International In-house Counsel Journal
Vol. 4, No. 13, Autumn 2010, 1

The Legal Implications of Data Governance in the Financial Services Sector in the UK

JULIE VARCOE-COCKS
Senior In-house Lawyer, UK

A. INTRODUCTION

Data governance has become one of the issues of key interest for those who work in the financial services industry in the United Kingdom (UK). Data protection laws have been around for a long time, yet in recent times there have been indications that regulatory authorities still do not consider financial services providers to have paid adequate attention to this aspect of their businesses. While each of the regulators have issued separate warnings, the principles underlying their concerns remain essentially the same.

Recent fines have been imposed by the Financial Services Authority (FSA) have again highlighted the importance for financial services organisations getting the issue of data governance and security right.. In August 2010, the UK branch of Zurich Insurance Plc was fined £2,275,000 by the FSA for failing to have adequate systems and controls in place to prevent the loss of customers' confidential information.

Adding to this has been the Information Commissioner Office's (ICO) new powers to impose monetary penalty for serious breaches of the *Data Protection Act 1998* (DPA). Since April 2010, the ICO has had the power to impose penalties of up to £500, 000 where the breach is serious and of a kind likely to cause substantial damage or distress, being deliberate or reckless. While the amount of monetary penalty imposed is likely to be determined by the nature and effect of contravention, this too should serve to focus the financial services industry's attention on the disciplines around the control, use and management of personal data.

The financial services industry is not being singled out in this increasing focus on privacy protection and data management. It sits in a wider context.

B. RECENT INCREASED FOCUS ON DATA PROTECTION LAWS AND ENFORCEMENT

Recently, the enforcement of data protection laws has posed major compliance challenges for industry. For example, a Milan court convicted three Google Inc executives earlier in 2010 for violating the privacy of an Italian boy with autism by letting a video of the boy being bullied to be posted on the site in 2006. In a letter addressed to Google, Yahoo and Microsoft on 26 May 2010, the European Union (EU) independent group of privacy regulators Article 29 Working Party (WP29) showed concerns related to data protection issues and urged the companies to improve online privacy. The group sent a copy of the letter to the United States (US) Federal Trade Commission and asked the US body to verify the behaviour of the three companies in terms of the *Federal Trade Commission Act* which prohibits unfair or deceptive acts of practices in the marketplace.

Legislators are also focusing on data breach the E-Privacy Directive (*2002/58/EC*) that was agreed in December 2009 and must be implemented in all EU member states before June, 2011. These amendments will introduce for the first time an EU security breach

notification law although for now it will only apply to breaches in the communications sector.

Increased ICO enforcement powers

The ICO from April 2010, also has substantially enhanced powers of enforcement and to impose monetary penalties. The IC has argued for a number of years that its powers and resources were inadequate and that a stronger approach was required to enable him to take effective action and so prevent unacceptable information handling. Significant losses of personal data in 2007 saw existing powers deemed inadequate. There were public calls for a criminal offence, but the preferred option was a new power to impose a monetary penalty with civil sanction. The new power inserted into section 55 of DPA by section 144 of the *Criminal Justice and Immigration Act 2008* (CJIA) came in force on 6 April 2010. This sanction is seen as a deterrent to data controllers who may otherwise ignore their responsibilities under the DPA, encourage data controllers to approach the ICO and promote compliance and improve public confidence.

The main feature of the changes is that the ICO may serve a monetary penalty notice on a data controller requiring the payment of a monetary penalty which must not exceed £500,000. This generally applies to all data controllers in the private, public and voluntary sectors.

Before the ICO may impose a monetary penalty, it has to be satisfied under section 55A, DPA that firstly, there has been a serious contravention of data protection principles by the data controller and, secondly, the contravention was of a kind likely to cause substantial damage or substantial distress. Further, either the contravention was deliberate or, the data controller knew or ought to have known that there was a risk that the contravention would occur, and that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but failed to take reasonable steps to prevent the contravention. Generally, this is seen to apply to serious contraventions of data protection principles and there may be wide variations depending on the circumstances of each case.

