FIRST-TIER TRIBUNAL
GENERAL REGULATORY CHAMBER
Information Rights

Tribunal Reference:	EA/2012/0212
Appellant:	Scottish Borders Council
Respondent:	The Information Commissioner
Judge:	NJ Warren
Member:	J Nelson
Member:	P Taylor
Hearing Date:	20 and 21 March, 17 and 18 July 2013
Decision Date:	21 August 2013

DECISION NOTICE

A. Introduction

1. Outside Tesco in South Queensferry there are some bins for recycling waste paper. They are of the "post box" type. On 10 September 2011 a member of the public found that one of the bins was overflowing. The material at the top, easily accessible, consisted of files containing pension records kept by a local authority ("Scottish Borders"). It turned out that a data processing company had transferred the information from hard copy files to CDs at Scottish Borders' request. The data processor had then disposed of about 1,600 manual files in the post box bins at Tesco and at another supermarket in the town.

2. The police took into their possession all those files which they could reach. They then secured the bins and, with the cooperation of Scottish Borders, it was ascertained that the files concerned had now either been pulped without manual intervention or were now back in the safe keeping of the council. So far as anyone can tell, no actual harm resulted. After this incident the Information Commissioner

(ICO) imposed a monetary penalty not on the data processor but on Scottish Borders amounting to a quarter of a million pounds. Scottish Borders have appealed against that decision.

3. We were assisted at the hearing of the appeal by Mr Hopkins, who appeared for the ICO, and Mr Motion and Ms Irvine who appeared for Scottish Borders. We record our thanks to all three.

4. This decision notice gives our conclusion on the preliminary issue of the liability of Scottish Borders to pay a monetary penalty.

B. Monetary Penalties

5. The Data Protection Act 1998 (DPA) has always contained (in section 13) a right to sue for compensation for damage, or in some circumstances distress, resulting from a contravention of the Act. It also proscribes (in section 55) some criminal offences.

6. The Criminal Justice and Immigration Act 2008 inserted new sections 55A – 55E which from 6 April 2010 gave the ICO power to impose monetary penalties, or in plain language, fines, on data controllers. There is a maximum of £500,000.

7. By Section 4(4) DPA a data controller must comply with the Data Protection Principles (DPPs) in relation to all personal data with respect to which he is the controller. By Section 55A a data controller who contravenes Section 4(4) may be subject to a monetary penalty if certain other conditions are satisfied. Those conditions can conveniently be divided, at the expense of using old fashioned Latin, into "actus reus" or the guilty act; and "mens rea" or the guilty mind.

8. In respect of the act, the contravention must be serious and it must be "of a kind likely to cause substantial damage or substantial distress".

9. In respect of the mind, the contravention must be "deliberate" or alternatively, it must be shown that the controller:-

   (a) knew or ought to have known that there was a risk of contravention AND

(b) knew or ought to have known that such a contravention would be of a kind likely to cause substantial damage or substantial distress AND

(c) failed to take reasonable steps to prevent the contravention.

This is something of a paraphrase. The precise wording is to be found in Section 55A DPA.

10. The Act and subsequent regulations impose procedural and policy requirements on the ICO.

11. The imposition of a monetary penalty is discretionary. The ICO may choose instead to use other powers given to him under the Act or indeed to take no action at all. It is convenient to refer to this step in the process as “the penalty discretion”.

C. Some General Points

12. The powers of the Tribunal are to be found in Section 49 DPA and are in terms very similar to Section 58 Freedom of Information Act. There are now enough dicta of the superior courts describing the Tribunal’s jurisdiction as a “full merits review”, practically indistinguishable from an appeal on fact and law. The ICO submits, and we accept, that we have a similar role under the DPA.

13. The ICO also submitted that it would be wrong for us to ignore the statutory guidance prepared by him. We accept this submission also. However, even though the guidance has been laid before Parliament, it remains the ICO’s document and he is one of the parties to the appeal. The guidance is not binding on us in the sense that a statute or a statutory instrument is.

14. One general question hovering over this appeal is whether proceedings in respect of monetary penalties are “criminal” in nature. There are certainly enough indications, not least in the title of the amending statute, to make an arguable case for them being so. In a sense, the European Convention on Human Rights (ECHR) is not of direct relevance here because Scottish Borders is not a private legal person; arguably, however, they are entitled to similar standards of fairness under

ordinary Scottish law. We have concluded that there is no need for us to make any decision or pronouncement in the abstract; but there is a need for us to be vigilant to ensure that the proceedings are fair.

