Review of the impact of ICO Civil Monetary Penalties

1. Introduction

1.1 Objective of the research

In February 2014, the ICO commissioned SPA Future Thinking to carry out research on the impact of Civil Monetary Penalties (CMPs).

The main purpose of the research was to review the extent to which CMPs influence or improve data protection compliance and practice by organisations. The research also measured awareness of the ICO's enforcement powers and furthermore, organisations' experiences of the ICO's processes when issuing CMPs.

The findings from the research will be used to measure and evaluate how effectively the ICO's use of CMPs:

- achieves its key corporate objective of improving information rights compliance and that it is using its enforcement powers proportionately; and

- meets the following specific aims of the ICO's Information Rights Strategy:
    - to ensure organisations are aware of the ICO's enforcement powers; and
    - that the ICO deploys its enforcement tools in a way that provides an incentive for organisations to 'get it right' first time.

The research was also commissioned with an eye to the European Commission's proposals for a new EU Data Protection Regulation, where draft provisions on sanctions extend data protection authorities' current

enforcement powers. The proposals could require mandatory breach notification by certain data controllers to regulators and individuals, and could raise fines of up to 2 per cent of turnover or €1m (Article 79). The European Parliament's amendments could increase this to up to €100m or 5 per cent of turnover.

1.2 Context

Since April 2010, the ICO has had the power to issue monetary penalty notices of up to £500,000 for serious breaches of the Data Protection Act (the DPA), and (since May 2011) serious breaches of the Privacy and Electronic Communications Regulations (PECR). Section 55A(1) of the DPA allows the Information Commissioner to serve a monetary penalty notice if he is satisfied that three conditions apply:

- there has been a serious contravention of a data protection principle and

- "the contravention was of a kind likely to cause substantial damage or substantial distress" and

- the data controller:

  "(a) knew or ought to have known —

  (i) that there was a risk that the contravention would occur, and
  (ii) that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but

  (b) failed to take reasonable steps to prevent the contravention".

The ICO uses CMPs as both a sanction and a deterrent against a data controller or person who deliberately or negligently disregards the law. The overarching aim is to promote compliance and improve public confidence.

The ICO is committed to reviewing its regulatory activities in line under its obligations under the Regulators' Code. The ICO reviews its regulatory action periodically:

- to ensure that policies and operational procedures are proportionate, consistent and targeted;
- to ensure it supports organisations to comply;
- to understand its impact on organisations' information rights practices and policies; and
- to evaluate against the ICO's objectives.

This helps to ensure that the ICO delivers its services and responsibilities effectively and efficiently.

1.3 Research methodology

The research consisted of:

- In-depth telephone interviews with 14 organisations who had received a CMP. This sample was made up of seven local authorities, three private companies, one local health authority, one police force, one central government department and one regulator. All of the organisations in the sample had self-reported their breach. Six respondents challenged the Notice of Intent.

- An online survey of 85 'peer' organisations (from similar sectors, or local regions) who had not received a CMP. The objective was:

    - to obtain an understanding of organisations' awareness of the ICO's regulatory action; and
    - to measure and evaluate whether CMPs had a wider impact on the data protection practices and policies of these organisations.

This report summarises the findings from the research and highlights some potential actions for the ICO to consider as part of its duty to review how it delivers its services and responsibilities.

2. Key findings

Although the research sample size was relatively small, the results clearly indicate that CMPs have had a positive impact on organisations' data protection compliance and practice.

Key findings include:

- The research findings indicate that CMPs are effective at improving data protection compliance. This was particularly clear for organisations that had been issued with a CMP; the research showed a clear impact on how those organisations managed their data protection responsibilities:
    - Organisations took their data protection obligations seriously, with revised practices and policies, and increased staff training.
    - Data protection was given a higher profile, with greater senior management buy-in.
    - Staff awareness was raised through targeted campaigns, with the importance of handling data properly made more prominent.
- The research confirmed that this positive impact was extended to 'peer' organisations, where CMPs had a wider impact as a useful deterrent and an incentive to 'get it right first time'. A substantial proportion of this sample said that they had reviewed or changed their data protection practices and policies as a result of hearing about CMPs being issued to other organisations. This indicates that CMPs effectively contribute to achieving specific outcomes in the ICO's Information Rights Strategy:
    - to ensure organisations are aware of the ICO's enforcement powers; and
    - the ICO deploys its enforcement tools in a way that provides an incentive for organisations to 'get it right' first time.

