

## **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](mailto: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:

**Q: 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?**

MacRoberts shares the Government's view that the penalties for data protection breaches must be increased. We do not, however, consider a £500,000 maximum fine to be appropriate for severe breaches of data protection principles. Organisations need to be reminded of the importance of data protection and the consequences of careless or deliberately unethical behaviour in relation to the processing of the personal information they hold. In many cases, the suggested maximum penalty which an offending company could be handed will not reflect the potentially long-lasting harm caused to data subjects whose personal information has been stolen, lost or otherwise removed from its lawful data controller or data processor. For example, if the medical records of a number of data subjects undertaking research in the hands of a commercial drug company were to go missing, then besides the possibility that the people involved could become the victim of some form of identity attack, the knowledge that a person's sensitive personal information is in the hands of a stranger (and used for purposes for which it was not originally obtained) could be a highly upsetting and distressing experience for those data subjects. In such a scenario it is difficult to argue that the penalty faced by the organisation concerned adequately reflects the overall loss, inconvenience and distress suffered by those individuals in both the short and long term.

It is particularly difficult to justify a £500,000 maximum fine in the case of large organisations with very high turnovers. Whilst regulatory bodies such as Ofcom, Ofwat and the OFT are capable of dispensing fines amounting to several million pounds in relation to their particular fields, a maximum fine from the ICO of £500,000 could look insignificant in relation to corporate entities with substantive turnovers.

We fail to see why the misdeeds of corporate entities in relation to bid rigging; cartels; price fixing and other similar anti-competitive practices should be differentiated in this manner. The end result of such bid rigging; cartels; and price fixing is potential harm to the consumer by increased prices for goods; reduced services or lack of choice. Why should the financial penalty to the corporate entity be potentially greater where say fixing prices for airline travel has resulted in the consumer paying more for their airline ticket; but where a large corporate entity is wilfully negligent in undertaking the security of sensitive personal it can suffer no greater than a £500,000 fine. The consequences of the loss of sensitive personal data potentially go much further than that of an overpriced airline ticket.

It does not make sense to give such regulators the power to hand out extensive and potentially business threatening penalties against offenders in consumer-based markets, but then fail to allow a similar power to be exercised in data protection cases, which will also cover those in consumer markets, and will cause potentially greater harm to those affected.

Given the likely emotional and financial harm that victims of personal data loss may endure, and the potential for large organisations and corporate entities to escape a proportionate financial penalty, it appears to us that the setting of a cap on the potential fine is inherently wrong and could be seen as "a cost of doing business" by those more unscrupulous organisations. In our view the power to penalise serious offenders should at least be on the same level as the power held by the likes of the OFT, in other words ensuring that the ICO is given the power to fine an organisation the equivalent of 10% of their annual turnover, irrespective of whether such a figure could be greater than £500,000.

It is well established that the ICO will consider any mitigating factors where attempts have been made to safeguard personal data, before taking action, and will obviously take into account an organisation's turnover and its ability to operate as a consequence of paying a fine. Only in the most severe cases would such a high penalty be imposed. It is therefore appropriate to allow the ICO to exercise the widest possible discretion in dealing with cases of data protection breaches.

Where putting into place such measures, it is equally important to ensure that data controllers are given clear and comprehensive guidance on how to meet its compliance requirements and the potential penalties for abuses. In light of the increasing number of high profile losses of personal data, data controllers should be encouraged to undertake both internal and external data protection audits, and also to seek advice on how to improve their data protection policies and training programmes, in particular covering such topics as: the use and encryption of portable media devices (such as laptops and USB drives); downloading of data; carrying out risk assessments of the internal and external transferring of data; safe disposal of data; and contingency plans for when a breach occurs.

There remains however a need to address the issue of breaches by "public authorities". It would appear that for any serious contravention of the data protection principles any penalty imposed results in the general public itself being penalised not just once but twice for the wrong doing of those in such an organisation; firstly in respect of the loss of the data; and secondly in respect of any fine to be paid (such fine effectively being paid out of the very public funding intended to fund the activities of the organisation). Where such breaches occur should it not be the case that the officials who lead and run such organisations are the recipient of such fines, just as those directors of companies who commit cartel breaches can be fined and even go to prison for their misdemeanours? This issue has yet to be addressed by any consultation thus far.

**MACROBERTS LLP**

16 December 2009