15. One aspect of this fairness relates to the date on which the monetary penalty provisions of the Act came into force – 6 April 2010. In our judgement there can be no penalty imposed for any contravention which is alleged to have taken place before this date; although it is right for us to draw on events which took place before then, where relevant, in assessing the evidence.

16. Another aspect of fairness is that the data controller must have clear notice of the activity for which it is being penalised. The detail of the contravention alleged is inevitably subject to some variation. Indeed the requirement that the process should include a "notice of intent" implies some opportunity for the data controller and the ICO to enter into discussion before the case reaches the stage of a penalty. We reject the submission made on behalf of Scottish Borders that they have been unclear as to what the case is against them. It seems to us that they have had clear notice that the alleged contravention relates to the arrangements they made for digitising pension records in summer 2011. If it was not clear before, the allegation is succinctly set out in para 8 of the ICO's skeleton argument delivered to Scottish Borders four months ago.

17. It is true that matters have not always been set out so plainly. In the course of the ICO investigation reference was made to concerns about other databases. The ICO now concedes that in assessing the amount of the monetary penalty he took into account information concerning one database even though this factor did not appear in the list of aggravating features in either the notice of intent or the penalty notice itself. We need not consider at this stage whether this was a proper course of action as it relates not to liability but to the amount of any monetary penalty (and possibly the penalty discretion).

18. Still on themes relating to the criminal law, Scottish Borders submitted that we should apply the criminal standard of proof in this appeal. They referred to R McCann v Manchester Crown Court (2002) UKHL 39 and Chief Constable of

Lancashire v Potter (2002) EWHC 2272 (Admin) as examples of circumstances in which it was held that the criminal standard of proof can apply even to proceedings which were characterised as "civil".

19. McCann, by which decision the court in the later case was bound, was argued and discussed in the context of what was then thought to be a "heightened" civil standard of proof. On this, see now In Re B (Children) (2008) UKHL 35.

20. In our judgement the statute itself here gives us sufficient guidance on which to conclude that parliament's intention was that the ordinary civil standard of proof applies. The offences in s55 are dealt with by proceeding in the criminal courts according to their rules, conventions and procedures. By contrast, the new s55A places the decision on whether to impose a monetary penalty on the ICO, someone who has traditionally decided issues on the balance of probabilities. Moreover, the right of appeal is to the Tribunal, not to a criminal court. We conclude that parliament intended the civil standard of proof to apply.

D. Was there a contravention?

21. At times in these proceedings it has seemed as though Scottish Borders conceded that there had been a contravention. At times their position seems less sure. It matters not because, in any event, there is a need for us to identify the contravention and the circumstances surrounding it reasonably clearly. Unless this is done, there is a real risk of error when it comes to assessing the seriousness of the contravention; its likely consequences; and the amount of any penalty that should follow.

22. The DPPs are set out in Schedule 1 Part 1 DPA. The seventh DPP is:-

> "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".

23. The DPPs are interpreted in Schedule 1 Part 2 DPA. Paras 9-12 are relevant to the seventh DPP and read as follows:-

The seventh principle

9 Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to—

(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and

(b) the nature of the data to be protected.

10 The data controller must take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.

11 Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle—

(a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and

(b) take reasonable steps to ensure compliance with those measures.

12 Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless—

(a) the processing is carried out under a contract—

(i) which is made or evidenced in writing, and

(ii) under which the data processor is to act only on instructions from the data controller, and

(b) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

24. We turn to consider the arrangements which Scottish Borders made with the data processor. Their business relationship was of long standing, some 25-30 years if you take into account the data processor's dealings with predecessor authorities. The data processor carried out work for several different departments of the council. The company's business had become smaller than it was in recent years. Originally the data processor arranged for a large paper waste company to destroy hard copy files which had been scanned but, unknown to Scottish Borders, the data processor ceased to use them from 2008 and had no secure destruction arrangements from then on.

25. Scottish Borders made arrangements for the scanning of pension records once every three years. These records related to what might be called "early leavers". They were former employees who had either received a refund of their pension contributions or who still retained some pension entitlement that they would be able to draw on when reaching pension age. Typically the files contained a name, an address, date of birth, national insurance number and salary. In some cases the files contained bank account details, a signature, a nominee to receive benefits in the event of death, and in a small number of cases a reason for leaving. This might refer to ill health but it is accepted that whilst there was much private personal data involved, it did not extend to the "sensitive personal data" to which the DPA gives special protection. In July and August 2011 there were two or three batches of files involved, 1,600 in total.

