BNA International

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 5 May 2009

Commentary

News

Publishing Director:
Andrea Naylor

Editors:
Jacqueline Gazey and Nicola McKilligan

Commissioning Editor: **Shelley Malhotra**
Production Manager: **Nitesh Vaghadia**

Submissions by Authors: The Editors of *World Data Protection Report* invite readers to submit for publication articles that address issues arising out of the regulation of data protection, either on a national or transnational level. Articles with an appeal to an international audience are most welcomed. Prospective authors should contact Andrea Naylor, World Data Protection Report, BNA International Inc, 29th Floor, Millbank Tower, 21-24 Millbank, London SW1P4QP, U.K. Tel. (+44) (0)20 7559 4800; fax (+44) (0)20 7559 4880; or e-mail: anaylor@bna.com. If submitting an article by mail please include an electronic copy of the article in a recognised software.

World Data Protection Report is published monthly by BNA International Inc., a subsidiary of The Bureau of National Affairs, Inc., Washington, D.C., U.S.A. Administrative headquarters: 29th Floor, Millbank Tower, 21-24 Millbank, London SW1P 4QP, England. Tel. (+44) (0)20 7559 4801; Fax (+44) (0)20 7559 4840; e-mail marketing@bnai.com. In the U.S. call toll-free on: 1-800-727-3116.

Subscription price: U.K. and rest of world £725; Eurozone €1,175; U.S. and Canada U.S. $1,245. Additional copies of this publication are available to existing subscribers at half price when they are sent in the same envelope as a standard subscription.

Website: *www.bnai.com*
ISSN 1473-3579

Welcome to May's WDPR which once again brings you all the latest European and Global data privacy news. For May's edition we also carry an overview of the European Commission guidelines for SMEs on personal data transfers to countries outside the EEA by Dominic Hodgkinson. We also have a very special report on the employment law consequences of violations of IT-security by Bernhard Trappehl and regular contributor, Michael Schmidl.

As ever, I hope you enjoy this edition.

Nicola McKilligan

Co-editor

Please contact us with your opinions or suggestions or if you would like to write for us, by phone on: +44 (0)7720 774224 or by email at nmckilligan@europp.co.uk, or jgazey@europp.co.uk

Topical Summary

Legislation and Guidance

Personal Data

Country Checklist

CANADA

CANADA

CZECH REPUBLIC

DENMARK

EUROPEAN UNION

EUROPEAN UNION

EUROPEAN UNION

EUROPEAN UNION

GERMANY

GERMANY

GREECE

HUNGARY

INDIA

IRELAND

NEW ZEALAND

SWEDEN

  WDPR ISSN 1473-3579

Legislation and Guidance

New EU code of conduct for computerised reservations systems

By Wim Nauwelaerts, Attorney at Law, Hogan & Hartson, LLP.

On March 29, 2009, Regulation (EC) No 80/2009 of the European Parliament and the Council (dated January 14, 2009) on a Code of Conduct for computerised reservation systems (CRS) entered into force. A CRS is a computerised system that permits subscribers, such as travel agencies, to locate travel information about flight schedules, seat availability and fares, with or without facilities to make reservations, issue tickets or make use of related services. The Regulation, which repeals Council Regulation (EEC) No 2299/89 of July 24, 1989, aims to ensure transparent and comparable terms of competition in the market for distribution of travel services through computerised reservation systems. The Regulation applies to any type of CRS offered for use in the EU, provided that it contains air-transport products involving passenger carriage.

System vendors' rules of conduct

The Regulation imposes certain obligations on system vendors that are responsible for the operation or marketing of a CRS. These obligations include, for example, ensuring that CRS contracts (with air carriers as well as CRS subscribers) do not contain unfair or unjustified conditions, and that users are free to avail themselves of alternative reservation systems. Furthermore, system vendors are not allowed to reserve specific CRS facilities for one or more participating carriers (including possible parent carriers that control or participate in the capital of the system vendor). System vendors should display participating carriers' travel information in a neutral and comprehensive manner, without discrimination or bias. The Regulation permits system vendors to release CRS-related marketing, booking and sales data, in so far as the data are offered to all participating carriers with equal timelines and on a non-discriminatory basis. With regard to these business data, the Regulation subjects system vendors to what could be viewed as a confidentiality duty: if the data result from the use of CRS facilities by subscribers established in the EU, the data cannot identify these subscribers (directly or indirectly), unless there is an agreement to the contrary or subscriber identification is essential for billing purposes.

Wim Nauwelaerts can be contacted at: wnauwelaerts@hhlaw.com

Protection of personal data

As far as processing of personal data in the context of a CRS is concerned, the Regulation includes ten provisions that particularise and complement the principles contained in EU Data Protection Directive 95/46/EC. The main data protection requirements in these provisions can be summarised as follows:

- Personal data collected in the course of the activities of a CRS for purposes of making reservations or issuing tickets can only be processed in a way compatible with such purposes;
- CRS system vendors will be viewed as data controllers, responsible for the processing of a data subject's personal data;
- Personal data can only be processed in so far as their processing is necessary for the preparation or performance of a contract to which the data subject is a party;
- Sensitive data (revealing, for example, racial origin, religious beliefs or health status) can only be processed on the basis of the data subject's explicit and informed consent;
- System vendors must ensure that identifiable booking information is stored offline within 72 hours of the booking. The maximum retention period for these data is three years and the data can only be used for handling billing disputes;
- Upon request, CRS subscribers must inform consumers of the name and address of the system vendor, the purposes of the processing, the duration of the retention period, and the means available to data subjects to exercise their data access rights. Data subjects must have free access to personal data relating to them;
- If system vendors operate other databases in addition to a CRS, technical and organisational measures must be in place to ensure that data protection rules are not circumvented as a result of database interconnections, and to ensure that personal data are only accessible for the specific purposes for which they were initially collected;
- System vendors can release marketing, booking and sales data provided that they do not make it possible to identify (directly or indirectly) natural persons or, where applicable, the organisations or companies that those natural persons represent. This last requirement raises the interesting question as to what extent corpo-

rate customers can invoke the Regulation's data protection provisions. In principle, information relating to legal persons is not covered by EU Data Protection Directive 95/46/EC. However, the Regulation stipulates that the data protection rights recognised in the Regulation are complementary to the rights laid down by EU Data Protection Directive 95/46/EC.

Enforcement by the European Commission

The Regulation empowers the European Commission with broad authority to investigate and, where necessary, sanction infringements, including violations of the Regulation's provisions on data protection and confidentiality. Acting on a complaint or on its own initiative, the Commission can require companies and companies' associations to provide all necessary information about their compliance with the Regulation. If the provisions of the Regulation have been infringed, intentionally or negligently, the Commission can impose fines of up to 10 percent of a company/association's total revenues in the preceding business year.

Employment law consequences of violations of IT-security

By Bernhard Trappehl and Michael Schmidl.

Establishing and maintaining IT-security is a management obligation. The legal framework points to a constant monitoring obligation for management in order to make sure that measures once taken continue to be adequate in a changing environment. Part of establishing and maintaining adequate IT-security is to put guidelines for employees into place, to train them regularly and to make sure that the guidelines are actually respected. The following article outlines IT-security as a management task (I), the role of IT-security within the employee relationship (II), possible general reactions to violations of IT-security (III) and particular examples of how violations of IT-security can be sanctioned (IV).

I. IT-security as a management task

Law of IT-security

The existing law does not provide for a standardised definition of IT-security. There is no law regulating in a definitive way all questions relating to IT-security. An important aspect in this context is illustrated by the legal provisions on the security of information technology. The law on the creation of the Federal Bureau of Security in information technology (BSIG) is, in several respects, important for the task of creating IT-security as part of a company's corporate governance. Sec. 2 (2) BSIG defines security in information technology as, "the compliance with security standards concerning the availability, integrity or confidentiality of information by security provisions in IT-systems or components or when applying information technology systems or components". Measures of relevance for IT-security may also be seen in the annex to Sec. 9 Federal Data Protection Act (FDPA). Also Secs. 25a German Banking Act (KWG), 33 German Securities Trade Act (WpHG) and 109 German Telecommunication Act (TKG) contain requirements for the IT-security for specific regulatory situations. In light of the fact that threats to IT-security also result from human behaviour, such norms may be seen as part of the law of IT-security and require the implementation of technical and organisational measures to prevent IT-risks based on inaccurate human intervention.

Dr. Trappehl is a partner of Baker & McKenzie Partnerschaft von Rechtsanwälten, Wirtschaftsprüfern, Steuerberatern und Solicitors, Munich and member of the firm's Employment Group. Dr. Trappehl is admitted as an attorney specialising in labour and employment law. He is also admitted as Abogado (Madrid). The author may be contacted at: Bernhard.Trappehl@bakernet.com.

Dr. Michael Schmidl, Maître en Droit, LL.M. Eur., is a partner of Baker & McKenzie Partnerschaft von Rechtsanwälten, Wirtschaftsprüfern, Steuerberatern und Solicitors, Munich and member of the firm's Information Technology Group. Dr. Schmidl is a specialised attorney for IT-Law and a lecturer for Internet law at the University of Augsburg. He may be contacted at: Michael.Schmidl@bakernet.com.

Corporations

The duty to establish and maintain adequate IT-security within a company is a task of the management. The relevant law for corporations is the Law of control and transparency within the company ("KonTraG") that came into effect on May 1, 1998. The KonTraG crystallised the requirements for the management of a corporation concerning the security of the company and obligates it to introduce corresponding prevention measures within the framework of the general task of risk management. The corresponding duty is contained in Sec. 91 (2) AktG. It was introduced by the KonTraG and obligates the board (*i.e.* all members of the board) as part of the duty of a diligent management, pursuant to Sec. 93 (1) first sentence AktG, to provide for adequate measures especially implementing a monitoring system that would recognise early enough, such developments that threaten the continuity of the company's business. Secs. 91, 93 AktG do not provide concrete specifications of duties serving as a guideline for CEOs and board members. Neither do the explanations of the scope of duties of the preamble of the KonTraG. But the Kon-

  WDPR ISSN 1473-3579

TraG made clear at least, that the "ordinary care" of the management also comprises detecting and fighting IT-risks and that violating these duties may lead to the personal liability of the corresponding manager (CEO and board members).

Other company forms

According to the prevailing opinion in Germany, the KonTraG and the clarifications regarding the management's duties in the area of establishing and maintaining IT-security effected by the KonTraG may be applied to the form of limited company (GmbH) and as a general principle also to other company forms. Pursuant to Sec. 43 GmbH (limited liability company law) the directors have to exercise the care of a prudent businessman. The measures required by the KonTraG for corporations concerning a general risk management and the reality that the "ordinary care" of the company management also comprises detecting and fighting IT-risks also apply to the interpretation of the legal term of the "care of a prudent business man" with the consequence that the violation of these duties may lead also, at the level of the GmbH, to the personal liability of responsible management. The described requirements also apply to partnerships (OHG) and limited partnerships (KG) if no individual person is liable. On this basis, OHG and KG are obliged to implement and maintain IT-security within the company. Equally, the elements of risk management and an early detection system have to be adequately considered as parts of the security of the company.

General limitations

The measures required to establish and maintain the IT-security have to be tailored to the specific company, its individual situation, its risk situation, and needs to be checked at regular intervals. This principle applies to all company forms. Typically, the size of the company, its structure and the exact branch of activity as well as possible changes of the layout and the scope of the business must be considered. A carte blanche for second-rate security measures cannot be deducted from this analysis. Rather, it must be possible to explain that, as a concrete result of one of the factors added to the overall analysis why in general or at repeated analysis, there are less risks and consequently why there is less need of risk management or prevention. Furthermore there are certain security standards that have to be complied with within every company for the simple reason, for example, in the form of measures of data backup (short-term storage of data, programs and configurations in a way guaranteeing access even in case of disaster), archiving (long-term storage of data even in case of migration of systems and data), virus protection (virus scanners and training of employees) and emergency prevention (development of possible disaster recovery scenarios and planning of counter-measures).

II. IT-security within the employment relationship

General statutory obligations

As shown above, members of the management are the addressees of statutory obligations in the field of establishing and maintaining IT-security. There are no comparable statutory provisions directly obliging employees to keep certain security standards within the company. The existing general statutory duties (*i.e.* obligations applicable to everyone) to act, such as Sec. 17 of the Act Against Unfair Competition (UWG), Sec. 201ff., 203, 206, 303a *et seq.* Penal Code are not tailored to the IT-security of companies in general. The norms may contain prohibitions serving to reach the aims of IT-security in certain situations. These norms, however, tailored to prevent certain specific violations, are no autonomous legal basis to establish and maintain IT-security within the company. What brings to bear here is that criminal laws or other norms prohibiting certain forms of behaviour are not suited as a basis for risk management and prevention in a company. Such laws are addressed to everybody, not only employees, and function as *ultima ratio* rather than as subtle measures of risk management in a company.

Security specific duties to act

There are isolated specific statutory duties to act that do not tie in with the position as an employee in general but with the assignment of a certain function. Pursuant to Sec. 4g (1) FDPA, the Data Protection Official has the task, for example, to work towards the compliance with the FDPA and other provisions of data protection. This duty also comprises the examination as to whether there are adequate technical and organisational measures pursuant to the annex to Sec. 9 of the FDPA serving the technical data protection. Because of the FDPA's objective to protect the individual against his right to privacy being impaired through the handling of his personal data (cf. Sec. 1 (1) FDPA), this technical data protection however is to distinguish from IT-security in general which does not lie within the scope of the data protection official and which serves in the broadest sense to maintain the operability of the company and the company value incorporated therein. Based on this definition, the duties of the internal data protection official, especially his duty to examine the existence and the adequacy of measures pursuant to the annex to Sec. 9 FDPA, may be seen as a part of reaching and maintaining IT-security, but are not a general specification of IT-security.

Fiduciary duty and auxiliary duties

Considering that there are no sufficient general and special statutory duties for employees towards their employer, the general fiduciary duty of the employee towards his employer and auxiliary duties resulting from the employment relationship come into consideration as sources for legal duties to maintain IT-security within the company. Independently of the function and position the employee holds within the internal organisation and the duties he is contractually obliged to fulfil, he always

meets several auxiliary duties in the form of a fiduciary duty. These comprise, for example, the duty to keep business secrets, the prohibition to intentionally open virus-infected email-attachments as well as the prohibition to make illegal copies by means of the company's IT-systems. Additionally, the employee has the obligation not to damage the employer through his own controllable behaviour even if such obligation merely results from the general prohibition of injuring third parties. With regards to the generality of the objective of optimal IT-security and the requirement of specific company decisions concerning the appropriate master plan, however, it is not possible to establish a final list of requirements on the basis of a fiduciary duty and auxiliary duties.

Agreed measures

As a consequence of the haziness of the objective of IT-security and with regard to the nonexistence of sufficient legal duties, the definition of obligations and prohibitions perfectly tailored to the situation of the specific company aiming to achieve and maintain optimal IT-security is indispensable. The conforming specification is regularly effected in the form of an IT-security-guideline that the employee is committed to as soon as the employment contract is concluded. If necessary, the obligation to comply with such a guideline may be imposed later by means of an instruction. Especially considering that a lot of IT-security risks result from unconscious misbehaviour of the employees (intentional misbehaviour cannot be prevented anyway), the IT-security guideline may be characterised as the central element of an IT-security concept. Exemplarily, the guideline of IT-security may contain provisions concerning the use of Internet and e-mail as well as the storage of private e-mails and the handling of e-mail-attachments, the handling of passwords, the downloading of programs and the installation of software, the use of USB-devices and the local storage of data on a notebook.

III. Possibilities of reaction and risk of establishment of custom and practice

Validity of general principles of employment law

If the employer does not want to ignore violations of (as recommended on the basis of an established IT-security guideline) duties of IT-security without any sanction, he can react basically with an admonishment, warning, an ordinary behaviour-based termination (as the final termination is only *ultima ratio* it has to be examined if the same purpose may be reached by means of a termination for change of contract) or a termination for cause. If the admonishment is chosen as the mildest form of a sanction, it must be borne in mind that it cannot serve as a reason for termination in case of a recurring violation. The warning reminds the employee of behaving in compliance with his contract. It has to point out the consequences of further violations due to reasons of proportionality and is, seen apart from extreme exceptional cases (when the employee could not expect that his behaviour would be tolerated by the employer), the necessary basis for a behaviour-based termination as "*ultima ratio*" in the case of a recurring violation. The termination for cause, in case of especially severe violations, as a rule only comes into perspective if the violation of duty has reached the border of criminal behaviour or if a violation of the duty to keep IT-security leads to an irreversible and complete break down of mutual trust because of extraordinary circumstances.

Choice of appropriate measures

The individual measures are classified into different ranks and have to be applied on the basis of an examination of proportionality. The admissible sanction cannot be determined schematically, but has to consider various criteria as the case arises. Relevant are the (i) character and severity of the breach of duty, (ii) former behaviour of the employer, (iii) seniority, (iv) age and perspectives of the employee on the employment market, (v) impacts of the breach of duty on the operationability of the company and (vi) a contributory negligence of the employer. Moreover, general aspects such as fault, damage, recurrence, information and explanation of the concerned person as well as the scope of security specifications of the company have to be taken into consideration. It depends decisively on whether the relevant know-how was transmitted to the employees responsible for the IT-security within the company and whether any warnings of the persons responsible within the company such as, for example, a system administrator, were communicated in a sufficient way. Equally, the position of the employee within the company is relevant – the employer must be able to rely on the system administrator who is responsible for the security of the systems to a much higher degree of trust (and especially on his behaviour adequate to security) than on the ordinary employee. Towards the former, the threshold for a sanction is much lower and thus, much more severe sanctions are possible.

Custom and practice as risk of IT-security

Tolerance and non-prosecution of continuing violations against an applicable guideline of IT-security within the company may possibly lead to the constitution of custom and practice. This can *inter alia* suspend once established prohibitions such as the prohibition of private use of Internet and e-mail. Custom and practice have the effect of creating a basis of trust, which the employees may deduct from the employer's leniency concerning the violation of certain prohibitions. From the point of view of the employer, it always has to be recognised that showing tolerance as the regular reaction to violations of guidelines of IT-security can suspend these as a whole. Custom and practice may also lead to different rules within the company. It is for example conceivable that the private use of Internet and e-mail is tolerated in one department but not in another. Custom and practice cannot be removed unilaterally. Depending on the legal qualification of custom and practice, instruments to remove custom and practice such as negative custom and practice, termination for change of contract or an amending works agreement are possible remedies. Against this background it is a clear organisational duty of the employer not to let custom and practice emerge that suspends existing guidelines of IT-security.

