in the agreement are that at some time the information will be obsolete and no longer important to the owner and, since the recipient is following special procedures to ensure confidentiality, it should be obliged to do so only to the extent to which it actually matters. Setting boundaries in this way is also easier for evidential purposes.

If the owner anticipates that the information really needs to remain confidential beyond a foreseeable period, it is generally preferable not to insert any time-limit. However, given the problems associated with monitoring and policing the security of the confidential information, particularly as time goes by and the individuals involved move on and are replaced, open-ended obligations should be reserved for exceptionally sensitive information which is unlikely to become desensitised over the foreseeable future.

Three or five years is normally the maximum term agreed, but the periods of time may vary from one part of the IT industry to another.

Administrative arrangements

A cavalier approach to the administrative aspects of NDAs can be a costly mistake for both discloser and recipient. In the event of a claim, in addition to establishing that information disclosed in confidence has been compromised in breach of contract, a discloser will have to be able to demonstrate that it has appropriate rules and controls in place to protect its confidential information: if the discloser does not think such steps are necessary, a court is hardly likely to be persuaded that the information in question was confidential for the purposes of the NDA. Similarly, a recipient who does not operate a credible system of controls will be in some difficulty when attempting to defend a claim that the terms of the NDA have been breached. Authorised signatories of both parties should sign an NDA only if they are satisfied that adequate administrative processes are in place within their respective organisations to manage the confidential information.

Information that is genuinely confidential and essential for the business transaction or relationship contemplated, should be treated seriously and made the subject of an enforceable NDA. ●

Paul Klinger is Sole Principal at Paul Klinger and Company and General Counsel at Speed-Trap Holdings Limited.

Rachel Burnett is a partner and heads the IT/IP team at the firm of Paris Smith LLP.

The third edition of Paul Klinger and Rachel Burnett's *Drafting and Negotiating IT Contracts* has recently been published by Bloomsbury Professional.

Data Protection Monetary Penalties: Absolutely Criminal?

A Tribunal has quashed two 'Civil Monetary Penalties' totalling £550,000. **Paul Motion** and **Laura Irvine** argue that such Monetary Penalties are properly categorised as criminal, with significant consequences for both the Information Commissioner and a data controller under investigation. See also, *Cake or Death?* (online or a bonus track in the e-pub version of this issue)

Monetary penalties

Since 6 April 2010 the Information Commissioner's Office has been able to impose monetary penalties of up to £500,000 in relation to certain breaches of the Data Protection Act 1998 by data controllers. These penalties were introduced following high profile security breaches by government departments, most notably the loss in 2007 of two CDs by HMRC containing the personal data of 25 million UK citizens. The power was granted by amending the DPA so as to insert new ss 55A to 55E. The new sections provide for Monetary Penalty Notices (MPNs) and the Notice of Intent Procedure. At no point does the legislation mention the description 'civil' in relation to monetary penalties though this term appears now to be in use on a relatively frequent basis.

The legislation chosen to introduce MPNs was the unlikely vehicle of the Criminal Justice and Immigration Act 2008, covering matters as diverse as nuclear terrorism, extreme pornography and criminal sentencing. As the DPA amendment was introduced at a relatively late stage in proceedings, there was limited Parliamentary debate in relation to MPNs. However, the choice of

an overtly *criminal* statute as the preferred delivery mechanism for MPNs is very pertinent to the thrust of this article.

A MPN can only be imposed in cases where:

- there has been a serious breach of the DPA;
- the breach was of a kind likely to cause substantial damage or substantial distress; and
- (i) the breach was deliberate *or* (ii) the data processor knew or ought to have known that the breach would be of a kind likely to cause substantial damage or substantial distress *and* the data processor failed to take reasonable steps to prevent the contravention.

Guidance

The DPA obliges the ICO to publish Guidance about MPNs. The first edition was published in January 2010, replaced by a January 2012 edition that also dealt with the issuing of MPNs for breaches of the Privacy and Electronic Communications Regulations ('PECRs'). This further power was made available to the ICO from 26 May 2011. The ICO has now also published its Standard Operating Procedures,[1] a Framework for Determining the Appropriate Amount of Monetary Penalty[2] and the Data Protection Regulatory Action Policy[3] which gives us some indication as to how MPNs ought to be calculated by the ICO.