26. When Scottish Borders were making arrangements for the 2005 round of scanning, one of their employees made the following enquiry of the data processing company:-

> "As you will appreciate the information that is to be scanned is personal information relating to individual scheme members. Can you provide me with any guarantees or assurance about the security and confidentiality of the data?"

The reply was:-

> "Yes. 99% of the work we do is confidential to our customers. All our staff are even MOD cleared for security but I can assure you I will personally collect the files in batches that can be brought here and scanned within the shortest time it takes and return to your self with the CDs."

27. About a year before the 2011 arrangements the data processor told the same employee (who was shortly to leave Scottish Borders employment) what his up to date prices were. The email included the statement:-

> "Finally, pick up and delivery and destruction of documents or return is charged at £25 per round trip."

No one suggests that in 2011 the arrangement was for the processor to return the files to Scottish Borders. We deduce therefore that on this occasion the data processor was accepting responsibility for "destruction."

28. How did all this fit in with the obligations of a data controller under Schedule 1 Part 2 DPA when making contracts with a data processor? It was obviously defective.

29. Para 11(a) required an informed choice of processor who should be able to provide sufficient guarantees in respect of technical and organisational security measures. In place of this there was no more than a sincere but somewhat generalised attempt for reassurance some six years earlier.

30. It followed that no action to ensure compliance was possible under para 11(b).

31. To some extent, but not fully, the contract for processing was evidenced in writing. However para 12(a)(ii) which requires a clause in the contract that the processor is to act only on instruction from the controller was simply not complied with. The same applies to para 12(b).

32. We therefore conclude that the arrangements made by Scottish Borders for processing pension records in July and August 2011 were in contravention of the DPA.

33. The papers refer to the CDs being returned by post on this occasion in unencrypted format but we were not asked to draw any conclusions on seriousness or harm from these facts. It is possible that information to be consulted in 20-30 years time may be at greater risk of loss if encrypted. We need not explore this issue further. It is perhaps just a symptom of the failure to keep control of the data.

E. Was it Serious?

34. Our answer to this question is "yes".

35. The first reason for this conclusion is that the duties in relation to data processing contracts in paras 11 and 12 of schedule 1 are at the heart of the system for protecting personal data under DPA. It is fundamental that the data controller cannot be allowed to contract out its responsibilities.

36. Our second reason for this conclusion is that the contravention was not an isolated human error. It was systemic.

37. For Scottish Borders, Mr Motion tried to persuade us that this was merely the action of a rogue employee who had failed to follow his employer's guidance by not obtaining the data processor's signature to a standard form "confidentiality/disclosure" agreement. We reject that contention. The agreement to which he referred (page 1160) may have been in general use by the council when dealing with outside contractors of any kind. It is, however, entirely inapt for a data processing contract and does not contain the safeguards required by the DPA. The reality was that Scottish Borders had no system for ensuring that the Act was observed in data processing contracts of less than £5,000. Nor was there any obvious system for those contracts of less than £20,000. Contracts above this level were the responsibility of a central procurement team and we have seen an example of one such large contract which did contain the provisions required by statute. There was no training provided by the council for any of the managers who were entering into data processing contracts of less than £20,000 on its behalf.

F. Was the contravention of a kind likely to cause substantial damage or substantial distress?

38. Turning to this question, it is right to record the repeated reminders from Mr Hopkins that we must focus on the contravention. We accept the importance of this especially because at some stages of the investigation confusion may have resulted from focussing on what happened at the paper recycling bins ("the trigger incident"). There will be some cases in which the contravention and the trigger incident are one and the same but the case put against Scottish Borders is not one of them.

39. Mr Hopkins also correctly reminded us that we have to assess whether the contravention was "of a kind likely to …." It was unnecessary for the ICO to establish that any actual harm had occurred. Actual substantial damage or actual substantial distress is not a necessary condition of liability to a monetary penalty; nor we would add is it a sufficient one. Sometimes harm can be caused which is unexpected or unlikely; or it can result from a contravention which is not serious.

40. In making our assessment of "likelihood" we do not consider that we are called upon to construct abstract categories of contravention, even if that were possible. We have to look at all the relevant circumstances. Only thus can we take into account such important issues as the nature of the data involved.