  WDPR ISSN 1473-3579

IV. Selected particular cases

Prohibited use of Internet and e-mail

Violations of IT-security occur frequently in connection with the prohibited private use of Internet and e-mail. It depends on the situation within the company, for example if the private use of communication facilities of the company, no matter of what sort, is contrary to the employment contract. In practice, limited private use of telephone and private use of Internet and e-mail are generally tolerated by the employer. The employer may, however, determine the scope of use in his own discretion and may for example block certain websites. In the rare case of a complete prohibition of private use of Internet and e-mail, the private use of Internet and e-mail (as well as the private use of the telephone) is a sanctionable violation against duties of behaviour because it reduces the contractually due working power and blocks company resources for their original purposes. However, a warning is required in cases of private use of Internet and e-mail, before a (ordinary) behaviour-based termination can be served, even if the possibility of termination was generally announced before.

Permitted use of Internet and e-mail

If the private use of Internet and e-mail is basically permitted or admissible due to custom and practice, the employee must not use it without any limitations. For example, a termination without notice may come into consideration if the employee misuses the existing permission by continually sending private e-mails or using the Internet intensively in a way that is obviously intolerable for the employer. This is particularly the case if the private use leads to a blatant reduction of the employee's performance and thus to a violation of contractual obligations. The same applies if the abuse of the permission does not result from the intensity but from the sort of private use, for example through the use (including the storage of the material on the company computer or designing a website on the company computer) of pornographic or right wing extremist content by means of the IT-infrastructure of the company or the attempt to promote fanatic or terrorist organisations. A right to termination particularly exists if business interests of the company are concerned. Child pornography is a special case, as pursuant to Sec. 184 (5) second sentence Penal Code the "possession" as such is punishable. In this case, a termination for cause should be admissible as a rule, even if, as always, it must be examined whether, exceptionally, the mutual trust could be reconstituted.

Handling of data and the company's software

Concerning the admissibility of measures of employment law against the prohibited access to data and software depends on whether the data contain business secrets, whether the data can be used in a fashion detrimental to the employer or if there is an intention to damage. A behaviour-based termination, in certain cases even without prior warning is admissible, if it was evident to the employee that the employer did not want to disclose the business secrets, which is regularly the case if sensitive personal data or salary information of other employees are concerned. Before choosing the sanction it must be checked, if the employer undertook security measures. If not, the termination might not be enforceable because of contributory negligence of the employer. If the employee overcomes existing security measures, damages the employer by transferring (no matter if paid or non paid) data (no matter if personal data or not) or makes copies for private use, a termination for cause of the employment relationship is admissible as a rule, for the reason that it is evident for the employee (independently of his intentions) that he acts contrary to the employment contract and misuses the trust of the employer in a considerable way. If the violation lies exclusively within the production of copies for private use, a termination for cause is admissible only in exceptional cases (*e.g.* in case of copyright offences).

Misuse of passwords

Transferring passwords to non authorised persons or persons outside of the company generally justifies an ordinary, and also in certain cases, a termination for cause, as the confidence of the employer in the regular keeping of secrets important to the business is irrecoverably damaged. If the employee obtains passwords without authorisation and if he accesses texts of his employer that are normally not accessible to him, an ordinary termination or even a termination for cause may be justified. This only applies, however, if the limitation of competences was sufficiently clear. Changing passwords for the computer system without authorisation resulting in paralysing the company for a longer time can be sanctioned with a termination for cause. In such cases, contributory negligence of the employer might have to be considered if the employer failed to implement measures providing the possibility to overrun a password or to annul the password through the use of specialists. For less severe violations such as forgetting the password repeatedly, not changing the password despite corresponding guidelines or using easily decodable passwords despite considerable danger for the company, only a warning is possible and, when the violations are repeated, a regular termination can be declared.

Prohibited download and improper use of technique

The prohibited private download of programs from the Internet is a violation of the contract but does not entitle to terminate for cause (without notice) if there was no prior warning. One might come to another result if the download leads to endangering the IT-infrastructure of the company with viruses. When handling technique in general the adequate reaction depends in a very special way on the particular scope of duties. The system administrator has more specific duties to act (*e.g.* installing security-patches) than the ordinary employee as a mere IT-user. The latter is likely to cause trouble because of negligent behaviour (opening suspicious e-mails, errors in operating equipment, careless handling of passwords). As a rule, a warning is the appropriate sanction. If inappropriate handling of the company's IT-systems repeatedly leads to system breakdowns and considerable hindrances for the company, because the employee is not capable of using the IT-systems, a behaviour-based

termination is not always possible as it requires that the employee can basically fulfil the requirements of the employer but wilfully does not do so. Based on lacking subjective skills, only a person-based termination or a termination for change of contract could be considered. This requires, however, that the employee's performance fails the purpose as stated in the employment contract in a significant way; insignificant discrepancies are not sufficient. In particular, the employee must be granted an adequate period of time to adapt to the new conditions. Instead of a person-based termination, the employee concerned has to be offered a workplace corresponding to his abilities as far as this is possible within the company's organisation. If such a workplace is not available or not reasonable, the employer has to offer training to the employee to correct the lacking of qualification in the area of IT.

Criminal offences

Criminal offences only justify a termination if the criminal offences are either committed against the company or if outside the company with relevance to the company. If the guidelines of the IT-security are disregarded, the company's interests are always affected, whereby the company is violated as such. Any (intentional) infiltration of computer viruses is sufficient for a termination for cause, such as an intentional change of data in the sense of Sec. 303 Penal Code can be effected, whereby the attempt as such is sufficient. A previous warning is dispensable if the employer is compellingly dependant on the use of the electronic data processing. Under certain circumstances computer sabotage in the sense of Sec. 303b Penal Code could come into consideration within this context. The same applies if the employee procures for himself, or another person, unauthorised access to specially secured data not destined for him (Sec. 202a Penal Code), fakes technical records (Sec. 268 Penal Code) or the results of a data processing (Sec. 270 Penal Code). As a reason for termination without prior warning, one might consider the violation of company or business secrets (Sec. 203 Penal Code, Sec. 17 UWG). The question is whether it is sufficient as a reason for termination if an employee gets knowledge that his colleague has unauthorised access to company and business secrets and does not inform his employer. The decision as to whether a termination may be justified will largely depend on the employee's position within the company. In the case of a senior employee/trusted position as a rule a termination (regular or for cause) may be justified. Furthermore, a termination is admissible if the employee uses the company's resources to commit crimes (*e.g.* espionage for third parties) as it is not acceptable for the employer to be involved in crimes using his property. Also included would be copyright infringements such as burning copies, using facilities of the employer as a considerable breach of trust and criminal infringement pursuant to Sec. 106ff. Copyright Law does not need to be tolerated by the employer. Insofar a termination based on copyright offences comes into consideration for example if the employee makes copies of the software used in the company for private use.

Conclusion

IT-security becomes more and more important not only as a management obligation but also for employees. Violations of the same can have serious consequences for both managers and employees. For managers, personal liability is possible. Employees might be subject to warnings or even lose their jobs. In order to turn IT-security into a *true employee obligation* it is important, however, to have explicit rules and regulations in place and to train employees regularly. In light of the erosive effects of custom and practice in a company it is also important to sanction violations of IT-security.

New data protection laws for India

By Robert Bond, Partner and Head of IP, Technology and Commercial and Vinod Bange, Partner, Speechley Bircham LLP.

- The Information Technology (Amendment) Act 2008 was published on February 5, 2009.
- The Act introduces legislation relating to use of electronic signatures.
- The legislation addresses the use of encryption and makes provisions for governmental interception.
- Legislation creates a civil offence in respect of hacking and creates more stringent legislation in respect of cyber terrorism and online pornography.
- Of particular interest to companies that outsource to India is that the legislation now makes a company that handles 'sensitive personal data' liable to pay compensation if it is negligent in relation to security.

Robert Bond and Vinod Bange can be contacted at: robert.bond@speechlys.com and vinod.bange@speechlys.com

Article 25 of the EU Data Protection Directive (Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data) states that personal data cannot be transferred to any country outside the European Union that does not provide adequate laws for the protection of rights of individuals in relation to their personal data.

Over the past few years the European Commission has 'approved' a number of countries who are deemed to have adequate data protection laws including Argentina, Canada, Faroe Islands, Guernsey, Jersey, the Isle of Man and Switzerland, but despite India being a significant recipient of personal data from Europe as part of its outsourcing offerings India has no such approval.

  WDPR ISSN 1473-3579

The European Commission does not regard India as having satisfactory laws providing protection for the rights of individuals in relation to personal data although it is still permissible to transfer personal data to India provided that the exporting company puts in place suitable contractual controls with the importing company in India. Usually these controls are in the form of 'approved model clauses' by the European Commission or the use of Binding Corporate Rules. Notwithstanding the introduction of the new legislation in India and the greater obligations placed on companies in India with regard to the handling of 'sensitive personal data' there will still be the need to meet the requirements of Articles 25 and Article 26 (which address trans-border data flows) of the EU Data Protection Directive.

It is unlikely that the new legislation in India will fast-track the country into a position of being an approved country by the European Commission for data protection purposes but it is a move in the right direction, especially with the widely accepted view that the outsourcing industry in India prides itself on the high levels of information security practices and controls adopted.

HIPAA privacy and security changes in the American Recovery and Reinvestment Act

By Brad M. Rostolsky, Associate, Gina M. Cavalier, Partner, Debra L. Hutchings Associate, Kerry A. Kearney Partner and Mark S. Melodia Partner at Reed Smith LLP (www.reedsmith.com).

On February 17, 2009, President Obama signed into law H.R. 1, the American Recovery and Reinvestment Act (the "ARRA").[1] This memorandum outlines significant changes and additions to the landscape of federal privacy and security law set forth in Subtitle D of the ARRA. In general, the privacy and security portions of the ARRA become effective 12 months after the enactment of the ARRA, which is approximately February 2010. It is also important to note that the ARRA directs the Secretary of the US Department of Health & Human Services ("HHS") to amend the HIPAA Privacy and Security Rules to implement the legislative changes. As such, the effective dates associated with the rulemaking process will vary.

A. Applicability of HIPAA security and privacy rules extended to business associates

1. Security Rule

The HIPAA Security Rule's information safeguards are not new considerations for Business Associates. Business Associate Agreements contractually obligate Business Associates to implement administrative, physical, and technical safeguards to reasonably and appropriately protect electronic protected health information that the Business Associate creates or maintains on behalf of a Covered Entity. The ARRA, however, changes the fundamental framework of the Security Rule in this regard. Specifically, Business Associates are now required to directly comply with the Security Rule's provisions on administrative, physical, and technical safeguards, as well as to develop implementing policies and procedures. As a practical matter, however, it is unclear whether these provisions only apply *vis-à-vis* the protected health information created or received from a Covered Entity, or whether they implicate other information of the Business Associate.

As a means to assist Business Associates (as well as Covered Entities) with effectively addressing the requirements of the Security Rule, HHS is required to publish annual guidance on "the most effective and appropriate technical safeguards for use in carrying out" the requirements of the Security Rule. Additionally, the ARRA requires that Business Associate Agreements reflect the new direct obligations of Business Associates. Finally, adding enforcement teeth, the ARRA provides that Business Associates will be subject to civil and criminal penalties for violating the Security Rule.

2. Privacy Rule

The ARRA requires a Business Associate that "obtains or creates protected health information pursuant to a written contract" to take direct responsibility for its uses and disclosures of protected health information. As a result of the new legislation, and regardless of the contractual obligations of a Business Associate Agreement, the manner in which Business Associates approach Privacy Rule requirements and obligations has been significantly altered, although the extent of these changes will not be clear until regulations are promulgated.

At a minimum, it is clear that Business Associates that violate the Privacy Rule obligations set forth in their Business Associate Agreements will be subject to HIPAA's civil and criminal enforcement provisions. The statutory language also appears to require a Business Associate to take reasonable steps to cure a Covered Entity's violation of a Business Associate Agreement if the Business Associate knows of a pattern of activity or practice of the Covered Entity that constitutes a material breach or violation of the Covered Entity's obligation under the Business Associate Agreement. If cure is not

Brad M. Rostolsky, Associate, Gina M. Cavalier, Partner, Debra L. Hutchings Associate, Kerry A. Kearney Partner and Mark S. Melodia Partner at Reed Smith LLP can be contacted at: brostolsky@reedsmith.com, gcavalier@reedsmith.com, dhutchings@reedsmith.com, kkearney@reedsmith.com and mmelodia@reedsmith.com

possible, and termination of the Business Associate is not feasible, then the Business Associate must report the problem to HHS.

It is likely that the requirement that Business Associates' new privacy and security obligations be reflected in Business Associate Agreements will, *de facto*, require the amendment of current Business Associate Agreements. Although the standard language typically found in Business Associate Agreements may be sufficient to address some of the increased privacy and security requirements, it may behoove Covered Entities and Business Associates to review their current Business Associate Agreements. Amendments to current Business Associate Agreements will enable the parties to ensure that both the Privacy and Security Rules are properly and thoroughly addressed. Furthermore, it seems likely that Covered Entities will want the security breach notification requirements discussed below to be set forth in detail in Business Associate Agreements.

3. Definition of Business Associate expanded

The ARRA expands the definition of "Business Associate" to any organisation that, with respect to a Covered Entity, provides data transmission of protected health information to a Covered Entity (or its Business Associate) if the organisation requires routine access to the protected health information. Examples include a Health Information Exchange Organisation, a Regional Health Information Organisation, an E-prescribing Gateway, or a Vendor of Personal Health Records. (ARRA provisions related to Vendors of Personal Health Records are described below.) The new universe of entities will be treated as "Business Associates", and must, among other things, enter into a Business Associate Agreement with Covered Entities.

B. Notification standards for breaches of "unsecured" protected health information

1. Covered Entities

Much like the security breach notification laws of many states, the ARRA imposes significant breach notification obligations on a Covered Entity that "accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information." Thus, any such Covered Entity that knows or should reasonably have known that protected health information has been acquired, accessed, used, or disclosed without authorisation, must provide notice of the breach to individuals and designated entities within a prescribed period of time.

The ARRA includes detailed requirements regarding when, how, and to whom notifications of a breach must be provided, but, generally, the notifications must be provided to the individual about whom the information pertains without unreasonable delay (and, in any event, no later than within 60 days of discovery of the breach). In addition to notifying the individuals, notification must always be provided to HHS (immediately if the breach involves more than 500 individuals, or annually otherwise), and, depending on the scope or severity of the breach, to prominent media outlets serving the respective state or jurisdiction. The one exception to a Covered Entity's obligation to provide a security breach notification is if a law enforcement official determines that such a notification would impede a criminal investigation or cause damage to national security. HHS will maintain a website that identifies Covered Entities involved in a breach of unsecured protected health information for more than 500 individuals.

The ARRA defines unsecured protected health information to mean "protected health information that is not secured through the use of a technology or methodology specified by the Secretary [of HHS] in" guidance that will be issued no later than 60 days after the enactment of the ARRA. In case the aforementioned guidance is not issued by HHS on the date promised, the ARRA provides the following default definition of unsecured protected health information, which appears to essentially require encryption – "protected health information that is not secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorised individuals and is developed or endorsed by a standards developing organisation that is accredited by the American National Standards Institute."

No later than 180 days after the enactment of the ARRA (approximately August 2009), HHS shall promulgate interim final regulations. The security breach notification provisions of the ARRA shall be effective 30 days after the publication of these interim final regulations (approximately September 2009). Note: This is sooner than the effective date for the ARRA generally.

2. Business Associates

The breach notification requirements extend to Business Associates insofar as Business Associates must report discovered breaches of unsecured protected health information to the Covered Entity following a Business Associate's discovery of a breach. If a Business Associate fails to provide the required notice in a timely fashion, the Business Associate may be subject to direct enforcement and penalties. Notification from a Business Associate must include the identification of each individual about whom the breached information pertains. Covered Entities will likely include specific notification timing requirements in Business Associate Agreements.

3. Vendors of Personal Health Records

The ARRA also imposes breach notification requirements on "Vendors of Personal Health Records". Under the ARRA, a Vendor of Personal Health Records is any entity "other than a covered entity [as defined in the HIPAA regulations] that offers or maintains a personal health record". The term "personal health record" is defined to be "an electronic record of [individually identifiable health information (as defined in the Social Security Act)] on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or for the individual".

Vendors of Personal Health Records must notify the individual about whom the information pertains, as well as

   ISSN 1473-3579

the Federal Trade Commission ("FTC") (which will in turn notify HHS) upon discovery of a breach of security with respect to the individually identifiable health information that is in a personal health record. The ARRA defines "breach of security" to mean any acquisition of the aforementioned information without the authorisation of the individual to whom the information pertains. Third party service providers engaged by Vendors of Personal Health Records are treated similarly to Business Associates, and must notify the vendor of a breach of security.

For Vendors of Personal Health Records and third-party service providers, the requirements regarding when and how they must provide notifications of a breach of security are the same as for Covered Entities and Business Associates, respectively. A Vendor of Personal Health Records or third-party service provider's violation of the notification requirements shall be considered an unfair and deceptive act or practice in violation of FTC regulations.

These provisions are intended to be temporary and will sunset if Congress enacts new legislation establishing specific security breach notification requirements for entities that are not Covered Entities or Business Associates under HIPAA. The FTC is required to promulgate implementing regulations within 180 days of the enactment of the ARRA (approximately August 2009), which will likely clarify the definitions and requirements set forth in the ARRA.

C. Enhanced privacy guidance and education initiative

Within six months after the enactment of the ARRA (approximately August 2009), HHS is required to designate an individual in each HHS regional office to offer guidance and education to Covered Entities, Business Associates, and individuals on their "rights and responsibilities related to Federal privacy and security requirements for protected health information". Additionally, within one year after the enactment of the ARRA, the HHS Office for Civil Rights is required to develop and maintain a multi-faceted national education initiative to enhance public transparency regarding the uses of protected health information.