Breach procedure

If the ICO becomes aware of a DPA or PECR breach, it will investigate and decide what action to take. Breaches can be self reported, though presently there is no obligation on data controllers to do so. If, after investigation, the ICO considers that it can impose a MPN, it has a discretion to do so. The data controller is served with a Notice of Intent upon which it may comment and thereafter the final MPN notice is issued.

Once a MPN has been imposed, the data processor has 28 days within which to appeal the penalty to the Information Rights Tribunal. This can be an appeal against liability and quantum, or effectively an appeal against conviction or sentence. In the *Central London Community Healthcare* appeal[4] the Tribunal decided that it could carry out a full merits *de novo* review where the Tribunal can start again and hear factual evidence, whether or not this has been considered by the ICO, to make its decision on whether the MPN is validly imposed and thereafter whether the amount is correct.

Appeals

Although several dozen MPNs have been issued, there have been few appeals. To date, the Tribunal has heard only three appeals. The first appeal (by Central London Community Healthcare NHS Trust) against a MPN of £90,000 was unsuccessful in March 2013.

The second appeal[5] was made by the Scottish Borders Council ('SBC') following the imposition of a MPN of £250,000. This appeal heard over four days in March then July 2013 was successful. The ICO seemed to endorse the *de novo* hearing approach in the *Scottish Borders* appeal. The Tribunal decided that it was not satisfied on liability and the MPN was cancelled.

A third appeal,[6] by Christopher Niebel in October 2013, involved a breach of PECRs and was also successful with an even higher (£300,000) fine imposed on an individual director being cancelled. *Niebel* was a very high profile case in the sense that Mr Niebel did not dispute sending hundreds of thousands of spam texts using hundreds of unregistered SIM cards.

In both of the successful appeals the Tribunal cancelled the MPN because it was not satisfied that the breach was 'likely to cause substantial damage or substantial distress'. *Central London* was appealed to the Upper Tribunal (see our *Cake or Death?* article on the SCL web site and in the e-pub version of this issue).

In the *Scottish Borders* appeal extensive written submissions had been made that MPNs were criminal penalties. As that appeal was disposed of without the need for argument on the point (and other issues) the questions remaining unanswered are whether a MPN is a criminal penalty and whether, as a consequence, MPN proceedings are criminal proceedings throughout, to which Convention Rights apply. It is submitted that there are strong arguments supporting the view that MPNs and MPN proceedings are criminal for the purposes of the ECHR.

What makes a penalty 'criminal'?

It is generally accepted that according to Strasbourg jurisprudence[7], there are three considerations when deciding on whether proceedings are criminal. These are:

1. the domestic classification of the 'offence' is relevant although the concept is autonomous;
2. the nature of the offence; and
3. the nature and degree of the potential penalty and the actual penalty.

The first and last of these are most significant in a discussion of MPNs. Despite any domestic classification, such as the ICO's adoption of the epithet '*Civil* Monetary Penalty', the main feature which Strasbourg case law focuses on is the stated purposes of the penalty. If it is 'punitive and deterrent' in nature, as opposed to 'compensatory or disciplinary', then Strasbourg considers a penalty to be criminal. Thus sanctions imposed by courts on soldiers and prisoners are likely to be criminal, but findings by professional regulators against doctors, dentists, nurses and other professionals are likely to be viewed as civil.

The ICO's Standard Operating Procedures[8] expressly and unequivocally state:

> *'[The power to impose a MPN] will be used as both a sanction and a deterrent against a data controller who deliberately or negligently disregards the law'.*

This could scarcely be more clearly expressed. The ICO's Standard Operating Procedures do not concern themselves with notions of compensation or discipline. The language is unequivocally of punishment and deterrence.

In the case of *Georgiou*[9] the Strasbourg Court held that a penalty in relation to assessments of VAT was 'criminal' even although it was classified as 'civil' in domestic law, coming to this view because the penalty was intended as a punishment to deter re-offending. Its purpose was both deterrent and punitive. As is also relevant to MPNs, the amount of the penalty was taken into account and was noted to be substantial.

Applying this case, the High Court of Justice Chancery

Division also held in *King v Walden*[10] that the imposition of a penalty constituted proceedings of a criminal character having regard to both the potential size of the penalty; the punitive and deterrent nature of the proceedings; and the consideration given to mitigation.

