Offshore IT Outsourcing and the 8\textsuperscript{th} Data Protection Principle – legal and regulatory requirements – with reference to Financial Services

\textit{Roger K. Baker*}

Abstract

In the global sourcing world, particularly in financial services, offshore outsourcing and associated data transfers are commonplace and increasing, searching out lower cost third countries, which may have even fewer data protections. In such an environment, the 1998 Data Protection Act’s 8\textsuperscript{th} Principle and associated 7\textsuperscript{th} Principle security provisions become critical protections for UK data subjects.

Yet the few statistics that exist indicate that unrestricted transfers appear to occur from several EEA countries. Further criticisms are that the UK 1998 Act does not fully align with the EEA Directive, the Schedule 4 exceptions are overly wide, the country assessment process can be ignored with the Information Commissioner’s ‘blessing’ and his powers and resources are limited.

Financial Services may be a contrasting exception, where the industry regulator, the FSA, ‘incidentally’ enforces many of the data protection requirements of overseas data transfers, has significant direct enforcement.

* Roger Baker BA, FBCS, ACIB, LLM (Strathclyde) is a senior consultant with ItemPlus Consulting, specialising in IT regulation in Financial Services. A former advisor to House of Commons Select Committee on Science & Technology, he is the founder of the British Computer Society’s Financial Services Specialist Group, and contributor to the Society’s publications on Offshore Outsourcing, e-Commerce, the Euro & Year 2000.
powers and a model ADR approach through the Financial Ombudsman. Although the UK banking law and regulation meets many privacy requirements, it falls short of the full data protection requirements, clearly illustrating the value that data protection legislation brings.

The alternative self regulatory approach exemplified by the US Safe Harbor illustrates the weaknesses of pure self regulation, recognized by the US financial services which are moving towards centralized data privacy supervision with the Gramm-Leach-Bliley Act, reinforcing the worldwide trend towards a more EEA-style supervised personal data protection world.

In short, seven years after the 1998 Act was passed, we are ready for an appropriate mid-course correction, with the 8th Principle (& 7th Principle) needed more than ever in the growing outsourced world.

1 Introduction - The offshore outsourcing context

The scale, extent and complexity of outsourcing have been expanding apace over the last decade. By 2003, the 100 largest outsourcing contracts were valued at between $70 million and $5 billion. The trend is set to continue with the worldwide total value for Information Technology (IT) outsourcing increasing from £100 billion in 2003 to £140 billion in 2008. These include IT operations, databases, services & infrastructure, e-business processing, call centres and related business processes – driven by financial and personal customer data (e.g. name, address, dependents, age,) and sensitive data, (e.g. health insurance data and lifestyle data relating to investment requirements.)

There are a mix of countries with which offshore outsourcing is conducted, some which meet the EEA adequacy requirements (e.g. Argentina, Canada, Guernsey), others which do not have adequate legislative frameworks (e.g. India, China). Some, like India and Australia have announced their intention to move towards the EEA Directive in order to attract data controllers, although not essential for data processors.

The largest sector in UK offshore outsourcing is IT (30% of all UK outsourcing), and Financial Services is the second largest UK sector with 12% of all UK outsourcing annually. In addition, Financial Services organisations are often truly global, with multiple administrative and IT centres spread across different continents and time zones where they have offices, subsidiary companies and third party processing arrangements, and hence

---

significant personal data flows. These factors make it an excellent focus area for assessing the effectiveness of the 8th Principle.

2 Privacy, Human Rights, Data Protection & the 8th Principle

“In the final analysis, the term ‘data protection’ is a misnomer, data protection or data privacy regimes do not seek to protect data themselves, they seek to protect the individual from unwanted or harmful uses of their personal data. As such, data privacy regimes do not seek to cut off the flow of data, merely to see they are collected and used in a responsible and accountable fashion”

2.1 Protections of Privacy under English law

Under English law, (before the Human Rights and Data Protection Acts) there was no general right to privacy. The House of Lords’ judgment in Wainwright v Home Office stated that English common law does not recognise or protect any free-standing right to privacy.

There were remedies such as action for breach of confidence or for publishing defamatory material. There were (and remain) Torts including negligence (including negligent misstatement), defamation, malicious falsehood and nuisance as well as trespass. These can and have been applied to invasions of personal privacy and associated physical, image and electronic data.

However, once the Human Rights Convention became part of English law in the Human Rights Act 1998, limiting the scope to invasions of privacy by official agencies, case law effectively extended this into the private sector.

Ironically, despite the championing of ‘privacy protection’ throughout this period, the 1998 Data Protection Act itself makes no reference to privacy nor need it (we argue), given the adequacy of the Human Rights Act, the Convention and case law. (In fact the Court of Appeal in Durant v FSA had to refer back to the European Data Protection Directive and the 1981 European Convention to reference privacy protection.)

Arguably, any third country abuse of a data subject’s privacy may be more successfully dealt with under Human Rights legislation or breach of confidence, rather than Data Protection’s 7th or 8th Principle, leaving the 1998 Act ‘out in the cold,’ not a protector of privacy whose omission from the 1998 Act may be justified in this respect.

---

7 M Douglas v Hello, N Campbell v Mirror Group Newspapers, von Hanover v Germany ECHR.
2.2 English Banking Law, Privacy and Data Protection

In English Banking law, the duty to maintain secrecy is comprehensively laid down by the Court of Appeal (L.J. Bankes) in *Tournier v National Provincial and Union Bank of England* (1924 1. K.B.461)\(^8\)

The duty is a legal one, arising out of contract, not merely a moral one. Breach of it, therefore, gives rise to a claim for nominal damages, or for substantial damages if injury has resulted from the breach. It is, however, not an absolute duty, as has been contended, but qualified, being subject to certain reasonable, if not essential, exceptions.’

This duty of secrecy starts when the banker-customer relationship is formed, normally on contract, and continues after the relationship ceases. However, details can also be divulged as part of the 4 categories of exceptions, (similar to some DPA Schedule 4 exceptions and Exemptions) and, in one case, significant personal detail disclosure was held to be justified\(^9\)

1. Where disclosure under compulsion by law, by court order etc
2. Where a duty to the public to disclose, for example where a danger to the state or public duty may supersede the duty of the agent to his principal. For example in time of war or conflict, the customer’s dealings indicated trading with the enemy. Also for the purpose of uncovering fraud
3. Where interests of the bank require disclosure, however banks will now not disclose for marketing purposes even within the same group, without customer (opt in) agreement
4. Where disclosure is made by the express or implied consent of the customer. However ‘it is difficult to argue that a customer impliedly consents to something of which he is not aware’ \(^{10}\) and hence this practice has given way under the new banking code to explicit customer consent required before disclosure.