D. Obligations related to electronic health records

1. Accounting of protected information stored in electronic health records

Although under the HIPAA Privacy Rule, Covered Entities are not required to account for uses and disclosures of protected health information for the purpose of treatment, payment, and health care operations, the ARRA specifically eliminates this exception for Covered Entities that use or maintain "electronic health records." The ARRA defines an "electronic health record" to mean "an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorised health care clinicians and staff."

A Covered Entity must provide the new, broader, accounting upon request. For disclosures made by a Covered Entity's Business Associates, however, the Covered Entity may provide an individual with a list of the Business Associates. If an individual is provided with such a list of Business Associates, then the Business Associates must provide the accounting to the individual upon request from the individual. Accountings made by Covered Entities and Business Associates that use and maintain electronic health records must cover a period of three years (as opposed to the six-year period required under HIPAA).

These accounting provisions are effective as follows:

- For Covered Entities, insofar as they acquired an electronic health record as of January 1, 2009, the accounting requirement applies to disclosures made on or after January 14, 2014.
- For Covered Entities insofar as they acquire an electronic health record after January 1, 2009, the provision will be effective for disclosures on the later of January 1, 2011, or the date upon which the entity acquires the electronic health record.
- HHS can impose a later effective date, but it can be no later than 2016 for the Covered Entities with an electronic health record as of January 1, 2009, and 2013 for all other Covered Entities with an electronic health record.

2. Access to protected health information in electronic format

Expanding on the Privacy Rule's access provisions, Covered Entities that use or maintain an electronic health record with respect to the protected health information of an individual must, per ARRA, provide access to such information by producing an electronic copy to the individual (or a recipient designated by the individual). Individuals making such a request may only be charged for a Covered Entity's labour costs associated with providing the requested information.

3. Sale of electronic health records or protected health information

The ARRA provides that a Covered Entity or Business Associate cannot directly or indirectly receive remuneration in exchange for an individual's protected health information (including such information stored in an electronic health record) except pursuant to a valid HIPAA authorisation that specifies the extent to which the recipient may engage in further exchanges of the individual's information.

This prohibition does not apply to the exchange of the information if the purpose for the exchange is one of the following:

- Public health activities, as defined by the Privacy Rule (45 C.F.R. § 164.512(b)).
- Research purposes (as defined in 45 C.F.R. §§ 164.501, 164.512(i)), subject to limitations on the remuneration.

- Treatment, unless HHS determines otherwise.
- Transfers in connection with the sale or merger of a Covered Entity.
- Remuneration that is paid by the Covered Entity to a Business Associate related to the Business Associate's services as to the exchange of protected health information.
- Providing an individual with a copy of the individual's protected health information.
- Other situations, as determined by HHS.

HHS is required to promulgate regulations implementing these provisions no later than 18 months after the enactment of the ARRA (approximately August 2010). Furthermore, this provision of the ARRA applies only to an exchange of protected health information that occurs at least six months after the regulations have been released.

E. Enhanced ability of individuals to control protected health information

1. Requested restrictions on or disclosures of protected health information

Prior to the enactment of the ARRA, a Covered Entity was not required to grant an individual's request to limit the use and disclosure of protected health information to carry out treatment, payment, or health care operations. The ARRA, however, requires Covered Entities to comply with an individual's request for such restrictions on disclosure if:

- The disclosure is made to a health plan for the purposes of carrying out payment or health care operations (unless the use or disclosure is required by law);
- The protected health information at issue pertains only to a health care item or service for which the individual pays (1) out-of-pocket, and (2) in full.

2. 'Minimum necessary' standard further explained

Under the Privacy Rule, a Covered Entity's use and disclosure of protected health information for purposes other than treatment, payment, and health care operations must be limited to the "minimum necessary" amount needed to accomplish the underlying purpose of the use or disclosure. To provide assistance to Covered Entities in this regard, the ARRA directs HHS to issue guidance on what constitutes "minimum necessary" no later than 18 months after the enactment of the ARRA. Until the release of this guidance, the ARRA provides that uses and disclosures unrelated to treatment, payment, or health care operations must be in the form of a limited data set (as defined by the Privacy Rule), unless a Covered Entity (or Business Associate) determines that a limited data set is not "practicable" for a particular use or disclosure, in which case the "minimum necessary" standard still applies.

3. Marketing and fund-raising communications

The ARRA contains new restrictions on marketing communications. Specifically, marketing communications to an individual from a Covered Entity or Business Associate that were previously considered "health care operations" (and therefore not curtailed by the Privacy Rule) are no longer considered health care operations (and therefore no longer exempt from the Privacy Rule's general prohibition against disclosure) if the Covered Entity or Business Associate receives or has received direct or indirect remuneration (as defined under federal fraud and abuse regulations) for making the communication, except where:

- The communication describes a drug or biologic that is currently prescribed for the recipient, and the remuneration received by the Covered Entity in exchange for the information is "reasonable" (as will be defined by HHS).
- The communication is made by the Covered Entity based on a valid HIPAA authorisation.
- The communication is made by a Business Associate of the Covered Entity in accordance with a written Business Associate Agreement.

Although fund-raising communications are still considered "health care operations", such communications must clearly and conspicuously provide individuals with an opportunity to opt-out of receiving further fund-raising communications. The decision by an individual to opt-out shall be considered a revocation of authorisation under HIPAA.

F. Continued focus on enforcement activities

Building on recent enforcement actions (settlements and informal compliance agreements) from the Office of Civil Rights and the Centers for Medicare and Medicaid Services, the ARRA amends the relevant enforcement provisions of HIPAA by, among other things, requiring HHS to "formally investigate any complaint of a violation of [the Privacy and Security provisions of the ARRA] if a preliminary investigation of the facts of the complaint indicate [that] such a possible violation [is] due to willful neglect". Notwithstanding this heightened focus on enforcement, the ARRA specifically permits the Office for Civil Rights to utilise corrective action without penalty as a means to address civil infractions of the Privacy Rule.

Except as separately provided in the ARRA, the amendments made to enforcement provisions shall be effective 24 months after the enactment of the ARRA (approximately February 2011).

1. State Attorneys General can initiate federal action for HIPAA violations on behalf of state residents

Furthermore, the ARRA authorises state Attorneys General to initiate civil actions in the federal court (for injunctive relief or monetary damages) on behalf of a state resident when the Attorney General reasonably believes that the resident's interests have been threatened or ad-

  WDPR ISSN 1473-3579

versely affected by a person or entity that violates HIPAA. Additionally, the court may award the costs of the action and reasonable attorney fees to the state. Prior to bringing any such claim, a state Attorney General must provide HHS with prior written notice of intent to file the action, after which HHS may intervene in the action. If HHS brings a HIPAA action against a person, then state Attorneys General may not bring an action against the person relative to the same HIPAA violation.

2. Enforcement clarification regarding individuals

The ARRA clarifies a point of confusion regarding the criminal enforcement of individuals for the wrongful access or disclosure of protected health information under HIPAA. The ARRA makes it clear that individuals (who are not Covered Entities, but who may be employees of Covered Entities) fall within HIPAA's enforcement purview.

3. Increased to civil monetary penalties

With regard to civil monetary penalties, the ARRA replaces the manner in which such penalties are determined with a new tiered approach:

- Unknown violations *(i.e.*, if a person did not know, and by exercising reasonable due diligence would not have known, that a violation occurred): The penalty shall be at least $100 for each violation not to exceed $25,000 for all such identical violations during a calendar year, but may be no more than $50,000 for each violation, not to exceed $1.5 million for all such violations of an identical requirement or prohibition during a calendar year.

- Violations as a result of reasonable cause and not because of wilful neglect: The penalty shall be at least $1,000 for each violation, not to exceed $100,000 for all such identical violations during a calendar year, but may be no more than $50,000 for each violation, not to exceed $1.5 million for all such violations of an identical requirement or prohibition during a calendar year.

- Violations as a result of wilful neglect (and the violations have been corrected): The penalty shall be at least $10,000 for each violation, not to exceed $250,000 for all such identical violations during a calendar year, but may be no more than $50,000 for each violation, not to exceed $1.5 million for all such violations of an identical requirement or prohibition during a calendar year.

- Violations because of wilful neglect (and that have not been corrected): The penalty shall be at least $50,000 for each violation, not to exceed $1.5 million for all such violations of an identical requirement or prohibition during a calendar year.

Also note that, within three years of the enactment of the ARRA, HHS is required to publish regulations that establish a methodology that distributes a portion of collected civil monetary penalties to the individuals harmed by a Covered Entity's act of wilful neglect. The application of this new tiered approach to civil monetary penalties applies to violations that occur after the date of enactment of the ARRA.

NOTES

[1] P.L. No. 111-5. The text of the Act and the accompanying conference report are available at http://thomas.loc.gov/home/approp/app09.html#h1

This article first appeared in ReedSmith's Life Sciences Health Industry Client Alert, March 2009.

News

INTERNATIONAL

World Anti-Doping Agency adopts revised data protection standard

At a meeting in Montreal on May 9, the Executive Committee of the World Anti-Doping Agency (WADA) adopted a revised International Standard for the Protection of Privacy to replace the Standard which entered into force on January 1, 2009. The revised standard follows an ongoing discussion between WADA and the EU over data protection implications surrounding the 'whereabouts rule' – (the need to track athletes' movements for drug testing). The revised standard takes account of recommendations made by the Article 29 working Party in its document, the '*Second opinion 4/2009 on the World Anti-Doping Agency (WADA) International Standard for the Protection of Privacy and Personal Information, on related provisions of the WADA Code and on other privacy issues in the context of the fight against doping in sport by WADA and (national) anti-doping organizations*'.

Further discussions on data protection matters were due to take place at the EU Anti-Doping Conference held in Athens on May, 13–15.

The revised standard will enter into force as of June 1, 2009.

The standard is available at: http://www.wada-ama.org/en/dynamic.ch2?pageCategory.id=807

A copy of the Working Party's Opinion is available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp162_en.pdf

CANADA

Could the controversial 'Do Not Call' Register be replaced?

A new anti-spam bill, the Electronic Commerce Protection Act, if passed, may result in a change of law asking individuals to opt-in rather than opt-out of receiving marketing calls. If so, it raises questions over the future of the heavily criticised 'Do Not Call' Register.

Since the launch of the 'Do Not Call' Register six months ago, six million Canadians have registered their

name on the opt-out list. The Canadian Radio Television Commission (CRTC) has, on average, received 20,000 complaints per month. However, the CRTC has been heavily criticised for its lack of enforcement and complaint handling. It has issued only 70 warning letters to organisations flouting the regulations and imposed no financial penalties to date. Privacy advocates who have been critical of the Register are strongly in favour of changing the legislation to require an opt-in to marketing calls.

IRELAND

Data Protection Commissioner issues data breach guidance

The Data Protection Commissioner, Billy Hawkes, has issued interim guidance for organisations on how to deal with the data loss arising from security breaches. Meanwhile, the Working Group set up by the Ministry of Justice is currently looking into whether there should be an amendment to the existing data protection legislation to account for security breaches.

For more information about the Work Group, visit: http://www.justice.ie/en/JELR/Pages/WP09000015

The Interim Guidelines are available from: http://www.dataprotection.ie/viewdoc.asp?DocID=901&ad=1

SWEDEN

Swedish ISPs will erase users' data to protect privacy

As the controversy surrounding the Swedish anti-piracy laws continue, three more ISPs say they will erase traffic data to protect their customers' privacy.

The laws known as Ipred, which came into effect on April 1, 2009, allow copyright owners to ask ISPs to provide information about customers illegally uploading or downloading copyright protected material with a court order. Although designed to protect against copyright infringement, the laws caused a stir amongst privacy advocates and ISPs over this requirement to reveal customer information. Since Ipred came into effect, there has been a 30 percent drop in Internet traffic.

UNITED KINGDOM

ICO review recommends an overhaul of the EU Data Protection Directive

The Information Commissioner's Office has published its review commenting on the strengths and weaknesses of the EU Data Protection Directive. RAND Europe was commissioned to conduct the review last year.

Their study has concluded that the Directive needs to be updated to reflect the global information society of the 21st century. Whilst the report acknowledges that the Directive has harmonised data protection across the EU, there is a general consensus that it is too burdensome and no longer addresses the current risks to personal information brought about by advances in technology.

Information Commissioner, Richard Thomas, said:

> "The Directive is showing its age. Modern approaches to regulation mean that laws must concentrate on the real risks that people face. . ., must avoid unnecessary burdens, and must work well in practice. . .Organisations must embed privacy by design and data protection must become a top level corporate governance issue. . .Safeguarding personal information has become a major reputational issue for businesses and governments. They must be held accountable if things go wrong. This study is not meant to be an immediate blueprint for a new Directive."

Recommendations from the report include:

- making the law and its aims clearer;
- focusing on the accountability of organisations for protecting the personal information they process; adopting a more strategic approach to enforcement; and
- improving the mechanisms for transferring data outside the EEA.

The ICO is hoping that the study will stimulate a debate about how to modernise the Directive.

A copy of the report is available at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf

A report summary is also available at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive_summary.pdf

UNITED STATES

FTC releases proposed breach notification rule for e-health data

Under the requirements of the American Recovery and Reinvestment Act 2009 (ARRA), the Federal Trade Commission (FTC) has released a rule for public comment which requires organisations to notify customers if their information has been breached. The ARRA includes provisions to help advance the use of technology for processing health data and strengthening the privacy and security requirements for such data. In doing so, the Act recognises the emergence of web-based services used to collect, store and manage sensitive health data. (See also in this issue, *HIPAA privacy and security changes in the American Recovery and Reinvestment Act*, by Reed-Smith.)

The ARRA requires the FTC, alongside the Department of Health and Human Services, to conduct a study on the potential privacy, security and breach notification requirements for vendors of health information and any related organisations. The study and subsequent report must be released by February 2010. The proposed rule

   ISSN 1473-3579

is an interim measure until the study and report have been completed. In addition to security breach notification requirements, there are also requirements governing the timing, type and content of the notification and organisations must inform the FTC if a breach occurs.

The FTC is accepting public comments on the rule until June 1, 2009 and these comments can be filed at https://secure.commentworks.com/ftc-healthbreachnotification

More information is available from the FTC at: http://www.ftc.gov

FTC delays enforcement of Red Flags Rule

The Federal Trade Commission (FTC) is to delay enforcing the Red Flag Rules until August 1, 2009. The delay is to give financial institutions more time to develop their identity theft prevention policies and procedures. The FTC is also set to release a template for organisations with a low risk of identity theft, for example, those that know their customers personally.

FTC Chairman, Jon Leibowitz explained the delay, saying,

> "Given the ongoing debate about whether Congress wrote this provision too broadly, delaying enforcement of the Red Flags Rule will allow industries and associations to share guidance with their members, provide low-risk entities an opportunity to use the template in developing their programs, and give Congress time to consider the issue further."

For more information and guidance about the Red Flags Rule, read: http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm, or visit: http://www.ftc.gov/redflagsrule

Government research shows privacy notices should be in a table format

A study by the US government has found that customers of financial institutions understand privacy notices when they are displayed in a table rather than as solid text. The Gramm-Leach-Bliley Act requires organisations providing financial services to provide privacy notices to its customers. Researchers were commissioned by the US government to examine the effectiveness of current privacy notices in conveying the relevant information to customers. They questioned 1000 people about privacy notices, giving them a sample set of notices to review. The notice in table format was voted the best for communicating the relevant information most effectively.

The research and report is available from: http://www.ftc.gov/privacy/privacyinitiatives/Levy-Hastak-Report.pdf

Personal Data

EC guidelines for data transfers to countries outside EEA: use with caution

By Dominic Hodgkinson, Solicitor and Correspondent, Calleja Consulting Ltd.

The European Commission has published a series of flowcharts and FAQs on the transfer of personal data from the European Economic Area (EEA) to countries outside the EEA to assist small and medium sized enterprises (SMEs) to ensure that they transfer such personal data in accordance with EU data protection law.

EU data protection law, data transfer and the Guidelines

The Data Protection Directive (95/46/EC) regulates the use (and abuse) of individuals' personal data. The Directive includes a prohibition on transferring personal data from inside the EEA to outside the EEA except where a permitted method is used.

Generally, businesses can find the transfer regime complex so the Commission (who are also in charge of ensuring that each Member State implements and enforces the Directive correctly) has published a series of FAQs and flow-charts to help small and medium sized enterprises determine whether they are caught by the Directive and if so, how they can transfer personal data in accordance with the Directive.

Guidelines' round-up of the EU personal data transfer regime

The flow-charts and FAQs are intended to help companies identify:

- whether they are dealing with personal data – the Directive only applies to personal data;
- whether the purpose of the transfer is compatible with the original purpose for which the personal data were collected – if not the transfer is prohibited;
- whether the data transfer is inside the EEA – this is acceptable and the company need not consider the data transfer regime any further;
- whether the data transfer is from inside the EEA to a country outside the EEA (a 'third country') – this will be acceptable only if:
- the country is a 'recognised third country' – this means that the Commission recognises that the country in question has adequate data protection laws – to date, only six countries[1] have been recognised;
- the company to which the data are being transferred is a US company that is also a member of Safe Harbor – Safe Harbor is a scheme set up by the US Federal Trade Commission and the European Commission which US companies can join if they promise to observe data protection principles broadly equivalent to those stipulated in the Directive;
- a permitted method is used by the EEA-based entity transferring the data – these include appropriate contractual clauses, Model Contract Clauses (MCC) and Binding Corporate Rules (BCR) for use between the companies transferring and receiving the data; appropriate contractual clauses and MCC are for use between EEA-based entities and unconnected third parties while BCR are for use between companies in the same group but they both have the same result – the companies transferring and receiving the data undertake to ensure that the Directive is not infringed;
- a permitted derogation applies – this includes, for example, where the individual gives his clear, free and specific consent.