In *Walden* the court decided that imposing penalties for fraudulent or negligent delivery of incorrect returns or statements *was* 'criminal' for the purposes of the ECHR, Article 6(2) for the following reasons given by Mr Justice Jacob (at [71]):

> *(a) Plainly the system is intended to punish the defaulting taxpayer and to operate as a deterrent;*
> *(b) The amount of fine is potentially very substantial;*
> *(c) The amount of fine is not related to any administrative matter. In particular the fine is not limited to the administrative and other extra cost of dealing with the taxpayer concerned. (Curiously I suspect the cost to the State of dealing with Mr King, taking into account the Revenue's internal costs as well as the cost of the Commissioners greatly exceeds the fine actually imposed, namely £58,000).*
> *(d) The amount of fine imposed depends upon the degree of culpability of the taxpayer, the less culpable the more mitigation there is. Mitigation is an essentially criminal rather than civil consideration.*
> *(e) It is accepted that generally . . . it is not for the taxpayer to show that the determination of penalties was wrong. On appeal the burden of proof lies on the Crown. In this regard there is a clear distinction between a penalty determination and an appeal against ordinary assessment where the burden of showing it was wrong lies on the taxpayer.'*

So what appears to be extremely significant is both the intention to punish and deter, as well as the magnitude of the penalty.

For the sake of completeness, Strasbourg has indicated[11] that the imposition of a term of imprisonment as an alternative to a fine etc is not essential to the matter being considered criminal. Nor is it essential for the breach/conviction to be entered into a database of previous convictions.

A potential Monetary Penalty of £500,000 is a very severe level of fine on any view. The ICO is exercising its discretion to impose significant fines. The maximum to date has been £325,000. In the *Scottish Borders* appeal the Deputy Commissioner indicated that he could see no situation where a fine of less than £75,000 would be appropriate. By comparison, in terms of health and safety law, a fine imposed under the Health and Safety at Work etc Act 1974 can be unlimited,[12] but the Sentencing Council has indicated[13] that the starting point where there has been a fatality is rarely less than £100,000 and £500,000 if the conviction is under the Corporate Manslaughter and Corporate Homicide Act 2008. Thus a fine of £250,000 on a local authority, had it been imposed under health and safety law rather than the DPA, s 55A, would most likely have involved multiple fatalities.

Practical consequences if the MPN regime is criminal

If MPN proceedings are criminal then not only will the ECHR, Article 6(1) be engaged (right to a fair trial), but the rest of Article 6 would be engaged and in particular the presumption of innocence. In addition, Article 7 would be engaged precluding the retrospective criminalisation of actions and retrospective punishment for actions. The ICO's procedures would require review not least to take into account issues of fairness: a point that was further highlighted by the *Niebel* appeal.

Following the *Walden*[14] case, where there is an HMRC investigation into whether or not a penalty is to be imposed on an individual for failing to pay tax, then in certain cases these penalties will be considered to be criminal, and therefore the individuals are to be treated as if they have been charged with a criminal offence. It is for this reason that HMRC advises its investigators to provide certain information to anyone being investigated who may receive a penalty. They are to be advised of their right not to answer any questions; their right to seek legal advice; the right to a decision without unreasonable delay; the right to an appeal or review; and the right to apply for legal aid.

This approach is not currently embedded in the ICO's investigative procedure. In the *Scottish Borders* case the ICO simply mentioned the possibility of issuing a MPN at the outset of its investigation along with other possibilities (including an Enforcement Notice) and then stated:

> *'At this stage we are still investigating the situation and have not yet formed a view on what action, if any, we will take. It is possible that, once we have considered all the relevant evidence, we will exercise our powers as set out above. Your full co-operation in establishing the facts is therefore appreciated.'*

If MPNs are criminal, this approach is not compliant with Article 6(1). The ICO's present investigation process, it is submitted, does not give fair notice to data controllers, especially public authorities who may be dealing with dozens of agencies at any given time, that the ICO's investigation process is more onerous than simply a collaborative exercise between agencies whereby one public agency is co-operating with another to ensure that a loss of data is managed correctly, that the cause is established and that the ICO can assist the public authority going forward. If the process is in fact a criminal investigation (indeed even if it is not, it is submitted) the potential consequences to the data controller are very serious. The data controller should have clear notice of the possibility of a MPN rather than this outcome being presented as simply one of a list of options. If the MPN procedure is criminal, the gathering of evidence during an ICO investigation should be open to scrutiny to ensure that it has been obtained fairly and is admissible. The current procedure is susceptible to the further criticism that it largely relies upon information volunteered in good faith by the data controller. Disclosure may be motivated by the desire to co-operate but in reality the data controller may be incriminating itself or proffering information that it would not do with the benefit of independent legal advice. It may not be presenting the full picture to the regulator because it is unaware of the use to which the information may be put.