41. The test of likelihood was the subject of some debate before us. It was submitted on behalf of Scottish Borders that we had to be satisfied that substantial distress or substantial damage would "on the balance of probabilities" flow from the contravention. Mr Motion and Ms Irvine were able to point to the ICO's own statutory guidance to that effect.

42. At the hearing Mr Hopkins was cautious about this guidance and referred us to R(Lord) v Secretary of State for the Home Department (2003) EWHC 2073 (Admin) especially at paras 99-100.

43. In our judgement Mr Hopkins was right to be cautious. The wording of the statute should not be confused with the terms in which lawyers express the civil standard of proof. As a matter of common experience, a single event may have two, three or more possible outcomes. Depending on the facts, two or more of those might reasonably be considered either "likely" – or "likely" to produce a given effect. It is true that in a civil trial a judge may be duty bound to find as a fact that just one outcome was "more" or "most" likely. No such duty is to be found in section 55A. It suffices for it to be likely that substantial distress or substantial damage should be caused. At the same time of course it is insufficient to point to such consequences merely being a possibility.

44. The statutory guidance includes definitions of "damage" and "distress". We have not felt in this case any need to define the ordinary English words "substantial damage" and "substantial distress" and it can sometimes be misleading to separate out single words from phrases.

45. The ICO's case on this question has developed somewhat over time. On this issue, the ICO penalty notice states:-

> "The Commissioner is satisfied that the contravention was of a kind likely to cause substantial damage or substantial distress to data subjects whose confidential personal data (including financial information) was seen by a member of the public who had no right to see that information.
>
> "Further, the data subjects would be justifiably concerned that their data may have been further disseminated even if those concerns do not actually materialise. If the data has been disclosed to untrustworthy third parties then it is likely that the contravention would cause further distress and also substantial damage to the data subjects such as exposing them to identity fraud and possible financial loss."

This passage is not particularly easy to follow and seems to be focussed on the trigger incident rather than the contravention. On the second day of the original hearing the ICO sought and was granted an adjournment to obtain evidence on the question of identity theft. He now relies additionally on that evidence and on two statements filed by one of the deputy commissioners, Mr Smith.

46. Having considered all the relevant circumstances we were not satisfied that the contravention in this case was of a kind likely to cause substantial damage or substantial distress. No doubt some breaches of the seventh DPP in respect of some data might be of such a kind. In this case, it seems to us that the fact that the data processor was a specialist contractor with a history of 25-30 years of dealings with

Scottish Borders carries weight. He was no fly by night. The council had good reason to trust the company.

47. Focussing on the contravention we have been unable to construct a likely chain of events which would lead to substantial damage or substantial distress. What did happen was of course startling enough. Again, though, looking at the facts of the case, what did happen was in our view a surprising outcome, not a likely one. The overwhelmingly likely result of the summer 2011 arrangements, it seems to us was that the data processor would arrange for the files to be properly destroyed – to the extent that we would not describe any other outcome as likely.

48. It was perhaps not without significance that when Mr Smith gave oral evidence to us his starting point seemed to be the trigger incident. He said:-

> "It's by going to the recycling point. The way they were put in to the skips."

During his evidence he referred to a number of scenarios as "possible" including one which he described as "an extreme example". He did not discuss these possibilities in terms of likelihood.

49. In a statement filed subsequently, Mr Smith does speak of likelihood but he still seems to focus on the trigger incident (see paras 13 and 15). We simply cannot accept his suggestion for example that it was likely that a newspaper would want to publish extracts from the early leavers' pension files given that he does not specify how it was likely that a newspaper should obtain them in the first place.

50. On the possibility of identity fraud, the ICO relied on the evidence of Mr Middleton who is a director of Delmont-ID Ltd. He has spent 30 years as a detective constable, the last three and a half years of which were spent in a special unit dealing with false identity crime. It seemed to us that for most of that time he had been concerned with the use of documents forged on computers rather than the use of genuine documents (see especially paras 10-11). Mr Middleton asserts (para 5) that without adequate controls over the disposal of the files that the information in them was in his view likely to come into the hands of people not authorised to

access it. He adds further that as it was likely to come into unauthorised hands then it was also likely to come in to the hands of those wishing to commit identity related crime. Scottish Borders relied on the contrary opinion of Mr Gee. Subject to one caveat we preferred the evidence of Mr Gee to that of Mr Middleton.