The IC has issued statutory guidance[1] on how he will use his new power to fine and has set out a number of factors which he is likely to take into account in setting the amount of the penalty, including the number of individuals actually or potentially affected; the nature of the personal information involved and whether the data controller took account of guidance or codes of practice published by the IC. Other behavioural issues will be taken into account including, for example, the robustness of the data controller's compliance regime, what steps were taken to avoid contravention and the attitude of the data controller once it became aware of the contravention. This is a new territory for the ICO and further guidance will be produced based on actual precedents.

The IC has also said that he will take into account the size and resources (both financial and otherwise) of the data controller so as not to impose undue financial hardship on an otherwise responsible controller.

Currently, most of the enforcement activity carried out by the ICO is directed at data security and, given some of the high-profile cases in this area; it may well be where we see the first fines. In May, 2010, the ICO reminded firms of their obligations to protect personal data after it logged its 1,000th breach of the DPA. The greatest losses were

[1] A copy of the guidance may be obtained at the ICO website at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_guidance_monetary_penalties.pdf

caused by stolen or lost hardware (305), 254 breaches were the result of erroneous disclosure, while 233 cases were the result of lost or stolen data.[2]

The IC has also been consulting on another new power to assess how data controllers process personal data. Currently, the IC may audit only with the consent of the data controller, but under this new power he will be able to carry out so-called "compulsory audits". This power is currently only to apply to public bodies and the IC has said he will use the power primarily where a risk has been identified and the data controller is refusing to engage voluntarily with the regulator. How often, and in what circumstances, the IC will rely on these increased powers remains to be seen.

Recent FSA enforcement activity

The FSA has been warning firms about the issues arising from the security of customers' personal data due to growing evidence of firms with inadequate data security systems and controls.

Fines levied by the FSA for data security failings over the past 4 years are summarised in table 1 below.

It shows the main breaches are due to the financial services organisation failing to take reasonable care to ensure it had effective systems and controls to manage the risks relating to the security of customer data and its outsourcing arrangements. This is mainly a breach of Principle of Business 3 (management and control) and the FSA's System and Controls rules.

Table 1 - FSA enforcements over the past 4 years for data security breaches[3]

Date	Company	Amount of fine	Reason for fine	Breaches
March 2006	Capita Financial Administrators Limited	£300,000	Failures in its anti-fraud systems and controls where customer details were changed, transactions processed without customer authorization and fraudulent payment requests were made.	FSA Principle 2 and Principle 3 of the FSA's Principles for Businesses and breaches of Senior Management Arrangements, Systems and Controls SYSC 3.2.6R
February 2007	Nationwide Building Society	£980,000	For information security lapses where a laptop, containing customer data that could have been used to commit financial crime, was stolen from the home of an employee. It took three weeks following the theft for the firm to investigate.	FSA Principle 3 states that a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.
May 2007	BNP Paribas Private Bank SA London Branch	£300,000	Weaknesses in the firm's systems enabled a senior employee to carry out 13 fraudulent transactions on customers' accounts, with a net loss to the firm of around £1.4 million.	FSA Principle 3 states that a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.
December 2007	CGNU Life Assurance Limited and other companies in the group	£1.26 million	Weaknesses in the firms' systems allowed fraudsters to use publicly available information to impersonate customers and obtain sensitive customer details from their call centres. The fraudsters then used the information to request the surrender of 74 customers' policies worth around £3.3 million.	FSA Principle 3 states that a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems
June 2008	Merchant Securities Group Limited	£77,000	Inadequate data security controls and not protecting customers effectively from the risk of identity fraud.	FSA Principle 3 states that a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems

[2] A detailed breakdown of the figures may be found at http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/breach_notification_spreadsheet_may2010.pdf

[3] Source: FSA website a www.fsa,gov.uk

July 2009	HSBC group (3 2firms)	£3 million	Fined for failing to have adequate systems and controls in place to protect their customers' confidential data from being lost or stolen. Staff were not given sufficient training on how to identify and manage risks like identity theft.	FSA Principle 3 states that a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.
August 2010	Zurich Insurance Plc (Zurich UK)	£2.75 million	Failed to oversee the outsourcing arrangement effectively and did not have full control over the data being processed by Zurich SA. Zurich UK was oblivious to the data loss incident until a year later. Zurich also failed to ensure that it had adequate systems to prevent the lost data from being used for financial crime.	Breaches of Principle 3, SYSC 3.1.1R and SYSC 3.2.6R in relation to systems and controls

The way forward from here…

The message from the regulators is clear. Ignore data governance at your peril. Data is a key currency for organisations: it is as important now as capital and labour. Good data governance (as a component of good corporate governance) provides the framework for maximising the value of personal information, while minimising the risks associated with handling personal information.