Complexities not addressed by the Commission's Guidelines document

The Directive's regime is more complex than the Guidelines' flow-charts and FAQ indicate so SMEs should consider the following when using the Guidelines:

- the Guidelines state on the front page that "they do not have any legal value and do not necessarily represent the position that the Commission may adopt in a particular case";
- the Guidelines do not address the topical problem of 'what is personal data?' – as stated, the Directive only applies to personal data; personal data is defined in the Directive as 'any information relating to an identified or identifiable natural person'; this is a very broad definition and companies should take care to ensure that they are not processing and transferring personal data without knowing it; an example where this could happen is IP addresses which global and online companies may process and transfer as part of their business model – however, the Article 29 Working Party in its paper 'On the Concept of Personal Data' (issued June 20, 2007) stated that IP addresses may be personal data and that the purpose for which such data is processed is a relevant factor in determining if the IP address is personal data;
- the Guidelines do not resolve the problem inherent to all Directives – while EU regulations are incorporated into Member States' legislation 'as is', there is no such

  WDPR ISSN 1473-3579

harmonised method to incorporate directives into Member States' legislation; accordingly, each Member State incorporates directives into their legislation with slightly different rules and sanctions to any other Member State; as far as the Directive goes, for example, Spain requires companies to notify their use of Model Contract Clauses while the UK does not, France's sanctions for infringement of the Directive are heavier than the UK's, Germany requires all companies with more than nine employees to have a data protection officer and the notification regimes where personal data is compromised in a third country may differ from Member State to Member State – all of this tends to devalue the usefulness of any EU overview;

- the Guideline's round-up of Binding Corporate Rules for use between companies in the same group does not properly convey the complexity, time and cost that are entailed in securing the appropriate approvals before a company can use the BCRs as a permitted method to transfer personal data to a group company based in a third country.

Conclusion

The EU data protection and data transfer regime is not a simple regime. The Commission's Guidelines document is a positive move by the Commission to try to answer questions that SMEs without the benefit of a General Counsel might ask.

However, the Guidelines do tend to gloss over the more complex areas of data protection and data transfer. Furthermore, because there is no harmonised method to incorporate directives into each Member State's legislation, it follows that although the Guidelines are a useful overview of the EU regime they are clearly of limited use to a company whose business model incorporates multiple EU entities and multiple data transfer processes to third countries – such a company should take legal advice on a Member State by Member State basis to ensure that it is not infringing the data transfer regime applicable to each individual Member State.

The Commission would no doubt reply that the Guidelines are not for the use of such an intricate organisation – the document clearly states that they are intended to 'particularly' assist SMEs' understanding of the regime. But therein lies the problem – the Guidelines gloss over the complexities of data protection so should be used with caution by SMEs.

The FAQs are available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

NOTES

[1] Argentina, Canada, Switzerland, Guernsey, Isle of Man, Jersey

E-Discovery: US and EU conflicts

By Renzo Marchini, Pierre-M Louis, Anthony Paronneau, Jonathan Schur and Jean-Yves Steyt, Dechert LLP.

The Article 29 Working Party[1] has recently considered the issue of the application of the EU data protection Directive (95/46/EC the "Directive") to the transfer of data outside of the EU for the purposes of pre-trial discovery obligations abroad; in particular in the US. The conflict between a multinational's obligations to give discovery or disclosure under US civil procedure rules when litigating in the US and its obligations (through any EU presence) to comply with the requirements under the Directive has been a concern for some time. The Working Party's paper[2] (published in February) will be helpful to those seeking to comply with both sets of obligations.

The conflict which arises for multinational companies with operations in both the USA and the EU is the apparent inconsistency between the American and European approaches to the movement of data. The US approach to pre-trial disclosure (or 'discovery', to give it its American term) in litigation is one area where a conflict arises[3] , and is increasingly prominent. The most recent Federal Rules of Civil Procedure, in common with their previous incarnations, allow a party to litigation to serve on another party a request that they be allowed to inspect any information which is in that party's possession, custody or control. This information need only be "relevant to any party's claim or defence", and US case law has developed this further: the common law duty of companies to preserve information in contemplation of litigation extends even to information that, while not relevant in itself, may lead to the discovery of admissible evidence. The key point is whether it is "reasonably likely" to be the subject of discovery in litigation.

The common law US system and the civil code systems on which the law of most members of the EU is based do not approach litigation and its attendant obligations in the same way, and this has resulted in a disconnect between the requirements of the US courts for litigants to provide information (which might contain personal data) and the requirements of EU Member State law relating to the processing of personal data. The issue is particularly relevant for US companies who have subsidiaries in Europe who are in possession of documents relevant to US litigation (and so discoverable as they are "controlled" by the US entity which is party to the litigation). The US courts take discovery extremely seriously and have so far not been entirely sympathetic to parties

Renzo Marchini (solicitor, London), Anthony Paronneau (avocat, Paris), Jonathan Schur (avocat and member of the Paris and New York Bars, Paris), Pierre-M Louis (avocat, Brussels) and Jean-Yves Steyt (avocat and member of the Brussels, Amsterdam, and New York Bars, Brussels) can all be reached on +44 (0)20 7184 7000.
The authors acknowledge the contributions of Philip Yanella of the Philadelphia office and Edward Green of the London office.

attempting to excuse a failure to comply with discovery requirements on the grounds of EU restrictions, even when those restrictions have been supplemented by so-called "blocking statutes" and the potential criminal penalties which some individual EU Member States provide.

These US discovery requirements are now specifically applied to electronic data, which is unsurprising since according to the Advisory Committee on Civil Rules in the US, 92 percent of all information generated today is in electronic form. The ease with which electronic data may now be transferred means that it may be held in Europe and still subject to the discovery requirements of US law.

The Directive and the issues raised

While the US sector-specific approach to privacy law offers protection to specific classes of data such as medical information or financial information, the definitions in the Directive extend protection to a very wide notion of "personal data" (any information "relating to" an identified or identifiable individual). The Directive applies whenever an entity "processes" personal data, and "processing" covers any set of operations performed on that data including (irrespective of a transfer outside of Europe) disclosing the information to an adversary in the event of litigation.

Legitimising condition

One of the fundamental tenets of the Directive, and the first issue to be considered in connection with a discovery exercise involving the US, is that any processing of personal data is only permitted if one of the conditions set out in Article 7 is fulfilled in relation to that processing.

Transfers of personal data

The last, and most often discussed, issue for US discovery which arises under the Directive is Article 25(1), which prohibits the transfer of personal data to any country or territory outside the EU (a 'third country') unless the third country "*ensures an adequate level of protection*" for the rights and freedoms of those individuals whose personal data is being transferred. The US generally does not offer such a level of protection (at least, to European eyes).

EU blocking statutes and other restrictions, and the US attitude

Some (mainly civil law) EU jurisdictions have laws (so-called "blocking statutes") which apart from data protection law also restrict cross border disclosure. There is little uniformity in how these laws operate, the relevant laws in France are summarised below. They can lead to criminal sanctions if breached.

The US courts have so far not accepted such provisions as providing a defence against discovery in relation to US litigation. A US court may order a person subject to its jurisdiction to produce evidence even if the information is not located in the United States[4] , and the existence of any blocking statute is only one factor to be considered by the court and would not generally provide a defence in itself. It is important to note that the US courts consider that if the company is subject to US law and possesses, controls, or has custody or even has authorised access to the information from the US territory (via a computer) wherever the data is "physically" located, US law applies without the need to respect any international convention such as the Hague Convention.

The Working Party points out that the US courts require a balancing exercise to be carried out with the aim that a party's request for production of information located abroad should only be allowed after weighing up a number of issues including the importance of the information requested, the degree of specificity, whether the information originated in the US, whether there are alternative means of securing the information, and whether non-compliance would undermine the interests of the US or compliance with the request would undermine the interests of a foreign sovereign nation.

Hague Convention

Requests for information may in many Member States be made through the standard procedure set out in the Hague Convention on the taking of evidence abroad in civil and commercial matters. The Working Party clearly advances the view that evidence should be obtained only through this process. The US by contrast sees the process as optional as opposed to mandatory.

Moreover, as will be seen below, some Member States have expressly provided that they will not execute "letters of request" which are issued by foreign (in our case, US) courts for the purposes of obtaining pre-trial discovery of documents.

Recommendation of the Article 29 Working Party

The stated aim of the recent Working Party paper[5] is to provide guidance to EU data controllers in dealing with requests to transfer personal data to another jurisdiction for use in civil litigation. Whilst it recognises that the Directive does not prohibit such transfers, it does adopt a cautious approach while at the same time recognising the need to reconcile the two systems.

The Working Party takes the view that discovery should if possible be restricted to anonymised (or pseudonymised) data. Anonymisation (if not pseudonymisation) neatly circumvents the restrictions on the processing of personal data by ensuring that no personal data (by the Directive's definition) is being processed[6] . However, this will often not be possible and so other ways to legitimise the transfer must be found. The Working Party makes it clear that the data controller has a duty to limit the discovery of personal data to that which is objectively relevant to the issues being litigated. This filtering should be carried out locally before any transfer takes place.

  WDPR ISSN 1473-3579

Legitimacy

As mentioned, irrespective of transfers outside of Europe, a ground for disclosure *per se* needs to be found as set out in Article 7 of the Directive. The Working Party helpfully considers in detail these potential grounds for the processing.

The most obvious to consider first is Article 7(a) – the consent of the data subject. However, the Directive definition of consent contains the requirement that it be "freely given specific and informed".

The Working Party certainly feels that it is not generally possible for employees to give consent for their employer to transfer the data because of fear of a sanction from the employer if they refuse; as such, any consent from an employee is not – they say – likely to be "freely given"[7]. Likewise, to be "specific" and "informed" a particular act of processing must be envisaged (and thus a general consent obtained, say in an employment or other contract, would not suffice).

As such, the Working Party considers that in most cases consent is unlikely to provide a good basis for processing.

The basis for processing under Article 7(c), compliance with a legal obligation, is also regarded by the Working Party as less reliable than it may appear. Compliance with a foreign legal obligation (in this case, the US code on civil procedure) may not qualify as sufficient legal obligation to legitimise data processing; the "legal obligation" (most likely[8]) has to be one imposed by a Member State.

However, in some Member States there may be a legal obligation, which as an internal obligation would qualify under 7(c), to comply with an Order of Court in another jurisdiction seeking discovery. A prominent example of this would be a requirement under the Hague Convention.

The final basis for processing data which the Working Party considers is Article 7(f), allowing compliance with a discovery request if it is necessary for the purposes of a legitimate interest pursued either by the data controller or by the third party to whom the data is disclosed (as long as the legitimate interest is not overridden by the rights of the data subject). This results in a "balance of interests" test, looking at proportionality, the relevance of the personal data to the litigation, and the potential consequences for the data subject. Using this as a basis will be easier if the data being transferred has been carefully filtered for relevance; and given the requirement of "necessity" it should be easier to fulfil that test if data is pseudonymised[9]. As will be seen below, it is indeed this condition which is most likely to apply in any Member State.

Transparency

Articles 10 and 11 of the Directive require information to be given to data subjects when their personal data is processed respectively when collected directly from the individual (Article 10) or from a third party (Article 11). The information to be provided includes in either case the purposes for which the data will be processed. The Working Party notes therefore, that general notice about the possibility of the data being processed for litigation should be given. Should the data actually be processed for litigation purposes, the subject should be informed of this, together with their right to object to any processing (set out under Article 14). The Directive provides an exception where there is a "substantial risk" that notifying the data subject would jeopardise the ability of the litigating party to investigate properly, as well as any exceptions in the laws of individual Member States.

Data security

In accordance with Article 17 of the Directive, data controllers must take all reasonable precautions to ensure the security of personal data. Transfers for the purposes of discovery therefore require the extension of this requirement to the parties who will be handling the data – generally the law firms involved. Somewhat surprisingly, perhaps, the Working Party seems to take the view that litigants can impose security standards on foreign courts: "*This would also include a requirement for sufficient security measures to be placed upon the court service in the relevant jurisdiction as much of the personal data relevant to the case would be held by the courts for the purposes of determining the outcome of the case.*"

It is perhaps unrealistic to expect a US litigant to obtain, say, an undertaking from a US court as to appropriate security!

Transfers to third countries

As mentioned above, Article 25(1) of the Directive generally prohibits the transfer of personal data to a country (including the US) which does not ensure an adequate level of protection.

An issue under this Article will obviously arise as a result of the transfer from the EU entity to its US affiliate which is engaged in the litigation (or to legal representatives if the EU entity is directly engaged in the litigation). However, it will also arise as a result of the disclosure by the US affiliate to the litigation opponent or even simply to a consultancy providing e-discovery services.

Where the third country is not generally considered to provide the proper level of protection, an adequate level of protection can equally be assured by some other well established grounds, and the Working Party recommends that the data only be transferred to the US on one the following grounds:

1. Where the recipient is part of the US Safe Harbor Scheme[10];

2. Where the recipient has entered into a transfer contract with the EU company transferring the data which provides for adequate safeguards (such as the EU model contracts[11]); or

3. Where the recipient is a member of a group which has in place a set of "binding corporate rules" which have been approved by the relevant data protection authorities.

These mechanics, however, as is well known and often criticised, generally do not allow further onward transfers and so do not obviously deal with the ability of the US litigating entity to give discovery to its opponent. Taking these three mechanics in turn: first, the Safe Harbor "onward transfer" requirement stipulates that an onward transfer (*i.e.* the discovery itself) can only happen if the opponent is part of Safe Harbor or agrees to sign a contract! Next, the US litigating entity may have signed a controller-to-controller set of clauses with its EU exporting affiliate. The original set of clauses only allows onward transfers either on consent of the data subjects or on the further recipient themselves signing up to the clauses. Lastly, binding corporate rules are simply inappropriate given that it is unlikely that the opponent in the US litigation will be in the same group.

The Working Party state that "*[w]here a significant amount of data is to be transferred the use of Binding Corporate Rules or Safe Harbor should be considered*" but do not discuss how the difficulties just mentioned can be overcome. They might perhaps be imagining that the adversary to the litigation may agree to joining Safe Harbor or signing model contracts. This may well be true if the problem is a mutual one, but otherwise seems unrealistic. And the US courts are unlikely to compel the adversary to perfect such mechanics.

All is not lost, however, for the EU entity that wants to comply with US discovery laws! Article 26(1)(d) provides a potential derogation from the Article 25 requirements where the transfer is necessary for the "establishment, exercise or defence of legal claims". Whilst this ground is somewhat relegated in importance by the Working Party, it does seem to present the only realistic ground in the Directive (subject to the detail of national implementations) under which a transfer can take place. As will be seen below, this is an important consideration certainly in the UK and France; in the latter jurisdiction after navigating the blocking statute issues.

Individual Member States

As previously noted, the problem is exacerbated by the fact that Member States have adopted different approaches to cross-border transfers of personal data, both under the Data Protection Directive and under the Hague Convention and in addition the variance in approaches to the issue of blocking statutes. In this section we set out the position in a sample of Member States (both common law and civil law jurisdictions).

Belgium

Discovery does not exist as such in Belgium, except for the "discovery lite" procedure laid down in articles 877 and following of the Belgian Judicial Code ("BJC"). Pursuant to these provisions, the Court may, at the request of a party, enjoin another party in the case or even a third party to produce a specific, identified document sustaining specified issues. This decision is left to the discretion of the Court and cannot be appealed (art. 880 BJC). Apart from this narrow exception, US-style "fishing expeditions" are therefore not possible before a Belgian Court.

Furthermore, contrary to the usual situation in common law countries, non-compliance with an order to produce a specific document does not constitute a contempt of court nor can it lead to the imposition of a fine, but it can lead to the payment of damages (art.882 BJC). However, as a less efficient alternative the requesting party may request the Court to also order a periodic payment penalty ("*astreinte*") to ensure the production of the relevant document. If a party decides not to produce the document notwithstanding the order, the Court may, in addition, take the failure to comply with its order into consideration during its decision-making process, by deducing all relevant consequences therefrom.

With regard to foreign procedures, Belgium does not (unlike some other civil law countries) have a general blocking statute preventing documents being transferred abroad for the purposes of pre-trial discovery. However, specific regulations may contain a limited prohibition to disclose information as part of legal proceedings abroad. This is for example the case of the Act of 15 September 2006 on the Protection of Economic Competition, which gives the Government (technically, the King) the possibility of adopting measures that prohibit companies transferring, under certain conditions, certain non publicly available information to foreign governmental entities. A similar prohibition is contained in the Act of 27 March 1969 on the Regulation of Sea and Air Traffic.

In line with applicable EU law, the Belgian Data Protection Act of 8 December 1992 ("BDPA") and its implementing Royal Decrees restrict the transfer of evidence, such as emails, that contain personal data.

Taking the main issues which arise under the Directive and are mentioned above in turn:

- It is likely to be possible to legitimise the disclosure of data under the Belgian equivalent of either of two grounds. It might be possible to obtain the informed consent of the data subject (art. 5.a BDPA, the Belgian equivalent of Article 7(a) of the Directive). Alternatively, and generally as a result of the Working Party's criticism of the consent route mentioned above, a disclosing litigant might be more likely to seek to rely on the Belgian equivalent of the "balance of interest" test in Article 7(f) of the Directive (namely, art. 5.f BDPA).

- The provision during pre-trial discovery of the special categories of data mentioned in Article 8 of the Directive ("sensitive" data), such as health data, is possible under the "defence of legal claims" exception under article 7.i BDPA provided that it must be "necessary for the establishment, exercise or defence of legal claims". Belgian law will also require a balance of the conflicting interests to be struck by the controller.

- The Directive prohibition to transfer personal data to countries that do not ensure an adequate level of protection is implemented in article 21 § 1 BDPA. The exemption to this prohibition laid down in article 26(1)(d) of the Directive (when necessary for "*the establishment, exercise or defence of legal claims*") has been literally transposed in article 22 § 1, 4 BDPA.

  WDPR ISSN 1473-3579

- The information requirements under articles 10 and 11 of the Directive were implemented by articles 9 and 10 BDPA. Article 9 § 2 BDPA, read in combination with article 30 of the Royal Decree of 13 February 2001, provides an exemption from these information requirements when it is impossible or if it would require "disproportionate efforts" to inform the data subject(s). An opinion given by the Belgian Privacy Commission in 1999 (Opinion 25/99, p.5), states that it may be disproportionate (subject to the specific circumstances) when a large number of data subjects are involved. However, this consideration has to be seen in the context of the sensitivity of the personal data at stake.

France

France has always been reluctant to allow what it views as denials of its territorial sovereignty and treats discovery as no more than real fishing expeditions. The fact that this could occur at a pre-trial stage renders discovery even more unacceptable. As a consequence, and when trying to respond to perceived abuses mainly originating from the United States, France enacted, in July 1980, Law n 80-538 (the "1980 Law") which provides that"*subject to treaties or international agreements and the laws and regulations in force, it is prohibited for any person to request, seek or communicate, in writing, orally, or otherwise, economic, commercial, industrial, financial or technical documents, or information leading to the constitution of evidence with a view to foreign judicial or administrative proceedings or in the context of such procedures*"[12] – its "blocking statute".

