# THE UNDERTAKING

## (the Commissioner's weapon of choice)

AMBERHAWK

A DATA PROTECTION ANALYSIS
FROM AMBERHAWK TRAINING LTD
DR. C. N. M. POUNDER, FEBRUARY 2010



# THE UNDERTAKING
## (the Commissioner's weapon of choice)

**First published in Privacy Laws & Business UK Newsletter, February 2010** ***(www.privacylaws.com)***

The Information Commissioner is not a powerful regulator. This plain fact will not substantially change on April 6th when the Monetary Penalty Notice should become part of the UK's data protection infrastructure. Although any penalty will attract the headlines, this new power will not be exercised often. That is why, when things go wrong, a data controller is more likely to be "invited" to sign an undertaking.

### *So when is an undertaking issued?*

Quite simply, an undertaking follows a significant data protection failing on the part of the data controller that has been established following an investigation by the ICO. The undertaking is a public document, signed by the CEO, which effectively promises that the data controller will take all reasonable steps to ensure that there is not another similar breakdown in data protection compliance.

Once a week, somewhere in the UK, a data controller signs an undertaking. Most of them relate to lost or stolen laptops or missing memory sticks containing unencrypted personal data. The undertakings signed by Billing Pharmacy Ltd, NHS Education for Scotland, Sandwell Metropolitan Council, Wigan Council, London Borough of Sutton, Repair Management Services Ltd, and UPS Ltd fall into this category.

However, security of personal data in manual form can attract an undertaking. In early January Bellgrange Mortgages & Insurance Services Ltd signed an undertaking for leaving files of personal data in a skip, whereas East Cheshire NHS Trust Accident and Emergency because its manual patient registers were found in a garden.

Similarly, loss of personal data by a data processor can result in the data controller signing an undertaking. For example the ICO required the Home Office to sign a formal undertaking when a contractor employed by the Home Office, PA Consulting, lost an unencrypted memory stick holding sensitive personal data (criminal records) of thousands of individuals in August 2008.

Although most undertakings relate to security breaches and the Seventh Principle, there have been undertakings relating to other Principles. For example, First Response Finance Ltd had to agree to comply with the first and third data protection principles following complaint regarding a form asking an employer for excessive details. Jubilee Managing Agency Limited, agreed to comply with the Fifth Principle when the loss of an unencrypted disk containing personal data, included financial details relating to cancelled or expired policies.

In summary, although most of the undertakings already in the public domain relate to serious security breaches, data controllers who breach ***any*** Principle in a significant way should anticipate that, if the ICO investigates, an invitation to sign an undertaking might be at the end-point of the procedure. The fact that the CEO has to sign the undertaking means that the ICO has leverage if another incident occurs; the signature should also enhance the effectiveness of management support available to the data protection officer.

## *What is in an undertaking?*

Most undertakings have a standard format. They contain the name of the data controller and a description of the reasons for the undertaking (e.g. lost laptop or whatever). This is followed by text something like the next paragraph (which is used when security breaches occur):

> "...The data controller shall, as from the date of this undertaking and for so long as similar standards are required by the Act or other successor legislation or from other data controllers in similar circumstances, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Schedule 1 Part 1 of the Act, and in particular, that..." (There then follows a list of actions needed to remedy the problem that has been investigated).





In the case of Stockport NHS Trust Undertaking, this list contained actions such as:

1. "Portable and mobile devices including laptops and other portable media used to store and transmit personal data, the loss of which could cause damage or distress to individuals, are encrypted using encryption software which meets the current standard or equivalent";

2. "Staff are aware of the data controller's policy for the storage and use of personal data and are appropriately trained on how to follow that policy"

3. "All computers and portable devices used by the data controller to process personal data are registered with the IT department" and that "adequate alternative data security arrangements are implemented when normal working practices cannot be followed".

Note that the key part of the Undertaking is not the "in particular" list of actions. The important commitment is in the statement that "from the date of this undertaking ... (the data controller ensures that) ... personal data are processed in accordance with the Seventh Data Protection Principle". The undertaking is a promise in relation to ***all*** of the Seventh Principle for ***all*** time in the future.

## *What is the difference between an enforcement notice and an undertaking?*

When the Commissioner serves an information or enforcement notice, certain precise specifics must be identified. This is because failure to diligently comply with a notice is a criminal offence and because there is a right of appeal to the Tribunal. The Commissioner when issuing a formal notice will be mindful of this prospect; the result is a notice that has to have all the legal niceties (including the evidence) tightly specified in advance of its serving. This is quite time consuming and costly in terms of the Commissioner's resources.

