dataprotectionlaw&policy

FEATURED ARTICLE
09/09

cecile park publishing

Head Office UK Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND
tel +44 (0)20 7012 1380 fax +44 (0)20 7729 6093 info@e-comlaw.com
www.e-comlaw.com

Local solutions to data breach notification issues

An increasing number of data breaches have been notified to individual Member States recently, which has led to extensive debate as to whether the EU should adopt a breach notification law. With a particular focus on the UK, France and Germany, Bridget Treacy, a Partner at Hunton & Williams, examines how individual Member States are devising local solutions to the data breach issue and how the recent debate surrounding the e-Privacy Directive contributed to the data breach debate.

A recent study claims that two out of every three Australian companies leak data[1]. We may not have equivalent statistics for the EU but, in the last 18 months some 600 serious data breaches have been reported to the Information Commissioner in the UK. Data breaches have also been reported in many other EU Member States. Increasingly, Europe is considering US-style data breach laws as a means of forcing organisations to safeguard the data they handle. To date, the primary EU debate surrounding a data breach law has taken place in the context of the review of the e-Privacy Directive, but increasingly we see individual jurisdictions exploring the merits of passing local breach laws. This article will explore some of those themes, with a particular focus on the UK, France and Germany.

What is data breach?

'Data breach' is a generic term applied to many situations in which the security or integrity of data is compromised, whether deliberately or not. Despite the data security requirements of our EU data protection law, there have been many recent examples of data breaches, suggesting that organisations do not comply with the basic data security requirement. A brief review of the reported UK breaches reveals many rudimentary mistakes, including data being downloaded onto unencrypted portable devices that are lost, data processed by third parties without adequate safeguards in place, numerous lost laptops and data that are carelessly disposed of. In this context, there have been calls for a US-style breach notification law in Europe.

US data breach laws

US data breach laws had their genesis in the California Computer Security Breach Notification Act (S.B. 1386), which came into effect on 1 July 2003. Over time, the Californian requirement to notify individuals of data breach incidents has come to include all affected persons, whether a resident in California or not. More than 45 individual states in the US have now enacted data breach laws. There has been much analysis of the effectiveness of US data breach laws, focusing on whether the notification requirement itself contributes significantly to reducing identity theft and other losses that may flow from a data breach incident. It is difficult to draw a clear conclusion that data breach laws reduce identity theft[2]. What is clear is that the existence of the laws and the consequences of breach act as incentives to organisations to ensure that data are adequately safeguarded.

EU data breach laws

There is currently no general provision in the EU Data Protection Directive requiring the notification of data breaches, whether to regulators or to the individuals whose data have been compromised. Notwithstanding this, many Member States have begun to develop their own notification requirements in light of the increasing public concern over data security.

UK breach laws

Since the HM Revenue & Customs data breach in 2007[3], the UK Information Commissioner has promoted a best practice requirement to notify his office of serious data breaches and, in some cases, to notify affected individuals. The notification requirement is based on a harm threshold. Notification is required where

- the breach is likely to result in significant harm to individuals;
- the breach involves a large volume of compromised data; or
- the compromised data are sensitive.

In the UK, the potential for harm to individuals is the most significant factor to consider when deciding whether to notify a breach. The assessment requires an organisation to consider the nature of the compromised data and the circumstances in which the data were compromised. If data are sensitive, such as health data, it may not matter that only a small number of records were affected. The risk of harm to the small number of affected individuals may be high. Where there is a real likelihood of harm, there is a presumption to report. Where the risk of harm is low, for example because the storage device was encrypted, there is no need to notify. Notification is made to the Information Commissioner, but organisations frequently take the initiative and notify individuals as well. The Information Commissioner expects to be informed of whether individuals have been informed and may require that individuals are notified. At a practical level, the decision to notify can be a finely balanced decision.

In the UK, the Information

Commissioner's powers to impose sanctions for a data breach are limited, but expected to strengthen in early 2010. At present, the Information Commissioner may issue an enforcement notice, but from April 2010 will be able to impose a fine, likely to be in the region of 5-10% of an organisation's turnover, where the breach is deliberate or reckless.