Cross border data transfers for production in a US judicial or administrative proceeding violate the 1980 Law and create potential criminal liability, unless an exception applies. There is no exception for voluntary compliance (even with the consent of all data subjects with respect to the transfer of their personal data), nor for disclosure of documents intended to defend against a claim.

The 1980 Law is intended to force US litigants to use the provisions of the Hague Convention, thus the exceptions for "*treaties or international agreements*". In the event that the Hague Convention procedures cannot be followed, it may still possible to refer to other international treaties or agency-to-agency agreements as a basis for an exemption request to the French authorities or to work out ad-hoc arrangements with the French authorities[13]. In such cases, the provisions of Law n 78-17 (the "1978 Law") which implemented in France the principles of the Directive would have to be complied with. Dealing with the issues which arise under the Directive:

- Under Article 7 of the 1978 Law, it is possible to legitimise the disclosure of personal data[14] without the consent of the data subjects. The most relevant one (as in Belgium) is Article 7(5) the equivalent of the "balance of interest" test in Article 7(f) of the Directive.

- It is also possible to transfer personal data abroad. Article 69 of the 1978 Law contains a litigation exemption when the transfer of personal data is necessary or legally required for "*the establishment, exercise or defence of legal claims*", which is of course the equivalent to Article 26(1)(d) of the Directive).

- However, Article 32 of the 1978 Law still requires information (including the purpose for which the personal data is collected) to be given to data subjects when their personal data is processed when collected or prior to their transfer, subject to certain limited exceptions which are not helpful in civil pre-trial discovery[15].

Until recently, potential criminal sanctions associated with the breach of blocking statute provisions were viewed as theoretical[16] as no person had ever been prosecuted under the 1980 Law. On December 12, 2007, the French Supreme Court[17] applied the provisions of the 1980 Law and ordered a French attorney to pay a fine of €10,000 for violation of the blocking statute. In this case, at the request of a US lawyer, a French attorney had sought from a former board member of a defendant information regarding how board decisions were taken, without using the means for gathering evidence provided by the Hague Convention. According to certain authors, this case shows the willingness of the French Supreme Court to apply the provisions of the 1980 Law strictly, and perhaps in the hope of forcing US courts to reconsider their position.

The Netherlands

Discovery as known in common law does not exist in general in the Netherlands due to the reluctance to allow "fishing expeditions". However, as in Belgium, a party may request a Court to require the production of a specific document by another party in the case or by a third party who has such document at its disposal or in its custody[18]. The court has an element of discretion here and the possibility is not always available.

With regard to foreign procedures, the Netherlands do not have a general blocking statute preventing documents to be transferred abroad for the purposes of pre-trial discovery, although limited prohibitions may exist in specific fields[19].

In accordance with EU law, the Dutch Personal Data Protection Act of 6 July 2000 ("PDPA") and related regulations restrict the transfer of evidence that contain personal data (including emails). Dealing with the issues which arise under the Directive:

- As in other Member States, the disclosure to a third party of personal data for the purposes of legal proceedings is possible under the PDPA if the data subject has unambiguously given his consent[20] or under the Directive "balance of interest" test[21].

- However, in accordance with the Directive, under article 16 of the PDPA, the processing of the "sensitive" personal data is subject to a stricter regime. As confirmed by the "Guidelines for personal data processing" of the Dutch Ministry of Justice, processing of this data is prohibited unless a specific exemption applies, and these include where the processing is necessary for the establishment, exercise or defence of a right in law.

- When discovery involves transfer abroad to a country which does not ensure an adequate level of protection, the Directive prohibition can also be dealt with by an applicable litigation exemption[22].

- The Dutch equivalents of the information requirements set out in articles 10 and 11 of the Directive[23] do not apply if it appears to be impossible to provide the required information to the data subject or if it would involve a disproportionate effort to provide it[24]. A further exemption exists under article 43 PDPA; the information requirements may be dispensed with to protect a person's or an entity's rights.

United Kingdom

In the UK, the Data Protection Act 1998 ("DPA") has implemented the principles of the Directive, adding (as permitted by the Directive) some additional provisions which make cross-border discovery easier. Exemptions for transfers for the purposes of legal proceedings have been added to the rules on cross-border transfers and many of the other data protection principles, making it more likely that transfers to the US for the purpose of discovery will be permitted and reducing the likelihood that it will be necessary to inform the data subject of such transfers.

Taking the main issues which arise under the Directive and mentioned above in turn:

- As with France and Belgium, it is likely to be possible to legitimise the disclosure of data under the UK equivalent of Article 7(f); namely, paragraph 6 of Schedule 2 of the DPA. The UK courts are clearly comfortable with the discovery process (albeit it is rather wider in the US than in the UK).

- The information requirements under Articles 10 and 11 of the Directive to inform the data subject of the purposes for which their data will be disclosed, and potentially to whom the disclosure will be made are implemented as part of the first of the "data protection principles" set out in Schedule 1 of the Act and in particular in the interpretative paragraphs 1 to 3 of Part II of that Schedule. However, UK law contains a wide exemption which would be applicable to these requirements. In particular, s. 35(2) of the DPA contains an exemption from the requirement to comply with certain of the data protection principles (including the first principle relevant here) where a disclosure is necessary in connection with legal proceedings, for the purpose of obtaining legal advice, or for the purposes of establishing, exercising or defending legal rights.

- Likewise, Article 25 of the Directive is implemented in the UK as the eighth "data protection principle". The UK has in Schedule 4 of the DPA set out a number of exemptions to this principle including where the transfer is for use in legal proceedings and in cases of "substantial public interest".

A recent case before the English courts has demonstrated how these exemptions work in practice in relation to the transfer of personal data to the US. In *Re Madoff Securities International Ltd* [2009] EWHC 442 (Ch), the joint provisional liquidators of an English company forming part of Bernard Madoff's alleged Ponzi scheme empire applied to the court for directions allowing the transfer of data to the American trustee in bankruptcy concerned with the liquidation of Madoff's American company[25]. The transfer could potentially have contravened the eighth data protection principle (*i.e.* Article 25). However, the judge considered that the need to unravel the details of such a massive fraud meant that the transfers of information would be justified "for reasons of substantial public interest" according to the exception in Sch 4 para 4(1) of the DPA (*i.e.* the equivalent of "public interest grounds" in Article 26(d)). In addition, the likelihood of legal proceedings in the unravelling of the fraud meant that the exemptions for legal proceedings and legal rights in Schedule 4 para 5 also applied (also reflecting a derogation in Article 26(d)). The judge therefore granted an order permitting the transfer of specified personal information to the US.

It is worth noting, however, that the judge refused to grant the second part of the requested order, which would have given the joint provisional liquidators the power to disclose further unspecified information as they considered it necessary. It was not the court's intention, he remarked, to make blanket orders without knowing what was being authorised.

Comments, practical tips and concluding remarks

Some of the guidelines will be viewed with concern by US litigators and seem to show no real understanding of the reality of conducting litigation in the US.

For example, take the idea that the transparency requirements in the Directive imply that specific notice should be given to individuals that their personal data is being disclosed as part of discovery to an adversary. It is not inconceivable that in, say, a contractual dispute the US courts would require a full disclosure of email exchanges involving the litigating parties and not uncommonly this may run into the thousands. Given the width of the definition of "personal data"[26] such a quantity of emails is likely to contain the personal data of many individuals (all senders, receivers (including those to whom it has been copied), and potentially all individuals simply mentioned). The Working Party's view would have the parties identify all those individuals, identify precisely whether any individual's personal data is in fact included, and then would require that a notice given to them (once they have been located) of the fact of discovery to a particular adversary. Moreover, they are to be given a right to object! Clearly, impractical and unrealistic. Whether this is a problem or not will depend upon the country, the litigation exemptions available in the UK and the exemptions in Belgium and the Netherlands (all mentioned above) may well apply in this scenario[27], but it seems not in France.

In short, whilst the working document is welcome as showing an awareness of the problems, at a Directive level at least there is little that the Working Party say

  WDPR ISSN 1473-3579

which is helpful in navigating them. The issue is primarily one of implementation in the various Member States. As shown from the position in the UK and France (once the blocking statute issue has been navigated), it is certainly open to Member States to have wide litigation exemptions which remove a great deal of the conflict which might otherwise have existed. Indeed when there is a blocking statute that will inevitably provide a greater hurdle.

Finally, the Working Party does recognise that this is only the beginning of a debate; they expressly invite a public consultation and dialogue with interested parties (although nothing formal appears to be suggested).

NOTES

[1] The Article 29 Working Party (set up as its name suggests under Article 29 of Directive 95/46) is the group of each of the data protection authorities of the (now) 27 Member States who meet to issue opinions and attempt to ensure as far as they can a harmonious interpretation of directive issues by the regulators.

[2] Working Document 1/2009 on pre-trial discovery for cross border civil litigation (WP 158 of February 11, 2009).

[3] Another area which presents a similar compliance problem is in the whistleblowing requirements of the US Sarbanes-Oxley legislation, and the attitude to such requirements by some European Member States. See Working Party Opinion 1/2006.

[4] The Restatement (Third) of Foreign Relations Law of the United States no. 442.

[5] See note 2.

[6] As to whether pseudonymisation can lead to the disapplication of the Directive rules, see the Article 29 Working Party paper Opinion 4/2007 on the concept of personal data (WP 136 of June 20, 2007).

[7] See further Working Party paper 114 ("Working document on a common interpretation of Article 26(1) of Directive 95/46/EC") where at paragraph 2.1 they state: "Valid consent in such a context means that the employee must have a real opportunity to withhold his consent without suffering any harm, or to withdraw it subsequently if he changes his mind."

[8] This is not dealt with in any length in this opinion but in its opinion on whistleblowing hotlines imposed by Sarbanes-Oxley the Working Party said ". . . *an obligation imposed by a foreign legal statute . . . .. may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate. Any other interpretation would make it easy for foreign rules to circumvent the EU rules laid down in Directive 95/46/EC*". See "Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime" WP 117 of February 1, 2006. Similar sentiments have been expressed in other contexts.

[9] If data is (properly) anonymised, of course, the Directive would simply not apply as the data would no longer be "personal data".

[10] http://www.export.gov/safeharbor/eg_main_018236.asp

[11] The US litigating entity will likely be a data controller and so it could sign one of the two sets of approved controller to controller clauses in the Annex to Decision 2001/497/EC.

[12] The sanctions provided for the non-compliance of the prohibition are imprisonment up to six months and/or a fine up to €18,000 (Article 3 of the 1980 Law).

[13] This interpretation is confirmed in the response of the French Minister of Justice dated September 28, 2005 to the French Data Protection Authority, in relation to the transfer of data to the United States in the context of discovery procedures.

[14] Article 7 of the 1978 Law.

[15] Article 32 does not apply to the processing of personal data whose purpose is to prevent, investigate or prove criminal offences.

[16] *Partenreederei M/S "Heidberg2 v Grosvenor Grain and Feed Co* [1993] 2 Lloyd's Rep 324.

[17] C.Cass., December 12, 2007, n 07-83228 (Executive Life).

[18] The Dutch Code of Civil Procedure (especially art. 843a).

[19] For example in the case of the former article 39 of the Dutch Law on Economic Competition.

[20] Article 8.a, PDPA

[21] Article 8.f, PDPA

[22] Article 77.1.d PDPA

[23] Articles 33 and 34 PDPA

[24] Article 34.5 PDPA

[25] Under s. 112 of the UK Insolvency Act 1986 a liquidator can apply to the court "to determine any question arising".

[26] At least as expounded by the Working Party in WP 136 (cited at footnote 6).

[27] Even if the UK didn't have this exemption, one suspects that this issue would be less of a concern in the UK given that, as the law presently stands following the judgment of the UK Court of Appeal in *Durant v Financial Services Authority* ([2003] EWCA Civ 1746), the UK takes a narrower view of the definition of "personal data" than the Working Party propounds in WP 136.

Why employee consent might not do the trick

By Dr. Michael Schmidl, Maître en Droit, LL.M. Eur.

It does not matter whether one tries to come to grips with European privacy legislation by means of reading the European Data Protection Directive 95/46/EC ("Directive") or by studying the various EU Member States' privacy laws implementing the Directive.

The basic rule, also applicable in the employment relationship, that a permission is needed prior to any collection, processing (this includes transfers) or use of personal data can be found everywhere.

The laws implementing the Directive, in Germany the Federal Data Protection Act ("FDPA"), provide for statutory permissions and also consent in order to justify the necessary collection, processing or use of personal data.

As regards statutory permissions the collection, processing or use of personal data is *inter alia* admissible,

- if this is necessary for the performance of the employment contract (cf. Sec. 28 (1) 1st sentence no. 1 FDPA); or
- if the employer/a third party has a legitimate interest in the collection, processing or use and the interest of the employer prevails after a weighing of interests or

Dr Schmidl is a partner of Baker & McKenzie Partnerschaft von Rechtsanwälten, Solicitors und Steuerberatern, Munich and member of the firm's Information Technology Group. Dr. Schmidl is a specialised attorney for IT-Law and a lecturer for Internet law at the University of Augsburg. The author may be contacted at: Michael.Schmidl@bakernet.com.

(in the case of a third party's interest) there is no reason to assume a conflicting interest of the employee (*cf.* Sec. 28 (1) 1st sentence no. 2/(3) no. 1 FDPA).

For transfers of personal data to recipients outside the EU/EEA according to Secs. 4b, 4c FDPA there is the additional requirement for the data exporter *(i.e.* usually the employer) to make sure that the recipient provides for an adequate level of data protection (*e.g.*, by signing an adequate Model Contract) or is located in a jurisdiction, which the European Commission has found to provide an adequate level of protection.

Faced with these requirements and the related analyses (necessity for performance of employment relationship, legitimate interest, weighing of interests *etc.*) companies quite frequently turn to employee consent, which seems to be a comparably simple solution for both levels of privacy compliance, *i.e.* the admissibility of the measure as such and the creation of an adequate level of data protection.

Employee consent, worded in the broadest possibly form, is then asked for already on the occasion of the conclusion of the employment contract, for example in the form of an attachment to the contract, or at a later stage, when the need for international data transfers arises for the first time.

On such basis, the collection, processing and use, even of sensitive data, is deemed to be possible without any restrictions.

This approach, however, ignores the following limitations for employee consent that might lead to the absence of a valid justification mechanism and entail substantial organisational, financial and penal risks:

1. The consent of the employee is normally not given voluntarily. It therefore can only come into consideration in exceptional cases in order to justify the collection or the processing of personal data (*cf.* Working Paper No. 114 of the Article 29 Working Group of November 25, 2005);

2. In the case where the collection, processing and use of data is admissible because it is necessary for the execution of the employment contract, it is misleading and inadmissible to obtain the consent of the employee additionally (*cf.* Working Paper No. 48 of the Article 29 Working Group of September 13, 2001) – the employee might be led to believe that he would endanger the execution of the employment contract, if he does not give or revoke his declaration of consent;

3. In case employees revoke their declaration of consent, which they are free to do at any time, all measures undertaken on the basis of such declaration of consent have to be discontinued or the measures have to be designed so as to avoid those employees who have revoked their declarations of consent or who have consented in the first place. What becomes necessary is (i) a complex and expensive differentiation between employees who have consented, who have consented but then withdrawn consent and those who have not consented at all and (ii) a privacy compliance concept in line with the statutory justifications for all the cases mentioned under (i);

4. A privacy infrastructure based on consent is not flexible and consent has to be asked for again in cases of a reorganisation or other significant structural changes of the group structure.

Ignoring the limitations (1) and (2) above leads to consent being null and void – measures carried out on such basis are most likely illegal and subject to fines of up to € 250,000 per case (*cf.* Sec. 43 FDPA) and potentially even criminal law sanctions (*cf.* Sec. 44 FDPA). The same applies to the continuation of processing measures after consent has been revoked or the carrying out of such measures despite the employees' refusal to consent (see limitation (3)). It is important to underline that employee consent cannot be made voluntary by expressly making reference to the possibility of not giving or revoking consent. According to the German data protection authorities even such express information does not change the fact that the employee will always be under a factual pressure to give his consent or alternatively risk not getting the job or losing it in the case of revocation.

In conclusion, one should use the instrument of the employee's consent in exceptional cases only. Statutory provisions provide possibilities for almost all measures. In the meantime the German data protection authorities even offer a solution for the transfer of sensitive data. It is of key importance for the application of statutory permissions to provide thorough information to the employees, especially when they work in complex matrix structures with matrix managers in other group entities (more will be published on this, especially a sample notification, in one of the following editions).

  WDPR ISSN 1473-3579

Switzerland authorises Safe Harbor Framework for personal data transfers to the United States

By Mauricio F. Paez, Partner, Joseph J. Bernasky and Gwendolynne M. Chen, Jones Day.

The new US–Swiss Safe Harbor Framework ("US–Swiss Safe Harbor"), effective February 16, 2009, facilitates transfer of personal data from companies in Switzerland to companies in the United States.

Previously, the Swiss Data Protection Act ("DPA") permitted only the transfer of 'personal data' from Switzerland to jurisdictions that the Federal Data Protection and Information Commissioner ("FDPIC") deemed to provide an adequate level of data protection. In order to transfer personal data from Switzerland to jurisdictions that the FDPIC did not deem to provide an adequate level of data protection, the exporting and importing organisations were required to sign an agreement guaranteeing that the importing organisation would provide the 'appropriate' level of data protection required under Swiss law. The FDPIC has found the following contractual agreements to provide an appropriate level of protection:

1. Standard Contractual Clauses of the European Union;
2. The Council of Europe's model contract for safeguarding an appropriate level of data protection in transborder data transfers; and
3. The FDPIC's model contract for the outsourcing of data processing abroad.

The parties would then submit the agreement to the FDPIC for inspection and approval prior to any transfer of personal data outside of Switzerland.

With the implementation of the US–Swiss Safe Harbor, organisations seeking to transfer personal data from Switzerland to the United States now have an alternative means to do so under the DPA.

