors – turnover and/or staffing

- Private: £25.9 million or more and >249 staff

- Public authorities: >249 staff

General news

- Overseas data transfers:
- Eighth data protection principle (paragraph 8, Part I, Schedule 1, DPA):
'personal data shall not be transferred to outside the EEA unless the receiving country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data'
- BCR - internal 'codes of conduct' used for intra-multinational corporate group data transfers outside EEA
- Need to be 'approved' by ICO - but multiple points of exit?
- WP74 (2008) – one point of contact + mutual recognition = parallel clearance of the BCR
- UK, Fr, De, Ie, It, Nl, No & Es
- **Hyatt Hotels and Resorts Business** – September 2009

Expanded enforcement powers of ICO

- ICO responsible for enforcing DPA on data controllers generally
- ICO has:
 - ‘*Information*’, ‘*Special information*’ and ‘*Enforcement*’ notices (s40-44, DPA)
 - DC consent based ability to assess processing (s51, DPA)
 - Court warrant based ability to enter premises without consent (Sch 9, DPA)
- [Coroners and Justice Act 2009 \(CJA\)](#) - Royal Assent November 2009
 - To come - assessment notices (Part 2, Sch 20, CJA):
 - government departments, public authorities or ‘by designation’
 - From [1 February 2010](#) – ICO to prepare code of practice for new functions re with assessment notices
 - To come - warrant for entry and inspection (Part 6, Sch 20, CJA)
 - tied to assessment notice...
 - [... for now?](#)

Expanded enforcement powers of ICO

- ICO responsible for enforcing DPA on data controllers generally
- [The Criminal Justice and Immigration Act 2008 \(CJIA\)](#) - Royal Assent on 8 May 2008
- Statutory instruments issued to give effect:
 - To come - civil financial penalties through monetary penalty notices (s144/CJIA - new s55A, DPA)
 - Expected from [6 April 2010](#).
 - Upper limit of [£500,000](#)

Expanded enforcement powers of ICO

- Financial penalty notices for breaches of data protection principles (Sch 1, DPA)
- ICO to confirm:
 - contravention was
 - [serious](#) and
 - of a kind likely to cause [substantial damage or distress](#) AND
 - data controller either:
 - [deliberately](#) contravened DPA or
 - knew/ought to have known of risk of contravention, its likely effects of substantial damage or distress [and still failed to take reasonable steps to prevent it from happening](#)
- ICO has process to follow
- [ICO Guidance](#) on how it will issue financial penalty notices

Impact of EU Telecoms reforms

- Widespread new package of rules for Europe's telecoms networks and services:
“The EU telecoms reform brings about consumer choice, a new dose of competition, an effective European system of independent telecoms regulators, new investment into competitive infrastructures, more space for new wireless services and a more open Internet for all citizens. The reform also strengthens the single telecoms market by promoting effective competition and consistent rules of the game across all 27 EU Member States. This will open up new opportunities for telecoms operators, for cross-border communication services and for European private and business consumers. And it will give a new boost to Europe's vibrant digital economy.”

Viviane Reding, EU Telecoms Commissioner

- In force December 2009 to be transposed into national law in UK by June 2011
- Data protection impacts:
 - strengthening of consumer [protection from personal data breaches](#)
 - re-enforcement of consumer [protection regarding cookie use](#)

Impact of EU Telecoms reforms

- Personal data breaches:

“breaches of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.”

- Scope - covers any [telecoms operator or Internet service provider](#) only
- Service provider obligation must notify ‘*without undue delay*’ the ‘*competent national authority*’
- Service provider may have to notify the subscriber/individual without undue delay if breach is likely to adversely affect s/i’s personal data or privacy

Impact of EU Telecoms reforms

- Use of Cookies:
 - Currently regulated by ePrivacy Directive at EU level and PECRs in UK
 - European Parliament Internal Market & Consumer Protection Committees: cookies to be used only where users have consented to their use
- Under reforms:
 - need user consent post “*clear and comprehensive information*’ or
 - cookie is ‘strictly necessary’ for services ‘explicitly requested’ by the user
- Consent ?
- “Where it is technically possible and effective...the user's consent to processing may be expressed by using the appropriate settings of a browser or other application”
- But Art 29 WP: default browser settings should be “privacy friendly” but **not a means to collect free, specific and informed consent of the users** as required in Data Protection Directive
- So we’ll see ...

