



PRIVACY & SECURITY LAW



REPORT

Reproduced with permission from Privacy & Security Law Report, Vol. 07, No. 12, 12/24/2007, pp. 439-442. Copyright © 2008 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

Enforcement

EU Data Protection

In the past, companies have taken comfort from the fact that many European data protection authorities have little real enforcement power. That position has changed. This article traces an increasingly proactive and creative approach to enforcement, including joint enforcement, the London Initiative, a call for Sarbanes-Oxley Act-style senior executive certifications of data protection compliance, the appointment of a judge to review data transferred from the EU to the United States via the SWIFT network, and a campaign for greater enforcement authority in the United Kingdom.

What a Difference a Few Months Make: A Changing Landscape for EU Data Protection Enforcement

By BRIDGET TREACY

For some time now, the European Union data protection regulators have threatened to adopt a more proactive enforcement strategy to encourage greater compliance with the EU Data Protection Direc-

Bridget Treacy is a partner in the Privacy and Information Management Practice at the London office of Hunton & Williams. She may be contacted at btreacy@hunton.com.

tive (95/46/EC). Recent events suggest this threat is becoming a reality.

A key milestone toward more robust enforcement was signalled by the Article 29 Working Party in a paper published in November 2004. Since then, we have seen the first attempts of the Article 29 Working Party to adopt a pan-European approach to enforcement, targeting the private healthcare sector. We have also seen the EU regulators look self-critically at their approach to regulation and enforcement as part of the London Initiative. Most recently, in the wake of serious data breaches that have occurred recently in the United

Kingdom, the U.K. Information Commissioner has called for senior executives to be required, Sarbanes-Oxley Act-style, to certify that their companies comply with data protection laws.

This article traces the emergence of this increasingly proactive approach to enforcement and examine the greater creativity with which the European Data Protection Authorities (DPAs) are approaching the issue of enforcement.

The Regulators' Renewed Focus on Enforcement

A renewed focus on data protection enforcement was signalled by the Article 29 Working Party in 2004 in its paper entitled "Declaration of the Article 29 Working Party on Enforcement." The report followed an internal survey carried out by the Article 29 Working Party on enforcement practices in Member States. The survey suggested that in most Member States, the data protection enforcement function is under-resourced and that the level of knowledge of data protection rights amongst individual citizens is low. These factors contribute to poor compliance by organizations given that there is only a slim chance of any non-compliance being detected. Consequently, the Article 29 Working Party signalled a desire to push for greater investigative powers and additional enforcement powers for DPAs. Specifically, authorities highlighted their desire to have "stop now" or injunctive powers and compulsory audit powers as aids to enforcement.

In addition, the Article 29 Working Party raised the prospect of DPAs using publicity as part of their enforcement strategies. Businesses generally regard the negative publicity which frequently follows data protection infringement with greater horror than a fine or other sanction. The prospect of regulatory authorities proactively using publicity as a means of enforcement is a powerful incentive for businesses to comply with data protection laws.

Further, the Article 29 Working Party suggested that synchronized enforcement actions would be considered. This concept is relatively new in the context of data protection regulation, but coordinated enforcement activity takes place in many other regulated activities, notably in the arena of antitrust law. Early signals were that the financial services and healthcare sectors would be the first targets of coordinated investigation, given that both sectors have a strong consumer focus and process vast quantities of personal data.

Joint Enforcement Action

Following these early signals, the European DPAs initiated a joint investigation into data processing within the private healthcare sector. WP 137, entitled "Report on the First Joint Enforcement Action: Evaluation and Future Steps," was published in June 2007. It reported on the investigation undertaken by each DPA within its own jurisdiction. There were no audits and no individual verification or inspection. Rather, the investigation was conducted on the basis of a common questionnaire, distributed to representative businesses within each jurisdiction. It will be for individual regulators to take specific enforcement action based on the findings in individual cases within their jurisdictions, but the Working Party emphasized the likelihood that they would continue to pursue collective enforcement actions as an "effective strategy in the supervisory sphere." In particular, they suggested that joint en-

forcement actions should become more like audits, with power to verify the truthfulness of representations and to conduct random checks on selected data controllers as part of the overall process. The Working Party also raised the prospect of collaboration with other regulators, on an international basis, including the U.S. Federal Trade Commission.