German breach laws

Recent data breaches in Germany have generated public outrage at careless data handling[4] and German businesses have spent significant sums dealing with breaches. Research published in December 2008 suggests the average cost of handling a data breach in Germany is €112 per compromised record. The total cost of handling breaches ranges from €267,000 to €6.75 million, with the average being over €2.41 million.

In response to public concern over the largest breaches, Germany has just passed Amendment II (Data Trading) to the German Data Protection Act. Amongst other measures, this includes a data breach notification requirement. After 1 September 2009, German organisations will be required to notify incidents involving unlawful data transfers or unauthorised access by third parties that cause a data loss likely to have a serious impact on the rights or protected interests of the individuals to whom the data relates.

As in the UK, the new German breach notification obligation requires a harm-based assessment. The legislative commentary to the draft law indicates that the type of data compromised, and the likelihood of harm to individuals, should be taken into account when assessing whether the incident is likely to have a 'serious impact'. Where notification is required, it will be made to the local data protection authority and to affected individuals, and must be made without delay.

The existence of the laws and the consequences of breach act as incentives to organisations to ensure that data are adequately safeguarded

Where notification to individuals would be disproportionately burdensome, particularly where a large number of individuals is affected, notice must be provided to the general public. Such notification must be made by placing at least a half-page advertisement in daily national newspapers, or by other means that would provide equivalent exposure for the notification.

French breach laws

Currently, there is no general data breach notification requirement under the French Data Protection Act, although telecom operators have an obligation to notify their subscribers if there is a particular risk of a breach of network security. Otherwise, there is a general requirement (as in other EU jurisdictions) that organisations must take all necessary measures, having regard to the nature of the data and the risk associated with the data processing, to preserve the security and confidentiality of personal data. A failure to comply with this requirement is punishable by a maximum fine of €300,000 and up to five years' imprisonment.

In addition, the French Data Protection Authority, the CNIL, has issued general security guidelines intended to assist data controllers to implement adequate security measures. As part of its investigatory powers, the CNIL can visit the premises of a data controller and inspect its data processing systems, including to determine whether adequate data security measures have been implemented. Following such an investigation, the CNIL may impose administrative sanctions on the data controller, ranging in severity from a warning to a fine, an order to stop processing the data or the withdrawal of an authorisation to process the data.

In a recent report on the 'right to privacy in the age of digital memories', the French Senate proposed creating an obligation for data controllers to notify the CNIL of data security breaches. The Senate observed that a well-structured and enforced obligation to notify data security breaches may act as an incentive to companies to reinforce their security measures. The Senate has also proposed that the CNIL's decisions imposing sanctions on negligent data controllers should be routinely publicised with a view to informing individuals about important security breaches. Discussions of data breach notification requirements in France are being keenly watched.

E-Privacy Directive

As individual EU Member States have considered whether and, if so, how to create a data breach notification requirement, the issue has been extensively debated as part of the review of the e-Privacy Directive. The review itself was broader than just data breach and included a package of reforms for the telecommunications sector. As part of this review, a draft directive amending the e-Privacy Directive is currently being finalised by the EU institutions under the co-decision procedure.

Finalising the draft Directive has been a difficult process. On the issue of data breach, there are five issues that have been the subject of exhaustive debate:

- devising a workable definition of 'security breach';
- determining which entities should be subject to any notification obligation;
- identifying the factors that would trigger an obligation to

notify;
- identifying the entity responsible for determining whether a breach triggers the notification obligation in (iii) above; and
- determining the recipients of any notice[5].

There has been general agreement amongst the European Parliament, the Council and the European Commission as to the definition of security breach. The definition is wide, being a 'breach of security leading to an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data'. Thus, unauthorised access to data as well as inadvertent data losses will be covered.

There was, however, disagreement as to which entities would be subject to a notification obligation. Ultimately, this will be restricted to internet service providers and telecommunications services providers, but there was extensive debate as to whether the providers of all online services (e.g. including banks and online retailers) should also be subject to these requirements.