Therefore there is a highly developed duty of confidentiality under the client contract, irrespective of location or media, (manual records, or IT data, processed in the UK or offshore) of a bank’s disclosures to third parties.

However, when we compare these ‘privacy’ or ‘confidentiality’ features to the data protection principles, we can immediately see the missing elements that Data Protection provides and its real nature and strengths, far exceeding ‘privacy protection’:

- Fair and lawful processing,
- Obtaining personal data only for specified and lawful purposes,

\(^{9}\) Sutherland v Barclays Bank Ltd 1938.
\(^{10}\) ref Note 8.
Adequate, relevant and not excessive for those purposes,

Accurate and kept up-to-date where relevant,

Only kept for as long as necessary for those purposes,

Data subject rights to prevent processing, prevent direct marketing,

Overseas transfer constraints,

A right to a description of the data held about them, its purposes and potential recipients and any automated decision-making logic,

The courts can award compensation under the act.

Hence the confidentiality/privacy protections have been extended greatly under the 1998 Data Protection Act. As data controllers therefore, English Banks acknowledge their direct responsibility for all processing including offshore processing.

Taking the general and financial services perspectives, we can confirm that Data Protection’s strengths far exceed ‘privacy protection’ - indeed a far cry from the original ‘wish to be let alone.’

3 Criticisms of data export protections
and potential proposals

The 8th Principle (& associated 7th) and the other national equivalents to the Directive Articles 25 & 26 have become the essential keystones for international protection, ‘taking data protection legislation to a new level of complexity and protection’\(^{11}\) required in the globally linked world.

The question is – how effective has this been generally and then more specifically in financial services? And what ‘mid-term course corrections’ are required?

The first European Commission report on the implementation of the Data Protection Directive\(^ {12}\) confirmed its overall internal EEA success, but focused on areas of concern, three of which appear relevant to the UK’s 1998 Act 8th Principle:

- **National differences in the implementation of the Directive** which ‘stand in the way of a simplified (harmonised) regulatory system.’

- **An ‘overly lax attitude’ to third country data export protections** in many countries, weakening the 8th Principle protections on data exports.

---


• Lack of independence, resources and powers by Information Commissioners which contribute to the above lack of export controls.

These concerns were endorsed by the European Parliament\textsuperscript{13} and solutions were integrated into the work programme\textsuperscript{14} and ongoing strategy\textsuperscript{15}. Each is analysed below in relation to the UK from publicly available information\textsuperscript{16}.

3.1 National differences in the Directive’s implementation

UK differences identified\textsuperscript{17} by the European Commissioner include the narrower definition and hence reduced scope of protected personal data where ‘identifiable information’ (as opposed to ‘identified’ information) may be excluded from personal data, and further exclusions of items after \textit{Durant v FSA} (and recently \textit{Smith v Lloyds TSB}) from the definition of a ‘relevant filing system’ where LJ Buxton stated that a manual filing system must be ‘on a par’ with a computerized system in order to be within the definition; structured or referenced by individual; a definition out-of-line with data protection in the rest of Europe.

The UK Information Commissioner subsequently confirmed\textsuperscript{18} that ‘Information that has as its focus something other than the individual will not be personal data’ and also excluded ‘any manual filing system that requires the searcher to leaf through files to see what and whether information qualifying as personal data is to be found there’ including files of personal data in chronological order. It concludes that very few manual files will be covered by the provisions of the DPA.

\textit{Smith v Lloyds TSB Bank}\textsuperscript{19} recently confirmed \textit{Durant} in that the paper archived information in this case was not biographical and the individual was not the focus of the information and did not have sufficient proximity to term this personal information. The appeal is expected to focus on the questions of ‘data’ and ‘personal data’ and whether this covers information from the past and information whether proximate or not.

\textit{Durant, Wozencroft and Relf, Smith} and the Information Commissioner’s position may be understandable responses to ‘vexatious or serial complainants’ trying to use the Act as an alternative to third party disclosure. However, such an established position makes English law out of line with


\textsuperscript{14} WP92 10650/04/EN.

\textsuperscript{15} WP98 in particular S3 – Challenges and Priorities.

\textsuperscript{16} As at April 2005.

\textsuperscript{17} EU Commission investigation into UK data protection legislation: new information 01/09/04 Bird & Bird.

\textsuperscript{18} The Durant Case & its impact on the Interpretation of the Data Protection Act 1998 4/10/04 Information Commissioner pg3.

\textsuperscript{19} The next step on from Durant: Terence William Smith v Lloyds TSB Bank 07-03-05 J Okines Bird & Bird.
the Directive and other EEA nations’ definitions and may incur infraction proceedings, especially regarding when ‘identifiable’ (as opposed to ‘identified’) information will be personal data.

Overall this could be viewed as ‘the failure of the UK government to guarantee the right of access to personal data.’ Further, being outside the definition of personal data, it is unprotected from unrestricted third country export. The EEA approach being adopted in the UK’s case is direct negotiation and potential infraction proceedings.

For sensitive data, the Directive defines some categories and permits member states to create their own conditions for processing of sensitive data – which recognises national differences in what can be processed and exported under normal or ‘sensitive data’ conditions. This was reinforced in *Lindqvist* - ‘a wide interpretation should be given to health data and this includes information covering all aspects of the physical and mental health of the data subject.’ Again for outsourcers there is no exact ‘one size fits all’ EEA-wide definition and perhaps this is not possible given cultural diversity behind definitions.

Although the 1998 Act does not contain a definition of ‘a transfer’, nor does the Directive, the Information Commissioner’s advice was that its ordinary meaning should suffice and that “placing personal data on the Internet potentially involves a transfer to any country worldwide.” With the advent of the internet, the ECJ in *Lindqvist* decided pragmatically that merely loading data onto a web server did not constitute data export (or a transfer), as substantive processing by an external party would be needed to access it – now reflected in the Information Commissioner’s advice.

Fortunately when considering the 8th Principle, all model contracts require comprehensive definition of the transfer, removing the above uncertainties in these circumstances. Binding Corporate Rule checklists also overcome this by requiring definitions of the extent of the transfers covered.

---


21 European Commission suggests UK Data Protection Act is deficient. Pinsent Masons 15/07/04 Out-Law.com

22 ref Note 20 page 85.

23 Information Commissioner letter Request for Information under FOI Act Jan.05. (Ref: JB/FOI/09/05):
- Letter from European Commission dated 7/7/04,
- Letter from the Information Commissioner to the DCA dated 7/9/04,
- Letter from the UK Government to the Commission (undated)
All were refused 8/5/05, on grounds that these “relate to potential action against the UK Government by the European Commission” and “because infraction proceedings are on going and these involve a series of negotiations between the parties …prior to any potential proceedings being commenced in the European Court of Justice.”

