

Data Protection Officer Conference in 2010

Workshop A

Monetary powers and penalties outcomes

Question and answer and group feedback following the scenario discussions

Q: What is the Commissioner's view on defined policies, processes etc? For example an individual rogue employee who flouts the rules?

Ans Sally: If there is good corporate governance but the fault lies with just one rogue employee then it is very unlikely that we would impose the monetary penalties.

Ans Mick: However, we would expect controls on what can and cannot be put on memory sticks or cards in the first place, and we might take exception to this – alarm bells may start to ring.

Group feedback

Group 1 – the first example is the most serious due to the sensitivity of the data.

Sally: We will be assessing on a case by case basis.

Group 2 – The fourth case is the most serious due to the sensitivity surrounding the police service in N. Ireland.

Mick – There will be differing fine levels and the income/ financial resources of each organisation will be taken into account.

Some delegates felt that case four may not attract a monetary penalty, and the point was made that not all cases would attract a penalty.

There was a comment that case two would not be suitable for monetary penalty, maybe just enforcement.

A comparison was made with motoring offences – a '3 strikes and you're out' type scenario.

Someone commented that in case two, you need to balance sensitivity and encryption.

Another delegate commented that there was a lack of detail within this exercise. We need to know how poor the governance is, whether it is a rogue individual etc. They felt the exercise is a bit of a party game and cannot be accurate. A balance needs to be struck.

One delegate said that it is a question of consistency, and the situation can vary across all sectors. We need a framework otherwise we will be challenged.

Sally – We will be taking many factors into account. There may be variations in terms of the amount of fines for similar breaches, depending on the organisation. Monetary penalties will refocus people's minds.

Mick – The purpose of each case in this exercise is to illustrate that the breaches were avoidable and that organisations need to take a bit more care. We have asked for this power. We have new teeth but we do not have to use them. It would be nice to come back next year and say we have not issued any penalties.

Sally – Organisations do have the right to appeal any fines, to the General Regulatory Chamber.

Delegates were then referred to the ICO website for further information.

Monetary powers and penalties

Mick Gorrill

Mick mentioned assessment notices and said there would be more information on the website. The example security breach cases the delegates have been provided with are seven of the most serious cases the ICO has had in the last 12 months or so. It was stressed that monetary penalties are not retrospective and will only come into force in April. It was also pointed out that all discussion/ answers regarding the cases would be anonymous and would not be held against the organisation in the future!

RAD will now be known as Enforcement. There have been approximately 850 self-reported breaches since November 07. Most contraventions are breaches of the 7th principle, but breaches of principles 3 and 5 are also common.

Our existing powers are deemed inadequate and there has been criticism that we are a toothless tiger.

Parliament decided that a civil monetary penalty was the best course of action as opposed to criminal action. We are hoping for as few monetary penalties as possible by this time next year.

All of this new legislation will be located under section 55 of the DPA. There will be a Notice of Intent followed by a decision and the issuing of any penalty.

It was stressed that monetary penalties will only follow a *serious* contravention of the principles. They will mostly be concerned with the 7th (and /or maybe 3rd) principle. Damage or distress will be 'likely' (not necessarily actual). An aggravating factor would be if we had previously issued a formal notice but the organisation had not adhered to it.

Of the approximate 850 breaches reported, the ICO has taken regulatory action in about 60 cases (about 5%) so this is a relatively low figure. This is new territory for us and further guidance will be produced. Penalties can also be appealed.

There are differences between these new powers and the current Section 40 enforcement powers. In order for the new penalties to be applied, the breaches must be serious.

Factors making monetary penalties more likely:

Risk assessment may be highly lacking.

It should be prohibited to be able to transfer organisational data onto personal devices.

Mick gave an example of a Trust employee (GP) taking home a laptop containing 12,000 patient details. This was deemed as excessive and an Enforcement Notice was issued.

All of the seven listed examples in the exercise were avoidable. It is not sufficient to just blame an individual; we need to look at the overall governance of the organisation. We will go through a rigorous procedure to decide if the penalty is appropriate.