- The findings indicate that ICO audits support organisations in complying with their information rights obligations. Four out of 14 respondents in the telephone interview sample proactively engaged with the ICO subsequent to the CMP process, with three undergoing a good practice audit, and one organisation setting up a series of workshops in conjunction with the ICO across ten of its sites. Two more respondents confirmed that at the time of the interview, their organisation was considering a good practice audit.

- Evidence suggests a lack of understanding of the interpretation of the conditions in Section 55A of the DPA, particularly around the meaning of 'serious' and 'substantial damage and distress' in relation to a contravention.

- Some respondents felt that there was a lack of transparency about how CMPs were calculated. This could be linked to some organisations expressing discontent about the clarity of the Notice of Intent.

3. The impact of Civil Monetary Penalties on data protection practice and compliance

3.1 Impact on organisations that had received a CMP

The research strongly suggests that CMPs are effective in improving and promoting compliance and practice by organisations. Receipt of a CMP had a positive impact on how data protection responsibilities were managed in the organisation. Organisations that had received a CMP gave data protection a higher profile; became more proactive in addressing their information rights obligations; and took steps to increase staff awareness of their responsibilities.

> *"…We've put together… an information security group, which meets on a regular basis, to talk through all aspects of the data protection policy…"*

> *"…We became more proactive in our relationships with subcontractors and people working with our data. We're using our ICO audit by invitation as a catalyst for change…"*

Following receipt of a CMP, organisations increased and improved staff training, and initiated stronger communication to staff about data protection, with the aim of changing behaviours when handling information. Five out of the 14 organisations made changes to relevant departments, with the addition of new staff, or restructures. Four organisations completely overhauled their information security policies.

> *"…It's a cultural shift but we always knew it would take some time to address. What we try to do, without being too heavy-handed about it, is to ensure that people understand the implication of getting it wrong and that may sound terribly self-evident, but people lose sight of the fact that the smallest mistake can cause a major incident further down the line."*

Some organisations proceeded to proactively engage with the ICO once the process was complete. For example, three organisations arranged a good practice audit with the ICO and two more reported that they are currently considering one. One organisation set up a series of workshops in conjunction with the ICO across ten of its sites.

Security was the main area that received attention following the receipt of CMP. This reflects that CMPs have been predominantly issued for data breaches related to principle 7 of the DPA, which requires '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'.

Half of the respondents reported that they felt more confident about their data security, but could not guarantee there wouldn't be another breach. Several said that reported incidents of breaches of data security had increased within their organisations.

3.2 Impact on organisations who had not received a CMP

There was a high level of awareness about CMPs being issued to sanction organisations which had seriously breached the DPA, with over 70 per cent of respondents reporting that they had heard about such incidents. The ICO's website was the most common source of information regarding CMPs that had been issued (57 per cent); followed by 'word of mouth' (47 per cent); and thirdly, media reporting (45 per cent).

For peer organisations, the research showed that CMPs had a wider impact as a useful deterrent, with the positive impact on data protection compliance and practice extended to these organisations. Around 60 per cent said that hearing about CMPs had influenced how their organisation managed its data protection responsibilities and the importance it attached to information rights. When asked about specific impacts the news of a CMP had, the research showed that for organisations who had not received a CMP:

- 58 per cent said that senior management had taken a greater interest in data protection because of CMPs.

- 47 per cent reviewed their data protection practices and policies.
- 47 per cent introduced more data protection training.
- Over a quarter (28 per cent) carried out some form of internal audit.
- Others introduced new systems (18 per cent); appointed new staff or added new responsibilities to existing roles (15 per cent).

3.3 Reputational damage

Eleven out of the 14 respondents who had received a CMP agreed that it is appropriate for the ICO to publish actions taken against organisations that breach information rights law. Ten respondents reported that their organisation received bad press as a result of the CMP, with most reporting that the negative publicity was short-lived. More respondents claimed that the damage to reputation had a greater impact than the CMP. For local authorities, the political dimension heightened their sensitivity to bad publicity.