Fair notice

A data controller appealing against a MPN should not have to find out about the case against it for the first time when Skeleton Arguments are filed six months after the date of the MPN. Article 6(3) sets out the right of a person to be informed *promptly,* in a language which he understands *and in detail,* of the nature and cause of the accusation against him. In the *Scottish Borders* case the data loss was self reported but part of the penalty was based on a database issue unconnected with the original data loss. That database had been mentioned in the course of the investigation as part of a large list of the Council's databases, voluntarily supplied by the Council following an audit. It was admitted in the course of the appeal that the Notice of Intent and MPN were defective because they did not mention the database issue. The Tribunal however rejected a submission that the Council had not had fair notice of the 'charge' and the facts of the breach, since these had become clear from the ICO's Skeleton Argument in the appeal. The difficulty with that approach is that it does not comply with the requirement of Article 6(3) which demands that notice of the facts must be given promptly, ie at the outset. The more recent *Niebel* decision appears to indicate that the Tribunal has moved close to accepting this, Judge Warren holding that:

> 'It is apparent that there is a need, when applying these new provisions, to identify the contravention and the circumstances surrounding it reasonably clearly.
> The detail may of course change in the course of proceedings. That is implicit in the statutory procedure whereby the ICO first sends a "notice of intent" giving the offender an opportunity to make representations and enter into discussion. A clear statement of the contravention is necessary in order to apply the words of the statute; to make a judgement on whether the contravention is "serious"; or to consider whether it is "of a kind likely to cause substantial damage or substantial distress". Such a clear statement is also required by the ordinary rules of fairness which attach to sanctions or penalty proceedings. It is essential that the *offender* should know what the case is against him or her. It is important to know the period of time which the contravention covers so that there is no repeat penalty covering the same period'. (emphasis added)

As the Tribunal made clear in the *Niebel* appeal, fairness to the 'offender' includes clarity in relation to what the case is against him or her, including the period of time and the extent of the contravention, so that the 'offender' can ensure that the penalty relates to the contravention and not any other behaviour. In addition the extent of the contravention must also be relevant to the size of the penalty imposed. These points had been taken in the *Scottish Borders* appeal where it was submitted that the number of lost files taken into account as justifying both the issue of the MPN and the amount appeared to vary widely.

Retrospective criminalisation of behaviourand punishment

It was also submitted in the *Scottish Borders* appeal that, regardless of the procedure being criminal or civil, the MPN appeared to be founded upon facts that occurred prior to the enactment of ss 55A to 55E DPA, thus amounting to retrospective criminalisation. In *Niebel*, this appears to have been the determining factor in the appeal, reflected in a late decision by the ICO to accept that the contravention related to 286 spam texts not hundreds of thousands. This was inevitable since the majority of spam texts predated 26 May 2011 when the PECR MPN provisions came into force.

If the MPN regime *is* considered to be criminal then the ECHR, Article 7 makes it unlawful for the state to punish an act which was not criminal at the time that the act was carried out, and it also makes it unlawful to impose a heavier penalty than the one that was applicable at the time the act was committed:

> *'No one shall be held guilty of any criminal offence on account of any act or omission which did not constitute a criminal offence under national or international law at the time when it was committed. Nor shall a heavier penalty be imposed than the one that was applicable at the time the criminal offence was committed'.*

In *Welsh v United Kingdom*[15] the accused was arrested on drugs charges in November 1986. In January 1987 new powers in relation to the seizure of the proceeds of crime came into effect. The applicant argued that if the new law applied to him then that would constitute retrospective criminal legislation and offend Article 7. The UK argued that the confiscation did not constitute penalties for the purpose of Article 7. The Court in Strasbourg indicated that there had been a breach given that the applicant faced more far-reaching detriment as a result of the government seizure than he would have at the time of the offence.

