

Data protection sanctions:
a practical quick reference guide

OLSWANG



Introduction



Yesterday saw the publication of the latest [Annual Report](#) by the Information Commissioner. Entitled "Upholding information rights in a changing environment" it details the ICO's activities and financial statements for the past year and summarises its aims for the next two years. So, what can private sector data controllers learn from this year's resume?

It has been a significant and busy year for data protection: the appointment of the new Commissioner, Christopher Graham, in June 2009 and the coming into force of tougher enforcement powers in the form of monetary penalties and assessment notices in April 2010. With security breaches never far from the headlines, May 2010 saw the achievement of a dubious landmark, namely the 1000th security breach notified to the ICO.

The report covers the period from April 2009 to March 2010, before the ICO's new powers came into force, so it still is too early to say what impact these will have on organisations' compliance with the data protection regime. At the time of writing, there have been no published reports of monetary penalties being imposed. The ICO's strategy gives prominence to "educating and influencing" data controllers as well as taking enforcement action. Perhaps it is the case that the use of undertakings will remain the ICO's "weapon of choice" for dealing with contraventions and instilling good practice.

For commercial organisations handling customer data, perhaps one of the most compelling factors in this year's report is not the number of formal enforcement actions taken by the ICO, but the statistic that complaints about subject access requests top the list of public concerns as reflected in complaints made to the ICO (28% of all complaints). Similarly, individuals' awareness of their data subject rights is at an all time high (91% of those surveyed by the ICO). In other words, in spite of the ICO's increased enforcement powers (and the recent call from the European Commission that these be strengthened even further), for many organisations, reputation and brand image will continue to provide the strongest business case for good data protection compliance.

In this short guide we:

1. pick out some highlights from the 2009/10 Annual Report and compare enforcement action figures with figures from the [2008/09 Annual Report](#) – the increase in undertakings given by organisations is staggering and, almost without exception, these relate to security-related breaches, which continue to be the biggest area of data protection risk;
2. highlight some key steps for organisations to take to avoid enforcement action; and
3. provide a quick guide to the ICO's extended enforcement powers and when they can be used.

Marc Dautlich
Head of Data Protection
Olswang

15 July 2010



1. HIGHLIGHTS FROM THE 2009/10 ANNUAL REPORT

- **Funding and audit of the ICO's income**

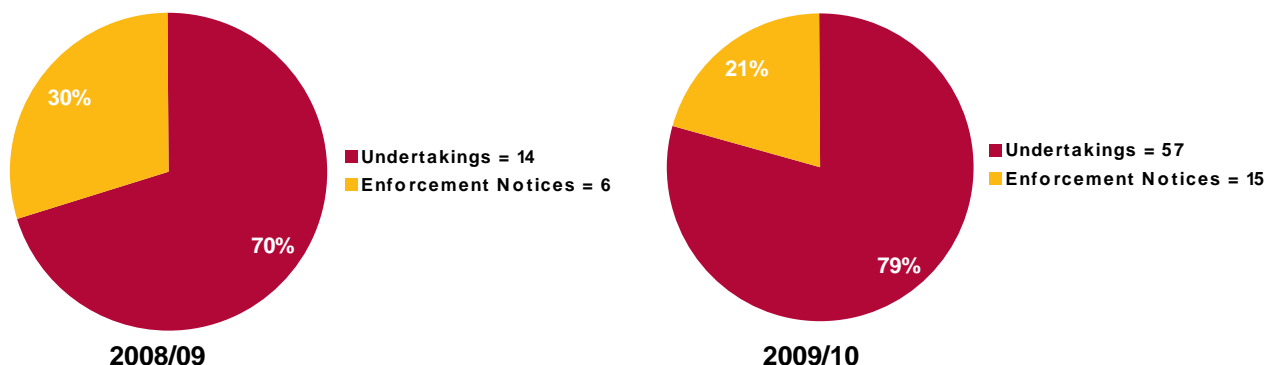
It will come as no surprise that one of the principal risks identified by the ICO's auditors is funding uncertainty, both in respect of the data protection responsibilities of the office (there being uncertainty about income from the new higher tier £500 notification fee) and grant in aid for the office's freedom of information responsibilities (see page 57). The lion's share of the 16.6% increase this year in the ICO's notification fees income is derived from the higher tier fees introduced on 1 October 2009, although a little under a quarter of the increase is derived from an increase in the size of the Data Protection Register – more organisations submitting their annual notification – itself (see page 58).

Interestingly, the second principal risk identified is the *"need to ensure we have the right staff and skills in place to implement new powers in the areas of audit and monetary penalties"* (this is not cited as a reason for the lack of issue of monetary penalty notices since their introduction in April 2010!) Read on for our summary of the range of enforcement powers now available to the ICO.