For example, the firm: PA Consulting lost a pen drive. An employee had downloaded data against contract and procedures. In such cases, it is unlikely that we would impose a penalty but we may examine their procedures and governance.

If the case/ organisation is linked with the FSA then we would discuss it with them and decide who should investigate it. The organisation in question would not be pursued by both the FSA and ICO, so there could only ultimately be one fine imposed.

(Monetary Penalty Notice was briefly touched on)

Self-reported breaches – an unencrypted portable device would usually be deemed as a serious breach. The NHS are obligated (by their own guidelines not by the ICO) to tell us about each breach. By comparison, private sector breaches are probably under-reported.

What does this mean for data controllers?

Undertakings can be issued as an alternative to Enforcement Notices. Or there is the possibility of an audit.

What is an appropriate penalty?

(Mick again highlighted that the discussion would be anonymous.)

Sally-Anne Poole:

Sally explained that the ICO has a new structure. She then provided an overview of her role.

Of the 7 cases provided, we have taken regulatory action in all of them. BUT what would we have done if the monetary penalties had been in force? (Again it was highlighted that the new law is not retrospective.)

Sally runs through all of the security breach cases provided to delegates. Group is asked to discuss if they think the ICO would have imposed penalties. If so, what level, and why?

Group feedback:

GROUP 1 –

Case 1 should be an Enforcement Notice and no monetary penalty. There is likely to have been a business need to transfer the data and there is a procedure in place for encrypting it. The error lay with the individual as the 'weakest link'. This was human error rather than corporate failure.

Case 2 – they felt a penalty of £10,000 would be appropriate. There has been a clear breach of Trust policy. They should have

taken steps to reduce the downloading of corporate data. Staff either were not given the correct tools or were acting in breach of them.

Case 3 - £100,000 penalty due to the volume of data and the fact there is no clear reason why it was downloaded. No business need. There was also a clear policy to report breaches but this was not adhered to.

GROUP 2 –

Case 1 – agreement with first group. Enforcement Notice. This needs to come back to employee accountability and an emphasis on increased awareness.

Case 2 – More severe due to unencryption, although policies were in place. Other factors – what is the value of danger? In this case there are less patients so not quite as substantial. They would fine on a lower level due to the fact that policies are there.

Case 3 – The group was unanimous in the fact that this should be classed as a major breach. Substantial amount of data, unencryption, sensitivity etc. The key to this one was the delay in reporting it. The group would impose a substantial fine.

GROUP 3 –

Case 1 – Similar viewpoints as other groups.

Case 2 & 3 – penalties should be imposed.

Case 4 – Smaller volume of data but high sensitivity so there would be a fine.

GROUP 4 –

Case 4 - £250,000 fine due to the high level of sensitivity of the information.

Case 5 – Mainly a case of bad procedures. Maybe Enforcement Notice. No penalty.

Case 6 – Highlights a lack of any sort of risk assessment. Definite fine and would probably for the full £500,000 fine.

Case 7 – Enforcement Notice. Even though there has been a loss of data, it is not that sensitive.

GROUP 5 –

Case 4 – The nature of the information has to be taken into account. They would fine £100 per record. There is also an issue of why the data is being held.

Case 5 – Penalty imposed due to embarrassment factor.

Case 6 – Potential for ID theft, so maximum penalty imposed.

Case 7 – The group were still debating this one as they were not sure about how to classify motoring information in terms of sensitivity. Enforcement Notice.

GROUP 6 –

Case 1, 2 & 3 – Suspended fine with Enforcement Notice
Case 4 – Fine imposed.

GROUP 7 –

This group decided to fine all cases 4-7. They could not decide on the level of the fine as they needed more information about the size of the organisation (especially in cases 6 and 7). There may also be a risk of fraud.

GROUP 8 –

Case 4 – Very sensitive information. £100,000 fine.

Case 5 – All the information was sent to only one individual so the risk was lower. Enforcement Notice.

Case 6 – They would impose a fine but it would depend where the laptop had been stolen from. Eg if it was stolen from within a locked building, there would have been less of a risk.