SWIFT

In addition to the experimental Joint Enforcement Action, in the past year the Article 29 Working Party issued their controversial and far-reaching Opinion on the data processing activities of SWIFT. The facts of this case are well known. The Brussels-based SWIFT provides a messaging service that enables international financial transactions to be settled. SWIFT transmits messages internationally. It is a cooperative, owned by the financial services institutions and had considered itself to fulfil the role of data processor. SWIFT's activities came to the attention of the Article 29 Working Party following a complaint. It transpired that, as part of SWIFT's business continuity arrangements, it had established a mirror database in the United States. This database was the subject of subpoena issued by the U.S. Department of Treasury as part of its post 9/11 investigations. The complaint highlighted the fact that EU data was being transferred to the United States and was processed by the U.S. government without the knowledge of EU individuals. The Article 29 Working Party published an Opinion, stating that the manner and circumstances of the transfers of data to the United States did not comply with EU data protection laws, and required SWIFT to take remedial action. Key to the Working Party's analysis was its characterization of SWIFT as a joint controller of the data it processed with its member banks.

The decision itself has been hotly debated and criticized. Ultimately, the Article 29 Working Party has required SWIFT to restructure its processing arrangements so that EU data are not automatically mirrored to a U.S. database. This represents a significant step in the enforcement of data protection obligations. Many businesses have been taken by surprise that the European DPAs are able to require companies to amend their processing activities in this way.

Of greater significance, perhaps, is the fact that this month the European Commission has appointed a French judge to review the procedures governing the handling, use and dissemination of data transferred from the EU to the United States via the SWIFT network, and processed by the U.S. Department of Treasury. In June 2007, the U.S. Department of Treasury unilaterally provided representations to the EU as to the safeguards applied to EU data processed as part of the Treasury's anti-terrorist activities. This step indicates that the European regulators wish to audit the implementation of these safeguards.

London Initiative

The DPAs have also looked at their own approach to regulation and enforcement of the data protection laws. The London Initiative refers to the proposal adopted by DPAs at the International Commissioners' Conference in London in 2006, calling for DPAs to look afresh at the manner in which they discharge their regulatory function. The initiative is led by the French and U.K. DPAs, in conjunction with the European Data Protection Su-

pervisor, but is not restricted only to Europe. The initiative challenges the regulators to assess their efficiency as regulators, refresh and upgrade their technological resources, develop a new communication strategy; communicate data protection in a more concrete way and promote the involvement of other stakeholders in data protection. The initiative does not have significant visibility to the public but there is a very real sense that it is strengthening the resolve of regulators behind the scenes and equipping them to adopt a pragmatic, risk-based approach to enforcement.

Increase in Auditing

A number of EU DPAs have begun to audit data protection compliance by controllers. In particular, the CNIL, the French DPA, has been conducting audits and compliance checks on an unannounced basis for over a year. Informally, other EU DPAs have also indicated an intention to begin conducting audits. Many regulators would like to be able to insist on audits being performed by certified third parties, at the expense of controllers, with results reported to the regulators.

Naming and Shaming

Meanwhile, in the U.K., the Information Commissioner has embarked on a strategy of maximizing his somewhat limited powers of enforcement by ensuring that any enforcement activity receives maximum publicity. In particular, Enforcement Notices or company undertakings are now regularly published on his Web site and disclosed to the media via a press release.

This somewhat controversial approach was used most notably in the context of breaches of the U.K. Data Protection Act 1998 by several U.K. retail banks in 2007. The specific breaches varied but involved completed application forms, deposit slips and correspondence containing personal data being carelessly discarded in rubbish bins outside bank premises. After investigation, the Commissioner secured a legally binding undertaking from each of the banks, conceding the breach and agreeing to take remedial steps, including additional staff training. Significantly, in most cases, the Commissioner required the banks to agree to submit data protection procedures to audit by his office, echoing the approach adopted by the Federal Trade Commission in response to data breaches. Banks that were the subject of this enforcement activity have indicated that having to deal with the prospect of audits is encouraging their businesses to treat data protection more seriously.