Almost 70 per cent of the wider sample agreed that the ICO should do more to publicise CMPs it issues for breaches of the DPA.

4. Perceptions and experience of ICO CMPs process

4.1 Fairness of the CMP

4.1.1 General perceptions

Public authorities expressed objections to money being taken out of the public purse, away from frontline services. There was also a misperception about what happens with the money collected through CMPs:

> *"… the public perception is they're doing it to generate income…. Where does it go? Nobody knows. What public benefit are we achieving by fining a public body?..."*

There was also anecdotal evidence expressing doubt about the inclination of private sector companies to report breaches, with an unfair impact on public authorities.

> *"There are a lot of private companies who aren't self-reporting where they should be, because the chance of them becoming public are pretty much null and void. I've attended training courses where people have been very open about incidents that have happened to them in their organisation which are far worse than our breach and they've never reported it. I would arguably say that the ICO could be seen to be picking the low hanging fruit"*

For the wider sample, there was a division in organisations' perception of the fairness of CMPs issued by the ICO, with 22 per cent reporting that they are 'fair'; 21 per cent said they are 'not fair' and 57 per cent said they 'don't know'. When this was explored in more detail, respondents who thought CMPs are fair and proportionate said that they were necessary as an incentive to make sure organisations handle personal data properly.

> *"it emphasises the importance of protecting personal data and the serious implication that may result from a breach…."*
>
> *"…large fines act as a deterrent…"*
>
> *"Public awareness is important"*

Those respondents who thought CMPs are unfair questioned the severity of them, the fact that they often hit public sector organisations and the fact they do not take human error (rather than a deliberate contravention of the law) into account.

4.1.2 Understanding the triggers for a CMP

Only four of the 14 who had received a CMP were able to explain what conditions must be met for a breach to trigger a monetary penalty notice. While respondents reported that the conditions were fair, the research showed that some respondents found them slightly ambiguous and open to interpretation, with comments suggesting that there was a lack of certainty about the meaning of 'serious' and 'substantial damage or distress' in relation to a contravention.

Several respondents also expressed a lack of understanding of the threshold for the conditions, expressing doubt as to whether the circumstances of the data breach in question actually satisfied the requirements of Section 55 of the DPA.

> *"… it comes down to interpretation… There was absolutely no proof in any way that these few misdirected faxes caused any harm to the individuals whose data it was. So, whilst I think those are good conditions for a fine, I don't think they were interpreted properly in our particular situation."*

> *"We had received no complaints from our staff at all about it. Once we informed our staff about the incident… we never received one complaint, one raised concern or one issue from any member of staff in connection with it. From the analysis we did we felt that the maximum number of people that could have actually accessed that spreadsheet would have been under 30."*

> *"…we were… a little bit perplexed about how any of this had caused harm of distress to individuals because we'd had no instances where we could identify that any fraud or distress had been caused to the customers. There was no evidence that had caused any problems for them."*

4.2 Perceptions about the ICO's CMP process

Most respondents considered that the time taken to determine the issuing of the CMP to be too long.

4.2.1 Transparency

Some of the organisations who had received a CMP expressed dissatisfaction in relation to the perceived lack of transparency around how the amount of the CMP was calculated:

> *"There's no explanation to the council and to our taxpayers who ultimately had to pay the fine as to what the rationale for the amount is."*

> *"…we remain unclear about the parameters which lead to a fine and about how the level of penalty as arrived at in our case…"*

This evidence potentially indicates a lack of awareness by organisations about the ICO's framework used to determine the amount of a monetary penalty, which is available on ico.org.uk.

Some respondents also felt that there were inconsistencies about the level of the penalty for data breaches.

4.2.2 Notice of Intent

Half of respondents were satisfied with the explanation provided in the Notice of Intent about the reasons for the issuing of the CMP. Those who did not think the Notice of Intent was clear enough reported that it was perfunctory and lacking a clear explanation of the rationale for the decision in their particular circumstances.

