

---

**NOTE ON SECURITY BREACHES INVOLVING PERSONAL DATA**

---



**KEMP LITTLE LLP**

**NOTE ON SECURITY BREACHES INVOLVING PERSONAL DATA**

**TABLE OF CONTENTS**

<b>A. INTRODUCTION.....</b>	<b>3</b>
<b>B. THE LEGISLATIVE CONTEXT .....</b>	<b>4</b>
1. EC Data Protection Directive .....	4
2. The Data Protection Act 1998.....	5
3. Relevant Definitions.....	5
4. Compliance with the Seventh Principle .....	5
<b>C. PREVENTING A PERSONAL DATA SECURITY BREACH .....</b>	<b>6</b>
1. Appropriate Measures.....	6
2. Appropriate Technical Measures – Standards .....	7
3. Appropriate Technical Measures – Encryption.....	8
4. Appropriate Organisational Measures .....	9
5. Contractual Measures .....	10
6. Third Parties and Security for Personal Data.....	11
7. Model Clauses.....	11
<b>D. RESPONDING TO A PERSONAL DATA SECURITY BREACH .....</b>	<b>12</b>
1. ICO and Security Breach Management.....	12
2. ICO and Security Breach Notification .....	13
3. FSA and Security Breach Notification.....	14
4. To Notify or Not to Notify? .....	15
5. Considerations if Notifying of a Breach.....	15
<b>E. RESPONSES TO DATA SECURITY BREACHES.....</b>	<b>16</b>
1. Commissioner’s Initial Response to Notification of a Breach .....	16
2. Commissioner’s Investigation of a Notified Breach .....	17
3. Enforcement by the Commissioner .....	17
4. Market Forces and Reputation.....	18
5. Additional Powers of the Commissioner .....	18
6. Other Consequences of a Notification of a Breach .....	19
<b>F. FUTURE LEGISLATION?.....</b>	<b>20</b>

## **NOTE ON SECURITY BREACHES INVOLVING PERSONAL DATA**<sup>1</sup>

### **A. INTRODUCTION**

Over the last couple of years there have been an increasing number of reports in the United Kingdom (“UK”) press of high profile personal data security breaches. Barely a week passes without the latest front page scandal, be it a lost laptop, misdirected postal CD or paper list dumped in a skip. As recently as last week, in response to a Freedom of Information Act 2000 request for information, the Welsh Assembly Government admitted sixteen separate incidents of its data being lost or stolen in the last three years with misplaced data stretching from documents left on a train to stolen laptop computers. Although a number of these breaches have placed a spot light on public sector bodies and government departments, compliance with data protection laws, including those concerned with the security of personal data, is equally important in the private sector.

Evidence from public and private sector sources suggests that this increased press reporting is no ‘folk devil’ or ‘moral panic’ whose genesis is in the desire of the forth estate to revive or bolster flagging circulation figures. Instead the numbers of incidents of security breaches involving personal data and the amount of individuals affected are both on the rise. Last Autumn the UK Information Commissioner’s Office (the “ICO”) published figures for personal data security breaches in the previous year<sup>2</sup> which showed :

- 80 reported breaches by the private sector;
- 75 reported breaches within the NHS and other health bodies;
- 28 reported breaches by central government;
- 26 reported breaches by local authorities and 47 by the rest of the public sector;
- of which the ICO investigated the 30 most serious cases.

In the month prior to the ICO’s publication, KPMG’s Advisory Practice published its data loss barometer<sup>3</sup> which identified the following global findings over three years to 2008 (primarily drawn from the UK and USA where public information is more readily attainable, if not, by any means, complete):

- 1034 incidents of data loss 280m people affected;
- 25% involving PC theft;
- 80% causing loss of personal details;
- 51% of losses from an internal source; and
- 46% of lost data has no protection.

---

<sup>1</sup> Calum Murray, Partner and Julia Jones, Assistant, Kemp Little LLP, London. This note is not legal advice or a substitute for it.