It does appear that in *Niebel* the Tribunal is of the view that nothing done prior to the possibility of a MPN being imposed can be taken into account when considering liability or quantum, but the ICO did not appear to accept that in *Niebel* , arguing that actions taken prior to that date could be taken into account, albeit they did not form part of the contravention. If it is established that the proceedings are criminal, then Article 7 would seem to clearly indicate that the Tribunal's approach is correct. Of course, the ICO will have to be clear about what they are taking into account in their Notice of Intent and, in the authors' view, prior even to that stage in proceedings, so that the issue is clear to any 'offender'.

Access to justice

The ICO itself is not an impartial and independent tribunal compliant with Article 6(1). It is in effect the prosecuting entity. So it has to rely on the Tribunal to deal with the matter *de novo* because if the ICO's decision can be reviewed by a court of full jurisdiction, including questions of fact and law, then this defect can be cured. However, is access to the ECHR compatible tribunal sufficiently free and unfettered? In our view it is not.

The ICO offers a 20% discount if the MPN is paid within 28 days. Scottish Borders paid the fine minus the 20% discount within 28 days *and* lodged an appeal but were told that they could not do both

and that they would only be entitled to a discount if they did not appeal. This matter was not resolved at the hearing as the MPN was cancelled, but the Tribunal did express some concern that this may appear to be like 'a fee for appealing'. The Tribunal was also concerned to see the ICO trying to discourage an appeal by reference in an e-mail to the appeal process entailing 'expensive litigation'.

Judge Warren stated:

'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'.

The standard wording of MPNs was changed for a short time in June 2013 to indicate that early payment would mean that the appellant forfeited its right to an appeal. But this has now reverted back to the original wording, which is not clearly excluding a discount if an appeal is lodged.

For more on this issue, see *Cake or Death?*, our online article on the Central London Community Healthcare NHS Trust appeal.

Criminal sentencing principles

In the *Scottish Borders* appeal, quantum was not discussed. It appeared from oral evidence that the sentencing process described in the ICO guidance had not been followed to the letter and that there had been a less structured approach than suggested in the guidance. However, the Deputy Commissioner was clear that the fact that a data processor was a public body was *not to* be taken into account when determining the amount of a MPN. The ICO's position was also that self-reporting would not result in a discount, or a lesser MPN, but a failure to self-report may result in a *higher* MPN. It is submitted that this view is simply wrong, out of line with the approach of other regulators and that credit ought to be given to any data controller who self reports a data breach.

Summary

Business and the public sector have been relatively slow to recognise their potential exposure to very large penalties, possibly because, unlike with death or personal injury, the loss of personal data is not yet instinctively pigeon-holed as a breach of the law that can result in half million pound fines. No doubt the Upper Tier Tribunal and perhaps the courts will have the opportunity to deal with all the issues raised in this article in due course. It will be very interesting to see if they determine that the proceedings are criminal and if so whether any of the issues addressed above will be explored in that context. ●

Paul Motion and Laura Irvine are both Solicitor Advocates with BTO Solicitors, Edinburgh. They acted for Scottish Borders Council in the appeal referred to. They can be contacted on *prm@bto.co.uk and lji@bto.co.uk* or via *www.bto.co.uk*

Endnotes

1. http://www.ico.org.uk/enforcement/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ico_standard_operating_procedures_for_monetary_penalties.ashx
2. http://www.ico.org.uk/enforcement/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ico_framework_to_determine_amount_penalty.ashx
3. http://www.ico.org.uk/what_we_cover/taking_action/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data-protection-regulatory-action-policy.pdf
4. Decision Notice Tribunal Reference number EA/2012/00111, 15 January 2013
5. Decision Notice Tribunal Reference EA/2012/0212, 21 September 2013
6. Decision Notice Tribunal Reference Number: EA/2012/0260, 14 October 2013
7. See for example *Engel v the Netherlands* (1976) 1 EHRR 647
8. Op cit at 1
9. *Georgiou v UK* (40042/98) [2001] S.T.C. 80
10. *2001 WL 513115*
11. Ozturk v Germany (1984) 6 EHRR 409
12. Health and Safety at Work etc Act 1974, Schedule 3A
13. http://sentencingcouncil.judiciary.gov.uk/docs/web__guideline_on_corporate_manslaughter_accessible.pdf at page 7
14. Op cit at 10
15. (1995) 20 EHRR 247