Data protection risks are not the risks traditionally considered by senior managers**,** nor are they widely understood. There may be a lack of knowledge about what constitutes personal information with a low priority for addressing this uncertainty as well as the regulatory requirements. Privacy risks may be assumed to relate only to financial data security and its functions, rather than looking holistically at the question of personal information as it applies to identity.

With the proliferation of social networking sites and online access to personal and financial data, protection of personal information needs to consider a whole range of elements. These include personal appearance, personal identifiers such as name, address, email and other contact points, collection, use, access and storage of information including financial data and patterns of personal use and behaviour.

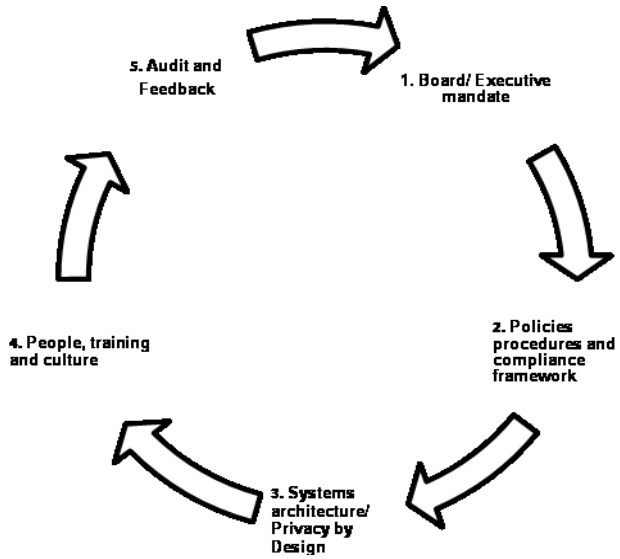
The response from financial services organisations needs to be a more strategic approach to data protection. A firm's investment in the privacy dividend makes good business sense that should earn the trust of individuals and their loyalty. A business with a sound data protection strategy is more likely to have effective, well run information systems and processes, which strengthens it operationally and improves resilience. Such an organisation is also likely to be more confident that it complies with the law and operates with lower levels of risk thereby increasing reliance and returns.

Once implemented, the business must continue to monitor ways of improving its systems and processes in relation to privacy performance and ensure these are updated to respond to changes in the business environment. Good data management and its ongoing protection may then be used by savvy organisations as a selling point to its customers.

C. WHAT DOES A DATA GOVERNANCE STRATEGY CONTRIBUTE?

Once identified what data an organisation needs to protect, an effective data governance strategy then requires a synergy between the 5 key elements illustrated in Diagram 1 below.

Diagram 1 – 5 elements of an effective data governance strategy



At its simplest, an effective data governance strategy combines corporate culture, policies and processes to make compliance with regulatory laws and good practices part of doing business.

An effective data governance strategy needs to include policies and processes to:

- improve the ability to deliver data to the business;
- provide controls for organisational processes at all levels;
- inform decision making;
- harness the necessary resources available within an organisation to make compliance part of doing business;
- detail the overall management of the availability, usability, integrity, and security of the data employed by the organisation;
- avoid assumptions and problems being addressed elsewhere;
- ensure data protection issues are considered from perspective of all stakeholders, especially customers;
- monitor and reports on whether data privacy measures are effective and how they can be improved to avoid future breaches; and
- encourage privacy threats and risks to be identified and addressed.

How these elements are addressed through the 5 key elements are examined in more detail below.

1. Board/ Executive mandate

Board level engagement requires an attitude and approach set by the Board that is woven into the culture of the organisation and then monitored by the Board at appropriate intervals. The Board needs to ensure measures are put in place that are procedural and systemic backed by sufficient funding for the initial implementation and thereafter, thereby making it part of the core business. This requires a strategic approach to ensure

that data protection risks are actively identified and mitigated and good personal information management is embedded across business as part of its culture.

Executive management should also be engaged to understand their privacy duties and the need to communicate the privacy dividend. The culture of the organisation must foster and promote a simple, shared language for discussing privacy concepts. This may be created by the popular mandate for Privacy by Design demonstrating business benefits, costs and risks of failing to comply with privacy requirements.