<sup>2</sup> see - [http://www.ico.gov.uk/upload/documents/pressreleases/2008/data\\_breaches\\_29\\_october\\_2008.pdf](http://www.ico.gov.uk/upload/documents/pressreleases/2008/data_breaches_29_october_2008.pdf)

<sup>3</sup> see - <http://www.kpmg.com/SiteCollectionDocuments/Data-loss-barometer-September-2008.pdf>

Going past simply capturing the number of security breaches and considering the combination of circumstances which are creating a fertile ground for the increase in security breaches, it is suggested that these include:

- creation of large scale databases by both public sector organisations and private sector service supplying corporations;
- hosting and storage of such personal data and databases for these data controllers by third parties;
- increase in availability (and inverse decrease in cost) of portable data storage devices and media containers like CDs, USB sticks and portable hard drives; and
- increase in ‘flow’ of personal data through channels such as websites for online service provision.

It is not suggested that these changes in how and where personal data are processed are not the sole causative factors in the rise in of data security breaches, but they all add to the circumstances in which personal data can be accessed (both legally and illegally), shared, transported, and ultimately lost by, or stolen from, data controllers.

As above, the great majority of published considerations of personal data security breaches suggest that such incidences are increasing. In light of the heightened public awareness of data security issues, the rise of the issue on the boardroom agenda following reported breaches and new legal powers which have been granted to the Information Commissioner (“**Commissioner**”) to address breaches of data protection laws, this note focuses on:

- the legislative context and application of that law in practice – **Section B**;
- the measures data controllers can take to minimise the risk of security breaches occurring in the first instance – **Section C**;
- action to be taken by data controllers in the event of a breach – **Section D**;
- the Commissioner’s (and other parties’) responses to personal data security breaches – **Section E**; and
- the future for legislative controls in respect of security breaches involving personal data – **Section F**.

## **B. THE LEGISLATIVE CONTEXT**

### **1. EC Data Protection Directive.**

Article 17(1) of the EC Data Protection Directive (the “**Directive**”) <sup>4</sup> requires EU member states to provide that the data controller must:

*“...implement **appropriate technical and organizational measures** to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized*

---

<sup>4</sup> Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L281/31) – see [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/95-46-ce/dir1995-46\\_part1\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf)

*disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. ”.*

Article 17(2) of the Directive further requires EU member states to provide that data controller must:

*“ where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures”.*

## 2. **The Data Protection Act 1998.**

The seventh data protection principle (the “**Seventh Principle**”) of the UK legislation implementing the Directive, the Data Protection Act 1998 (the “**DPA**”), replicates the requirements of Article 17(1) by setting out:

*“Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data”<sup>5</sup>.*

## 3. **Relevant Definitions.**

Any consideration of the scope of the Seventh Principle requires an understanding of the underlying defined terms of the DPA<sup>6</sup> which set out:

- a “**data controller**” is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed;
- a “**data processor**”, in relation to personal data, is any person (other than an employee of the data controller) who processes the data on behalf of the data controller;
- a “**data subject**” is an individual who is the subject of personal data;
- “**personal data**” are data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller; and
- “**processing**”, in relation to data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data.

Throughout this note where the above terms are used it is intended to refer to those terms as defined in the DPA.

## 4. **Compliance with the Seventh Principle.**

As can be seen from the terms of the Seventh Principle set out in **Section B2**, data controllers must determine the ‘*appropriateness*’ of security measures for protecting personal data which they are processing on a case-by-case basis and by reference to any available guidance. It should be also noted that the Seventh Principle pertains to not just establishing means of preventing security breaches, but instead to the security of data processing under the DPA generally.

The DPA gives limited guidance on how data controllers might assess whether security measures are ‘*appropriate*’. At the heart of the ICO’s approach is that data controllers should adopt a risk-based

---

<sup>5</sup> paragraph 8, Part I, Schedule 1, DP Act – see [http://www.opsi.gov.uk/acts/acts1998/ukpga\\_19980029\\_en\\_9](http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_9)

<sup>6</sup> set out in section 1(1), DP Act – see [http://www.opsi.gov.uk/acts/acts1998/ukpga\\_19980029\\_en\\_2#pt1-11g1](http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_2#pt1-11g1)

approach in attempting to determine what measures are appropriate. This is to be done by:

*“Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to—*

*(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and*

*(b) the nature of the data to be protected”<sup>7</sup>.*

It is the Commissioner’s opinion that given the breadth of the terms of reference for the data controllers as set out above, there can be no standard set of security measures required for compliance with the Seventh Principle. Consequently data controllers must get by with this broadly brushed guidance, even if the absence of prescriptive regulation may prove difficult for data controllers in assessing the merits of the measures they have in place.