24 Criminal Proceedings against Lindqvist Case C-101/01, 6 November 2003, ECJ.


27 Information Commissioner SR/HC/BCR Checklist 11/2/04 pg1.
It may be extreme to assert that the UK could become a data haven as S. Chalton suggests\(^ {28}\), however these differences in personal data definitions can reduce subject access, remove the protections of fair and lawful processing from that data under the first data protection principle and the protections of data transfer to third countries under the 8\(^ {th}\) Principle and its security under the 7\(^ {th}\) Principle. It also may make English law less acceptable as a basis of standard offshore outsourcing contracts involving other EEA countries, the UK and a third country controller or data processor.

Such differences in definition are compounded for global organisations, exporting data from multiple country locations, often for different types of data, subject to different legal jurisdictions, laws and definitions of terms. Where outsourcing the location of processors may actually vary and with subcontracting, the specific physical location of processing may not be known.\(^ {29}\) Hence the importance of EEA and global moves to align data protection laws including such definitions, to simplify compliance for such organisations, currently forced to carry out painstaking country-level legal audits in each exporting country as well as the third country, to ensure compliance.

3.2 An overly lax attitude to data exports?

Lack of consistency in decision-making across Europe on international transfers and notification requirements is ‘one of the most prominent issues in the field of data protection.’\(^ {30}\) Some national authorities were criticised as overly strict, submitting all transfers to third countries to administrative authorisation even when only notification may be required. However, the major criticism (supported by an admittedly early survey – May 2001) was an overly lax attitude by some member states in contravention of the Directive’ Art 25(1) (corresponding to the 8\(^ {th}\) Principle) weakening the protections’ to a point where that nation becomes the ‘least burdensome’ point of export. It noted that those states (believed to include the UK) which allow data controllers to make the adequacy assessment – or to avoid it – have ‘very limited control of the data flows.’

This was evidenced further by the very few national enforcement actions and notifications received by the European Commission under Art 26(2) – ‘derisory compared to what might be reasonably expected.’ However, we could argue that the data controllers remain liable in such cases and data subjects can gain recompense for damage. However, avoidance of data misuse in the first place is preferable (and is the objective of the 8\(^ {th}\) Principle).

\(^{28}\) ref Note 6.
In the UK, the approach to assessing adequacy of protection under the 1998 Act Schedule 1 Part II, Provn 13 is given in the Information Commissioner’s 4-step ‘Good Practice’ Approach.

Four key features appear questionable in comparison to the above issues:

- the presumptions of adequacy
- the acceptability of the omission of the adequacy assessment
- the authorization process
- the breadth of derogations allowed

The presumptions of adequacy

Even for ‘approved’ countries, there is a presumption of adequacy, but it is still necessary for the data controller to check for each particular transfer contemplated, since adequacy findings can be qualified and additional protection measures required. Also, not all economic sectors are uniformly covered.

For third country transfers, the Information Commissioner’s Guide (pg 7) includes the ‘presetmption of adequacy in most of, but not all cases’ where a UK data controller remains subject to the 1998 Act and remains responsible for ensuring compliance to the 7th Principle Terms – a sweeping statement even when liability rests with the data controller.

A presumption of adequacy is considered reasonable by the Information Commissioner in certain specific circumstances, for example transfers within an international or multi-national company or group where an internal agreement, policy, code of practice or binding corporate rules can be effectively applied. (The UK banking code falls short as will be discussed.) Also transfers within an established consortium of independent organisations set up to process international banking or travel transactions for instance or with the added protection of adequate sectoral laws, professional codes of conduct, a requirement for a contractual relationship or effective internal codes of conduct/company policies.

However this hardly applies to ‘most if not all cases’ certainly of financial services offshore outsourcing to third countries.

Nor does it meet the Art.29 Working Party risk-based criteria for reviews of external data transfers by national information commissioners, highlighting transfers with a risk of financial loss; in which case the data controller should not be permitted to make a presumption of adequacy and disregard the adequacy test that information commissioners are advised to check.

The acceptability of the omission of the adequacy assessment

The Information Commissioner allows that many UK data controllers (particularly small companies) are likely to omit the country adequacy test as ‘inappropriate, difficult, time-consuming and/or costly for exporting controllers to carry out ......for every data transfer and third country’ and
'recognises this (omission) to be an alternative, pragmatic approach which will be widely adopted in practice.'

However, this allows data controllers to avoid the adequacy assessment process, moving directly to derogations, (e.g. standard contract terms without an adequacy test) when in reality the assessment is and should be a major essential determinant in the decision on data export to third countries; the EEA should be making the process easier for data controllers to carry out effectively rather than avoid.

In fact, not processing data in a country without adequate protections must be seen as a successful outcome of an adequacy assessment. In such a case, looking to the derogations must be seen as against the spirit of the Directive and the 1998 Act, just as skipping the assessment and moving ‘in doubt’ directly to the derogations is also inadvisable, despite the UK Information Commissioner’s wish to be helpful.

The authorisation process
The Article 29 Working Party recognized early on\(^{31}\) the difficulties a national commissioner would face in assessing the huge number of transfers and the inability of doing a risk analysis on each, even if an authority allows data transfers and then carries out \textit{ex post facto} checks afterwards. Prioritisation is essential. The Working Party set criteria based on the level of threat to privacy: including transfers of sensitive data (e.g. insurance health data) transfers with risk of financial loss (e.g. credit card payments over the internet), transfers for decision-making significantly affecting the individual (e.g. granting credit).

Several Data Protection authorities do carry out an active prior approval process over their data exports to such third countries. e.g. France, Austria. Others an \textit{ex post facto} review process.

The fact that the UK Information Commissioner has not in the past carried out prior or \textit{ex post facto} review draws one to the conclusion that there are inadequate controls on such data exports, believed to be the second issue that concerns the European Commissioner with the UK.

In stark contrast, an adequacy test has to be carried out, documented and retained for inspection by all UK Financial Services organisations for each significant data export arrangement, as mandated by the Finance Services Regulator the FSA on all significant offshore outsourcing activities. Fortunately for financial services data protection, the Financial Services Regulator (FSA) \textit{has} to review and give its \textit{prior approval} to such data exports and associated controller uses, data processing and associated security, systems and controls. In this, it effectively carries out the Information Commissioner’s responsibilities and in fact exceeds the requirements under the 1998 Act.