Similar to the existing Safe Harbor structure between the European Union and the United States ("US–EU Safe Harbor"), the US–Swiss Safe Harbor allows US companies to self-certify to the US Department of Commerce that they will uphold the same seven data protection principles contained in the US–EU Safe Harbor Framework: Notice, Choice, Onward Transfer, Security, Data Integrity, Access, and Enforcement. Applicants may certify to the US–Swiss Safe Harbor alone or along with the US–EU Safe Harbor on the same Certification Form by selecting Switzerland as a country from which they receive personal data. Switzerland will recognise certified companies as meeting its required standard of data protection and allow transfer and access to Swiss personal data by these companies. The US–Swiss Safe Harbor also provides for special dispute resolution boards in cases of data protection breaches and permits the US Federal Trade Commission to take action against certified companies in cases of egregious or repeated data protection infringement. These remedies are in addition to possible private actions.

The significant overlap in substantive requirements and certification procedures for both the US–Swiss and US–EU Safe Harbors will likely benefit entities seeking to streamline compliance policies and procedures for transferring data from both the European Union and Switzerland to the United States. One notable distinction, however, is that the Swiss DPA defines 'personal data' to include all information relating to natural and legal persons, *e.g.*, companies, associations, *etc.* By contrast, both the US–Swiss Safe Harbor and the US–EU Safe Harbor cover only personal data of natural persons. Thus, organisations seeking to transfer other types of data from Switzerland may still need to enter into cross-border data transfer agreements and seek approval from the FDPIC.

Mauricio F. Paez, Joseph J. Bernasky and Gwendolynne M. Chen can be contacted at: mfpaez@jonesday.com, jjbernasky@jonesday.com and gchen@jonesday.com

What is personal data? Part 2

By Peter Church, Professional Support Lawyer, and Georgina Kon, Associate, Linklaters.

The Information Commissioner recently issued guidance on what constitutes 'data' for the purpose of the UK Data Protection Act 1998.

It follows his earlier guidance on when such 'data' is personal data under the Act. This earlier guidance which attempted to reconcile the inconsistent approaches adopted by the English courts and other European regulators met with mixed reactions. (As reported in the November 2008 issue of WDPR.)

However, the latest guidance should cover safer ground. There has been a less heated debate at a European level as Member States have more discretion over the definition and the Article 29 Working Party has yet to issue substantive guidance on this point. In addition, most information is now stored on computer, which makes it automatically 'data', so difficult questions are less common in practice. However, issues remain, especially for organisations that store substantial amounts of informa-

Peter Church and Georgina Kon can be contacted at: peter.church@linklaters.com and georgina.kon@linklaters.com

tion offline, for example on microfiche. This article considers the impact of the new guidance for these organisations.

What is 'data'?

Information is only subject to the Act if it constitutes 'data'. This definition is divided into four categories:

- information processed, or intended to be processed, wholly or partly by automatic means *(e.g.* on a computer);
- information processed, or intended to be processed, that forms part of a 'relevant filing system';
- information in an accessible record (*e.g.* health records, educational records and the like); and
- information held by a UK public authority, the so-called category (e) data.

What does the guidance say?

The guidance consists of a set of eight questions in the form of a flow chart, as set out. Unsurprisingly, it focuses on the definition of 'relevant filing system' as this raises the most difficult issues in practice, with four of the eight questions addressing this point.

The questions work through the requirements of the relevant filing system definition, namely:

- whether the system uses the names of individuals or other criteria relating to individuals to structure the system; and
- if so, whether the system is indexed to allow ready access to *specific* information about individuals or whether it only contains one category of information.

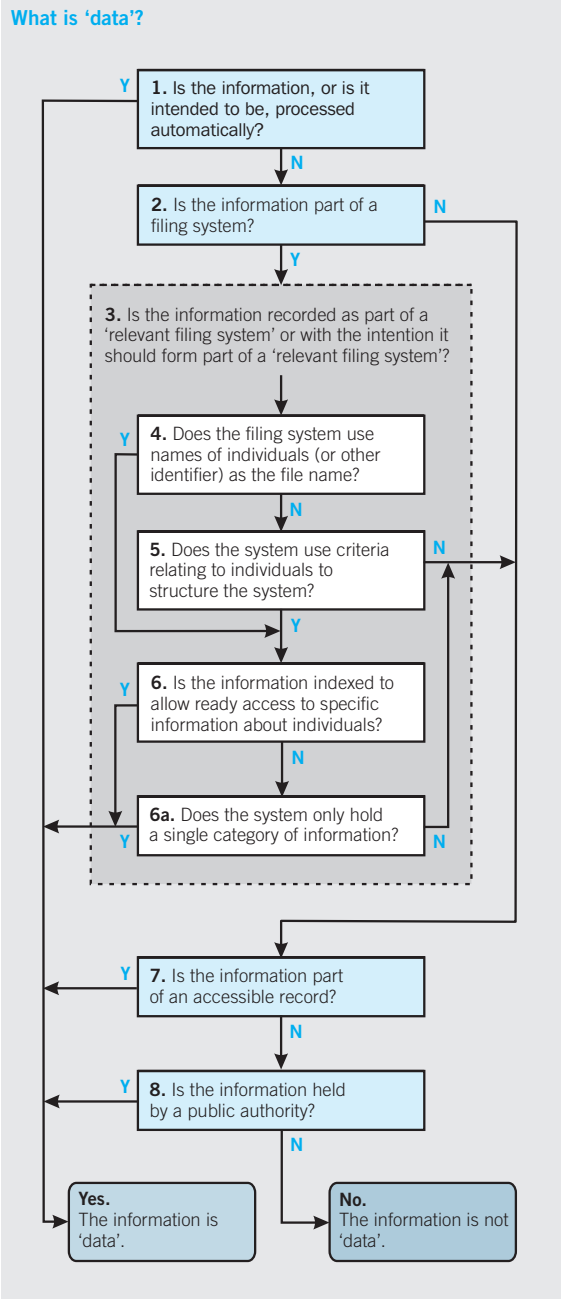
What about *Durant*?

So far so good. Questions as to whether information is 'data' or not rarely arise and if they do, the flowchart provides a useful summary of the issues to address. However, other comments in the guidance are difficult to reconcile with English courts' approach to personal data and, in particular, the Court of Appeal's decision in *Durant v Financial Services Authority* [2003] EWCA Civ 1746.

The most prominent example relates to the cost and effort in extracting the information. The guidance states, "*accessing the required information may on occasion be time consuming and demand a high level of resource [However,] the key consideration is not the time and effort involved but whether there is a system in place that allows the organisation to find information . . . without searching through every item in every record*".

This is hard to square with a view in *Durant* that the filing system in question must provide "*easy access to the personal data in question*" and that it must be "*of sufficient sophistication to provide the same or similar ready accessibility as a computerised filing system*". The Court of Appeal came to this conclusion on the basis that the legislation must act in a proportionate manner and that the Act is intended to protect the privacy of personal data, not mere documents.

This latest guidance also moves away from some of the statements made by the Information Commissioner in 2006 (see *The 'Durant Case' and its impact on the interpretation of the Data Protection Act 1998*[1]) which, for example, advocated a "temp test" to determine if information was 'data' *i.e.* whether a temporary worker would be able to extract the information without any particular knowledge of the background and with only a short induction. Similarly the bald statement that "*very few manual files will be covered by the provisions of the [Act]*" is gone. Arguably this was an overly restrictive approach to the definition of 'data'. Time will tell if the current guidance is perhaps over liberal.



The guidance on what is 'data' is available at:

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/what_is_data_for_the_purposes_of_the_dpa.pdf

NOTES

[1] http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/the_durant_case_and_its_impact_on_the_interpretation_of_the_data_protection_act.pdf

This article first appeared in Linklater's Technology, Media & Telecommunications newsletter, Issue 50.

EC launches infringement proceedings against UK government

By Oliver Bray, Partner, and Tom Cadwaladr, Trainee Solicitor, IP and Technology Group, Reynolds Porter Chamberlain LLP.

The European Commission has announced that it is taking legal action against the UK government for failing in its duty to properly implement EU e-privacy and data protection rules protecting the privacy of online communications. While the announcement does not set out the exact nature of the alleged infringement, it would appear that the UK is to be accused of failing to protect Internet users against the unlawful interception of communications data, specifically with regard to the profiling of user behaviour for the controversial online behavioural advertising (OBA) service based on Phorm's deep packet tracking technology.

Background

The announcement refers specifically to the two secret trials conducted in 2006 and 2007 by British Telecom (BT) using technology to profile Internet use by users without their consent. Following a substantial number of complaints from users, the Information Commissioner's Office (ICO) launched an investigation into the trials. The ICO indicated, on the assurances given to it by Phorm, that there had been no breach of any UK laws by BT or Phorm, the provider of the tracking technology. However, the Commission has taken a very different view and having completed its own enquiries into the ICO's investigations of the trials, has decided to bring proceedings against the UK government in the European Court of Justice for allowing the trials to operate and for failing to take action. EU Commissioner for Information Society and Media, Vivian Reding, has made the Commission's motive clear – reform of UK law is needed to bring it closer in line with the ePrivacy Directive (2002/58/EC). As she said in a statement released on April 14, 2009,

> "we have been following the Phorm case for some time and have concluded that there are problems in the way the UK has implemented parts of EU rules on the confidentially of communications. . .I call on the UK authorities to change their national laws and ensure that national authorities are duly empowered and have proper sanctions at their disposal to enforce EU legislation".

Phorm – the stimulus for EC intervention

Phorm developed the products used by BT to conduct the 'secret trials'. Phorm maintains that the technology protects against 'phishing' and improves the relevance of advertising based on the interests of the user. Webwise is the customer facing web feature whilst OIX is the advertising exchange platform. The running and operation of these products have been explained in detail in previous WDPR articles (see *ISP data 'pimping' – Phorm under fire over privacy concerns for targeted advertising technology*, April 2008 and *Information Commissioner's Office opinion on Phorm's targeted advertising technology*, June 2008, Oliver Bray and Simon Griffiths). It is claimed by BT that Webwise mirrors a user's request to visit a website at the moment he requests to enter it. This mirrored data is profiled and anonymised to erase any trace linking the data to the user, *e.g.* the IP address. At the same time a randomly generated ID is allocated to the user and held on their computer in the form of a cookie. This ID and anonymised data is sent to a Phorm managed server, which categorises the data so that it can be linked with relevant advertising through its OIX product. The result is that advertising targeted to the user appears on his computer screen.

What is the case against the UK government?

This method of advertising is certainly pioneering and is transforming the industry. However, its future appears uncertain following the Commission's recent move to take the UK government to the ECJ. At the time of writing, the Commission had not made the detail of its case against the UK government public. However, it is expected that its case will focus on the UK government's alleged failure to maintain the confidentiality of communications of users subscribed to BT's consumer broadband service during the trials of 2006 and 2007. Under Article 1(1) of the ePrivacy Directive, Member States are required to ensure the confidentiality of communications and related traffic data by prohibiting unlawful interception and surveillance unless users have consented. During the trials, BT did not seek consent from any of the thousands of users concerned. Further, under Article 2(h) of the Data Protection Directive (95/46/EC) users' consent must be "freely given specific and informed".

The ICO completed its investigations into the BT trials and found that UK data protection law had not been breached. As a result, it decided not to take any further action. Notably it confirmed that it did not consider there to have been a breach of the ePrivacy and Electronic Communications (EC Directive) Regulations 2003 (the Regulations), which were introduced to implement the ePrivacy Directive. However, the Commission alleges that this was inadequately implemented. Vivian Reding has said European rules on privacy are "crystal clear" and that "Europeans must have the right to control how their personal information is used".

Oliver Bray and Tom Cadwaladr can be contacted at Oliver.Bray@rpc.co.uk and Tom.Cadwaladr@rpc.co.uk

Under the Regulations it is unlawful to use an electronic communications network to store information, or to gain access to information stored, in the terminal equipment of a user of that terminal equipment unless he is given "clear and comprehensive information" as to the purposes for the storage or access to the information and is offered the opportunity to refuse such storage or access. This provision mirrors the requirement on Member States in Article 1(3) of the ePrivacy Directive and goes further than the Data Protection Act 1998 as it covers not only the processing of data but also cookies which store information under the Phorm system. The Commission is likely to allege that such clear and comprehensive information was not given to users during the BT trials in 2006 and 2007.

Following the news that the Commission had commenced proceedings against the UK government, the ICO issued a statement saying that the,

> "infringement proceedings from the EU appear to relate to the interception of communications, which is not part of the ICO's remit. Interception of communications is covered by the Regulation of Investigatory Powers Act. . ."

The Commission has expressed its concern over the lack of an independent regulatory body responsible for monitoring the interception of communications in the UK and it is expected that this will form part of its case.

Under s 1 of the Regulation of Investigatory Powers Act 2000 (RIPA) it is an offence to intercept any communication in the course of transmission without lawful authority. However, interception is permitted where it is unintentional or where there are reasonable grounds for believing that the user has agreed to the interception. The UK government has not made it clear whether it considers this Act to have been contravened during the BT trials. The Commission is expected to allege unlawful interception took place which the UK failed to notice.

At the time of writing, the UK had less than two months to reply to the Commission's letter of formal notice. The UK must adopt a position on the points of fact and of law. In the event that the UK's observations are unsatisfactory or it fails to respond at all, the Commission may then address a reasoned opinion to the UK setting out why it considers there to have been an infringement of Community law and obliging the UK to comply within a specified timeframe (usually two months). A failure to do so may result in the Commission referring the matter to the ECJ for final adjudication.

It appears that Ms Reding's position to "not shy away from taking action" against Member States is strongly supported in Brussels. In a keynote speech to a round table on online data collection, targeting and profiling held in Brussels at the end of March calling on Member States to act against lack of transparency and "commercial discrimination", Consumer Commissioner Meglena Kuneva said that "the current situation with regard to privacy, profiling and targeting is not satisfactory". The current case being brought against the UK is part of a wider co-ordinated move by the Commission to crack down on Deep Packet Inspection.

The Commission is certainly not alone in its view. There are many critics of Phorm's technology, including Tim Berners-Lee, director of the World Wide Web Consortium which oversees the development of the Web. He has recently said that a line must be drawn where third parties are using data gathered by systems such as Phorm's for political ends or commercial interests. He has said that "there's a gap between running a successful Internet service and looking inside data packets".

Further, BT is trialling Webwise again, albeit this time with users' consent. Critics, however, have taken issue with the fact that the proposed system will be on an opt-out rather than an opt-in basis so that users and websites will have their respective data monitored and 'mirrored' unless they opt out of the service.

UK government's position

At the time of writing, a series of email exchanges dating back to August 2007 between the UK government's Home Office and Phorm, were claimed by the BBC to have been revealed under the Freedom of Information Act 2000. The BBC claim that these emails show, amongst other things, the Home Office asking Phorm whether it would be "comforted" by its position, what Phorm thought about advice being drawn up by the Home Office at the time and specific references being made to Phorm's technology.

The BBC claims that in an email dated August 2007, a Home Office official wrote to Phorm's legal representative stating that his or her personal view accorded with Phorm's legal representative's view and that ". . .even if it is 'interception', which I am doubtful of, it is lawfully authorised under section 3 by virtue of the user's consent obtained in signing up to the ISPs terms and conditions."

In a later email dated January 22, 2008, the BBC claim that the Home Office wrote to Phorm asking it to "review" an attached document and let the Home Office know what it thought about it. In the same month, the BBC claims that the Home Office thanked Phorm for changes to its draft paper and that such changes and deletions made by Phorm can be seen through the course of the disclosed email correspondence.

The revealing of these emails has led many to publicly question the UK government's position over behavioural advertising technology. BBC News has quoted Baroness Miller, Liberal Democrat for Home Affairs, to have said that "the fact the Home Office asks the very company they are worried is actually falling outside the laws whether the draft interpretation of the law is correct is completely bizarre". In reply the Home Office has told the BBC that it did not consider that it had given "any advice to Phorm directly relating to possible criminal liability for the operation of their advertising platform in the UK". Despite the Home Office's clear denial of any

  WDPR ISSN 1473-3579

wrongdoing it is expected that the Commission will raise difficult questions on this in its case against the UK government.

There is a further question mark over the neutrality of the UK government's position based on its previous support for a communications database. It has previously considered, only now to withdraw on privacy grounds plans for the creation of such a database, which would intercept and record every website visited and email header sent and received by every ISP user in the UK using a not too dissimilar Deep Packet Inspection method as Phorm. In its recent report, *Database State*, The Joseph Rowntree Reform Trust, chaired by Lord Shutt of Greetland, classified the proposed communications database as a red database signalling that ". . .it is almost certainly illegal under [human rights or] data protection law and should be scrapped or substantially redesigned". This classification placed the proposed database in the same category as the controversial National DNA Database. The report went on to say that "the public are neither served nor protected by the increasingly complex and intrusive holdings of personal information invading every aspect of our lives". The fact that the UK government originally proposed a communications database based on data obtained through a comparable method as that employed by the Phorm system led privacy groups to question its neutrality when turning its attention to BT's Webwise.

This is not the first time that the UK government has locked horns with the Commission over data protection laws. The Commission previously threatened proceedings in 2004 against the UK for failing to properly implement almost a third of the Data Protection Directive. In response, the UK government publicly stated that it had "properly implemented the Data Protection Directive via the Data Protection Act 1998 and other relevant provisions of UK law". Further, the ICO issued a press release on July 7, last year, declaring that the said Directive was in need of reform implying that the onus was on the Commission to modernise its creation.

The advertising and communications industries will be hoping that the UK government does not capitulate on the question of OBA. The Incorporated Society of British Advertisers, for example, has said that concerns over the Phorm technology "can and should be addressed by the UK's successful system of advertising self-regulation" although some may consider this disingenuous as the privacy of communications would stretch the remit of advertising regulators, self-regulating or otherwise.

Comment – what can we expect?

At this point it is unclear as to the specific case that the Commission is putting to the UK government. It is, however, almost certain that whatever it may be, the Commission will not shrink from its objective. Ms Reding and Ms Kuneva have both stated emphatically that the Commission will take action against any Member State which fails to protect its citizens' online privacy. At the time of writing, the All-Party Parliamentary Group on Communications had just announced that it would be investigating online traffic, including the specific issue of Deep Packet Inspection and behavioural advertising. The government's reaction to the outcome of this investigation will be eagerly awaited by both the industry and the Commission.