## **C. PREVENTING A PERSONAL DATA SECURITY BREACH**

### **1. Appropriate Measures.**

The ICO has given some limited further guidance on how data controllers might evaluate the adequacy of any technical and organisational measures they are taking with regard to safeguarding personal data. In doing so the ICO looks back to the Directive for inspiration, confirming that security measures should be taken both:

- at the time of the design of the processing system; and
- at the time of the processing itself.<sup>8</sup>

The ICO further encourages data controllers to make use of ‘*privacy enhancing techniques*’ as a means to satisfying their obligations under the Seventh Principle. The ICO has also confirmed that it views management and organisational measures as equally important as technical ones in protecting personal data<sup>9</sup>.

Whilst it is set out to be illustrative and not prescriptive, the ICO has suggested that any data controller seeking to assess and manage the security controls of its system should review and implement<sup>10</sup>:

- security management
  - a management supported security policy committing to information security
  - management responsibility for the security policy on a person/team
  - sufficient resources and facilities for the management responsibility to be fulfilled
- controlled access to information

---

<sup>7</sup> see paragraph 9, Part II, Schedule 1, DP Act – see [http://www.opsi.gov.uk/acts/acts1998/ukpga\\_19980029\\_en\\_9](http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_9)

<sup>8</sup> see page 40 of - [http://www.ico.gov.uk/upload/documents/library/data\\_protection/detailed\\_specialist\\_guides/data\\_protection\\_act\\_legal\\_guidance.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf)

<sup>9</sup> see note 9

<sup>10</sup> see note 9 at pages 41-43

- access to buildings and data rooms
- access to screens and soft and hard copy documents
- access to systems by regularly changed passwords or other authorization
- access to information controlled on hierarchy of access need
- access to and cleaning of data storage media
- use of document shredding
- scripts for telephone calls where personal data may be disclosed
- policy, procedure and related security measures for all temporary removal of personal data from the data controller's premises
- clear definitions of security obligations by party
- business continuity
  - adequate precautions against burglary, fire or disaster
  - back-up technologies in place and back up data stored separately from live files
  - virus and other code intrusion protection in place
- staff selection and training
  - full consideration of discretion and integrity of staff who may access personal data
  - regular and adequate training for staff on their responsibilities
  - enforceable disciplinary rules and procedures taking account of the DPA
  - ability to withdraw staff access to personal data immediately if necessary
- detecting and dealing with breaches of security
  - systematic audit trails of attributable access to personal data
  - procedures for investigating and remedying breaches of security.

## 2. Appropriate Technical Measures - Standards

In providing legal guidance on how data controllers can ensure the appropriateness of any technical measures implemented to safeguard personal data, and so satisfy their obligations under the Seventh Principle, the ICO direct data controllers to further advice in “*BS 7799 and ISO/IEC Standard 17799*”<sup>11</sup>. Since this guidance was produced these standards have been re-written as ISO standards 27001 and 27002 (together the “**Standards**”), relevant to information security management and information security respectively.

The Standards espouse an approach of constant monitoring of data security systems and management and in particular set out a PDCA/Plan; Do; Check; Act cyclical methodology. This is echoed in the ICO's guidance that security measures should be taken at the time of the design of the processing system and at the time of the processing itself (as identified in **Section C1** above).

---

<sup>11</sup> see - [http://www.ico.gov.uk/upload/documents/library/data\\_protection/detailed\\_specialist\\_guides/data\\_protection\\_act\\_legal\\_guidance.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf)

The ISO 27001 standard for information security management<sup>12</sup> is based on the principles of:

- asset management;
- access control;
- business continuity management;
- communications and operations management;
- compliance;
- HR security;
- information security incident management;
- information systems acquisition, development and maintenance;
- organising information security;
- physical and environmental security; and
- security policy.

The standard generally requires an organisation-wide coherent approach such that:

- HR ensures through guidance and training that employees take personal responsibility for management of information assets in the workplace;
- there is resultant censure if this is not complied with; while
- the technical team ensure that ever-changing devices are technically secure.

Again all of this activity takes place in an environment of ongoing monitoring of adherence to the standard. In its current topics statement “*Our approach to encryption*” updated last on 23 December 2008<sup>13</sup> the Commissioner proposes the use of ISO 27001 as a best practice methodology.