The breadth of derogations allowed – ‘consent’ and ‘necessity’:

A lack of uniformity in permitted exceptions under the Directive’s Art 26(1) derogations is the most significant current focus area needing tightening up as it should effectively force all Information Commissioners to act consistently on the specific terms under which a transfer can go ahead or a derogation invoked. In the UK, this will involve the 1998 Act Schedule 4 cases where the 8th Principle does not apply:

- The statutory definition of ‘consent’ in the 1998 Act Schedule 4, is not stated to be either express or explicit, nor in writing, (apart from for sensitive data). Hence implied consent in all its unacceptable forms (for example notification in a bank circular, or an empty tick box) appears to be acceptable from a strict reading of the Act, (although not from the Commissioner’s guidance); hardly ‘a tightly drawn exception to be interpreted restrictively.’ Consent itself can be ‘ephemeral’, as Carey states, because it can be withdrawn by the individual and thus does not constitute a solid foundation on which to build data processing activities. 32 However one has to conclude that although consent is not defined in the Act, it is likely to mean informed consent that is freely given and specific. 33 Yet since the data subject is not in a position to assess adequacy of a financial services organisations’s offshore outsourcing data processing arrangements, consent cannot be informed in such cases and cannot form the basis of a valid derogation.

- ‘Necessary’ is not defined under the 1998 Act and therefore takes its normal meaning – effectively where the contract could not be performed in any other way. The UK Information Commissioner’s examples of ‘necessary’ in information notes to Sched 4.2 and 4.3 for the performance of a contract, do not recognise the realities of global sourcing and the large number of purely cost-motivated offshore located processes which are therefore possibly the subject of ‘illegal’ transfers, nor are they ‘in the interest of the data subject’. However, Lord Woolf said in relation to ‘necessary’ throughout the Act that this is unlikely to be taken in the strict sense of being “absolutely essential”; it is a question of proportionality and depends on the importance of the goal sought to be achieved and the sensitivity of the data. 34

The text of the Act is out of alignment with these permitted realities.

32 Note 11, pg 88-89 relating to medical insurance and personal financial planning.
33 S Room DPFB Handbook 2004 Rowe Cohen.
3.3 Lack of independence, resources & powers of Information Commissioners

Some Data Protection Authorities lack sufficient independence, powers and resources, to accomplish their enforcement tasks especially given the growing volume of international data transfers. In the UK, review is on a resource-driven priority basis, covering the statutory assessable checking and also any high-risk transfers. However there may well be a resource issue, given the Information Commissioner’s focus on the Freedom of Information Act during 2004/2005. Any EEA-led change in strategy would require increased staffing, which appears to have started recently.

Enforcement Powers

The Art.29 Working Party defines pure enforcement as ‘an important instrument in the compliance “toolbox”’ – the undertaking of ex officio investigations or inspections with a view to checking compliance; the use of formal powers and the imposition of sanctions – ‘a necessary and often last resort, means to ensure compliance’. Enforcement discourages non-compliance and encourages those complying to continue to do so. This has been amply illustrated by the UK FSA banking regulator’s activities - demonstrably absent from the self-regulated Safe Harbor by contrast, with a corresponding lack of compliance as shown by web-based privacy surveys.

The EU Commissioner and the UK Information Commissioner (informally quoted as concurring) believe the investigative powers available under the 1998 Act and regulations require enhancing to include the power to directly award compensation and/or impose actual penalties for breaches. Individuals can take action through the courts in civil proceedings and S13 of the 1998 Act grants rights to compensation for damage and then distress. Court proceedings are unlikely to be satisfactory as the recourse for an individual data subject unless backed and managed by the Information Commissioner, for example a data subject trying to enforce a third party beneficiary arrangement relating to a third country data processor.

The financial services lesson indicates the use of ADR backed by a strong Financial Ombudsman-style commissioner service produces better results. The Art.29 Working Group rightly advocates additional ‘proactive enforcement strategies’ including EEA-wide synchronised national investigations into specific sectors in specific time periods, similar to those practiced for some time by European Financial Services regulators in assessing multinational organisations. Prior to the investigation, there

---

37 European Commissioner suggests UK Data Protection Act is deficient ref to Richard Thomas quoted in June 2003 Outlaw.com 15/07/04.
would be an awareness exercise, and following the investigation an assessment of whether and how the rules are applied; enforcement actions would follow in the member states.

3.4 UK Proposed Changes

It is likely that infraction proceedings will force changes to the 1998 Act definitions of ‘data,’ ‘personal data’, ‘choice’ and ‘necessary’ although these may be dealt with via IC information notices. There will also be a need for clarification on the 8th Principle Schedule 4 third-country transfer derogations and an upgrade in the UK Information Commissioner’s powers. These are part of an EEA-wide alignment, modest in size, reasonable and necessary seven years after the Act was passed, in particular, given the increased scale and importance of personal data exports to third countries.

A batch of other measures to assist organisations to comply would be welcomed to recognise the effort and cost otherwise involved and the current apparent disregard for the law on transfers;

- **Increased production & publication of EEA adequacy findings on a wider range of third countries** – a central EEA resource of third country adequacy assessments regularly updated, identifying areas where additional protections are required – so data controllers can rely generally on these, although still requiring to assess each specific transfer on a case by case basis. Such would also encourage third countries towards full compliance.

- **A wider choice of standard model contract clauses** – Although the new controller-controller contract is more data controller-friendly, (the original’s joint and several liability now removed as commercial organisations regarded it as ‘worrying and almost unacceptably un-commercial,’) care will be needed to ensure the success of data subject ADR mechanisms under the system of subsidiary liability and their ongoing monitoring, and not to rely solely on Information Commissioners in extremis. The 8th Principle may be at risk if controllers, hiding behind ‘due diligence’ and ‘reasonable efforts,’ force data subjects to accept ADR rather than a direct resolution by the exporter. Even in extremis, the data subject may be worse off with minimal assistance from a resource-starved Commissioner. (Banking experience of ADR however gives more cause for more optimism).

---


40 WP84 11754/03/EN Opinion 8/2003 on the draft “the alternative model contract” 17/12/03.
• And with regard to the anticipated data processor new model contract, any similar reduction in controller liability, along the above lines, may reduce the incentives to close management by the controller\(^{41}\), increasing risks to data subjects and threats to the 7th and therefore 8th Principle.

• In Financial Services offshoring, the Regulator (FSA) requires close controller management supervision of processing, ensuring good communications to and from the UK Head Office and regular security audits.\(^{42}\) To ensure this, larger financial organisations are moving to their own sites, subsidiary companies within the Corporate Group, (either a wholly owned or joint venture company) to enhance control of the data processor. The selection of a data processor follows extensive well-documented due-diligence methods and the implementation of the agreement requires the prior approval of the choice by the banking regulator, far exceeding Information Commissioner’s involvement. In data protection and banking terms, the data controller retains the liability and has to actively manage this.

