Legal update

Don't bin your Data Protection responsibilities

Ewan Nettleton

is a senior associate solicitor in the Intellectual Property Department at the Technology Law Firm, Bristows. He specialises in Intellectual Property Law with an emphasis on litigation. He has an MA in Chemistry and a DPhil in Protein Chemistry and is particularly interested in matters relating to the IT and pharmaceutical industries.

William Jensen

is a trainee solicitor at Bristows currently sitting in the Intellectual Property Litigation Department. He has a BSc degree in Physics and French.

Abstract Database marketers being 'data controllers' within the meaning of the Data Protection Act ought to be aware of the UK's data protection legislation and may even have had dealings with the UK regulator, the Information Commissioner's Office (ICO). This paper describes some recent enforcement action taken by the ICO, including action taken in relation to unsolicited marketing mailings, and looks in detail at how the approach adopted seeks to ensure compliance.

Journal of Database Marketing & Customer Strategy Management (2007) **14,** 311–314.
doi:10.1057/palgrave.dbm.3250060

INTRODUCTION

Information technology has grown at an exponential rate over the last three decades, with systems becoming increasingly powerful and more and more data being stored and processed. Database marketers more than most are businesses to which data is an essential resource, as accumulation, buying and selling of customer data and marketing contacts are key aspects of everyday business. They should be aware of the UK's central piece of legislation governing the protection of data, the Data Protection Act 1998 and will no doubt be familiar with dealing with the UK's regulatory body, the Information Commissioner's Office (ICO). Recent actions taken by the ICO would, however, indicate that not all those who process personal information are as familiar with the Act as perhaps they should be. In March 2007, several banks were found to be in breach of their data protection responsibilities following customer complaints about sensitive information found in rubbish bins outside their premises.[1] More recently, action has been taken against Littlewoods in relation to unsolicited marketing mailings. This paper describes some of the ICO's recent enforcement actions and considers how the ICO is seeking to achieve compliance with the UK's data protection requirements. In doing so, it provides an overview of the requirements concentrating on those most likely to be relevant to database marketers.

Ewan Nettleton
Bristows,
3 Lincoln's Inn Fields,
London WC2A 3AA, UK
Tel: +44 (0) 20 7400 8000;
Fax: +44 (0) 20 7400 8050;
e-mail: ewan.nettleton@bristows.com

THE DATA PROTECTION ACT 1998 — AN OVERVIEW

With growing amounts of data came the need for legislation to regulate how the data were handled, and this gave rise to the Data

Protection Act 1984, and more recently the 1998 Act (the Act), which implemented EU wide legislation on the protection of data. The Act gives individuals rights such as the right to ascertain what information is held about them. The Act also imposes obligations on those who hold data to ensure it is dealt with properly. Importantly, the Act only applies to 'personal data',[2] defined as any data relating to a living individual who can be identified from the data or from the data and other information in, or likely to come into, the possession of the data controller. 'Data controllers' are those who determine the purposes for which and the manner in which any personal data are processed.

In order to promote openness and transparency in the use of personal information, the Act requires[3] every data controller who processes personal data notify the ICO unless they are covered by an exemption,[4] and not doing so is a criminal offence. The exemptions are too numerous to cover in detail, but the ICO provides a useful self-assessment guide.[5]

To ensure information is handled correctly, the Act sets out eight data protection principles, which data controllers must comply with. The principles, which are also referred to as the principles of 'good information handling' require that data controllers ensure that information is:[6]

1 fairly and lawfully processed;
2 processed for limited purposes;
3 adequate, relevant and not excessive;
4 accurate and up to date;
5 not kept for longer than is necessary;
6 processed in line with an individual's rights;
7 secure and
8 not transferred to other countries without adequate protection.

The Act sets out what each of these principles requires, and the ICO publishes guidelines to help data controllers to comply with the principles.[7] These data protection rules, coupled with the rules relating to unsolicited marketing communications set out in the UK's Privacy and Electronic Communications Regulations that have been summarised in previous articles in the Journal,[8] are the principal rules, which the ICO will expect database marketers to comply with.

The guidelines published by the ICO to assist data controllers to comply include helpful good practice notes and compliance checklists. Of particular interest to database marketers are the ICO's good practice notes on the buying and selling of customer databases,[9] electronic mail marketing[10] and the Telephone Preference Service.[11]

ENFORCEMENT BY THE ICO

The ICO has various powers to ensure the Act is complied with. It can assess and request information from organisations, and if they are found in breach, it may serve enforcement and 'stop now' notices requiring organisations to take specific steps to ensure compliance. It can even prosecute those found guilty of a criminal offence under the Act. Presently, the sanctions that can be imposed on those found guilty of such offences are limited to fines. This is set to change and although this is unlikely to affect reputable businesses, it is worth mentioning that the government has announced its intent to crack down on those who trade illegally in personal data and concrete proposals for custodial sentences for certain offences involving the misuse of personal data have been put before parliament.[12]

One notable absence from the ICO's armoury is a right of audit — the ICO does not have the statutory right to inspect the processing of data at a business' premises — and perhaps for that reason the ICO has been reluctant to serve enforcement notices, preferring instead to take a more conciliatory approach. For instance, in March 2007, several UK banks were found

in breach of the seventh data protection principle, which aims to ensure that data are held securely. The principle requires 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'. The institutions had used bins located outside their premises to discard material such as customer application forms and bank cards that contained personal data.