The means by which the undertakings were obtained is noteworthy. The Information Commissioner has the power to issue an Enforcement Notice compelling remedial steps to be taken where he considers and organization to be in breach of the Act. Instead of proceeding to that stage, the Commissioner has been prepared to negotiate the terms of legally binding undertakings with companies suspected of breach. Significantly, these undertakings must be signed by an authorized signatory. In many cases, this will be the CEO, ensuring that breaches of the Data Protection Act are drawn to the attention of senior management.

In addition to obtaining undertakings, the Commissioner publishes them on his Web site and also issues a press release, ensuring maximum media coverage for these transgressions.

Coextensive Jurisdiction

Another theme which is evident from the recent enforcement activities of European DPAs is a greater degree of cooperation between regulators with overlapping jurisdiction, but different powers of enforcement. In the U.K., we saw this most clearly in 2007 when the Financial Services Authority (FSA) fined Nationwide Building Society £980,000 (\$1.9 million) and Norwich Union £1.26 million (\$2.5 million) for events which, in both cases, could have constituted breaches of data protection laws.

In the case of the Nationwide, the lapse concerned an employee downloading customer data onto an unencrypted laptop which was then stolen from the employee's home. The employee did not think to report the theft until after a vacation, some three weeks after the theft. Staff at Nationwide received little guidance from existing procedures and did not know how to respond to the data security breach. The FSA, which regulates financial services institutions, has particular responsibility for ensuring that regulated entities have adequate systems and controls and found Nationwide's training and procedures to be inadequate. Unlike the Information Commissioner, the FSA does have the power to impose fines and, in fining Nationwide £980,000 (\$1.9 million), it explicitly stated that the amount of the fine reflected Nationwide's inadequate procedures and was intended to serve as an example to others.

Similarly, in the case of Norwich Union, the breach concerned poor security procedures. As in the case of Nationwide, these could have fallen to the Information Commissioner to investigate but, instead, the FSA took the lead and imposed a substantial fine.

Data Breaches

In Europe, the growing awareness of data breaches has led to increased scrutiny by regulators of how companies are handling these incidents. This is significant given that, for the most part, European data protection laws do not contain a data breach notification requirement. In the U.K., which has experienced the most significant data breaches during the past six months, the aftermath of the U.K. government's loss of 25 million records in November 2007 has resulted in stronger enforcement action and calls for legislative changes to further encourage companies to take their data protection obligations seriously. The Information Commissioner has demanded changes to the U.K.'s data protection legislation, to make a serious breach of the Data Protection Act 1998 a criminal offense. Further, with clear overtones of U.S.-style Sarbanes-Oxley reporting requirements, the Commissioner also suggested that CEOs should certify, perhaps in the company's annual report, that they are satisfied that appropriate safeguards are in place to protect personal data.

HMRC Data Breach

On Nov. 22, 2007, the U.K. government admitted that its tax office, Her Majesty's Revenue and Customs, (HMRC) had lost two CDs containing the unencrypted personal details of 25 million U.K. residents. The data was simply downloaded onto two CDs by a junior employee who then thought nothing of sending the CDs in the post to the National Audit Office.

Significantly, the HMRC data breach was not an isolated incident.

- Days after the HMRC breach was announced, the Foreign and Commonwealth Office was publicly named and shamed by the Information Commissioner for a security breach involving an online visa application process. The Web site, which enabled individuals to make online applications for visas to the U.K., was defective, so that the personal details of applicants were available to other users of the site.
- The personal details of three million British learner drivers were lost by a U.S. contractor to the Driving Standards Agency. This incident was used by trade unions to question why the British public sector is relying on private sector vendors to process data, some of whom are perceived to be largely unaccountable. Others began to query whether transfers of personal data abroad for processing are sufficiently secure.
- A number of Primary Healthcare Trusts admitted that they had suffered several data breaches involving patient records.
- On Jan. 19 it was revealed that the Ministry of Defence suffered a laptop theft which compromised 600,000 individuals who had applied to join the British armed forces. These records contain copies of passports, bank account details, and details of next of kin, as well as name, address and health records. This breach was announced at the same time individuals were convicted for trying to obtain details of and kidnap a Muslim soldier in the British Army as part of a terrorist plot. The carelessness of this data breach by the Ministry of Defence caused public outcry.