The EU data breach debate has focused on the desirability of devising a harms-based trigger to the notification obligation. Many data protection authorities and commentators observing the US' experience of data breach notification requirements have recommended a harms-based test for notification so as to reduce the likelihood of notification fatigue. The current draft of the Directive states that where a personal data breach is 'likely to adversely affect the personal data and the privacy of a subscriber or an individual' an additional notification must be made to such subscriber or individual unless the organisation has applied 'appropriate protections' to the data which render it unintelligible to any unauthorised person who may subsequently gain access to such data (i.e. encryption). This position departs significantly from the Council's original position, where such an obligation was triggered only by a 'serious breach'. Where the organisation fails to notify an individual, the national regulator may do so in its place.

The notification to the subscriber or individual must set out, at a minimum:
- the nature of the breach;
- contact points from which further information relating to the breach can be obtained; and
- recommendations to mitigate the possible negative effects of the breach.

In addition, any notification to the national regulator shall include a description of the consequences of, and the measures proposed or taken by the provider to address, the data breach.

The draft Directive purports to provide the national regulator with additional auditing powers to ensure organisations comply with their notification obligations. The national regulator may impose appropriate sanctions where the organisation fails any such audit. Organisations must also maintain a record of any breaches.

In terms of the overall passage of the amendment to the e-Privacy Directive, the Council failed to accept Parliament's amendments in full, although the data breach notification provisions are agreed. A conciliation committee will negotiate a compromise text to be approved by both institutions in a third reading, due in December.

Conclusion

Once the draft Directive has been implemented it will be interesting to see whether the EU institutions have succeeded in striking a balance between ensuring that there are sufficient safeguards to protect the public against harm from security breaches and ensuring that the national regulators' resources are not over-stretched by the additional notification requirements. The success or otherwise of the draft directive will be keenly watched. The incidence of serious data breaches has increased in Europe and individuals are calling for organisations to be held to account for data breaches, and punished. It may well be only a matter of time before we see an EU-wide breach notification requirement, with very general application.

Bridget Treacy Partner
Hunton & Williams
btreacy@hunton.com

This article was written with assistance from Dr Jorg Hladjk, Olivier Proust and Shveta Ohri.

1. www.pgp.com/insight/research_reports/ponemon_2009_encryption_trends.html
2. 'Do Data Breach Laws Reduce Identity Theft?' Recent research suggests that notification requirements have only reduced identity theft by 2%. weis2008.econinfosec.org/papers/Romanosky.pdf
3. The entire UK child benefits database was downloaded by a junior employee onto two unencrypted CDs and posted to the National Audit Office in 2007. The CDs were lost in the post.
4. T-Mobile and Deutsche Telekom (parent company of T-Mobile) data breach, October 2008, where 17 million German customer records held on a storage device were stolen. http://www.theregister.co.uk/2008/10/06/t_mobile_records_lost/
Government data breach, December 2008, where 332 top secret files were lost during the preceding 10 years. There is no indication of where they are now. http://www.thelocal.de/national/20081213-16113.html
In December 2008, credit card information, names, addresses, bank account information and transaction information of customers of Landesbank Berlin was anonymously sent to Frankfurter Rundschau newspaper. http://www.thelocal.de/national/20081213-16107.html
5. Second Opinion of the European Data Protection Supervisor on the Review of Directive 2002/58/EC, para 12.

cecile park publishing

Head Office UK Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND
tel +44 (0)20 7012 1380 fax +44 (0)20 7729 6093 info@e-comlaw.com
www.e-comlaw.com

Registered number 2676976 Registered address 141 Wardour Street, London W1F 0UT VAT registration 577806103

e-commerce law & policy

Many leading companies, including Amazon, BT, eBay, FSA, Orange, Vodafone, Standard Life, and Microsoft have subscribed to ECLP to aid them in solving the business and legal issues they face online.
ECLP, was nominated in 2000 and again in 2004 for the British & Irish Association of Law Librarian's Legal Publication of the Year.
A twelve month subscription is £420 (overseas £440) for twelve issues and includes single user access to our online database.