Useful URL's

- Data Protection Act 1998
http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1
- British Standard – BS 10012:2009
<http://shop.bsigroup.com/en/Navigate-by/Assessment-Tools/Assessment-Tools/Self-assessment-tools/DP-Online/Data-Protection-/>
- ICO Guidance on changes to the notification fee system for data controllers
http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/notification_fee_changes.pdf
- Coroners and Justice Act 2009
http://www.opsi.gov.uk/acts/acts2009/ukpga_20090025_en_1
- The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010(SI 2010/31):
http://www.opsi.gov.uk/si/si2010/uksi_20100031_en_1
- The Data Protection (Monetary Penalties) Order 2010 (*draft*):
http://www.opsi.gov.uk/si/si2010/draft/ukdsi_9780111490723_en_1
- ICO Guidance on issuing financial penalty notices:
http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_guidance_monetary_penalties.pdf
- EU Telecoms Directive
<http://register.consilium.europa.eu/pdf/en/09/st03/st03674.en09.pdf>

Specific issue: use of online personal data



Susannah Sheppard, Partner, Competition and Regulatory
Corporate Counsel Forum - 11 February 2010

European Commission

- *March 2009* - the European Consumer Commissioner called for self-regulatory “principles of acceptable behaviour” as consumers feel “uncomfortable”. It covers: targeted messages and viral marketing.
- *November 5 2009*: - European Commission: Blueprint for Consumer Policy in Europe: Making markets work with and for people:
 - includes 3 actions to promote trust on-line one of which is ensuring collection and use of personal and behavioural data is fair
 - ‘technology never ceases to amaze and today we are faced with this relatively new issue of on-line data collection on an unprecedented scale and mostly without any user awareness
 - Convened Stakeholder Forum on Fair Data Collection to meet several times in 2010 to analyse the problems and to inform the Commission on actions to be taken

UK - Parliament

- *May 2009* – UK All-Party Parliamentary Group on Communications announces investigation into Deep Packet Inspection and behavioural advertising - key findings out on [October 15th](#)
- *October 2009* - UK All Party Parliamentary Group on Communications Report recommends:
 - *“that the Government review the existing legislation applying to behavioural advertising, and bring forward new rules as needed, to ensure that these systems are only operated on an explicitly, informed, opt-in basis.”*

UK – OFT

- *October 2009*: OFT launched a study into **online targeting of advertising practices and prices** to be completed Spring 2010 covering:
 - Behavioural advertising
 - Customised pricing: where prices individually tailored using information collected about the customer's internet use

OFT Market Investigation - Targeted Advertising

- To consider whether some targeted advertising practices may result in consumer detriment, e.g.:
 - Where data collected for profiling is identifiable to a specific person or a specific computer
 - Where data is collected and used by a single website: i.e. ‘first party’ behavioural advertising
 - Where advertising is based on a single visit or search criteria and involves no retention of data: i.e. ‘*contextual behavioural advertising*’
- Terms of study imply a recognition that any detriment that may arise is likely to depend on the practice
- AIM: To clarify how [existing legislation](#) may apply to online [behavioural](#) advertising and assess existing self regulatory measures

OFT Market Investigation - Targeted Prices

- The targeted prices study will consider:
 - ways in which online retailers use consumer profiles and segmentation to target specific products and prices to individual consumers
 - whether these practices cause consumer detriment where consumers are unaware that they are being targeted, e.g. affecting the extent to which they compare products as well as potentially raising privacy concerns

Conclusion

- Wide ranging investigations in to behavioural advertising practices
- General unrest amongst regulators due to consumer concerns
- Differences between:
 - the collection of personal data
 - the collection of consumer behaviour; and
 - what can be done with either once obtained?
- New regulations?

Current data protection issues in HR



Chris Middleton, Partner, Employment
Corporate Counsel Forum - 11 February 2010

Current data protection issues in HR

What we're covering

- Particular rules in the HR context
- How employees use data protection as a sword
 - Subject Access Requests
 - Damages claims
- And as a shield
 - Limits on employers' right to undertake monitoring

Particular rules in the HR context

- Employers process a lot of personal data and sensitive personal data about their employees
 - EG CVs, appraisals, disciplinary and grievance matters, attendance records, health matters etc
 - so employers must comply with the data protection principles
 - Typical issues –
 - disclosure of information internally and externally
 - retention of information
 - security
 - references

Particular rules in the HR context

- The Employment Practices Code
- Lengthy guidance for employers on complying with the Data Protection Act
- Four parts
 - Recruitment and Selection
 - Employment Records
 - Monitoring at Work
 - Information about Workers' Health

Subject Access Requests

- Data subject can ask a data controller –
 - what information is being processed about them
 - why it is being processed
 - who it may be disclosed to
 - what the source of the information was
- Fee/timescale
- Consequences of breach
 - request to the Information Commissioner
 - application to court
 - claim for damages?

