ThirtyNine
ESSEX STREET

MONETARY PENALTY NOTICES

RORY DUNLOP

Thirty Nine Essex Street

Introduction

1. The purpose of this paper is to provide an introduction to monetary penalty notices. The law is complex and you cannot assume that the ICO has got it right, even though they have published guidance for themselves to follow.[1]

2. Before issuing a monetary penalty notice, it is necessary for the ICO to establish the following:
   (1) There has been a contravention of the data protection principles;[2]
   (2) That contravention was serious;[3]
   (3) The contravention was of a kind likely to cause substantial damage or substantial distress;[4]
   (4) The data controller knew or ought to have known that there was a risk that the contravention would occur and would be of a kind likely to cause substantial damage or substantial distress and failed to take reasonable steps to prevent it;[5]
   (5) In the circumstances, a MPN is appropriate; and
   (6) A notice of intent has been properly served.[6]

(1) The data protection principles

3. The crucial data protection principle is almost always the seventh one which provides:

   "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

[1] https://ico.org.uk/media/for-organisations/documents/1569/ico_guidance_on_monetary_penalties.pdf
[2] S.55A(1)(a) of the Data Protection Act 1998 ("the DPA")
[3] S.55A(1)(a) of the DPA
[4] S.55A(1)(b) of the DPA
[5] S.55A(3) of the DPA
[6] Section 55B of the DPA

4. The First Tier Tribunal and the Upper Tribunal have stressed the need for the ICO to identify, with clarity, what contravention of data protection principles he is relying on, when issuing a MPN. Otherwise, there is a real risk of error when assessing the seriousness of the contravention and its likely consequences (see *Scottish Borders Council v ICO* (EA/2012/0212) at [21]; *Information Commissioner v Niebel* [2014] UKUT 0255 (AAC) at [25]-[41]).

5. Two things follow. First, it is important to distinguish between the breach of the data protection principles and the trigger incident.

6. *Scottish Borders Council v Information Commissioner* (EA/2012/0212) is an example of this. It began with an overflowing bin outside Tesco, where a member of the public found files containing the pension records kept by the appellant local authority Scottish Borders. A data processing company had turned Scottish Borders files into CDs and then dumped the files in bins. So far as anyone was aware, no actual harm resulted. The ICO imposed a MPN of £250,000 on Scottish Borders.

7. The FTT allowed the appeal, holding that:
   (1) Scottish Borders were in contravention of DPA, Schedule 1 Part 2, para 12(b) because its contract with the data processor did not impose the same obligations on the processor as it had itself – para. 32.
   (2) It was necessary to focus on the likely harm that would flow from the contravention, rather than from the trigger incident (i.e. what happened at the paper recycling bin) – para. 38.
   (3) The test of 'likelihood' requires something more than a mere possibility – para. 43.
   (4) In this case, the contravention was not likely to cause substantial damage or distress. The data processor had a relationship of 25-30 years with the council and they had good reason to trust him. What happened was a surprising outcome, not a likely one.

8. Likewise, I have had a case that involved the ICO wanting to fine a local authority because a personal computer with sensitive data was stolen from a councillor's home. In the notice of

intent, the ICO failed to distinguish between the contravention (i.e. failing to conduct a risk assessment in relation to the use of personal emails) and the trigger incident (i.e. the theft of the computer).

9. Secondly, the ICO can only rely on the contravention identified in the notice, not on something else. *Niebel* is a good example of this. It involved a company that was engaged in 'sending unwanted text messages on an industrial scale' seeking potential claims for mis-selling of PPI loans or accidents, contrary to Regulation 22 of the Privacy and Electronic Communications (EC Directive) Regulations 2003. In the appeal against the MPN, it was crucial that the ICO had only relied on 286 of the many thousands of unwanted texts. This was too low a number for it to be likely that they would cause substantial damage or distress.

(2) Contravention was serious

10. *Niebel* is potentially helpful here. It is authority that the ICO cannot have regard to incidents, which are not part of the pleaded contravention, when considering whether that contravention was serious (see *Information Commissioner v Niebel* [2014] UKUT 0255 (AAC) at [28]-[41]). Thus, in my computer case, we argued that it was impermissible to have regard to the fact that the local authority may have been guilty of other incidents in the past – that was a factor which could only have come into the reckoning at a later stage if there was a serious contravention.

(3) Of a kind likely to cause substantial damage or distress

11. When considering this question, the ICO needs to focus on the contravention, not on the trigger incident, and see if there is a likely chain of events which would lead to substantial damage or substantial distress (see *Scottish Borders Council v ICO* (EA/2012/0212) at [38]-[47]).

12. The ICO does not need to prove that substantial damage or distress was actually caused (*London Community Healthcare NHS Trust v IC* (EA/2012/00111)). However, it does need to show that such damage or distress was 'likely'.