- **Enforcement action as compared to 2008/09**

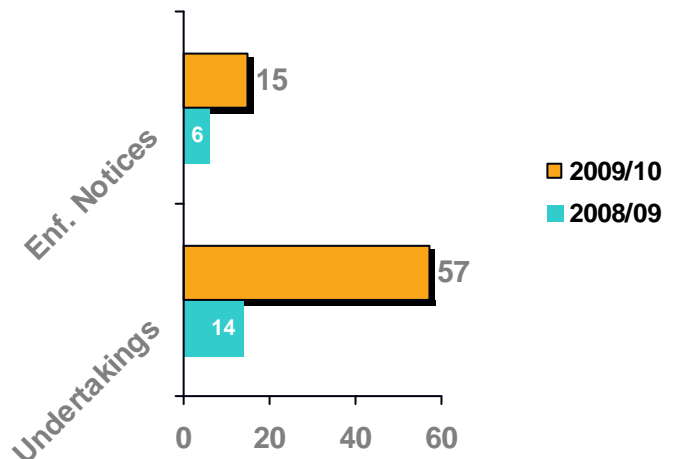
There were 57 undertakings given in 2009/10, which is an increase of over 300% from the 14 undertakings given in 2008/09. In the diagram below, these figures are compared to the number of enforcement notices given in the respective years and, although it is a small sample, it supports the view that the ICO's increasingly preferred enforcement option, where some form of enforcement is appropriate, is to obtain an undertaking from a data controller. Note that the proportion of undertakings vs enforcement notices in 2009/10 is distorted, since 14 of the 15 enforcement notices were handed out in one day to a group of construction firms for unfairly obtaining personal information about construction workers.¹ If one removes this instance, the ratio of enforcement notices to undertakings in 2009/10 is even lower than illustrated below.

Undertakings as compared to enforcement notices in 2008/09 and 2009/10



¹ See p.36 of the Annual Report under "Consulting Association".

Increase in enforcement action in 2009/10



The analysis above is based on published figures in the 2008/09 and 2009/10 Annual Reports.

As well as undertakings and enforcement notices, other data protection-related enforcement action includes prosecution for failure to notify, and the Annual Report 2009/10 reported that the ICO prosecuted seven bodies for failing to notify as data controllers with the ICO. There were also two prosecutions for failure to respond to enforcement notices.

Note that these highlights do not address the sections in the Annual Report on Freedom of Information. For more information, see our [Datonomy blog](#) or our separate publications on FOI.

2. AVOIDING PROBLEMS: DATA PROTECTION COMPLIANCE STEPS

Of the 57 undertakings given between April 2009 and March 2010, all but one related to compliance with the seventh data protection principle.²

The other data protection principles that were the subject of the undertakings were the fifth (data not to be kept for longer than necessary), the third (data to be adequate, relevant and not excessive) and the first (data to be processed fairly and lawfully) (i.e. some of the undertakings, breach of more than one principles was at issue).

What constitutes "appropriate security" for the purposes of the Seventh Principle will depend on the circumstances of and resources available to the particular organisation and the nature and quantity of personal data it holds. The ICO endorses the adoption of the BS ISO/IEC 27001 standard on information security management as a means to demonstrate good practice. For organisations not wishing to undertake such an extensive compliance programme, there are a number of "must have" measures and themes which recur both in the relevant ICO guidance and in recent undertakings, which all data controllers should consider.

² The Seventh Principle provides that: "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." This statistic would appear to justify trends in the market prioritising information security.

Set out below is a non exhaustive list of five essential steps to consider.

1 As a matter of good corporate governance, ensure someone suitably senior has day to day responsibility and accountability for data security measures.

2 Take reasonable steps at the recruitment stage to check the identity and reliability of staff and contractors who will have access to personal information. Ensure staff and contractors are made aware of their obligations with regard to data protection and confidentiality, in simple, readily understandable ways.

3 Ensure that portable and mobile devices, including laptops and other portable media used to store and transmit personal data, are encrypted using encryption software which meets up to date standards; ensure that personal data is only transferred to removable media when absolutely necessary. Where possible, sensitive personal data should be accessed remotely or hand-delivered. All other post should be adequately tracked.

4 Don't underestimate the importance of physical security measures e.g.: control of access to the premises, "locked cabinet" and "clear desk" policies, secure transportation and disposal of hard and soft copy records.

5 Carry out and document a risk assessment to identify the sensitivity of personal data held and the likely effect of a security breach, both on data subjects and on your organisation.

FURTHER GUIDANCE ON DATA SECURITY

The ICO has published a number of guidelines which provide practical points for data controllers on complying with the Seventh Principle.

[Good practice note on security of personal information](#). This contains tips on organisational, physical security and computer security measures and staff related issues.

[Guidance on data security breach management](#).

[Guidance about the issue of monetary penalties](#). Section 3 of this guide describes the circumstances in which the ICO would consider it appropriate to impose a fine for deliberate or reckless breaches of the DPA. In effect, this is a non exhaustive checklist of steps which a prudent organisation should take in order to protect itself from potential liability for reckless breaches.