Other U.K. Data Breaches

These incidents are not limited to the public sector.

- In addition to the Norwich Union example, the Carphone Warehouse and TalkTalk were given 35 days to rectify various breaches of the Data Protection Act. Significantly, the alleged breaches went beyond breaches of security and included poor data collection practices and a failure to ensure data remain accurate and up to date. As is becoming customary, the Information Commissioner secured an acknowledgement of breach and an undertaking to undertake remedial steps to rectify the breach. The undertaking is published on the Commissioner's Web site and was the subject of a press release.
- In January, Marks & Spencer were the subject of enforcement action following the theft of a laptop from a third party advisor to the company. The laptop contained details of the pension plans of Marks & Spencer's staff. The Information Commissioner found that Marks & Spencer had failed to safeguard its staff data. It would seem, however, that Marks & Spencer sought to negotiate a confidentiality clause as part of its undertaking to the Commissioner. The Commissioner refused to grant confidentiality and proceeded, unilaterally, to issue an Enforcement Notice and a press release, both of which were published on the Commissioner's Web site. This incident is significant because of the Commissioner's refusal to grant confidentiality.

Unsurprisingly, these events are creating momentum for change to U.K.'s data protection laws.

Extension of Existing Enforcement Powers

A key fact highlighted by the HMRC data breach is that in the U.K. the Information Commissioner has limited powers to take enforcement action following a breach of the data protection laws. There is a power to prosecute, but only in limited circumstances. There is

an exemption from prosecution for a government department that breaches the law. There is no power to fine. The Commissioner's power to conduct spot checks or audits on data controllers is subject to the controller consenting in advance. This position looks certain to change.

Shortly after the HMRC breach, the Information Commissioner called for better enforcement powers, including:

- (i) a new criminal sanction to apply to data controllers who knowingly or recklessly fail to comply with the Data Protection Act and where the failure gives rise to a substantial risk that a person will suffer damage or distress.
- (ii) a duty to notify data breaches. The Information Commissioner left open for debate the issues of whether notification should be made to individuals, to the regulator, or to both, and what the harm threshold for notification should be.
- (iii) the ability to require an organization to commission an independent review into its data protection compliance. The Information Commissioner sees this proposal as simply an extension of the modern regulatory agenda to the data protection arena and noted that such reviews might be conducted concurrently with inspections carried out by the Information Commissioner's Office.
- (iv) a requirement for CEOs to certify, perhaps in the organizations annual report, that they are satisfied that appropriate security safeguards are in place to protect personal data.

The last of these proposals is the most radical but perhaps the most likely to result in data protection issues attracting board level attention within organizations.

The U.K.'s contemplation of specific data breach laws mirrors discussions taking place in other jurisdictions, notably in Canada, Australia and New Zealand, as well as discussions in the United States relating to a federal data breach law. In addition, in the context of the European Commission's recent review of the Data Retention Directive, a data breach notification requirement was proposed. The U.K.'s consideration of a data breach law is driven by the experience of some very significant data breaches but should be seen as part of the wider international debate of how best to safeguard the vast quantities of personal data processed by the public and private sectors.

Conclusion

In the past, companies have taken comfort from the fact that despite conservative data protection laws, many of the European DPAs have little in the way of real enforcement power. That position has now changed. Recent enforcement activity across Europe is part of wider initiatives on the part of data protection regulators to ensure that personal data is respected and processed fairly and legitimately. As we have seen, there is a discernible refocusing of efforts to ensure that data controllers are accountable for the data they collect and process. Perhaps the most significant indication of this is the call from the U.K. Information Commissioner for senior executives to be more visible in assuring staff and customers that their data will be respected. How many senior executives would be prepared to give such an assurance today?