By contrast a signed undertaking has no statutory standing and does not have to be specific as there is no appeal. Failure to comply with an undertaking is not an offence but will be likely to

result in the issuing of an immediate enforcement notice (e.g. if the problem re-occurs and there is no evidence that the data controller took the remedial action outlined in the undertaking). The result is the undertaking is a far more flexible and cost-effective as far as the Commissioner is concerned; an undertaking gets the attention of the data controller's senior management to take action, and leaves the data protection equivalent of the "sword of Damocles" hanging in the air.

To press home the contrast, have a quick look at the detail needed in the enforcement notice issued to the construction industry following their use of the blacklists processed by the Consulting Association. It contained provisions such as:

> "Ensure that if any personal data relating to recruitment is obtained from a source other than the data subject, the data subject is, in so far as is practicable, provided with the information specified in paragraph 2(3) at Part II of Schedule 1 to the Act in accordance with the First Data Protection Principle".

Note that there is no long term commitment such as: "The data controller shall, as from the date of this undertaking and for so long as similar standards are required by the Act or other successor legislation...".

## *An offer you can't refuse?*

If your employer, as data controller, is asked to sign an undertaking, would it sign up? If you do not, then you should expect an enforcement notice. This policy was made public at a NADPO conference in Autumn 2009 when questions arose with respect to the enforcement notice issued to Marks &Spencer in 2008. That notice related to a data loss following the theft of an unencrypted laptop which contained the personal information of 26,000 M&S employees.

Evidently M&S was offered an undertaking which they were reluctant to sign because a contractor was at fault. David Smith, Deputy Information Commissioner, pointed out that it was the policy of the Commissioner to issue an enforcement notice if a data controller refused to sign





an undertaking. In other words, if you are "invited" to sign an undertaking it really is an "offer you can't refuse", to quote Don Corleone.

The alternative to not signing is far worse. With an enforcement notice the Commissioner has, by law to, identify what needs to be done and by when. The enforcement notice will be in the public domain (so the publicity angle is no different) and of course and there is a threat of criminal sanction if action is not taken. With an undertaking there is, at least, the possibility of negotiating the terms of surrender.

## *Final comment - the aftermath of the signing ceremony*

Suppose a data controller signs an undertaking and then there is, say nine months later, another significant breach in data protection compliance in another area. If you were the Commissioner, would you want another undertaking from the same errant data controller or would you go for immediate enforcement? The point being made is that, for the immediate future after a signature, there is an implicit element of "drinking at the last chance saloon" – so it would be a mistake to limit data protection remedial action to the bare necessities of the undertaking. So take the opportunity to fix the other obvious problems as well.

Additionally, as is well known, the ICO is gearing up for inspections and auditing. If you were planning an audit inspection, who would you audit - a data controller who has signed an undertaking or one that has not appeared on your radar. In other words, if you have already signed an undertaking, anticipate a visit to check up on progress (especially if you are geographically close to Wilmslow).

I am sure that in the coming year, there will be a lot of commentary, agitation and froth about the Monetary Penalty Notice. In practice, however, I think it will be the undertaking that will be the enduring enforcement weapon of choice for the Commissioner. In short, an undertaking is a quick way of getting a compliance issue off the Commissioner's books and committing a data controller to future action – expect more of them.

**Dr C. N. M. Pounder, Amberhawk Training Ltd, February 2010**

AMBERHAWK

# APPENDIX C: ADVERTS

## DATA PROTECTION FOR USA AND EUROPEAN PRIVACY OFFICERS

We have developed a course to provide USA and European privacy officers with rounded knowledge of European Data Protection law based on the Directive 95/46/EC and the Privacy & Electronic Communications Directive 2002/58/EC (the latter in the context of e-commerce). An assessment of understanding can be obtained by written exam – this is a variant of the data protection qualification for the UK offered by the ISEB, a qualification body linked to the British Computer Society. The ISEB have told us they are prepared to set an exam. If interested please contact ***info@amberhawk.com***.

## COURSES FOR DATA PROTECTION OFFICERS IN THE UK

Amberhawk provides a wide range of public training suitable for data protection officers in the UK. These include courses leading to the ISEB qualification in data protection. With respect to on-site training, Amberhawk can provide sector specific training (e.g. on rights of access, PECR, CCTV, Human Resources, Data sharing) as well as on-site ISEB courses.

We have a Data Protection Audit courses as well as a course on Level 1 of the Government's Information Assurance Strategy (the HMG Security Framework). If interested please contact us at ***info@amberhawk.com***

## COURSES IN FREEDOM OF INFORMATION

Amberhawk provides a wide range of public training suitable for those dealing with Freedom of Information and the Environmental Information Regulations. These include courses leading to the ISEB qualification. With respect to on-site training, Amberhawk can provide sector specific training aimed at those helping a public authority meet its obligations. Courses can include Re-use Regulations by Public Sector Bodies.

If interested please contact us at ***info@amberhawk.com***