Subject Access Requests

Limits on what must be provided:

- Information relating to/identifying a third party need not be disclosed unless
 - the third party consents
 - it is reasonable to disclose without consent
 - factors to take into account

Subject Access Requests

Limits on what must be provided:

- Durant v FSA - limits what constitutes personal data
 - Facts
 - Durant made complaint to FSA re Barclays
 - later sought disclosure of personal data held by FSA
 - FSA disclosed electronic records, not paper files
 - Amongst other things said paper files didn't contain 'personal data'
 - Court decided
 - To be 'personal data' information must
 - be biographical
 - have the individual as its focus
 - SARs not designed to assist in litigation

Damages claims

- Anyone who suffers damage through a data controller's failure to comply with the DPA is entitled to compensation
 - defence available where data controller used 'such care as in all the circumstances was reasonably required'
 - generally no claim where the individual has suffered only distress

(section 13 DPA)

Damages claims

Johnson v MDU

- An attempt to reply on section 13
- Facts
 - J – a surgeon, MDU provided indemnity cover
 - Various complaints against J, MDU had opened 17 files on him
 - Risk manager assessed the files, J's membership of MDU terminated, indemnity insurance terminated
 - J claimed unfair processing of personal data
- Court decided
 - processing fair in relation to 15 of the files
 - but not the other 2
 - but that failure not determinative
 - not its job to comment on the risk management policy

Monitoring

Common types of monitoring

- Internet usage
- Emails
- Telephone usage/telephone calls
- Drug/alcohol testing
- Searching employees

Main legal considerations

- Data Protection Act
- Regulation of Investigatory Powers Act 2000
- Human Rights Act

Monitoring

Data Protection Act

- Some of the relevant principles include the requirement for
 - fair and lawful processing
 - data to be adequate, relevant and not excessive
 - data to be subject to adequate technical/organisation measures to protect against unauthorised processing and accidental loss/destruction/damage

- Expanded on in Part 3 of the Employment Practices Data Protection Code
 - not binding –
 - a guide to compliance with the Act
 - lengthy (91 pages!)

Monitoring

Employment Practices Code – key principles

- Proportionality
- Impact assessments
 - alternatives to monitoring
- Provision of full information to employees
- Technical/security measures

Monitoring

Regulation of Investigatory Powers Act

- Section 1 RIPA – an offence to intercept a communication in the course of its transmission
- Section 3 – not unlawful if both parties to the communication consented to the interception or the interceptor reasonably believes that both parties consented
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 provide various defences including:
 - eg to investigate or detect the unauthorised use of the telecommunications system

Monitoring

Human Rights Act

- Article 8 – right to respect for private and family life
 - not an absolute right
 - but some application in the workplace
- Application to private sector employers?

- See for example: McGowan v Scottish Water, E.A.T.
 - employee believed to be falsifying timesheets
 - employer's surveillance of him was capable of infringing his private life
 - but was proportionate
- But compare Mills v Mid Sussex District Council, E.T.

Monitoring

Practical advice

- Put in place a communications policy
 - guidelines on acceptable email/internet usage
 - including the extent to which personal usage is permitted
 - explain that monitoring will/may be undertaken
 - types/purposes/extent
 - explain employer's policy on retention/deletion of data
 - should also cover passwords/encryption
 - cross-refer to disciplinary policy as appropriate
- Circulate copies to employees/let them know where they can get a copy eg intranet
- Periodically remind employees of its existence
- A little proportionality goes a long way

Questions?



Chris Middleton

Employment Partner

Kemp Little LLP

chris.middleton@kemplittle.com

Tel. +44 (0) 20 7710 1622



Calum Murray

Head of Commercial Technology

Kemp Little LLP

calum.murray@kemplittle.com

Tel. +44 (0) 20 7710 1615



Susannah Sheppard

Head of Competition and Regulatory

Kemp Little LLP

Susannah.sheppard@kemplittle.com

Tel. +44 (0) 20 7710 1659