13. The ICO routinely finds that such distress was 'likely' even in cases where one might have thought it was unlikely. In *Central London Community Healthcare NHS Trust v IC* (EA/2012/00111), the appellant Trust had been faxing highly sensitive medical information in relation to patients receiving palliative care to the wrong fax number. Eventually a member of the public telephoned to say that he had been receiving these faxes and shredding them. The Trust reported itself and cooperated fully with the investigation. The ICO decided to fine the trust £90,000. No substantial damage or distress had been caused but the ICO and FTT thought it was likely to be caused because very sensitive personal data was being sent out to the public.

14. In the North East Lincolnshire Council Decision Notice of 15 October 2013[7] a teacher lost an unencrypted memory stick with sensitive personal data relating to children. The ICO thought it was likely that not encrypting memory sticks would lead to substantial damage and/or distress. The ICO relied both on the data subjects' distress at knowing that the sensitive personal data may have been accessed and on the possibility that 'untrustworthy third parties' might expose them to 'damage to their health, education and personal relationships'.

15. The distress of the data subjects in knowing that their personal data might have been accessed is often relied on by the ICO – see Aberdeen City Council notice of 27 August 2013.[8]

16. That does not mean that you cannot push back, or that the FTT would take the same approach. In my stolen computer case, the computer was password protected and the sensitive personal data was buried among many thousands of emails. We argued that it was

[7] https://ico.org.uk/media/action-weve-taken/mpns/2658/north-east-lincs-council-monetary-penalty-notice.pdf
[8] https://ico.org.uk/media/action-weve-taken/mpns/2652/aberdeen-cc-monetary-penalty-notice.pdf

very unlikely that the burglars would break the password and access the sensitive personal data. We also argued that the chance was so remote that it was not appropriate to tell the data subjects.

(4) The data controller knew or ought to have known that there was a risk that the contravention would occur and would be of a kind likely to cause substantial damage or substantial distress and failed to take reasonable steps to prevent it

17. This highlights the importance of having written policies and risk assessments and training. If your client has a policy of doing things in a way that complies with data protection principles and you train the staff but one member of staff failed to comply with that policy on one occasion, you can argue that your client took reasonable steps to prevent the contravention and the distress/damage. That won't work if the policy is routinely being ignored, or if the policy is not backed up with training (see *North East Lincolnshire* case).

(5) Whether a MPN is appropriate

18. The ICO explains in its guidance that it will have regard to a number of factors:
    (1) Seriousness of the contravention;
    (2) Likelihood of damage or distress;
    (3) Degree of fault;
    (4) Need to maximise deterrent effect.

19. Self-reporting is not a mitigating factor but failing to report would be an aggravating factor (*Central London Community Healthcare NHS Trust v IC* [2013] UKUT 0551 (AAC) at [128]).

20. If an MPN is appropriate, the ICO will then look at wider behavioural issues of the organisation (e.g. past breaches). In some cases, it will look at number of reports but that is inappropriate. It should only have regard to the number of previous breaches (but not the number of previous reports) and the ICO should, in my view, compare that with the size of the organisation. A few contraventions by a very large organisation is arguably less

significant than the same number of breaches by a small organisation. The maximum MPN is £500,000.[9]

(6) Notice of Intent

21. Section 55B(1) requires the ICO to serve a notice of intent before serving a MPN. This notice of intent must inform the data controller:
    (1) that he may make written representations against the proposal to serve a MPN within a period specified in the notice;[10] and
    (2) the name and address of the data controller or person;[11]
    (3) the grounds on which the Commissioner proposes to serve a monetary penalty notice, including the following[12]-
        (i) the nature of the personal data involved in the contravention;
        (ii) a description of the circumstances of the contravention;
        (iii) the reason the Commissioner considers that the contravention is serious;
        (iv) the reason the Commissioner considers that the contravention is of a kind likely to cause substantial damage or substantial distress; and
        (v) whether the Commissioner considers that section 55A(2) applies, or that section 55A(3) applies, and the reason the Commissioner has taken this view; and
    (4) an indication of the amount of the monetary penalty the Commissioner proposes to impose and any aggravating or mitigating features the Commissioner has taken into account;[13] and
    (5) the date on which the Commissioner proposes to serve the monetary penalty notice.[14]

[9] See Reg. 2 of The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010
[10] See s. 55B(3)(a) of the DPA.
[11] See Reg. 3(a) of The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010
[12] See Reg. 3(b) of The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010
[13] See Reg. 3(c) of The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010
[14] See Reg. 3(d) of The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010

22. The data controller can appeal against any MPN under s.55B(5) of the DPA. If there is a failure to comply with these procedural aspects that is arguably a ground to allow the appeal – i.e. that the notice was in accordance with the law. However, if the data controller appeals, they lose the right to obtain the early payment discount (*Central London Community Healthcare NHS Trust v IC* [2013] UKUT 0551 (AAC) at [71]). Also, although a data controller can appeal on quantum only,[15] the FTT will only look at whether the fine was 'within a range of reasonable responses' (*Central London Community Healthcare NHS Trust v IC* [2013] UKUT 0551 (AAC) at [139]).

RORY DUNLOP

[15] S. 55B(5)(b) of the DPA