Although the actions of the banks could have resulted in serious consequences such as identity theft and defrauding of their customers, the ICO chose not to serve enforcement notices in the first instance. Instead, it obtained undertakings[13] from each of the banks to ensure they would comply with the seventh data protection principle in the future, and the undertakings were subsequently published on the ICO's website as a deterrent to others. While the undertakings did not impose any punitive measures as such and sought instead to ensure that the Act would be complied with in the future, they provide the ICO with a right to audit the banks' data protection procedures in the future, which the ICO would not otherwise have had. So, as well as receiving an embarrassingly public slap on the wrist, the banks know that their activities will be subject to the scrutiny of the ICO and that in the event of further transgressions, additional sanctions may follow. In this way, the ICO seems to be taking practical steps that are likely to ensure a higher degree of compliance than might have been achieved through serving an enforcement notice in the first instance.

More recently, in June this year, similar action was taken against Littlewoods Shop Direct Home Shopping Limited after a customer had complained to the ICO about receiving unsolicited mailings. Undertakings were required by the ICO to maintain the sixth data protection principle, which requires that data be processed in accordance with an individual's rights, following the customer receiving continued mailings despite assurances given that the customer's details had been removed from Littlewoods' mailing lists. In particular, the undertakings required that:

1 the personal data of the customer in question be suppressed from all company databases thereby ensuring that she would not receive any future marketing material from Littlewoods and
2 Littlewoods would review procedures currently in place to ensure that customers' rights under Section 11 of the Act (which gives individuals the right by written notice to require a data comptroller to cease or not to begin to process their personal data for the purpose of direct marketing) are upheld.

CONCLUSIONS

The recent actions of the ICO against a range of businesses demonstrate that it is seeking to ensure data protection compliance, and they underline the need for data controllers such as database marketers to be acquainted with and adhere to the data protection rules in addition to the requirements that apply to electronic marketing communications. The ICO has tended to require undertakings as to future compliance from businesses it has found to be in breach of the data protection rules, including breaches in relation to the sending of unsolicited marketing communications. While unlike sanctions imposed for data protection violations by other bodies such as the Financial Services Authority,[14] such undertakings do not in themselves impose any punitive measures, they allow the ICO to scrutinise these businesses' future activities in a way it would not otherwise be able to under its statutory powers under the Data Protection Act. As punitive sanctions may follow in the event of further breaches by these

businesses, this course of action by the ICO may be viewed as a practical approach to ensuring compliance.

Notes

1 See ICO press release entitled 'Banks in unacceptable data protection breach' dated 12th March, 2007 (available at http://www.ico.gov.uk/upload/documents/pressreleases/2007/bank_pr_130307.pdf).
2 Data Protection Act 1998, s.1 (1).
3 Data Protection Act 1998, Part III — Notification by Data Controllers.
4 Data Protection Act 1998, Sections 27–39.
5 Guide entitled 'Notification Exemptions. A Self Assessment Guide' (available at http://www.ico.gov.uk/upload/documents/library/data_protection/forms/notification_exemptions_-_self-assessment_guide.pdf).
6 Data Protection Act 1998, Schedule 1, Part I.
7 Available at http://www.ico.gov.uk/what_we_cover/data_protection/guidance.aspx.
8 See for example the following articles published in the *Journal of Database Marketing and Consumer Strategy Management*: 'Electronic marketing and the new anti-spam regulations', Vol. 11, No. 3, pp. 235–240; 'Getting tough on spam', Vol. 12, No. 4, pp. 357–361; and, 'Telephone marketing out in the cold?', Vol. 12, No. 2, pp. 172–176.
9 Good practice note entitled 'Buying and selling customer databases' (available at http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/buying_and_selling_customer_databases_v2.pdf). It should be noted that this note is for use when a business is insolvent or closing down, or when an asset is being sold, either by the owner or an insolvency practitioner, rather than when data are brought or sold more generally.
10 Good practice note entitled 'Electronic mail marketing' (available at http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/electronic_mail_marketing_12_06.pdf).
11 Good practice notes entitled 'Calling customers listed on the TPS' and 'Corporate Telephone Preference Service' (available at http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/calling_existing_customers_on_the_tps.pdf and http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/corporate_telephone_preference_service_gpn.pdf,respectively).
12 The Criminal Justice and Immigration Bill has had its first reading in the Commons and would introduce custodial sentences for offences for the misuse of personal data under s55 of the Data Protection Act 1988.
13 See http://www.ico.gov.uk/what_we_cover/data_protection/enforcement.aspx.
14 On 14th February, 2007, the Nationwide was fined £980,000 by the Financial Services Authority as described in the article entitled 'Regulators Get Their Teeth Into Data Breaches' by Mark Watts dated 9th March, 2007 (see http://www.bristows.co.uk/articles/detail.asp?frmAreaID=3&frmarticleid=950&frmpdtid=2).