

World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Volume 9, Number 4

April 2009

UK ICO seizes covert database of construction workers

By Rohan Massey, Partner, IPMT, McDermott Will & Emery UK, LLP who can be contacted at: RMassey@mwe.com

The Information Commissioner's Office (ICO) has, for the first time ever, issued an Enforcement Notice under the Data Protection Act 1998 (DPA) with a seven day compliance condition. The recipient is one Ian Kerr whose business, the Consulting Association in Droitwich, West Midlands, was raided by the ICO on 23 February 2009. The action followed an article entitled *Enemy at the Gates*, published in The Guardian newspaper on June 28, 2008 which referred, amongst other things, to the blacklisting of trade union activists in the construction industry. The ICO's investigation revealed that for over 15 years Mr Kerr had been running a database of construction workers used by over 40 construction companies containing personal information, including sensitive personal data such as individuals' trade union activity, construction workers' employment history, personal relationships and political affiliations. Descriptions linked to individuals in the database included "*ex-shop steward, definite problems*" and "*Irish ex-Army, bad egg*" other notes identified individuals who had raised concerns over health and safety issues on construction sites, such as asbestos removal. Firms subscribing to use the database, some of them household names in the construction industry, could consult it before deciding whether to offer an individual employment.

Investigation

The allegations against Mr Kerr were that contractors in the construction industry would send a list of the names of potential staff to the Consulting Association which would then check the names against a list and then advise the contractors of intelligence information which it held in relation to those named on the list. The contractor would then make a decision whether or not to employ that individual on the basis of that information.

On February 23, 2009 a warrant, granted under Schedule 9 of the DPA, was executed at Mr Kerr's premises. A search revealed a ring binder containing 3,213 entries in relation to individuals. The entries contained information such as names, dates of birth, national insurance numbers, locations and trades alphabetically listed on pages which had been processed on electronic media. A comprehensive card index system constituting an intelligence database contained information, some of which was over 30 years old, including personal data relating to an individual's union activity, his employment conduct together with any information that the individual may pose a threat to the industrial relations between an employer and its employees. This database was linked to the information contained in the ring binder.

The ICO uncovered evidence at the premises that

named construction firms subscribed to Mr Kerr's system for a £3,000 annual fee. Companies could add information to the system and pay £2.20 for details held on individuals. Invoices to construction firms for up to £7,500 were seized during the raid.

Data protection breach

Section 4(4) of the DPA provides that, subject to section 27(1), it is the duty of the data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller. The relevant provision in this case is the First Data Protection Principle which states essentially that personal data must be processed fairly and lawfully. In the Information Commissioner's view, Mr Kerr contravened the First Data Protection Principle in that, amongst other things, he had processed personal data unfairly by failing to provide the individuals with the standard information required by the DPA of a data controller such as his identity and the purpose for which data is intended to be processed.

Moreover, information as to whether an individual is a member of a trade union is "sensitive personal data" under section 2(d) of the DPA. In addition, the Commissioner considered that none of the conditions for processing in Schedules 2 and 3 to the DPA had been met as required by the First Data Protection Principle.

Special circumstances

Such were the circumstances of this case that the Commissioner considered that the notice should be complied with as a matter of urgency under section 40(8) of the DPA. This gave Mr Kerr until March 10, 2009 at the latest to comply with the notice even if he intended to exercise his right of appeal. The Commissioner's reasons for reaching this conclusion were that it was likely that Mr Kerr and/or his subscribers would continue to use the database and thus process the personal data specified in the Enforcement Notice to the continuing detriment of the individuals named on the list. The Commissioner acknowledged that as the processing had apparently been going on for many years it might appear difficult to justify action under the urgency provisions. Nonetheless, in the light of the nature of the per-

sonal data, the Commissioner believed that if Mr Kerr continued to provide it to employers there was a very significant risk that this would cause some individuals to be denied employment on the basis of adverse information of which they were unaware and which they were unable to challenge.

Comment

Mr Kerr now faces prosecution and no doubt a fine. The level of the fine will, for many, be unacceptably low in light of the wrongdoing that has occurred. On this point the courts and ICO can only act in accordance with current legislation, but had the proposed section 55A of the DPA been in force, the ICO could have been flexing its muscle with a much larger fine that would have a real commercial impact.

The activities described in the Enforcement Notice appear to show that this business was operated in such a way as to completely flout data protection law. One disconcerting aspect of the case therefore is that those who subscribed to such activity were "household names" in a major manpower intense industry. Not surprisingly, the ICO is considering what regulatory action to take against those construction firms that had been using Mr Kerr's system. One area that the ICO will no doubt be focusing on will be the function that enabled subscribers to add information to the database. Although there may be some interesting arguments raised in defence of this, it is likely that any subscriber adding personal data or sensitive personal data to the database will be in breach of its obligations as a data controller.

In a March 6, 2009 press release announcing the action against Mr Kerr, Deputy Information Commissioner, David Smith, takes the opportunity to

"remind business leaders that they must take their obligations under the Data Protection Act seriously. Trading people's personal details in this way is unlawful and we are determined to stamp out this type of activity"

One suspects that the ICO believes it is by no means a one-off incident. From March 16, the ICO has also been operating a dedicated enquiry system for people who believe personal information about them may be held on Mr Kerr's database.