• Despite disadvantages, the potential benefits of contracts – recognized as early as 1992 by the Council of Europe\(^{43}\) – has been fulfilled as later experience proved\(^{44}\) particularly where companies were ‘making broad use of these instruments in a very positive and encouraging way’ in particular using standard clauses with many parties to the contract. Carey suggests these especially suit multinational companies subject to public scrutiny and regulation, and making similar and repetitive transfers (as exemplified by UK Financial Services.)

• **Binding Corporate Rules** – offer for internal company transfers, according to the ICC\(^{45}\), compliance by a ‘proactive approach to data protection’ via the company culture rather than ‘thousands of contracts’ and registration applications and associated changes and existing ‘compliance via punitive measures.’

• However based on current experience, it is not an ‘easy option’; with EEA-admitted ‘grey areas’ – in Germany and in Holland acceptance has been ‘a lengthy process.’ It requires legal instruments to

---


\(^{42}\) Currently being exercised by concerned Banking sector controllers of Indian data processors in the light of recent security breaches, despite meeting security standards.

\(^{43}\) Council of Europe Report 2nd Nov 1992 Conclusions of 13th Conference of Data Processing Commissioners Strasbourg 1991 Mr E Harremoes Director of legal Affairs summing up.

\(^{44}\) Binding Corporate Rules WP74 in June 2003.

\(^{45}\) ICC Report 28/10/04 – Binding Corporate Rules for international transfers of personal data.
be put in place to meet company-wide adequacy-proving to the satisfaction of all affected EEA data protection authorities – a significant workload worldwide, for multinationals, to verify that:

- the corporate rules comply with content principles
- the companies in the group are bound by those rules in practice
- The companies are bound in law
- The employees are bound in law; however binding employee practices to contracts of employment with disciplinary procedures have proved difficult to enforce, given current employment protection and collective agreements.\(^46\)
- Legal redress mechanisms currently appear to require review by all data protection authorities to ensure effectiveness in protecting data subjects rights.

Particular ongoing risks to watch for will relate to:

- The effectiveness of data subject redress mechanisms internationally
- Over-arching BCR’s unreasonably replacing existing model contracts
- the extension of BCR’s outside the internal arena to external companies who become ‘associates’ or part-owned joint venture companies or broad partnerships, where model contract protections are essential and BCR’s inappropriate; ‘creeping BCR!’

However, BCRs are of great potential value to multinational companies who recognise their potential to implement a single set of internal data protection controls worldwide\(^47\). This matches their pattern of activity in standardising work processes and IT worldwide into a single simpler (lower cost) structure rather than in differing national structures.

Multinationals involved in BCR applications and the Art 29 Working Party agree that BCRs are a method of ensuring compliance within companies – and are not a ‘paper tiger.’ Properly managed and regulated, these should strengthen the effectiveness of the 8\(^{th}\) Principle.


\(^{47}\) Public Hearing on international codes of conduct for multinationals Art.29 WP 24/11/04. Also WP108 Model BCR checklist application 14/04/05.
• **enhanced data subject ADRs** – Financial Services offers an example of good practice, as exemplified in the next section.

• **easier notifications by Multinationals** – The Art.29 Working Party added recommendations⁴⁸ (now being implemented⁴⁹) for the simplification of notification requirements including ‘one-stop shopping’ notification for EEA-based multinationals – so reducing the company’s administrative burden and other Information Commissioner workloads.⁵⁰

  However, the assumption that notification raises the data controller’s awareness of data protection requirements and allows the Information Commissioners to keep abreast of the data processing situation – have been challenged. Studies particularly from Germany point to the lack of access by data subjects to the national register, entries that contain entirely standard predictable information, that are of little help to commissioners to verify processing. Hence the argument for notification as an incentive to compliance appears less than compelling.

• **The formal adoption of existing UK company data protection officers into the regulatory framework.** Under the Directive and in several EEA countries, notification is not required where a data protection official is established within the data controller organisation. According to encouraging country-wide case studies from Germany, Sweden, Holland and Luxembourg and recent French experience under the new 2004 Data Protection Act, such officers actively maintain the register details (unless prior approval is necessary) and improve compliance and enforcement effectiveness in their organisations.⁵¹

  In UK financial services, existing bank data protection officers have long been involved in ensuring data protection requirements are met, including third country personal data transfer and data processing requirements; this includes ensuring controller and data processor responsibilities under model contracts are correctly established and monitored.

---

⁴⁸ The obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union Art.29 WP Report 18th Jan 2005 WP106 10211/05/EN.

⁴⁹ Art.29 Working Party 18/01/05 WP106 10211/05/EN Section 6 ‘Simplification by means of international co-operation: first approach to a simplified system for organisations with more than one establishment in the EU.’ WP107 Co-operative procedures for opinions 14/04/05.

⁵⁰ Putting the concept into practice in the United Kingdom UK information Commissioner guidelines on Notification (JB v.1.2 22/09/03) Also WP74 section 6.

Formally adopting data protection officers into the UK regulatory framework within UK Financial Services in particular would be relatively straightforward with its existing data protection managers, although the UK data protection regulatory framework would need amendment to allow for these.

- **Modern regulatory techniques of audit, review and prompt enforcement** will require changes at the UK Information Commission – the really urgent next step, which appears to have commenced.

### 4 The 8th Principle, Banking Regulation, Supervision and Enforcement

#### 4.1 Introduction
With the growth of offshore outsourcing, from 1999 onwards, banks carried out broad strategic ‘global sourcing’ investigations into suitable processing locations for a range of standardised banking functions. Each was constrained by the need to meet the highest (EEA) data protection standards required of its constituent company nations when exporting data to the chosen outsource country. Offshore country adequacy assessments were carried out using the Good Practice Approach. Due-diligence studies were then carried out into third party processors in countries meeting adequacy assessments and contract negotiations followed incorporating standard processor contract terms (once established). Ongoing monitoring continues.

#### 4.2 The Financial Services Regulatory Environment and Data Protection
The Financial Services and Markets Act (FSMA) 2000 and its’ regulatory/ supervisory arm, the FSA, have as a major objective the maintenance of confidence in the financial markets, protection of consumers (including data protection) and public awareness. This parallels the Data Protection Directive’s objectives of promoting confidence in trade and protecting exchange of personal data.

The FSMA S5(2)(d) states ‘the general principle that consumers should take responsibility for their decisions.’ However, consumers lack knowledge and expertise to make decisions on the safety and soundness of banks, because they are at an informational disadvantage when they enter a contract and subsequently in monitoring the bank’s internal activities and performance – ‘informational asymmetry.’

---


53 ref Note 8.
‘The existence of informational asymmetry is one of the principal justifications for intervention in the marketplace’ and for its regulation.54

Hence using data subject consent as the data export derogation in Financial Services must be considered inadvisable since it is ill-informed and acknowledged as such.