e-commerce law reports

You can now find in one place all the key cases, with analysis and comment, that affect online, mobile and interactive business. ECLR tracks cases and regulatory adjudications from around the world.
Leading organisations, including Clifford Chance, Herbert Smith, Baker & McKenzie, Hammonds, Coudert Brothers, Orange and Royal Mail are subscribers.
A twelve month subscription is £420 (overseas £440) for six issues and includes single user access to our online database.

data protection law & policy

You can now find in one place the most practical analysis, and advice, on how to address the many problems - and some opportunities - thrown up by data protection and freedom of information legislation.
DPLP's monthly reports update an online archive, which is an invaluable research tool for all those who are involved in data protection. Data acquisition, SMS marketing, subject access, Freedom of Information, data retention, use of CCTV, data sharing and data transfer abroad are all subjects that have featured recently.
Leading organisations, including the Office of the Information Commissioner, Allen & Overy, Hammonds, Lovells, BT, Orange, West Berkshire Council, McCann Fitzgerald, Devon County Council and Experian are subscribers.
A twelve month subscription is £390 (public sector £285, overseas £410) for twelve issues and includes single user access to our online database.

world online gambling law report

You can now find in one place analysis of the key legal, financial and regulatory issues facing all those involved in online gambling and practical advice on how to address them. The monthly reports update an online archive, which is an invaluable research tool for all those involved in online gambling.
Poker, payment systems, white labelling, jurisdiction, betting exchanges, regulation, testing, interactive TV and mobile gaming are all subjects that have featured in WOGLR recently.
Leading organisations, including Ladbrokes, William Hill, Coral, Sportingbet, BskyB, DCMS, PMU, Orange and Clifford Chance are subscribers.
A twelve month subscription is £520 (overseas £540) for twelve issues and includes single user access to our online database.

world sports law report

WSLR tracks the latest developments from insolvency rules in football, to EU Competition policy on the sale of media rights, to doping and probity. The monthly reports update an online archive, which is an invaluable research tool for all involved in sport.
Database rights, sponsorship, guerilla marketing, the Court of Arbitration in Sport, sports agents, image rights, jurisdiction,domain names,ticketing and privacy are subjects that have featured in WSLR recently.
Leading organisations, including the England & Wales Cricket Board, the British Horse Board, Hammonds, Fladgate Fielder, Clarke Willmott and Skadden Arps Meagre & Flom are subscribers.
A twelve month subscription is £520 (overseas £540) for twelve issues and includes single user access to our online database.

priority order form

FAX +44 (0)20 7729 6093
CALL +44 (0)20 7012 1380
EMAIL dan.towse@e-comlaw.com
ONLINE www.e-comlaw.com
POST Cecile Park Publishing 17 The Timber Yard, Drysdale Street, London N1 6ND

☐ Please enrol me as a subscriber to **e-commerce law & policy** at £420 (overseas £440)
☐ Please enrol me as a subscriber to **e-commerce law reports** at £320 (overseas £440)
☐ Please enrol me as a subscriber to **data protection law & policy** at £390 (public sector £285, overseas £410)
☐ Please enrol me as a subscriber to **world online gambling law report** at £520 (overseas £540)
☐ Please enrol me as a subscriber to **world sports law report** at £520 (overseas £540)

All subscriptions last for one year. You will be contacted at the end of that period to renew your subscription.

Name			
Job Title			
Department		Company	
Address			
Address			
City		State	
Country		Postcode	
Telephone		Fax	
Email			

1
Please **invoice me** Purchase order number
Signature Date

2
I enclose a **cheque** for the amount of
made payable to *'Cecile Park Publishing Limited'*

3
Please debit my **credit card** VISA ☐ MASTERCARD ☐
Card No. Expiry Date
Signature Date
VAT No. (if ordering from an EC country)

Periodically we may allow companies, whose products or services might be of interest, to send you information.
Please tick here if you would like to hear from other companies about products or services that may add value to your subscription. ☐