> *"…there wasn't really much explanation. It was just the Notice of [Intent]… followed [by] the standard monetary penalty notice where it lists the aggravating circumstances and behavioural competencies of the organisation… but there was no additional conversation."*

> *"The Notice of Intent… reiterated what was in the policy and the guidance… and then related it to the facts… I don't think it analysed that third [condition] in terms of what precautions we'd put in place. It was almost a case of you lost the data and therefore whatever precautions you put in place were insufficient, so that part of it I don't think they analysed particularly well."*

> *"… a lot of it was factually incorrect, so even though we'd supplied them with information, they'd actually not correctly reported that in their Notice of Intent."*

> *"It didn't really explain or justify the level of the penalty. It's very legalistic. The mitigating features that they've taken into account and other considerations are less than one page of eleven page document."*

While six contested the Notice of Intent, the remaining respondents felt that the CMP was fair, or they didn't think that their challenge would be successful.

4.2.3 Suggestions for alternative enforcement approaches

Respondents suggested ways the ICO could work with organisations to support them to comply post-CMP.

> *"[The ICO] should have offered to re-look at our [data protection policies and] plans work with us to make sure we haven't missed anything obvious and then offer, say in 12 months' time, to come in and do a bit of a 'where are you now' review."*

> *"… it's about what can they do differently to raise the awareness and I think it's more about how are they engaging with some of the chief executives or the trust directors or whoever it is, chief constables… how are they really engaging with them to get them to accept ownership and responsibility for data privacy…"*

Others suggested that the ICO should take mitigating factors into consideration when determining the amount of the CMP - citing factors such as general good behaviour; robust damage limitation; actions taken to reduce risks. This can be countered by the fact that the ICO does consider wider mitigating factors when assessing whether a CMP should be issued and the amount. This misunderstanding indicates an opportunity for the ICO to ensure that organisations are aware that this is the case.

One respondent commented on the practical use of good practice audits, and suggested that they could become a more integral part of the CMPs process:

> *"… I believe [the ICO's] audits are more of a benefit than a monetary fine. And I think possibly, depending on the severity of the fine, perhaps they should incorporate an audit process as part of that investigation to see whether it was just a one off incident or whether there are continual errors within an organisation to actually determine the severity of the fine."*

Two respondents suggested that there should be some reimbursement from the penalty to be diverted to investment in data protection improvements in their own organisation.

> *"They might have said 'this is the level of fine but if you spend half of this money on improving your resources allocated to this, if you do this and demonstrate to us that you've done something to stop this happening again then the fine will be moderated'…."*

> *"There was a feeling from people saying fair enough to impose a fine, but couldn't some of that come back to the organisation to be spent on improving data protection."*

5. Conclusions

5.1 ICO corporate objective – improving data protection compliance

The findings show that CMPs are effective in achieving the overarching objective of improving data protection compliance. This was particularly clear for organisations which had been issued with a CMP; the research showed a clear impact on how those organisations managed their data protection responsibilities:

- Organisations took their data protection obligations seriously, with revised practices and policies, and increased staff training.
- Data protection was given a higher profile, with greater senior management buy-in.
- Staff awareness was raised, with the importance of handling data properly made more prominent.

The wider sample study shows that there was a high level of awareness amongst peer organisations about the use of CMPs as a sanction for organisations in breach of the DPA/PECR. The findings indicate that the positive impact on data protection compliance was extended to peer organisations, where CMPs were viewed as an incentive for them to get it right first time. The majority reported that there was greater senior management buy-in; just under half said they had reviewed or changed their data protection practices and policies as a result of hearing about CMPs, and some increased training and initiated internal audits.

These findings indicate that CMPs effectively contribute to achieving specific outcomes in the ICO's Information Rights Strategy:

- to ensure organisations are aware of the ICO's enforcement powers;
- good information rights practice embedded into culture and day-to-day processes of organisations; and
- the ICO deploys its enforcement tools in a way that provides an incentive for organisations to 'get it right' first time.

5.2 Supplementary findings – perceptions and experience

The research indicates that ICO good practice audits support organisations in complying with their information rights obligations. Four out of 14 respondents in the telephone interview sample proactively engaged with the ICO subsequent to the CMP process, with three undergoing an audit, and one organisation setting up a series of workshops in conjunction with the ICO across ten of its sites. Two more respondents confirmed that at the time of the interview, their organisation was considering a good practice audit.

The research suggests a lack of understanding of the interpretation of the conditions in Section 55A-E of the DPA, particularly around the meaning of 'serious' and 'substantial damage and distress' in relation to a contravention.