2. Proper policies, procedures and compliance framework

Senior managers should understand the opportunities to improve existing corporate data privacy and security practices. This often means taking a more strategic role in championing organisational wide data governance, verifying that policies are continually and effectively enforced and an adherence with relevant legal, contractual and regulatory requirements.

A good data policy will have specific business cases for all categorisations of corporate data access and usage. Such cases will help formulate a unified and well-defined collection of standards that support regular monitoring and auditing. [4]The policy should comprise of many functional components and address the following:

- ***Access control***: Controls should be put in place so only those who need or are required have access to the data.
- ***Risk assessment:*** The business value of all personal information must be benchmarked, along with existing risks to this information.
- ***Monitoring:*** All activity on company networks and systems must be monitored, logged and audited for unusual patterns.
- ***Accountability***: Sufficient logs of all network activity must be kept by monitoring processes so that both processes and individuals may be accountable for their actions.
- ***Incident and exception handling:*** A chain of command must be put in place for tracking, reporting and responding to security breaches/violations, equipment loss and occurrences of non-compliance with data governance precepts.
- ***Customer transparency:*** Customers must be aware of how their data is being protected or exposed to tracking technologies such as cookies or Web beacons.
- ***Education***: All users of enterprise data must be educated with respect to good data security practices. Especially important is a full understanding of company internet usage policies.
- ***Dispensation***: Occasionally there will be a business requirement for the use of non-supported firm hardware devices. Such an exception means that the advantages of such use must be greater than the risks of usage.
- ***Data profiling***: It is often prudent to assign various classifications (such as public, confidential or highly confidential) to various strategic sets and collections of data.

[4] 'Corporate Governance and Data Security and Privacy', Information Management Magazine, December 2006, Author: William Laurent

- ***Mobile and remote computing controls***: Activity conducted on corporate mobile devices must be tightly controlled. Such devices must also be physically secured at all times, especially when off company premises. Careful attention should be paid to firm-approved authentication mechanisms such as token cards or smart cards. If any mobile or remote communications device that contains (or has access to) firm information resources is lost, stolen or suspected to have been tampered with, management must be informed immediately.
- ***Architectural best practices***: All entry points to company networks should be secured by up-to-date access control gateways with multiple and layered security control points. Intrusion detection systems (IDS) will eliminate single points of (protective) failure, making security breaches less probable.
- ***Consistency of coverage:*** Appropriate quality and security controls must be consistently implemented on all business processes and data distributed outside company boundaries.

3. Systems architecture / Privacy by Design

'Privacy by Design' principles involves a systematic evaluation of the impact of a new technology or new data processing activity on an individual's privacy during the design stage of the technology, so that privacy is embedded into the new technology from the outset.

The concept is not new: it was first proposed by the Ontario Commissioner, Ann Cavoukian in the 1990s, and since been promoted elsewhere, including by the ICO in 2008. Dr. Cavoukian advocates[5] that Privacy by Design's objectives may be accomplished through adoption of seven foundational principles. The foundational principles are linked to the essential elements of accountability, therefore good governance:

The ICO commissioned some research to help articulate the business case for investing in proactive privacy protection and for organisations to understand the business rationale for, and benefits to be gained from, building in better privacy protection. A key barrier was the absence of a soundly argued business case for investing in privacy friendly systems and business processes.

The Privacy by Design report[6] was launched on 26 November 2008. The report highlighted the lack of management engagement on the issue. It showed that organisations did not put an appropriate value on personal information. Nor did they adequately identify the potential cost of having poor privacy and data protection safeguards in place.

The aim of the ICO's Privacy by Design programme is to encourage organisations to ensure they develop information systems that hold personal information, which identify and address privacy concerns. The report examines the barriers to widespread uptake of privacy-enhancing technologies (PETs) and the means of designing privacy protection into plans and projects. It also looks at some of the solutions available and recommends what organisations may do to improve the level of protection. This includes ensuring that managers understand their privacy duties and communicate their privacy policies across the organisation. Establishing more rigorous compliance and enforcement mechanism

[5] Information & Privacy Commissioner of Ontario, Canada, Toronto, ON, Canada website for Privacy and Design see http://www.privacybydesign.ca.