Furthermore, the FSA go further than the Information Commissioner, insisting on prior authorisation of material data exports and carrying out ongoing supervision of outsourced data processor functions, including data processing Principle 7 & 8 aspects, holding the data controller bank responsible in all cases:

- Guidance on outsourcing, (in the mandatory Systems and Controls Regulatory procedures SYSC 3.2.4) relating to senior management controls over data processors55 noting that ‘A firm cannot contract out of its regulatory obligations.’ So for example, under Principle 3 (of SYSC 3) ‘a firm should take reasonable care to supervise the discharge of outsourced functions by its contractor.’ and ‘A firm should take steps to obtain sufficient information from its contractor to enable it to assess the impact of outsourcing on its systems and controls.’

- The Interim Prudential Sourcebook – IPRU (Bank)56 details the information the FSA requires to see ‘to consider the proposal and raise any concerns’ before granting approval for a material outsourcing ‘which could impact the overall risk profile and the banks internal systems and controls.’ Section 5.3 details confidentiality requirements, specifically Ss7; ‘Where the supplier operates abroad, the Data Protection Act sets out the legal requirements governing the transfer of data across borders.’

UK and overseas experience57 is that regulatory objectives in general are more likely to be met by setting and enforcing prior authorisation standards, rather than having to deal with major problems later – as exemplified by Safe Harbor.

Hence, Banking regulation demonstrably exceeds enforcement requirements by the Information Commissioner which require only notification under the 1998 Act assuming either adequacy under the Good Practice Approach or a Schedule 4 acceptable exemption, (excluding ‘assessable processing’), in contrast to the 1984 Act which did require authorisation.58

55 FSA Handbook, Senior Management Arrangements; Systems and Controls SYSC 3.2.4 Also FSA The firm – risk assessment framework para 34 Outsourcing.
Certain UK transfers could be investigated by the Information Commissioner, based on the level of threat to privacy, including transfers of sensitive data (e.g. insurance health data) transfers with risk of financial loss (e.g. credit card payments over the internet), transfers for decision-making significantly affecting the individual (e.g. granting credit). However, generally, since the Financial Services regulation exceeds the 1998 Act’s requirements a strategy of co-operation between the Commissioner and such industry regulators in enforcing the 7th & 8th Principles would reduce the Commissioner’s workload and increase effectiveness.

Similarly, ongoing FSA banking supervision is used to ensure that banks and their key personnel continue to meet minimum criteria, through regular reviews, regular reporting (including complaints monitoring), inspections and ‘Arrow’ themed visits including inspections of offshore outsource data processors. International co-operation between banking regulators via cross-border supervision is an important part of managing multinational banks with operations in countries other than the ‘home’ country; in this way third country data controllers and processors can be assessed – a lesson in inter-working and co-operation for data protection supervisors.

Such continued supervision ensures required standards are observed in these critical processes. This explicitly includes data protection and in particular the 7th principle security and organisational controls and contracts under the 8th Principle, although the focus is on the full range of oversight and controls, rather than data protection alone. Once again, banking regulation appears to enforce the Information Commissioner’s requirements.

4.3 Regulatory powers and approaches – compliance strategies
The empirical evidence on enforcement in regulation in a number of sectors including Financial Services suggests that informal measures to ensure compliance are cost-effective and cause a minimum of ill will. As Ayres and Braithwaite argue ‘adopting punishment as a first choice strategy is ‘unaffordable, unworkable and counter-productive in undermining the good will of those with a commitment to compliance.’ All know that the FSA has the ultimate ability to remove the licence of the bank concerned. Therefore the approach is to ensure compliance, not conflict.

Similarly, the Information Commissioner in its dealings with data controllers prefers to work more informally by letter soliciting views, further discussions, giving opportunities to make further representations, and obtaining written undertakings regarding remedial action. Formal enforcement measures (Part V of the 1998 Act) would only be used against the data controller as a last resort, and in the case of offshore data export (International Cooperation Order SI 2000 No.190) working with other nations

60 Responsive Regulation: Transcending the Deregulation debate Ayres & Braithwaite OUP 1992.)
authorities regarding a third country and subsequent processing, where there was adjudged to be an ‘imminent risk of grave harm for the data subjects within the meaning of Article 4.1c of the Commission Decision 497/2001/EC.’

4.4 Handling data subject complaints

Similar to the Information Commissioner, the Financial Ombudsman Service (FOS) more effectively resolves banking complaints than does individual court action with its need for knowledge of legal remedies, expertise, and high transaction costs often exceeding the benefits to the complainant; ‘if left to private law, many wrongs will go uncorrected’ unless ‘superspite’ is invoked. Use of such alternative dispute resolution (ADR) in financial services has produced far more satisfactory results than the use of the courts; banking consumers believe it is the only effective means of redress.

If banking experience is a guide, then introducing such ADR in the new model contract and BCR central data subject complaint provisions should be welcome moves, that other industry bodies and companies themselves can successfully emulate, although the FSA powers in the background effectively enforce ADR fairness.

4.5 The Banking Code – an alternative BCR ‘adequacy’ assessment?

The principal tool of banking self-regulation is the British Bankers Association personal banking code which sets out customer-facing standards of good banking practice when dealing with customers, including data protection, data subject access requirements and direct marketing protections.

The code does not exist alone; it is backed by the banking legal and regulatory framework discussed earlier. The code is cited by the ICC in its paper on BCRs suggesting it as a ‘candidate’ for a BCR arrangement, even though voluntary.

However, the code does not explicitly cover all data protection aspects required for Adequacy under the 1998 Act 8th as detailed by the Information Commissioner in particular the lack of coverage of the whole industry, not being binding on all members (although contractually on those who join it) and lack of audit/checking of compliance to the code, only being ‘taken into account’ by the FOS in disputes. As such it may not qualify directly as a code under the 8th Principle. However, taken together with the legal and regulatory framework and the historic fact that data protection managers have ensured all data protection aspects are included within underlying worldwide standard banking practices and processes, multinational UK-based

---

61 ref Note 54.

banks would be an excellent case study for development of the code world-
wide or more likely as a basis for binding corporate rules.

4.6 Lessons from Financial Services?
Since Offshore Outsourcing is a focus area for the Financial Services regu-
lator currently, banking regulation may be more rigorous and effective in
protecting the 7th & 8th Data Protection Principles than actions carried out
by the Information Commissioner. Perhaps this indicates a complementary
role for sector regulators, as well as the opportunity for regulator co-operation
and sector delegation. Certainly for financial services, the FSA complemen-
tary regulations give the resulting control a unique strength the Data
Protection Act implementation would not otherwise have.

5 Does Self Regulation work? – lessons
from the USA
Although Financial Services are excluded from Safe Harbor, it has lessons
for the voluntary approach to data protection.

