

meeting	STANDARDS COMMITTEE	
date	16 MARCH 2010	agenda item number 6

REPORT OF THE MONITORING OFFICER

DATA PROTECTION ACT UPDATE

Purpose of the Report

1. To inform the Standards Committee about the ability of the Information Commissioner (**Commissioner**) to impose monetary penalties for breaches under the Data Protection Act 1998 (**DPA**).

Information and Advice

2. The DPA regulates the use of personal data by the County Council and any other organisation or individual who is registered to deal with personal data (known as the data controller). The latest developments in the field of data protection which are examined in this report relate to the Commissioner's ability to impose monetary penalties for data protection breaches and the new statutory guidance on monetary penalties (**Guidance**) which has been produced by the Information Commissioner's Office (**ICO**).
3. The Commissioner is empowered to impose a monetary penalty notice on any data controller who has seriously contravened any of the data protection principles and was likely to cause substantial damage or substantial distress. The monetary penalty notice requires the data controller to pay a specified monetary amount which is determined by the Commissioner.
4. The Data Protection (Monetary Penalties)(Maximum Penalty and Notices) Regulations 2010 provides the Commissioner with the ability to issue monetary penalties by setting a prescribed maximum amount of £500,000 which can be imposed for data protection breaches. These Regulations also prescribe the information which must be included in a monetary penalty notice. The Regulations will come into force on 6 April 2010.
5. Prior to issuing a monetary penalty notice the Commissioner will issue the data controller with a notice of intent which will notify the data controller that the Commissioner intends to issues a monetary penalty notice. The Data Protection (Monetary Penalties) Order

2010 requires the Commissioner to consider written representations made by a data controller in relation to the Commissioner's intention to serve a monetary penalty notice. The Commissioner has a duty to consider the representations made and can vary the amount of monetary penalty or cancel the monetary penalty notice. The Order also makes provision for appeals against monetary penalty notices.

6. The Guidance states that a monetary penalty is reserved for the more serious data protection breaches and that as a general rule a Data Controller with substantial financial resources is more likely to attract a higher monetary penalty than a data controller with limited resources.
7. The Commissioner will consider the particular facts and circumstances of the case before deciding whether to impose a monetary penalty. The Guidance highlights some of the factors the Commissioner will take into account in determining whether to impose a monetary penalty and in relation to determining the size of the penalty. In more serious cases the Controller may set a higher penalty as a deterrent to others.
8. The Guidance provides examples of what the Commissioner would consider a serious contravention; for example a failure to take adequate security measures resulting in the loss of a compact disc containing personal data. An example of substantial damage would be where following a security breach financial data is lost and an individual becomes a victim of identity fraud. Substantial distress may occur where a security breach leads to medical records being stolen and as a result an individual suffers worry and anxiety that the sensitive personal data may be made public.
9. The Guidance also states that in addition to there being a serious contravention of the data protection principles causing substantial damage or distress the Commissioner will consider whether the data controller knew or ought to have known there was a risk of such a contravention, but failed to take reasonable steps to prevent the contravention or whether the contravention was deliberate.
10. An example of a deliberate contravention would be where a data controller knowingly discloses data without consent to populate a tracing database for commercial purposes without informing the individuals involved. An example of where a data controller may be deemed to have "knew or ought to have known of a contravention" would be where a data controller had been warned by its IT department that employees were accessing sensitive personal data but the data controller had failed to carry out a risk assessment or implement a policy of encrypting all laptops and removal media as appropriate.
11. The Commissioner will consider whether a data controller had taken reasonable steps to prevent a contravention evidence of this may be provided by the data controller carrying out a risk assessment,

introducing policies and procedures and taking steps to address risks which may lead to a contravention, having good governance and audit arrangements in place, following guidance or codes of practice published by the ICO or others.

12. In addition to serving a monetary penalty notice, the Commissioner may still issue an enforcement notice on the data controller or take other enforcement action against the data controller.
13. Any monetary penalty notice will be published on the ICO's website.
14. Appeals against monetary penalty notices and variation notices may be made to the General Regulatory Chamber (First-tier Tribunal).
15. The County Council intends to raise awareness of data protection issues and communicate to employees and Members the importance of data privacy. It proposes to take the following actions:
 - a. Reporting the changes to management;
 - b. Updating the intranet guidance on data protection;
 - c. Printing and distributing the "Think Privacy" publicity material produced by the ICO and making them available on the intranet;
 - d. Publishing a news item on the intranet and/or the In Contact publication to raise awareness of the issue.

Statutory and Policy Implications

16. This report has been compiled after consideration of implications in respect of finance, equal opportunities, personnel, crime and disorder and those using the service and where such implications are material they have been described in the text of the report.

RECOMMENDATION

17. That the contents of the report be noted and consideration be given by the Standards Committee to the actions proposed by the County Council to raise awareness of data protection issues.

**JAYNE FRANCIS-WARD
MONITORING OFFICER**

Comments of the Service Director – Finance (MB 08/03/10)

There is no budget to cover any monetary penalty that might be imposed on the authority. Penalties would have to be met from within existing resources.

Legal Services Comments (SLB 25/02/2010)

By virtue of Article 9 of the Council's Constitution Standards Committee has the function of monitoring the operation, and advising the Council on the update and revision, of all codes of conduct and practice of the County Council. It is appropriate for Standards Committee to consider the content of this report.

Background Papers Available for Inspection

The ICO Guidance can be found at:

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_guidance_monetary_penalties.pdf

The ICO publicity material can be found at:

http://www.ico.gov.uk/upload/documents/think_privacy_toolkit/ico_think_privacy_toolkit.pdf

Electoral Division(s) and Member(s) Affected

All.