Ministry of JUSTICE

Civil Monetary Penalties – Setting the maximum penalty CP 48/09

List of questions for response

We would welcome responses to the following question set out in this consultation paper. Please email your completed form to: victor.riega@justice.gsi.gov.uk or fax to: 020 3334 2245. Thank you.

Question 1. **Do you consider that a penalty of up to £500,000 provides the ICO with a proportionate sanction for serious contraventions of the data protection principles?**
Comments: In our view, this represents a good starting point in what we assume will be an ongoing process at assessing proportionate sanctions for serious contraventions of the data protection principles. It is interesting to note that the Financial Services Authority has levied fines exceeding £500,000* for significant breaches of the 'Management & Control' principle ("*A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems*"). Such fines arose in situations that could be considered similar to those in which there may be non-compliance with the seventh data protection principle i.e. data/information security issues. This FSA principle is, of course, much broader in scope than the seventh data protection principle, which requires data controllers to take "*appropriate technical and organisational measures … against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data*". As such, it is possible that non-compliance with the FSA principle could occur in situations where there was DPA compliance. Notwithstanding this point, breach of this data protection principle will always be cited by the ICO when it issues Enforcement Notices for incidents of data loss/inadequate data security. As such, a situation could arise where a data controller is in breach of both of the abovementioned principles, but would face a smaller fine from the ICO compared to the FSA. This apparent inconsistency between the fining powers of these two regulatory bodies has the potential to undermine the effectiveness of the regulatory 'strength' of the ICO.

These points aside, we welcome the opportunity for the ICO to levy fines for serious non-compliance with the data protection principles. We would hope that the current level could be reviewed if the ICO was forced to levy the maximum penalty on a frequent basis in the future. We do, however, stress the importance of balancing the maximum level of such monetary penalties against the risk of significant disruption to business. This is a risk that could be mitigated by, for example, provision of useful compliance guidance/toolkits, as well as very clear guidelines as to how the ICO applies principles of proportionality when calculating penalties.

This response was submitted on behalf the **EnCoRe Project** on 21 December 2009.

Ensuring Consent and Revocation www.encore-project.info

EnCoRe is a multi-disciplinary research project, spanning across a number of IT and social science specialisms, that is researching how to improve the rigour and ease with which individuals can grant and, more importantly, revoke their consent to the use, storage and sharing of their personal data by others.

The overall vision of this project is to make giving consent as reliable and easy as turning on a tap, and revoking that consent as reliable and easy as turning it off again.

We are a UK research project, with 6 academic and industrial participants, that is partially funded by the UK Government's Technology Strategy Board, Economic & Social Research Council and Engineering & Physical Sciences Research Council.

* Nationwide was fined £980k (14 February 2007); Norwich Union £1.26m (17 December 2007); and HSBC £3.185m (22 July 2009).