5.1 Concerns vindicated
The Article 29 Working Party raised concerns over Safe Harbor from its
inception, in its working papers WP2/99 through 7/99 and despite
progress, reaffirmed these in WP32 Opinion 4/2000, which Recital 10 of the
Safe Harbor Commission Decision stated ‘have been taken into account.’
However, these resurfaced in the first progress report in 2002. The latest
Safe Harbor assessment in October 2004 by the Commission Services
relates the continued lack of compliance despite technological advances,
and ascribes this to the voluntary nature of the scheme and the lack of active
supervisory power (the FTC ability to be proactive and interventionist is
severely limited by its legal status and constrained scope for action except in extremis
and although it has received ‘thousands of complaints’ it has
issued few opinions. This resulted in some Safe Harbor companies lacking
visible privacy policies, not publicly adhering to The Principles and not
translating these appropriately into their data processing policies.

---

63 2000/520/EC: Commission Decision of 26 July 2000 on the adequacy of the safe harbor privacy prin-
ciples and related FAQs.
66 S5 of the Federal Trade Commission Act ‘unfair methods of competition in or affecting commerce
and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.’ Taking
action will be the decision of the FTC, under the False Statements Act (18 USC 1001).
67 Jan-Peter Ohrtmann Bird & Bird website Implementation of Gramm Leach Bliley: Replacing the Safe Harbor
Principle in the Financial Sector 01-10-03.
Zinser suggests\textsuperscript{68} that given the FTC’s constraints, self regulation must give way to independent verification and suspension of dataflows on request from EEA data controllers and/or data subjects. The general advice, even post introduction of Safe Harbor was to rely on the alternative approaches (i.e. adequacy assessment and then contracts\textsuperscript{69}). The consensus appears rightfully unanimous.

5.2 Financial Services move towards the EEA model?

Given the deep concerns over the lack of effectiveness of the voluntary approach and the threats posed to internet commerce in finance and medical areas in particular, the US Congress implemented a new policy via the Gramm-Leach-Bliley Act (GLB Act) to provide ‘a federal minimum standard for protection of non-public personal information collected by financial institutions.’\textsuperscript{70}

It may be highly significant to our discussion of the 8th Principle (and with our financial services focus) in that it indicates a revised stance and increased protections by the major advocate of self-regulation worldwide, the USA, albeit in a highly sensitive environment – financial services; a move towards the EEA standard, but not without shortcomings\textsuperscript{71} in the areas of definition, coverage and enforcement compared to the EEA model:

- Privacy Notices\textsuperscript{72} cover disclosure but not notification of use
- Choice is Opt-out, rather than the EEA Opt-in
- Permitted transfers to certain third parties and ‘persons holding a legal and financial interest relating to the customer’ are wider than the EEA
- Data Subject Access & Correction rights are missing
- Security requirements are likely to be capable of meeting the EEA/UK 7th Principle.\textsuperscript{73}
- There are no clauses protecting data quality, relevance, accuracy, ‘currency’ and reliability.

\textsuperscript{69} ref Note 29.
\textsuperscript{70} Internet & Online Privacy; A Legal & Business Guide, Frackman, Martin & Ray. ALM Publishing New York 2002 pg 65 onwards and 232.
\textsuperscript{72} ref Note 67.
\textsuperscript{73} 36484 Federal Register / Vol. 67, No. 100 / Thursday, May 23, 2002 / Rules and Regulations; 36484 16 CFR Part 314 Standards for Safeguarding Customer Information; Final Rule.
• Definitions (S6809) need to be examined, in particular (4) ‘personally identifiable financial information’

• Enforcement (S6805) – The GLB focus is on ensuring minimum standards, whilst State legislators are focused on greater protections, such as penalties, the private right of action and whether damages should be made available. Hence in any particular case, a UK data exporter would have to check relevant states’ laws.

• Administration & Enforcement through Eight Federal agencies has never included this level of privacy and data subject protection, which together with the FTC track record on Safe Harbor casts doubt on short term effectiveness.

Despite the inadequacies (currently being reviewed by the EEA) the legislation for the financial sector in the USA has moved towards the stricter EEA model of regulation and away from self-regulation.

5.3 US Concerns over third country personal data exports

A further recent twist has been given by the USA’s own rapid increase in offshore outsourcing and associated export of US personal data to third countries without protections. This has awakened less laissez faire instincts and raised US concerns over missing GLB Act protections in particular:

• Consumers are unable to refuse transfers to countries with little or no privacy protections.

• ‘No (federal) statute provides for a private cause of action against a service provider to protect information.’

In searching for a model, to meet these requirements, key EEA Directive components (UK Act 7th & 8th Principles) have been identified74 and are being championed.

5.4 Towards a more centralized world

Given that the majority of the USA’s major trading partners are moving towards the EEA model of centrally supervised data protection laws, including Japan, Australia and S American countries75, any US move towards the EEA standard – albeit only in finance and medical data areas – strengthens the 8th Principle’s importance and acceptance generally in


75 ref Note 70 pg 107.
this interconnected world. Uncommitted third countries will take their lead, if only to data processor standards.

6 Conclusions on the 8th Principle and offshore outsourcing

Five key conclusions arise from this study into the relevance of the 8th Principle in the global offshore outsourcing world, whether it can really work successfully and be enforced internationally and what needs to change.

1 The relevance of the 8th Principle is well established

The true objective of all data protection standards – EEA, OECD, CoE – is not ‘privacy’, but to control the obtaining, maintaining, processing, and transferring of personal data, to avoid unauthorised uses. In the global sourcing world, particularly in financial services, offshore outsourcing and associated data transfers are commonplace and increasing, searching out lower cost third countries, usually with even fewer protections. In such an environment, the 8th Principle and associated 7th Principle security provisions become critical protections.

2 UK Financial Services, in particular ‘best practice’ organisations, meet the requirements that others can flaunt

Statistics are few, but based on early surveys and on the small number of notifications from national authorities, the EEA conclusion is that unrestricted transfers appear to occur.

The adequacy assessment process is unnecessarily complex for all but the largest ‘best practice’ organisations and the Information Commissioner’s advice on avoiding assessment needs revocation; the capability to move directly to model contracts without due diligence checks is inadvisable and the Information Commissioner can only check a small number of transfers, given resources and other commitments.

UK Financial Services tend to meet best practice requirements, where the regulator fulfils the prior checking role across management, control and security areas.

3 Some re-alignment and ‘tightening up’ of the 1998 Act to the Directive is needed

The requirements for change to the 1998 Act involve alignment of basic interpretative provisions into line with the Directive (although apparently conflicting with case law), clarifying and tightening certain Schedule 4
derogations to ensure consistent protections EEA-wide – essential for internal EEA country alignment and external consistency. These will also simplify the position of multinationals intent on one-stop single contractual and BCR solutions. One notable specific is that ‘consent’ may not be informed and hence be unacceptable as a derogation, given the regulator-accepted ‘information asymmetry’ in Financial Services.