Some respondents felt that there was a lack of transparency about how CMPs were calculated. This could be linked to some organisations expressing discontent about the clarity of the Notice of Intent. There is also evidence to suggest that the operational process for investigating and issuing a CMP should be expedited to avoid diminishing the impact.

6. ICO actions for consideration

The research findings clearly suggest that CMPs are effective in fulfilling the ICO's key corporate objective of improving and influencing organisations' data protection practice and compliance. Overall, the report supports the ICO's approach to issuing CMPs to date, and warrants the use of CMPs as a major part of our enforcement strategy. We believe we have targeted the right cases and breaches and set the right amounts, though we will continue to learn from the outcomes of Information Rights Tribunal appeals.

While there isn't any evidence to suggest a need to significantly alter the ICO's approach, the research raises some points around transparency, communications and the process in issuing CMPs, which this section responds to below. The ICO is keen to address these points as part of its aim to use our enforcement powers effectively and proportionately to better support organisations to comply with their information rights obligations. Approaching five years since CMPs were introduced, this research presents an opportunity for the ICO to reflect on its enforcement action and explore the potential for new and improved ways of applying its regulatory powers.

CMPs process

- Whilst we do believe the Notices of Intent issued to date have provided reasonable explanations of why the CMP was issued, the ICO will consider how information provided in the Notice can be improved, for example, whether we can explain how the conditions apply in individual circumstances in more detail.

- The ICO will consider what more can be done in terms of transparency about how the CMP is calculated. The research indicates a potential lack of awareness by organisations about the ICO's framework used to determine the amount of a monetary penalty, which can be accessed through ico.org.uk – we could consider how we can promote this document. Furthermore, we could consider the merits of publishing a 'case study' to show the process the ICO goes through to decide when a CMP should be levied and how much it should be. This would demonstrate how we

engage and consult with the organisation, how we assess conditions, what factors we take into consideration, including mitigating factors.

- The ICO will continue to consider the issues related to interpreting substantial damage and distress. We will review the ICO's statutory guidance and operational policies to assess whether they require updating. We will continue to press DCMS to lower the threshold for CMPs issued for breaches of PECR which, if implemented, will provide greater clarity for the ICO and data controllers.

- The ICO will consider how to better communicate what happens to the money received from CMPs - ie that the money goes to the HM Treasury consolidated fund. As part of our broader work on future ICO funding, we will look for opportunities to press the case for the necessary changes to be made to the DPA to enable the ICO to retain a portion of the money from CMPs and explore how it could be used to support data controllers to comply.

Other regulatory tools

- The ICO will consider how it can further promote its good practice audits as a way of supporting data controllers to comply with their information rights obligations. In relation to the CMP process, we will consider whether we could do more to encourage organisations that have been issued with a CMP to undergo a good practice audit. Furthermore, we could explore whether there is scope to extend the ICO's assessment notice powers to oblige such organisations to undergo an audit.

- The positive feedback on the effect of good practice audits suggests there is a case for the ICO to continue to press for strengthened compulsory audit powers – these are imminent for the health sector and we have made a case for extension to local government.

- We should continue to publicise the existing tools provided by the ICO to help organisations comply and get it right in the first place and avoid CMPs – for example, we could link CMP press releases to relevant ICO guidance and codes of practice to explain how the breach could have been avoided; and promote newer mechanisms

such as the good practice self-assessment tool for public authorities and SMEs.

- We should build on our recent report on the top IT data security threats and associated ICO blogs - continuing to publicise the lessons learned through our investigation of CMP cases and reflecting these in our good practice guidance.

- The ICO could do more to publicise 'success stories' resulting from the issuing of CMPs. For example, we know Belfast Health Trust have publicly presented about how their CMP was a catalyst for change in their organisation. This would help demonstrate the value of CMPs more widely.

- While the research findings indicate that there is a high level of awareness about the use of CMPs as a sanction for serious breaches of the DPA/PECR, the ICO will explore other potential routes of communication to further raise awareness about the ICO's enforcement action. We will continue to use trends data to strategically target communications and promotions work. We could issue a regular press release (or report or blog) which summarises recent CMPs and identifies the key themes. It could also be used to provide information of the sort of actions organisations have taken since the breach to mitigate the risks – along the lines of the 'success stories' suggested above.