[6] .(see http://www.ico.gov.uk/upload/documents/pdb_report_html/html/1-foreword.html)

requires the widespread use of privacy impact assessments throughout a system's lifecycle, developing practical privacy standards and promoting technologies which enhance privacy protection.

The ICO has also published an implementation plan which sets out the steps the ICO will take in support of the Privacy by Design programme.[7]

The European Data Protection Supervisor ('EDPS') in March, 2010 also published an 'Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy.'[8] It provides a very practical perspective for additional ways of ensuring better privacy and data protection.

The Opinion highlighted that technology is developing so quickly where technology companies and consumers simply do not evaluate the impact of new technologies on privacy. Organisations have therefore been slow to embrace Privacy by Design and the related concept of Privacy Impact Assessments. Still, the benefits of designing privacy into technology from the outset, and the risks of failing to do so, have not been clearly or widely explained to organisations. Accordingly, Privacy by Design should be mandatory in the data protection legislative framework in a technologically neutral way. Compelling Privacy by Design implementation on data controllers, information and communication technologies designers and manufacturers would offer more legitimacy to enforcement authorities to require its effective application in practice.

4. People, Training and Culture

Employees of an organisation must understand how to put data policies, obligations and corporate values into effect. Employees need to consider privacy principles prior to design and during implementation to minimise business investment, reputation and compliance risks.

Staff need to understand why privacy is relevant to their work and what they need to do in practice to comply with the firm's policies and procedures. Regular checks should be carried out to ensure that staff actually understands their firm's data policies.

Senior management also need to recognise that staff may pose a threat to data security, particularly staff who may have access to significant volumes of customers' personal data, such as call centre staff. The vetting, recruitment and staff management process should give the organisation comfort that their staff are not susceptible to stealing customer data or committing fraud. Enhanced vetting procedures when recruiting for posts with access to large volumes of customer data may be needed e.g. by carrying out criminal record checks.

The staff vetting process should be repeated regularly to identify changes in circumstances that may make a member of staff more susceptible to getting involved in financial crime, such as suffering from financial difficulties.

5. Internal audit and compliance monitoring

Internal audit and compliance monitoring provides organisational benefits of a qualitative assurance to verify that the data protection system works and is effective. It also provides

[7] (see http://www.ico.gov.uk/upload/documents/pdb_report_html/pbd_ico_implementation_plan.pdf)

[8] (see http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf

a measurement of compliance and identifies risks which may be mitigated. Overall, the audit should increase awareness of data protection amongst staff and be a catalyst for change.

A firm's objective should be to transform data governance from yearly audits to real-time change driven processes that will enable it to assess and manage risks in parallel across all business segments and ensure compliance with the regulatory laws.

The internal audit and compliance monitoring in relation to data is variable. Audit and compliance staff need to have the necessary understanding and expertise on data areas. The data reviews must cover all relevant areas of the firm, including information technology, security, human resources, governance and third party suppliers.

Compliance monitoring of data should be risk-based. The risk-based approach should be looking at:

- complaint history;
- self-reported breaches;
- any undertakings / enforcement action;
- media reports / internet sources;
- privacy impact statements on internal controls;
- document review of policies, processes and procedures,
- governance structure / roles; and
- any staff guidance or training material provided.

These are then evaluated to determine compliance with the DPA, their completeness, usability and whether they are up-to-date.

Meetings should also be arranged with staff to discuss governance, business procedures, staff awareness and security. Physical evidence should be gathered and a review undertaken of any relevant forms, computer and manual personal data records, control records and storage and transportation.

Once the investigation is completed, the audit report should be formulated outlining the audit opinion and findings. This report usually includes identified areas of good practice and those areas in need of improvement. The audit findings should also raise issues, suggest recommendations, contain risk assessments and data controller comments, which may be acted upon by the business. A follow up visit will usually be undertaken to update the report and provide a revised audit opinion.

External assistance should be obtained, if required, but over-reliance on external consultants must be avoided who adopt a "one size fits all" approach.

D. THE LEGAL REQUIREMENTS FOR MANAGING PERSONAL INFORMATION

In the UK, at a minimum the DPA requires that anyone who processes personal information must comply with eight principles, which make sure that personal information is:

1. fairly and lawfully processed;
2. processed for limited purposes;
3. adequate, relevant and not excessive;

4. accurate and up to date;
5. not kept for longer than is necessary;
6. processed in line with your rights;
7. secure; and
8. not transferred to other countries outside the European Economic Area without adequate protection.