The use of Phorm's technology remains a highly contentious issue amongst users. We can expect more major Internet names to follow Amazon and Wikipedia's lead of publicly opting out of the Phorm technology monitoring its sites to avert any fall in its visitor numbers. Attempts at self-regulation in this area have come under attack from the privacy lobby, most notably the recently published Internet Advertising Bureau's (IAB) Good Practice Principles for Online Behavioural Advertising which a number of major businesses have signed up to, including Google and Microsoft.

The IAB's principles are based on three commitments: notice, user choice and education. Firstly, they require that each signatory provides clear and unambiguous notice to users that data is being collected for the purposes of behavioural advertising. Secondly, they require that each signatory provides an approved means for declining behavioural advertising, interestingly the IAB has approved Webwise as an example of an "approved means". Finally, they require that each signatory make information available and accessible to users to educate them on behavioural advertising. Privacy groups have argued that the principles are limited in effect as they are by their nature voluntary and therefore hold no legal force. Further, privacy campaigners claim that the principles fail to make any real steps forward as users are still required to delete their cookies or actively inform their ISP that they wish to 'opt out' to decline behavioural advertising.

Meanwhile on second reading, following recommendations by the European Parliament's Internal Market and Consumer Protection Committees, proposed amendments to the ePrivacy Directive look set to include a requirement that cookies may only be used where users have consented to their use (*i.e.* an opt-in rather than the current opt-out requirement). It is proposed that the reference to "electronic communication networks" in Article 5(3) is removed thereby broadening its scope to cover cases where cookies are sent and received on a user's computer via external storage media.

It should also be remembered that Phorm is not the only company to supply such behavioural advertising systems to ISPs, others include NebuAd and Front Porch. The outcome of the current proceedings against the UK and the reaction of Member States generally to the Commission's call to action could shape the future of online behavioural advertising. Ultimately, OBA providers may need to cede greater control to the user in order to operate lawfully.

Cloud computing and data protection

By Hazel Grant, Partner, and Tessa Finlayson, Trainee Solicitor, Bird & Bird.

Cloud computing raises difficult data protection issues. In this article we highlight just three of these issues which are relevant for businesses looking to use cloud computing:

- Responsibility for data protection compliance;
- Data security; and
- Data location.

There will be many other commercial issues such as the risk of lock-in to the service, the service levels offered and long term viability of the service offering.

What is cloud computing and how is it regulated?

Cloud computing is a way of providing services over the Internet. Service providers make available web servers that can accept and store data from users to provide the services. Users access the services using their web browsers. Some services are free; others are provided on a pay-as-you-use or subscription basis.

The social networking site Facebook implements cloud computing. A user can log on to the Facebook site through a web browser in order to send messages, chat and share files. Microsoft Hotmail is a widely accessible email service which operates as a cloud computing facility.

Cloud computing is not just limited to consumer use, and can be attractive to SMEs or to larger organisations. The 'cloud' can be an external, public cloud such as Facebook or Hotmail, or an internal, private cloud within one organisation. So, cloud computing is rapidly growing both on an individual basis and amongst commercial entities. It offers a flexible and easily accessible alternative to conventional IT outsourcing and has the potential to offer vast cost savings in the provision of IT infrastructures.

There is currently little regulation specific to cloud computing. Data protection regulation will be relevant where the services are used to handle personal data.

The 'Open Cloud Manifesto' (available at http://www.opencloudmanifesto.org published in Spring 2009) provides high level principles that providers should adhere to. The Manifesto was created by IBM, Cisco, SAP, EMC and a number of other leading technology companies. This document is not intended to form formal guidance, but rather initiate debate on what such a guidance document should, or indeed could, contain while cloud computing and its practices are still very much in evolution. Interestingly, Microsoft, Amazon.com, Google and Salesforce.com declined to take part in the Manifesto, indicating that industry agreement may not be close.

Hazel Grant and Tessa Finlayson can be contacted at: Hazel.Grant@twobirds.com and Tessa.Finlayson@twobirds.com

Responsibility for data protection compliance

Where a business is located in the UK, it will be subject to the Data Protection Act 1998 (the Act) when handling personal data. As a result if that business decides to use cloud computing it will need to ensure that the cloud computing services comply with the Act. Most cloud computing relationships are complex and involve the transfer of data across multiple jurisdictions. As the data controller, the customer is solely responsible for compliance with the Act. This includes the obligation to ensure that the customer retains close control over its personal data, even when the data is being processed by a third party on the customer's behalf. It is likely that the cloud computing service provider will consider itself to be a data processor for the purposes of the Act. The relationship envisaged by the Act between data controller and data processor, is a simpler and cleaner one. Not the type of relationship which is likely to exist in a cloud computing service, where the customer is very unlikely to know if and when the data is moved, how it is stored, who has access and the security measures in place. It is quite possible therefore that the basic decision on who is responsible for data protection compliance will be in dispute, with customers or data protection regulators believing that service providers are at least partly responsible and acting as data controllers.

Whatever the decision on the status of the service provider, prevention is better than cure. So using services which do not suffer data losses or unauthorised disclosures will reduce the risk of individual complaint and investigation by the data protection regulators. Therefore it is essential that customers choose reputable and effective service providers who are able to offer the necessary assurances that their services will meet the requirements of the Act. Contracts for cloud computing services should address compliance with the Act (covering the obligation to process in accordance with the customer's instructions and ensure adequate technical and organisational security measures) and identify the extent to which a service provider will recover lost data or cover the cost of re-inputting data. While obtaining such assurances may increase the service costs, this will be money well spent as it will improve the security of the data and the protection available to the customer in the event of data losses or unauthorised disclosures.

  WDPR ISSN 1473-3579

Data security

When negotiating the contract for cloud computing services, customers should particularly consider the following:

- Gain as much information as possible about the likely third parties that may potentially access the data in order to ensure that they are fulfilling their obligations as data controller. The nature of cloud computing means that many third parties may access the data across a number of jurisdictions;
- Obtain warranties from the service provider as to the treatment of personal data processed within the cloud;
- Seek an independent security audit of the service provider and ensure adequate ongoing audit rights;
- Aim to set out their own security policy surrounding data and have the service provider agree to that where possible;
- Ensure that the service provider is willing and able to comply with any relevant sector-specific regulation, for example within the healthcare industry;
- Consider whether they wish their applications to be hosted on hardware that is specific to them, however this may significantly limit the financial benefits of cloud computing;
- Ensure that there is continuous physical security at the service provider's premises and that physical entry to those premises is limited to authorised personnel only;
- Ensure that they have rights to change the way their data is treated should new legislation or circumstances require it; and
- Ensure that all of the service provider's personnel with access to the data have been security vetted; and ensure that there is a sufficient and effective system of back-ups should there be a security breach.

Location of the data

Customers will need to be aware that local laws may apply to the data held on servers within the cloud. This raises, for example, concerns about access to data in the US under the Patriot Act or US litigation. However the more obvious data protection issue relates to the distributed nature of the data within the cloud computing service.

In order to benefit from optimised use of infrastructure and resources, cloud computing assumes that data will be moved geographically. Therefore it would be rare to see a contract for cloud computing where the customer is guaranteed that their data would not be transferred outside a specified country or region. (Although we may start to see cloud computing services which are restricted to a specified geographic location, see, for example, Amazon Web Service's Availability Zones).

Under the Act, transfers of personal data outside the European Economic Area (the EEA) are prohibited, unless adequate protection is shown. (The EEA includes all countries in the European Union, together with Iceland, Liechtenstein and Norway). Therefore, where a cloud computing service is provided within the EEA there will be no issue. Equally, if the service is provided within the approved jurisdictions only there will be no data protection issue (*i.e.* within Argentina, Guernsey, Isle of Man, Jersey and Switzerland together with Canada and the USA in certain circumstances). However these scenarios are unlikely. In reality, the customer will need to address a situation where the personal data may be sent to any number of servers in any number of jurisdictions worldwide.

As a data controller, the customer again has responsibility to ensure that this part of the Act is complied with and that adequate protection is given to the data which is held within the cloud computing service. Without knowing the jurisdictions where the data may be sent, it will be difficult to do this. In practice, unless the service provider will commit to using a specific geographic region, the customer will take some risk.

Customers may consider using the consent of individuals to permit the transfer outside the EEA. However, using consent is difficult. (How would it show that consent was freely given, specific and informed? What if the consent is withdrawn?)

In practice therefore customers are likely to look to a contractual situation, using the EU approved standard contractual clauses for data processors established in third countries (both the EU drafted and approved clauses (Commission Decision 2002/16/EC) and the ICC version, once the ICC version is approved by the EU). Under these clauses the data processor (the service provider) commits to comply with EU-equivalent data protection standards. In many jurisdictions (but not the UK) there are notification or registration requirements whereby the contracts once completed must be sent to the local data protection regulator. In addition, amendments to the contracts can negate the protection and therefore result in the contract not fulfilling its purpose of showing adequate protection. Therefore this solution can be restrictive and time-consuming.

Conclusion

Many business users are looking for ways to increase efficiency and reduce the costs of their operation. Cloud computing is recognised by businesses, particularly SMEs, as a cost-effective way to gain access to complex IT and communications facilities. The challenge for businesses and service providers is to ensure data protection responsibilities are not forgotten.

Information as an asset

By Andrea Simmons, Managing Director, Simmons Professional Services Ltd.

Information as an asset

In recent times, almost every vendor report, technology related (and other) industry initiative, professional ICT membership publication and relevant organisational policy statement issued, have at their heart the kernel that is 'information'. Many of these often weighty tomes articulate:

- The increasing importance of information (yet IBM research shows knowledge workers spend up to 30% of their time searching for data and are unsuccessful 30% of the time, while Gartner claim up to 25% of the data is inaccurate or missing);
- The increased time spent on statutory reporting;
- The need to share information with external parties;
- Evidence that good use of information directly correlates with better performance (and that lack of information sharing can have terrible consequences (*e.g.* High profile cases in the UK such as the Soham murders, Harold Shipman, and currently in the news, the case of the child abuse and resulting death of Baby P *etc.*);
- that investment in the information culture is already delivering value for money.

Case study

There have been three high-profile data loss incidents at Addenbrook's Hospital in recent months.

In April 2008, a female member of staff lost printed information on types of medical tests to be undertaken by 1,252 patients, along with their NHS numbers, while she was travelling on public transport.

In November 2008, Haverhill resident Nicola Marsh received letters containing medical records of two other patients from Addenbrooke's.

Early in 2009, an Addenbrooke's member of staff lost an unencrypted memory stick containing the medical details of 741 patients – it was left "in an unattended vehicle" and found by a car wash attendant.The attendant "was able to access the contents to establish ownership". The information was downloaded without the permission of Addenbrooke's and the Trust reported the loss.

The Information Commissioner's Office has ordered Addenbrooke's to sign a formal undertaking that it will process information in line with the Data Protection Act, with immediate effect.

Andrea Simmons can be contacted at: info@simmonsprofessionalservices.co.uk

http://www.cambridge-news.co.uk/cn_news_home/displayarticle.asp?id=412764

Without sending ourselves into a spiral of philosophical debate about an appropriate meaning of 'information', contextually, it is intrinsically understood as many things to many people. Information can be available, necessary, shared (exchanged), lost, accessed or destroyed. As an asset, information can be appreciated as important, vital, critical, useful – and clearly profitable. In the wrong hands, or handled carelessly, it can be also be hugely risky – just ask Bob Quick.[1] In the words of the Assistant Information Commissioner, it can be considered to be 'toxic'.[2] As with physical laws, for every action there is an equal and opposite reaction.[3]

Worse still, there is a "dark economy" exploiting our carelessness with information. For example, live 'crimeservers' (Crime as a Service) can be found on the Internet offering current black-market value prices for the most common types of stolen data, including 'dumps' – copies of the magnetic stripe information on the back of a credit card – generally obtained from a compromised retailer and used to make fake credit cards.

So if information can be seen to be conversely volatile and valuable, surely it deserves the same priority and protection as other business assets. Given the level of ongoing data breach that we have seen in the UK over the past couple of years (Table 1 refers to some of the more high profile data breaches which have occurred within government during this period), it is necessary for every organisation to get to grips with finding out:

- what information they have;
- why they have it (in the context of Data Protection, for example, this is described in terms of the Fairness Principle, the First Principle – *i.e.* what is the original purpose of the data collection and intended use);
- with whom it is shared – *i.e.* where it flows – both within and without the organisation;
- where it is stored – 'at rest' (on servers, on memory sticks, laptops *etc.*, paper documents *etc.*), 'in transit' (on the move).[4]

Information assets can be categorised as follows:

- personal data (name, address details *etc.* – often referred to as 'personally identifiable information' PII)
- financial management/data
- operational management information
- personnel management
- regulated information (health information, financial data, government classified, *etc.*)
- proprietary information/intellectual property

  WDPR ISSN 1473-3579

- trade secrets
- patents
- copyrights
- trademarks

Information asset owners

Nuggets of gold are being buried every day[5] – and users need to appreciate that they can be both *owners* as well as *custodians* of important organisational information.[6] Responsibility and accountability extends to all employees as well as the extended enterprise including consultants, contractors, sub-contractors, part-time employees, temporary employees, interns, teaming partners, and associates. However, not unsurprisingly, risk management needs to be in the mindset of every user, at some level, for a number of reasons.

Appointing Information Asset Owners has already been identified as a mandatory minimum measure required across UK central government departments.[7]

Information Asset Owner (IAO)

IAOs are senior individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good, and provide written input to the Senior Information Risk Owner (SIRO) annually on the security and use of their asset.

The very first key aspect of the role of an IAO is to "lead and foster a culture that values, protects and uses information for the public good". This has been a mandatory requirement since mid 2008, so should we really be talking about this as something new, difficult or surprising in mid 2009?

This appears to need a significant cultural shift to embed information successfully, but it also needs to be supported by an awareness, education and training programme to ensure that those who are appointed as the IAO know what their duties are and how to communicate with organisational staff.

Information Asset Registers (IARs)

Central government departments have all been tasked with producing Information Asset Registers in response to a requirement that would ultimately fulfil the needs of the EU Directive implemented in the UK under the Regulations on the Re-use of Public Sector Information (RPSI)[8] . RPSI recognised the enormous value of public sector information (PSI) and the contribution PSI could make to stimulating the development and growth of Europe's information industry, especially as part of the wider 'information protection' agenda.

However, the (*non mandatory*) requirement to produce an IAR crossed over with existing *mandatory* public sector work required to produce a Publication Scheme (by way of the Freedom of Information Act Statute) – which is equally separate from the work many public sector bodies are doing to provide A–Z directory listings of all available information through their online services.

Producing an IAR has been seen by many as part of a number of competing agendas that public sector organisations have had to juggle on any given day, budgets are always stretched when it comes to the information agenda issues – and yet the costs of mop up after breaches can be seen to have been disproportionate to the investment in preventative strategies and innovative information management programmes of activity. Carrying out a robust IAR creation *should* have included reference to a perceived value of the information assets identified. This was intended to acknowledge its onward wider sale and/or re-use so that the public sector could recoup at minimum the original creation cost plus some administrative expenses. The exercise alone would have at least started the intellectual discussion around the value of information assets. This is something that the Ordnance Survey[9] appears to have worked out well.

Significant efforts have thus been made across the public sector to identify information sources and resources, but this has not been tackled, in all cases, as part of a robust 'information governance' led programme of activity. Therefore, the available resultant benefits from the outputs have not all been fully realised.

The value of information

The idea of *information asset profiling* is to gather as much information as is necessary to support any particular organisational process and seek a better grasp of the protection requirements – it should not be seen as a cumbersome overhead.

Protecting information assets needs to consist of identifying, valuating, classifying, and labelling in an effort to guard against unauthorised access, use, disclosure, modification, destruction, or denial.[10] The relevant ISO27001 control is found in area 7 – Asset Management and existed in its predecessor, BS7799, since 1995.

ISO27001:

7.1 clearly identify all the assets, maintain an inventory, identify owners; acceptable use should be documented and implemented

7.2 classify the information "in terms of its value, legal requirements, sensitivity and criticality to the organisation" and have a documented and implemented procedure for document labelling and handling in accordance with the adopted classification scheme.

It is the purpose of Information Security to identify the threats against, the risks and the associated potential damage to, and the safeguarding of Information Assets.[11]

The meaning of Information Security is based on three fundamental tenets, represented as the 'CIA' below:

- **Confidentiality**: Protecting information from unauthorised disclosure or intelligible interception. Ensuring that information is accessible only to those **authorised to have access.**
- **Integrity:** Safeguarding the **accuracy and completeness of information** and processing methods and computer software.
- **Availability:** Ensuring that authorised users have **access to information, vital services and associated assets** when required.

Again, these are not new concepts but are represented within this context in order to ensure that they are not *lost* – they need to be seen as intrinsic elements of the one whole 'information' agenda. Once the information assets have been identified, a risk assessment is undertaken to ensure that the CIA elements are adequately addressed. Thereafter, the appropriately controlled information asset can then be adequately valued as its value can include the cost of the controls in place to protect it. Valuing assets is not new and has been around, conceptually at least, for over a decade – and yet it has still not been effectively embedded as to be recognised as appropriate for inclusion in accounting terms.

In reality, for information to be taken seriously as an *asset*, it needs to be factored into the annual accounts. But an information asset can only be put on the balance sheet if a value can be demonstrated with reasonable certainty – and this needs to involve everyone in the organisation. Changing the culture of an organisation is usually necessary for ensuring that information is valued as an asset by everyone.

Information as an asset does not diminish in value through usage, but may do so through time. Information assets all have one or more of the following characteristics:

- They are recognised to be of value to the organisation;
- They are not easily replaceable without cost, skill, time, resources or a combination;
- They form a part of the organisation's corporate identity, without which the organisation may be threatened;
- Their classification would normally be Protected, Restricted, Secret or Top Secret.

Tangentially, *data minimisation* and the management of *retention* and *replication* of data have been topics of discussion in recent times – (*e.g.* see the Database State report[12] . Remember the 'dark economy' – what's redundant data to you (and thus appears to be of no value), may in fact be of profitable value on the black market.