4. SANCTIONS

Undertaking

Following breach of a data protection principle, an organisation may be invited by the ICO to sign a formal undertaking, wherein the CEO of the organisation undertakes to put certain measures in place in order to avoid a similar data protection failure in future. This undertaking is published on the ICO website and, although most undertakings do not contain deadlines, it is possible for the ICO to provide a deadline for those measures to be introduced, for example, for breach of the seventh principle, a common undertaking is for the organisation to ensure that computers are encrypted with encryption software meeting the current standard or equivalent and, in some cases, a one to four month deadline is given for compliance.

It is not a criminal offence to fail to comply with an undertaking (in contrast to an enforcement notice), however, it is likely that, if the breach recurs and it is clear upon investigation by the ICO that the undertaking was not complied with, an enforcement notice will be issued.

Enforcement notice

For particularly serious or persistent breaches of data protection provisions the ICO is likely to issue an enforcement notice requiring the organisation to take, or refrain from taking, specified steps. In essence, enforcement notices have the level of precision of court orders, since failure to comply with an enforcement notice carries criminal penalties.

Assessment notice and audit

An organisation may be subject to a voluntary audit to assess whether the organisation's processing of personal data follows good practice. Alternatively, an organisation may be subject to a compulsory audit following the issuing of an assessment notice. This Olswang article provides further information on assessment notices and audits:

<http://www.olswang.com/newsarticle.asp?sid=121&aid=2903&de=&mid>

Monetary penalty

Since 6 April 2010 the ICO has had the power to issue a formal notice requiring an organisation to pay a monetary penalty of up to £500,000. This brings the ICO's powers in line with those already available to many national supervisory authorities around Europe. This will be imposed if an organisation has seriously contravened the data protection principles and the contravention was of a kind likely to cause substantial damage or substantial distress. In addition the contravention must either have been deliberate or the data controller must have known or ought to have known that there was a risk that a contravention would occur and failed to take reasonable steps to prevent it.

This Olswang article provides further information on monetary penalties:

<http://www.olswang.com/newsarticle.asp?sid=121&aid=2880>

It is interesting to note that, three months after the ICO's powers to issue this penalty came into force, no monetary fines had yet been issued. Unlike undertakings, monetary penalties do not themselves provide the data controller with any understanding of how to put matters right and so in that sense are less useful from the perspective of the Commissioner's statutory role of promoting good practice. Clearly they play a deterrent role as part of the ICO's "purposeful risk-based enforcement action" (as described in the Annual Report under "Our Corporate Plans") and we look forward in due course to evidence of their usefulness in this regard.

Criminal offences

Failure to notify: it is an offence to process personal data without a valid registration or outside the scope for which the organisation is registered.

Unlawful obtaining and disclosing of personal data: this is aimed at data theft and although currently the penalty is limited to a fine, there was a Ministry of Justice consultation in January 2010 on introducing a custodial sentence and this could also form part of the Ministry of Justice's Call for Evidence on the data protection legislative framework, which opened on 6 July 2010 and closes on 6 October 2010.

Claims by individuals

Individuals have the right to claim compensation from an organisation in respect of damage caused by a breach of any of the requirements of the Data Protection Act 1998 although few compensation claims have reached the courts for consideration.

For further information and comment on ICO sanctions and a range of data protection news and issues, why not subscribe to the Datonomy blog at <http://www.datonomy.eu/> (you can do this by requesting an RSS feed or providing your email address in the right hand tool bar of the homepage. We use this only to send you posts from Datonomy).

Key contacts



Marc Dautlich
Partner
+44 (0)20 7067 3142
marc.dautlich@olswang.com

Marc has a broad TMT, IT and outsourcing practice and is Head of the firm's Data Protection Unit. His work includes software development and licensing, data protection and privacy, complex IT and outsourcing/offshoring and online content acquisition and e-commerce. Marc launched the firm's data protection blog, Datonomy (<http://www.datonomy.eu/>) in 2009. Marc is a member of the Firm's Outsourcing Group and of the Open Source Unit. Prior to joining Olswang, Marc served as legal counsel at Equifax, and he has also been seconded from the Firm to legal projects at Microsoft.

The information contained in this update is intended as a general review of the subjects featured and detailed specialist advice should always be taken before taking or refraining from taking any action.

© 2010 Olswang

OLSWANG

London
Olswang LLP
90 High Holborn
London WC1V 6XX
T +44 (0) 20 7067 3000
F +44 (0) 20 7067 3999

Thames Valley
Olswang LLP
Apex Plaza, Forbury Road
Reading RG1 1AX
T +44 (0) 20 7067 3000
F +44 (0) 20 7071 7499

Berlin
Olswang LLP
Potsdamer Platz 1
D-10785 Berlin
T +49 (0) 30 700171-100
F +49 (0) 30 700171-900

Brussels
Olswang LLP
Avenue Louise 326 bte 26
Louizalaan 326 bus 26
B-1050 Bruxelles/Brussel
T +32 2 647 4772
F +32 2 644 2165