The ICO has outlined key guidance for various business activities and functions to comply with the DPA, other regulatory requirements and best practices which may be found on its website. It is beyond this paper to examine the specific ICO guidance, but the ICO guidance and any updates should be regularly reviewed to ensure they are incorporated in the organisation's data protection policies and procedures as a matter of course.

For the financial services industry, the FSA also has statutory requirements which should be embedded in the company's policies and procedures. Firms have been encouraged to take a risk based approach which is also managed within their risk strategy as required by the FSA.

FSA data protection requirements for financial services organisations

The FSA's key concern in data protection compliance is that firms with weak systems and controls, in particular for data security, where the risk the loss and theft of their customers' personal data, may then be used to commit fraud and other financial crime. The FSA considers that firms with weak data security systems and controls pose a risk to some its statutory objectives under the *Financial Services and Markets Act 2000* (FSMA).

The FSA's key requirements relating to data protection are found in the FSA's Principles for Businesses (PRIN) and in the Senior Management Arrangements, Systems and Controls sourcebook (SYSC). Failure to comply with these requirements may result in a firm facing FSA enforcement action, as well as other reputational, commercial, legal and regulatory consequences.

The key principles for businesses that are relevant to data security are:

- ***Principle 2*** - requires firms to conduct their business with due skill, care and diligence.
- ***Principle 3*** - requires firms to take reasonable care to organise and control their affairs responsibly and effectively, with adequate risk management systems.
- ***Principle 6*** - requires firms to treat their customers fairly (known as "TCF").

The rules in SYSC set out further high level requirements in relation to the systems and controls firms must have in place to mitigate the risk of financial crime. The senior management of a business is ultimately responsible for making an assessment of the financial crime risks associated with their customer data. They need to ensure that the business has appropriate systems and controls in place to mitigate the risks identified. These systems and controls must be comprehensive and proportionate to the nature, scale and complexity of the business activities. Businesses need to carry out regular assessments of the risks, and the adequacy of the systems and controls, to ensure continued compliance with the FSA's requirements.

The FSA published a fact sheet in April 2008[9] for small organisations to make it easier for their senior management to understand their data security responsibilities. The fact sheet highlights that for good governance, it is good practice for senior management to assess data security risks and put in place appropriate policies, procedures and controls to reduce these.

These principles are not confined just to smaller businesses and are equally relevant for large organisations. To highlight the similarities in approach between the ICO and the FSA, the elements of an effective compliance framework in section C2 above have been included in brackets after each of the elements from the fact sheet.

Some of the key points highlighted in the FSA Fact Sheet include the following:-

- Data security should be considered as a specific risk and responsibility assigned to a specific person. (*Accountability*)
- Data security should involve key staff from across the business (such as those with responsibility for human resources, security and countering financial crime) in their data security work. (*Accountability, Systems Controls, Monitoring, Architectural Best Practice*)
- Firms should make an assessment of the risks to their customer data. (*Risk Assessment*)
- It is good practice to have written data security policies and procedures, which are proportionate, accurate and relevant to the day-to day business. (*Education, Consistency of Coverage*)
- Having simple lists of 'do's and don'ts' in place of procedures may be an effective approach which makes the importance of data security easy for staff to understand. (*Access Control*)
- Firms should encourage an open and honest culture which allows staff to report data security concerns (*Monitoring, Incident and Exception Handling*)
- Staff should understand why data security is important and know what to do to keep customer data safe. (*Data Profiling*)
- External assistance should be considered or liaison with peers about data security risks and implementing good internal controls.

Where businesses have outsourced functions, they should take reasonable care to supervise the outsourced functions carried out by their contractors. This may be done by way of service agreements that set out responsibilities for maintaining information security and a related right of audit for checking compliance.

E. HOW DOES AN ORGANISATION ASSESS ITS CURRENT LEVEL OF COMPLIANCE AND KNOWLEDGE?

An initial high level checklist to check the organisation's current level of compliance and knowledge should cover the following considerations:

- The importance of personal information to the firm?
- Is there senior executive awareness and support?
- Has it assessed its privacy risks?
- Does it have a plan for managing these risks?

