

Protect Privacy Online – and avoid a fine

The Information Commissioner’s Office (ICO) has published a new Code with “do’s and don’ts” for the processing of personal data gathered online.

It’s worth remembering that, whilst the Code itself is not legally enforceable and therefore compliance with it not mandatory, data controllers are well advised to follow the Code where possible in order to avoid falling foul of the provisions of the DPA. The Code is at:

http://www.ico.gov.uk/for_organisations/topic_specific_guides/online.aspx

A summary of the main guidance provided:

- Don’t be secretive or misleading when you collect personal data – people won’t trust you and will go somewhere else.
- Do be clear about the purposes for which you use or disclose personal data, and don’t change these purposes without consent once the data has been collected.
- Don’t collect personal data you don’t need or collect it too early in the process – people don’t like organisations that collect too much information about them.
- Don’t keep records about people that are inaccurate or out of date – everyone expects their information to be correct.
- Don’t keep personal information for longer than you need to in a personally identifiable form – people don’t like too much information being retained about them.
- Respect individuals’ rights over the information you hold about them – for example, don’t deny them access to their personal data.
- Make sure you have adequate security and maintain responsibility for the personal data you collect – everyone expects their information to be looked after properly.
- Ensure the personal data you are responsible for is protected properly if it is transferred overseas, i.e. using cloud computing.

Remember that the provisions of the DPA apply to the “processing” of “personal data”. “Processing” is very broad in scope, and includes everything that happens to personal data collected online. “Personal data” is information relating to a living individual who can be identified from that data. So if you process personal data, read the Code and try to comply with its guidelines where possible.

It’s also important to train staff on data protection, as non-compliance can potentially incur hefty fines. Three UK Councils recently suffered a public rebuke as they came under fire from the ICO regarding their lack of staff training on data protection. The poor training resulted in personal data on thousands of children being lost or stolen. The incidents included an unencrypted laptop containing data on children and their families being stolen; an employee downloading data on 9,000 children and their families onto an unencrypted, non-password-protected USB stick which was then stolen from their home; and a social worker losing documents in a plastic wallet. All

councils have now signed undertakings with the ICO that they'll ensure staff are made fully aware of their policies regarding storage and use of personal data.

It's essential for all businesses to appreciate the importance of not only implementing data protection policies, but also communicating them to staff and conducting regular staff training. Non-compliance with data protection law could potentially cost £500,000 in penalties and could also result in court actions where the disclosure of the data has caused damage to the individuals concerned.

David Flint is a Partner and Head of the Technology Media & Communications Group at MacRoberts LLP. For further information, please contact david.flint@macroberts.com

This article featured in the September 2010 issue of CABLEtalk.

[See our website for full Copyright notice and Disclaimer.](#)

© MacRoberts LLP 2010