Model contracts are ‘the only show in town’ at present for offshore outsourcing however the new contract(s) potential reduction in data controller responsibilities in favour of ADR potentially reduce data subject protections and will need monitoring. The influence of the banking regulator and the surrounding infrastructure of controls, Financial Ombudsman and the banking code will help avoid this in banking, but other sectors are not similarly protected.

Binding Corporate Rules hold the promise of simplifying intra-group company transfers and could be extended to cover associate partner companies, using existing legally binding instruments.

There is also a need to empower UK company data processing officers to assist in compliance activities as in other EEA countries.

Additional enforcement powers for the Commissioner are also required to allow imposition of penalties and to directly award compensation.

4 Enhancements are needed to the surrounding regulation and enforcement mechanisms

Enhancements to support the enforcement mechanisms, are:

• Provision of more third country adequacy findings to facilitate adequacy assessments

• Support for company data protection officers from the Information Commission to ensure successful assessments and due diligence activities

• Prior approval required for a larger range of ‘at risk’ third country transfers

• One-stop shopping for multinationals, matched by increased inter-country co-operation and inter-working by national Information Commissioners

• The use of modern regulatory enforcement techniques in particular increased audit activities by the Information Commissioner.

• Increased Commissioner work with Industry Regulators

• Monitoring of company and industry ADR activities and follow-up
5 The broader picture of what needs to be done?

Whilst contracts are a convenient ‘sticking plaster’ for the legal lacunae, they should never remain a substitute for national legal provisions in third countries in the longer term. Data protection regulatory organisations and their member states (OECD, CoE, EEA and the relevant US Authorities) need to enhance their cooperation internationally at a strategic and practical level in the same way as financial services regulators. This co-operation, involving third countries should accelerate moves to spread the standards worldwide.

In short, seven years after the 1998 Act was passed, we are ready for this mid-course correction, with the 8th Principle (& 7th Principle) needed more than ever in the growing outsourced world.76

---

76 Further references include:


DPA Law - The International Regime Stuart Room University of London. 2003, at website http://www.dpalaw.info

Offshore Outsourcing: Eduardo Ustaran. e-Commerce Law & Policy July 2003 vol 5 Issue 7

Data Protection Implications of ‘Offshoring’ Charles Russell 26/10/04 at http://www.cr-law.co.uk/articles


Roles and Tasks of a Company Data Protection Official/Correspondent in Europe – European Survey/Country-by-country report. 09/03/05 Bird & Bird

Model Clauses for International Data Transfers Eduardo Ustaran Article in Volume 1, Issue 5 (April/May 2001)

Binding Corporate Rules for International data transfers, Eduardo Ustaran. World Data Protection Report. 07/03 World Data Protection Report BNA ISSN 1473-3579


Summary of the contributions received to the Article 29 Working Party consultation on Binding Corporate Rules European Commission website. October 2003

ICC report on binding corporate rules for international transfers of personal data. ICC Task Force on Privacy and Protection of Personal Data (Christopher Kumer, Chair Robert Bond, Chair, BCRs Working Group. 28/10/04

Public hearing on internal codes of conduct for multinationals. 24/11/2004 The Article 29 Working Party. Official summary of the hearing drafted by the Dutch Data Protection Authority

Transfers of Personal Data to Third Countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules... Putting the concept into practice.’ England & Wales Information Commissioner. Also Required Contents of a Submission for Approval of ‘Binding Corporate Rules’ to the Information Commissioner

Safe Harbour Decision Implementation Study by Jan Dhont, María Verónica Pérez Asinari, and Prof. Dr. Yves Poulllet(Centre de Recherche Informatique et Droit, University of Namur, Belgium) & others European Commission, 19 April 2004

EU Commission critical of US Safe Harbor programme 06-03-05 Emilia Linde Bird & Bird
Concerns over data protection Safe Harbor 01/11/2004 Out-law.com, Masons
Gramm-Leach-Bliley Act 15 USC, Subchapter I, Sec. 6801-6809 Disclosure of Nonpublic Personal Information
http://www.ftc.gov/privacy/glbact/glbubhl.htm & associated FAQs
A Comparative Analysis of Data Protection Laws in Australia and Germany
The Shape of Things to Come: Swedish Developments on the Protection of Privacy (including Lindqvist) Rebecca Wong University of Sheffield
Outsourcing in India: Data Protection help at hand Simmons & Simmons; Applicable law: India. August 2004 http://www.elexica.com
NASSCOM – Privacy & Data Protection Regulation in India
Source: http://stlc.iii.org.tw/asocio/india/india-1.htm
Associated Case Law & Commentary
– Durant v FSA Oct 2002 Edmonton County Court & Ct of Appeal Dec 2003
– P. v David Wozencroft 2002 EWHC 1724 (Fam)
– European Court of Justice first ruling on EU data protection law. Judgement of the Court on 6th November 2003 in Case C-101/01, ref. to the Court under Article 234 EC by the Göta hovrätt (Sweden) for a preliminary ruling in the criminal proceedings before that court against Bodil Lindqvist
– Opinion of Mr Advocate General Tizzano delivered on 19 September 2002. European Court reports 2003; Criminal proceedings against Bodil Lindqvist. 62001C0101
Related Articles:
Durant case: Data protection: access denied. Daniel Wise of Speechly Bircham, 19/1/05 http://www.mondaq.com
European Court of Justice’s Landmark Decision on EU Data Protection Directive Accords Broad Scope to EU Privacy
Regime Raul, McNicholas, Dwyer, Sidley & others.
Durant v FSA A Court of Appeal decision on 8 December 2003 has dramatically cut down the scope of the Data Protection Act 1998 Bird & Bird. Data protection: landmark judgment 09/1/04 (Article)
– Durant is based on faulty reasoning – a broader construction. C Pounder Masons 17/7/04
UK Financial Services Authority – other references: At http://www.fsa.gov.uk/pubs/E-Banking: Risks & Responses – Carol Sergeant Director Banks & Building Societies Financial Services Authority 29th March 2000
The FSA’s approach to the regulation of e-commerce June 2001 Discussion Paper
Safe Harbor
Art 29, Working Party – Other Reports referenced:
WP12,37,38,47,85,87,88,95,97,100, country reports WP22,24,39,40, 63, 79,82
WP 32 Article 29 Data Protection Working Party Opinion 4/2000 on the level of protection provided by the “Safe Harbor Principles” Adopted on 16th May 2000 (Also separately reviewed opinions on level of data protection in USA and ongoing discussions WP15, WP19,WP21 & WP23

ROGER K. BAKER