[9] See http://www.fsa.gov.uk/smallfirms/resources/factsheets/pdfs/data_security.pdf

- Do staff understand their roles and responsibilities in managing these risks?
- Does it have the right skills and technical capabilities?
- Is data protection management adequately embedded across the firm?

F. IMPLEMENTING A DATA GOVERNANCE FRAMEWORK

In summary, the following elements are needed for a successful data governance framework and assist in meeting a financial services organisation's legal obligations.

1. **Board/ Executive engagement** - the data governance strategy should be developed and endorsed at Board level and become an integral part of the culture of the organisation. Executive management should ensure availability, usability, integrity, and security of the data employed in the organisation. The culture of the organisation must create and promote a simple, shared language for discussing privacy concepts.
2. **Data protection policy** - should be developed that specifies which senior executive is responsible for the policy and those executives accountable for various portions or aspects of the data, including its accuracy, accessibility, consistency, completeness and updating. A set of standards and procedures must be outlined that defines how the data is to be used by authorised personnel. The policy objective should be to transform data governance to real-time change-driven processes that will enable it to assess and manage risks in parallel across all business segments and ensure compliance with the regulatory laws.
3. **Privacy by Design** - a sound data governance program should be established a defined set of procedures and a plan to execute those procedures. Processes must be defined concerning how the data is to be stored, archived, backed up, and protected from mishaps, theft, or attack. This will include looking at the systems architecture. Privacy by Design advocates a systematic evaluation of the impact of a new technology or new data processing activity on an individual's privacy during the design stage of the technology, so that privacy is embedded into the new technology from the outset. This may be through use of a central privacy office / area that via the company policy will review and approve all new or revised products/ projects/ programs for the business to ensure compliance with data protection policy. Where there is identified non-compliance with the data protection policy, laws or best practices or unacceptable risks, these will be highlighted for further remedial action to be taken until the design is acceptable. The financial services organisation must take reasonable care to ensure it has effective systems and controls to manage the risks relating to the security of customer data and its outsourcing arrangements. This also includes documenting all outsourcing arrangements so they may be properly reviewed and monitored.
4. **Staff training and culture** - staff training should be conducted outlining the firm's data policies and procedures. Data training should focus on legal and regulatory data requirements e.g. the risk of financial crime and how the firm's procedures may reduce this risk. This should include simple and effective methods of raising staff awareness, such as group discussions and poster campaigns. The FSA has highlighted[10] that for financial organisations the implementation of data security procedures requires staff awareness of data security risks.
5. **Audit and compliance monitoring** - key set of controls and audit procedures must be put into place that ensures ongoing compliance with ICO, FSA and any other best practices. This will involve reviewing both internal and external outsourcing arrangements for the business where recommendations are made to improve compliance and minimise risks.

The above practices should be reviewed on a regular basis to ensure that the data governance framework and strategic plan, privacy policy, processes and procedures are updated in response to any new or revised changes in any business, regulatory, industry or other relevant environment.

Failure by a financial services organisation to comply with these requirements may result in a firm facing the ICO or even worse, FSA enforcement action as well as other reputational, commercial, legal and regulatory consequences.

[10] See http://www.fsa.gov.uk/smallfirms/resources/factsheets/pdfs/data_security.pdf

G. CONCLUSION

Each organisation needs to judge the weight and value of personal information in its own business context. One size will not fit all, but will be a combination of different components looking at its own value and benefit. Protecting personal information must not be left to chance; the privacy protections have to be expressly built in. There are business benefits to be gained from investing in privacy protection and tools to build the business case where the privacy dividend benefits all.

However, the business reality is for an organisation to succeed and survive; a financial services organisation must manage its risks and deliver value to all its stakeholders. Personal information is a key business asset that may fuel economic growth. The ability to process personal information strategically and efficiently is often the secret to success. Data information is the new currency for organisations where data governance provides the framework for maximising the value of this information, while minimising the risks associated with handling it.

In summary, adopting a pro-active data governance strategy allows the implementation organisational, procedural and technical measures for overcoming legal barriers and making the privacy dividend part of the business success.

Julie Varcoe-Cocks is a senior in-house lawyer with over 15 years in the corporate environment including the financial services, automotive, telecommunications and publishing industries. She has a broad range of legal and commercial experience working on compliance, strategic and commercial matters and has worked as a lawyer in private practice and in-house, holding various legal roles in Australia and in the UK.