51. First, without being disrespectful of Mr Middleton, it seemed to us that Mr Gee's expertise in this area was both broader and at a much higher level. He is director of counter fraud services for a large global accountancy and business services firm. He is visiting professor at and Chair of the Centre for Fraud studies at the University of Portsmouth. He has provided expert guidance to a number of government departments and committees. By and large, we accept his analysis of Mr Middleton's more diffuse evidence and, whilst we do not consider that the answer to the question before us is to be found entirely in arithmetic and statistics, it seems to us that Mr Gee's report buttresses our own conclusion on likelihood. Mr Gee even goes further and argues cogently from the paper bank incident that substantial damage or substantial distress was unlikely. His conclusions are supported by a detailed field assessment.

52. Our one reservation about Mr Gee's evidence is that although at para 30 he rightly states that the tribunal is primarily interested in what is "likely" rather than what is merely "possible", in one paragraph (para 57) he seems to equate this, as we have not done, with the civil standard of proof. We noted this but did not consider that it affected the validity of the conclusions in his report on which we rely.

53. Our conclusion therefore was that there was no liability to a monetary penalty in this case because looking at the facts and circumstances of the contravention, whilst it was serious, it was not of a kind likely to cause substantial damage or substantial distress.

54. The effect of the Data Protection (Monetary Penalties) Order 2010 SI 910 is that we may therefore either allow the appeal or substitute such other notice or decision as could have been served or made by the ICO. On the information we have so far we were not prepared to simply allow the appeal. Our concerns about Scottish Borders' procedures in relation to contracts for data processing were too serious for

that. We delay consideration of whether to issue an enforcement notice or take some other action to allow a conversation to take place between Scottish Borders and the ICO about the placing of data processing contracts and the training given to staff involved. It may be possible for the parties to agree a way forward.

G. Unfinished Business

55. It is almost always a mistake to give in to the temptation to comment on other issues canvassed in the course of an appeal but which it has not been necessary to resolve. However, in a comparatively new legal regime it may be helpful to draw attention to some other potential difficulties to allow time for contemplation before their resolution.

(a) Deliberate contraventions – We have indicated that one of the two forms of "mens rea" or "guilty mind" which can found liability for a monetary penalty is that the contravention should be "deliberate". In a number of the materials before us it seems to be assumed that this involves knowingly breaking the law rather than deliberately doing an action which is a contravention. It has never been suggested that "contravention" in section 13 DPA requires a claimant to prove that a defendant knew they were breaking the law. It may also be that taking this view makes it difficult to apply the alternative "mens rea" to acts which are deliberate.

(b) The significance of actual harm – It is clear that there may be liability for a penalty based on potential or, to be more correct, likely harm. There is no need to demonstrate actual harm. It would follow that the extent of the likely harm would be a factor to consider in fixing the amount of a penalty. Scottish Borders argued that insufficient attention had been paid to the fact that, in the end, so far as anyone can tell, no one suffered from the contravention in this case. In oral evidence advanced by the ICO, it was suggested that this did not matter. It may be necessary at some future stage to explore the rationale for saying that the extent of harm caused cannot be reflected in the amount of the penalty or in the exercise of the penalty discretion.

(c) Admissions and self reporting – It is traditional for penalties to be discounted where liability is not contested. One point made by Scottish Borders in this appeal was that insufficient credit had been given for their willingness to respond to the trigger incident and to report it to ICO. Although the argument was not developed before us the ICO did not seem to suggest that self reporting was an irrelevant factor in the amount of a penalty. Rather, (see page 1189) the way to deal with it was to increase the penalty of a data controller who did not self report. At some stage, it may be necessary to consider whether this novel approach gives adequate prominence to a factor, which seems to be agreed to be relevant, in the reasons given for the amount of any penalty. It may also be asked whether self reporting is a relevant factor in the exercise of the penalty discretion.

(d) Early payment scheme – The ICO operates an early payment scheme. There is a discount of 20% if payment is made within 28 days. In the ICO's response to this appeal, it was submitted that any data controller who makes an early payment under the scheme "effectively forfeits its right to appeal". Scottish Borders took strong exception to this suggestion. At some stage the question may have to be answered as to whether this approach constitutes an unfair obstacle to access to the judiciary.

NJ Warren
Chamber President
Dated 21 August 2013