

Data protection compliance tips

Wed, 28 Jul 2010 | By Stephanie Pritchett, data protection lawyer, Pritchetts solicitors

Recruiters are particularly at risk from failures to protect the data they hold, and because of serious financial harm and distress to individuals if a breach occurs. For example:

- they keep detailed files on prospective employees containing information about jobs they are seeking, qualifications, job history, financial constraints and interview feedback. It is too easy to add notes like 'indecisive' or 'punching above their weight' that could unfairly affect their ability to obtain a job
- they are probably not informing clients about their right to a copy of their information and to rectify inaccurate data. Disclosure of inaccurate information may lead to an individual missing a job opportunity.
- an unsolicited 'headhunting' approach could lead to an employer assuming its employee is seeking a new job which may adversely affect their current job prospects.

The recession has meant both a greater desire for businesses to exploit information assets and to make compliance cuts which creates dangerous business risks. Particularly as new penalties of up to £500,000 were brought into force from 6 April 2010 for serious contraventions of the Data Protection Act. Before imposing these fines, the Information Commissioner's Office (ICO) must be satisfied that:

- there has been a serious breach of the Act;
- likely to cause serious harm or distress; and
- it was either deliberate (e.g. passing on a client's details without consent) or the agent should have anticipated the risk but hadn't taken reasonable steps to prevent it (e.g. by encrypting laptops or properly protecting client details which could be passed to a competitor by a disgruntled employee).

How likely you are to receive a fine for breaches? The Justice Minister has said that the new penalties will ensure the ICO can impose robust sanctions on those committing serious contraventions and it is hoped that the new penalties will also act as a strong deterrent.

These fines, together with personal criminal liability for directors and officers and the ICO's new rights to spot check public sector bodies - with similar powers for private sector bodies likely to follow under the new coalition - mean data protection can no longer be ignored.

To avoid your agency being the next 'named and shamed' for data protection breach, follow Pritchetts' top 10 compliance tips:

- 1 review and audit your agency's data protection compliance in light of the increased risks of a £500,000 penalty for breach.
- 2 health check data protection policies and procedures – including privacy policies, data collection forms and internal data protection and retention policies.
- 3 ensure marketing team practices are compliant with the Act and Privacy Regulations - via appropriate use of databases, opt-ins, opt-outs, telescripts, 'recommend a candidate' and headhunting schemes.

4 ensure all arrangements with third parties who process data on your behalf (eg mail-houses and marketing companies) are in writing and contain the legally required data protection clauses.

5 review your ICO notification to ensure it is accurate and up to date. Failure to notify new processing activities within 28 days is a criminal offence.

6 have robust subject access request procedures – failure to comply with these requests (e.g. by disgruntled job applicants) is the main reason for ICO complaints.

7 have a data security and security breach policy in place.

8 ensure CCTV policies and signages around stores are compliant.

9 ensure data protection moves up the corporate compliance agenda.

10 carry out staff data protection training and stay abreast of legal developments

Stephanie Pritchett is a data protection lawyer at Pritchetts solicitors



Advertise
your vacancy




Sign up for **FREE**
email services



black
book 2010

Your first
resource for
services & tools



FREE TRIAL!

START FREE TRIAL >