The Children's Database is an example of personal information being collected for the best of motives that nevertheless risked having the worst of outcomes, with front-line staff being presented with too many false positives. Government seems to undervalue the concept of data minimisation – only keeping the information needed because it has value for delivering a service. And yet these kinds of issues have already been highlighted through work done by, for example, the Audit Commission when it set out its Key Lines of Enquiry (KLOES) in 2007 in relation to Data Quality Standards.[13]

There is also the consideration of *value loss* associated with inaccurate data, data breaches and compromised databases, which raises the question of how to value the information, or collect the associated costs. *Deprival value* is a complementary approach asking what would be the cost to the organisation if it did not have certain information, and may be the key to unlocking the problem of how to value information. This latter will depend on *replacement value* (if it can in fact be replaced) and its *recoverable value*. This could include *compliance cost value* – the cost of complying with statutory regulations, post breach rectification *etc.* The *exchange value* should be covered under the RPSI, in terms of public sector information re-use. The valuation methods will differ as the context of the valuation changes.

All of these elements contribute to an area of cost that would need to be factored into the consideration of the ultimate value of an information asset – but this is not to set out a stall that makes it ultimately too difficult to do.

Financial standards need to be brought up to date in order to incorporate, and adequately address, the information needs of organisations.

Conclusion

En route to the Information Age, our journey has been from *IT Security*, where our focus has been on the data – protecting our networks at a firewall level, and then with anti virus products. Subsequently, when this failed to solve all of our security needs, we set about embracing the need for an *information security* management framework to be put in place (ultimately ISO27001).

Information Assurance was a government-led agenda intended to restore public confidence in the ability of the public sector to protect their data. So far, success has been limited, and Government is not trusted. *Information Governance*[14] is the ultimate goal which leads to the proper linkage with corporate governance and thus the full realisation of information as part of the corporate agenda and reporting structure – as can be evidenced already in the health sector where it is part of the reporting framework.

We have to get to grips with this in spite of a need for greater understanding as there remain great rewards to be gained from better, more secure and controlled, information sharing and usage across the public sector and beyond.

MPs and politicians need to *listen* to those information management, security, assurance and governance experts who have been long describing and articulating the challenge in terms of the requirement to value information assets and protect them accordingly – and move this agenda forward proactively.

  WDPR ISSN 1473-3579

Table 1: Data breaches roll call

Date	Area	Headline/Issue
February 20, 2007	Her Majesty's Government (HMG)	DWP struggles to uncover cause of public data breach Department for Work and Pensions discovered that it accidentally sent bank, national insurance and personal details to the wrong people – how did its systems and processes allow this confirmation on up to 26,000 people be compromised?
November 20, 2007 (Oct 07)	HMG	UK families put on fraud alert Government (HM Revenue and Customs) admits personal details of 25 million child benefit recipients are lost. Two computer discs holding the personal details of all families in the UK with a child under 16 have gone missing.
December 1, 2007	HMG	Fresh benefit data lapse admitted An ex-contractor at the Department for Work and Pensions had two discs with thousands of benefit claimants' details for more than a year, the DWP says. (Discs held in unencrypted form). A third party contractor error.
December 12, 2007	HMG	A deadly new data blunder "Blundering civil servants sent personal details of violent criminals about to be freed from jail to the wrong address. Documents with names, birth dates, criminal histories and addresses of more than 40 murderers, rapists and paedophiles should have gone to a police HQ….."
December 12, 2007	DVLA	Driver and Vehicle Licensing Agency data bungle No 2 Two discs with names and addresses of 7685 drivers have gone missing in the post. They were sent from the DVLA in Northern Ireland to the DVLA in Swansea – but disappeared at a Coventry depot. The discs also had car details and were not encrypted. Earlier in December the DVLA sent 100 forms with details of driving offences to the wrong addresses.
December 17, 2007	HMG	Millions of L-driver details lost Private details of 3 million learner drivers are missing, the Government admits.
December 23, 2007	NHS	Nine NHS Trusts lose patient data Thousands of patients affected as National Health Service Trusts admit losing records.
June 30, 2008	HMG	NI numbers of 140,000 on tax envelopes HM Revenue and Customs admits more than 140,000 tax forms were posted with the recipients' national insurance numbers visible on the envelope.
August 21, 2008	HMG	Home Office contractor loses memory stick containing personal details of UK criminals Home Office says a contractor lost a memory stick containing details of the UK's most prolific criminals (84,000 of them….). Again, a third party contractor error .
August 28, 2008	Police	Gangland witness files found dumped in skip Secret police documents exposing the personal details of witnesses in a £17 million drugs trial found in a recycling bin – HM Courts Services to investigate.
September 7, 2008	HMG	New lost data blunder puts thousands at risk Government admits that the lives of 5,000 staff have been put at risk in a new Government missing data scandal …. EDS…. One year since the disk was actually lost….and no-one noticed…. (Confidentiality, Availability)
October 10, 2008	MoD	Ministry of Defence computer hard drive missing This may have contained the details of up to 1.7 million potential recruits for the armed forces. The information was 'unlikely' to have been encrypted.
October 16, 2008	DVLA	You can't fine my son…these are his ashes Bungling civil servants insisted on prosecuting a dead teenager – so his mother took the boy's ashes to court to prove he was no longer alive. The DVLA wanted to put xxxx in the dock after claiming he had failed to notify them that he had sold a vehicle. But not only had he never owned the vehicle, he had been dead for nearly two years…. (Integrity). Why did this even have to go to court?
November 2, 2008	HMG (DWP)	Probe into data left in car park An inquiry has been launched after a memory stick with user names and passwords for a key government computer system was found in a pub car park. This affected the Government Gateway and the error was on the part of a third party contractor.

NOTES

[1] Inadvertent information disclosure http://www.guardian.co.uk/uk/2009/apr/09/bob-quick-terror-raids-leak

[2] Information as a 'toxic liability' – http://news.bbc.co.uk/2/hi/uk_news/7575766.stm

[3] Newton's laws of motion – http://en.wikipedia.org/wiki/Newton's_laws_of_motion

[4] Verizon Data Breach Report 2009 http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

[5] Information nuggets – http://www.bearingpoint.com/Solutions/Information+Management/Information+Asset+Management

[6] Read Information Asset Profiling, Author James F. Stevens 2005, CMU/SEI-2005-TN-021,

http://www.cert.org/archive/pdf/05tn021.pdf – for a great expose on the differences between the two (and the need for both) as well as further details regarding information asset identification.

[7] Cabinet Office Mandatory Roles – see http://www.cabinetoffice.gov.uk/media/45149/guidance_on_mandatory_roles.pdf. Also, for a more detailed expose of requirements regarding Information Asset Protection read ASIS GDL IAP 05 2007, Information Asset Protection (IAP) Guideline, Copyright © 2007 by ASIS International, ISBN 978-1-887056-70-0

[8] RPSI – http://www.opsi.gov.uk/si/si2005/20051515

[9] Ordnance Survey http://www.ordnancesurvey.co.uk/oswebsite/

[10] See Information Asset Profiling http://www.cert.org/archive/pdf/05tn021.pdf

[11] See all these resources for more information:

http://www.yourwindow.to/information-security/gl_informationasset.htm

http://www.berr.gov.uk/administration/foi/information-asset-register/page19080.html

http://www.techsoup.org/learningcenter/techplan/archives/page9763.cfm

Information as an Organizational Asset – Creating a culture that values data, By: Marc Osten and Diane Remin, December 14, 2001

InfoSecurity Professional Magazine, Issue Number 5, An (ISC)2 Digital Publication, http://www.isc2.org

[12] The Database State Report can be found here: http://www.jrrt.org.uk/uploads/database-state.pdf

[13] And yet search on the KLOE document for 'retention', 'destruction' or 'duplication' and they do not appear as data quality related concepts: http://www.audit-commission.gov.uk/reports/NATIONALREPORT.asp?CategoryID=&ProdID=F4E13DD0-2808-4f3a-98FF-358AF9010155

[14] See https://www.igt.connectingforhealth.nhs.uk/ for an explanation of the Information Governance toolkit in the NHS – which is a longstanding reporting tool, recently updated to reflect the government's Information Assurance Framework agenda. The wider public sector will need to be producing an Information Governance Statement of Compliance in order to prove that they have their information under appropriate control and security, so that they can connect to the government secure network.

News

INTERNATIONAL

Wikipedia becomes latest company to opt out of Phorm

Wikipedia becomes the latest company to request an opt-out from the scanning and profiling of its domains by Phorm's Webwise services. Wikipedia has contacted Phorm asking it not to record anything about URLs from domains controlled by Wikipedia. The company has asked that its domains are excluded arguing that third party profiling of its website users' behaviour, is an invasion of their privacy. Last month, Amazon made a similar request. (See also in this issue *EC launches infringement proceedings against UK government*, by Oliver Bray and Tom Cadwaladr.)

A copy of the email sent to Phorm is available on the Wikipedia blog: http://techblog.wikimedia.org/2009/04/wikimedia-opting-out-of-phorm/

Phorm launches site to set record straight

Phorm has launched a new website to set the record straight about its behavioural advertising services following what it describes as a smear campaign and misrepresentation of the company. The 'stopphoulplay' website aims to counter the alleged smears against the company found in the press and online blogs.

The website is available at: http://www.stopphoulplay.com/

CANADA

Privacy concerns over scans at homeless shelters

The Alberta Privacy Commissioner, Frank Work, has raised concern about the use of a handprint security system at Calgary's Drop-In Centre. The system is being tested because three members of staff were attacked. Centre officials want such a system to keep out drug dealers and gang members who in the past have simply given a false name to gain entry to the centre. The Commissioner is concerned about how the information stored on a database will be used and kept securely and whether it could be disclosed to third parties such as the police.

Although no complaints have been received to date, the system has raised privacy concerns about the growth in popularity of such biometric security systems.

If a complaint is made, the Commissioner may not have the authority to intervene as privacy legislation applies only when personal information is used for commercial purposes.

Poll reveals consumer concerns about their privacy during economic downturn

A new poll conducted by the Privacy Commissioner reveals that Canadians are worried about the effects of the economic downturn on their privacy. Concerns stem from how corporate cost-cutting may see results in less stringent measures for privacy security.

Commenting on the poll, Privacy Commissioner, Jennifer Stoddart said, "The risks to personal information may be higher than ever during an economic downturn because criminals will undoubtedly be looking for ways to exploit vulnerabilities".

The poll also revealed that people are not doing enough to protect themselves from the risk of identity theft. The Privacy Commissioner has been calling for the government to develop a comprehensive strategy for dealing with identity theft.

The poll also looked at other privacy issues including matters relating to national security, data security breaches and new technologies.

The results and the final report are available at: http://www.priv.gc.ca/information/survey/2009/ekos_2009_01_e.cfm

CZECH REPUBLIC

Czech government admits data breach involving EU leaders

The Czech government has confirmed that the personal information relating to European Union leaders was mishandled during an EU–US summit held in Prague at the beginning of April 2009.

The information was found by a Finnish national on a computer in a Czech hotel after the summit. It included passport numbers, flight details, blood groups, allergies of approximately 200 participants including prime ministers and presidents. No information about the American participants was found. The Czech government which currently holds the EU Presidency chose to play down the affair, attributing the incident to human error. The file was removed from the computer and the Czech government said that steps would be taken to prevent such an incident from happening again.

  WDPR ISSN 1473-3579

DENMARK

Facebook under scrutiny

The Danish Data Protection Authority is looking into whether Facebook meets the requirements of Danish data protection legislation. The investigation follows complaints that users of the social networking site have to relinquish many of their rights when they create a profile. The Authority has sent Facebook a list of questions it wants answered which include:

- How Facebook adheres to the requirements of Danish data protection legislation;
- Whether Facebook is registered in an EU country;
- What information Facebook shares with third parties;
- How may a dead person's profile be removed from the site once they have passed away?

GREECE

Greek DPA puts a temporary ban on Streetview

The Hellenic Data Protection Authority (HDPA) has temporarily banned Streetview from collecting images until Google provides additional privacy safeguards. The HDPA wants Google to provide information on how the images taken will be stored and processed and protected against misuse. Furthermore, it wants to know how Google plans to inform the public that its vehicles are mounted with cameras, taking photos.

In an unofficial translation of the statement, the HDPA said,

> "Simply marking the car is not considered an adequate form of notification. The authority has reserved judgment on the legality of the service pending the submission of additional information, and until that time will not allow (Google) to start gathering photographs"

For further information visit: http://www.dpa.gr

HUNGARY

Privacy concerns follow Streetview to Budapest

While the Greek Data Protection Authority has issued a temporary ban on Google capturing images for its Streetview service, the Hungarian Data Protection Commissioner, Andras Jori, has expressed concerns about Streetview's arrival in Budapest. Google cars arrived to scan the streets of Budapest at the beginning of May. Jori, who is also a member of the EU's Data Protection Working Group has said that he will monitor Streetview carefully. His concerns surround the legal basis for managing personal information processed for use as part of Streetview's images.

NEW ZEALAND

Survey shows risks to data held on PSDs

A survey of the main government departments has revealed that there are fundamental security risks to personal information held on portable storage devices (PSDs).

The findings revealed:

- 35 out of the 37 agencies which responded made PSDs available for staff use;
- nearly two-thirds of agencies allowed staff to use their own PSDs for work purposes;
- only nine agencies had mandatory encryption for PSDs;
- 62 percent of those surveyed kept a PSD register;
- only 22 percent of those surveyed would be able to track the data transferred onto PSDs;
- 75 percent had policies governing the use of PSDs but only half of these included information on how to delete content;
- 70 percent had incident reporting procedures for the loss/theft of a PSD but these did not address personal PSDs used for work.

Commenting on the survey, Privacy Commissioner, Marie Shroff voiced these concerns,

> "We are particularly [worried] about the use of personal PSDs in the workplace because it is so easy to lose one, or to accidentally disclose sensitive information by, for example, lending a USB stick to a friend. . . .If you are using your own personal PSD for work, then you are more likely to accidentally take that corporate information with you when you change jobs. Government agencies have a responsibility to try and prevent that sort of thing."

The survey is the first of its kind undertaken in New Zealand and is based on a similar survey undertaken by the Victorian Privacy Commissioner. It did not cover the private sector. The Australian Privacy Commissioner has also undertaken a similar survey on PSDs the results of which were released this month.

More information about the survey is available at: http://www.privacy.org.nz

UNITED KINGDOM

Government drops plans for communications database

The government has dropped plans to create the controversial communications database citing privacy as the reason. The database would have been used to store emails, web use and phone calls.

The proposed Communications Database was heavily criticised by privacy advocates and the Information Commissioner's Office which referred to it as a 'step too

far'. The Home Office has launched a consultation paper, 'Protection of the Public in a Changing Communications Environment' and is looking for responses to questions based on the various options outlined in the document.

Commenting on the reasons for dropping the database, Home Secretary, Jacqui Smith, wrote,

> "I know that the balance between privacy and security is a delicate one, which is why this consultation explicitly rules out the option of setting up a single store of information for use in relation to communications data."

The consultation paper is available at: http://www.homeoffice.gov.uk/documents/cons-2009-communications-data?view=Binary

Government to retain DNA despite ECHR ruling

The UK government is considering keeping DNA for up to 12 years despite a ruling last year by the European Court of Human Rights which stipulated that the "blanket and indiscriminate" retention of DNA samples was unfair and a "disproportionate interference" with the right to 'respect for private life'.

It is conducting a consultation exercise over its proposals which include:

- Automatically deleting DNA profiles of those arrested but not convicted of serious violent or sexual crimes after 12 years;
- Automatically deleting profiles of those arrested but not convicted of all other crimes after six years.

The Home Office is looking for comments on the consultation document entitled, 'Keeping the right people on the DNA Database' by August 7, 2009.

A copy of the consultation is available at: http://press.homeoffice.gov.uk/press-releases/new-proposals-for-dna-database

Accenture and Atmel gain approval for binding corporate rules

The Information Commissioner's Office has approved the transfer of personal information from the UK to outside the EEA under Binding Corporate Rules (BCR) for both Accenture and Atmel. The ICO has made it clear that both organisations have a global infrastructure which provides an adequate level of protection for such transfers of data. The ICO has been assessing the adequacy of both Accenture and Atmel's BCRs alongside its European counterparts who will issue their authorisations for transfers of data in due course.

Deputy Information Commissioner, David Smith said,

> "Accenture and Atmel should be commended for their commitment to the concept of binding corporate rules and their respect for the privacy of individuals. The ICO welcomes approaches from multinational organisations that need to share personal information within their own group but outside Europe and who want to use binding corporate rules to do that. Using binding corporate rules is a responsible approach to handling people's personal information."

Atmel Group of companies was authorised on April 22, 2009 to transfer employee personal information from the UK to outside the EEA on the basis of their BCRs. Approval to the Accenture Group of Companies was given on April 30, 2009.

For more information about binding corporate rules, visit: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_bcr_faqs_v1.1.pdf

UNITED STATES

Federal government increases DNA collection

US law enforcement agencies are expanding their portfolio of DNA samples to include DNA collected from people who have been arrested or detained but not convicted. As of May, the FBI will collect DNA samples from individuals awaiting trials and collect samples from immigrants who have been detained. 15 US states already operate such practices. The FBI database already holds 6.7 million DNA profiles. Critics of the move are voicing privacy concerns about the need to keep samples from individuals who are not convicted of a crime.

LexisNexis suffers data security breach

LexisNexis has warned 32,000 people that their personal information may have been accessed as part of a credit card fraud scheme. Databases held at LexisNexis in New York and a company called Investigative Professionals based in Santa Fe were accessed. Although the fraudsters had access to over 32,000 customer records, approximately 300 people's data was used fraudulently. The information, which included names, dates of birth and social security numbers, was used to set up fake credit cards.

UBS cites Swiss privacy laws as part of its refusal to release data to US

UBS AG has cited Swiss privacy laws as part of its refusal to hand over information about American customers to the US Internal Revenue Service when the company filed papers with a Miami federal court. This is part of an ongoing legal battle between UBS, the US Justice Department and the IRS after the IRS won a court case last year. The outcome of that case ordered UBS to hand over the names of UBS American customers who may have avoided paying income tax in the US.

UBS is arguing that forcing it to hand over client information is forcing it to violate Swiss privacy laws that prevent organisations from disclosing personal information pertaining to bank accounts to third parties. The IRS are claiming access to the information under a US–Swiss Tax Treaty. A hearing in Miami is scheduled for July.

  WDPR ISSN 1473-3579