### **3. Appropriate Technical Measures - Encryption**

As set out in **Section C1** above, the ICO also encourages data controllers to make use of ‘*privacy enhancing techniques*’ as a means to complying with the Seventh Principle. The ICO guidance on the Seventh Principle does not clarify for data controllers which type of technology or security should be used, other than to make mention of password protected access to personal data. There is no specific mention of data encryption. However, in the Commissioner’s current topics statement referred to in **Section C2** above, the Commissioner states that where laptop computers, containing personal information are stolen or lost without being protected adequately, enforcement action will be pursued. The Commissioner continues to state his view that using adequate protection will require the use of encryption software.

This view is supported by the Commissioner’s recommendation that:

*“all portable and mobile devices including magnetic media, used to store and transmit personal information, the loss of which could cause damage or distress to individuals, should*

---

<sup>12</sup> see - <http://www.27001-online.com/>

<sup>13</sup> see - [http://www.ico.gov.uk/about\\_us/news\\_and\\_views/current\\_topics/Our%20approach%20to%20encryption.aspx](http://www.ico.gov.uk/about_us/news_and_views/current_topics/Our%20approach%20to%20encryption.aspx)

*be protected using approved encryption software which is designed to guard against the compromise of information”<sup>14</sup>.*

Lastly the Commissioner recognises that encryption standards are always evolving, and so, akin to continual monitoring under ISO 27001, data controllers should ensure that the solution which they implement meets the current standard such as the recommended FIPS 140-2 (cryptographic modules, software and hardware) and FIPS – 197.

#### **4. Appropriate Organisational Measures.**

In addition to implementing technical measures to comply with their obligations under the Seventh Principle, data controllers must also consider how they will ensure those technical measures become part of the fabric of their operations and are adopted as standard practices by their employees and contractors. Commonly this is done through a combination of processes, policies and supportive training on all of them.

Security processes can be both physical and virtual and tend to be put in place to control what personal data employees and contractors can see. Such restrictions can include:

- security fobs, swipe cards, locked rooms and cabinets, shredder use and paperless practices – physical; and
- categorising personal data by security level and password protecting or encrypting – virtual.

All types of access controls allow organisations to create hierarchies of data sensitivity and do what they can to ensure only those who should access personal data can do so. In addition, the virtual parsing out of personal data facilitates practices to be established as to what can be done with each type of data, such as what can be downloaded or copied.

As well as having standard practices for their employees and contractors, data controllers should consider introducing policies to underpin the practices they are seeking to institutionalise and to provide a touchstone for staff to refer to when in doubt. Policies come in many shapes and sizes according to operational practices and issues but some regular topics feature as constants in most organisations working to comply with the Seventh Principle:

- IT and Telecommunications use policy – setting out matters such as any restrictions on employees' use of IT and telephone resources; portable equipment use and transport; requirements for encryption;
- Internet use policy – clarifying use of: email; retail, social media and online service provider websites, including hosted storage and SaaS applications;
- Data Protection policy – establishing what personal data is collected for what purposes; where it is stored; who it is shared with and who has access to it;
- Data Retention policy – making clear what systems and procedures are used and when to ensure that personal data is protected, properly stored and destroyed in a DPA compliant manner; and
- Security Breach response policy – ensuring that all relevant stakeholders in the organisation are aware of their respective roles and responsibilities in the event of a personal data security breach.

Lastly, all of these practices and policies should be introduced and regularly re-enforced with

---

<sup>14</sup> see note 13

employees through training (often made part of performance) and with contractors as early as possible through the contractual arrangements which are to be or are in place between them and the data controlling organisation.

## 5. Contractual Measures.

In the middle of last year the Office of Government Commerce (“OGC”) established that where public sector bodies were procuring information technology or communications services using an OGC Model ICT Services Contract, or where there was any other kind of procurement involving personal data processing, contractual clauses (and related schedules) covering data protection, confidentiality and security were either:

- deemed mandatory and to be applied without amendment of any sort; or
- otherwise suggested as necessary for inclusion <sup>15</sup>.

These terms include

- *staff vetting* – imposing obligations, including a mandatory warranty and if required, full staff vetting provisions, on data processors to take measures to ensure the reliability of their employees. This is aimed at assisting data controllers to monitor and require correction of personal data security breaches;
- *audit* - data controllers will also need to build audit terms in contracts to allow them to track compliance with the Seventh Principle obligations and require rectification of non-compliance;
- *reporting and remediation*– with particular regard to personal data security breaches, whether through specific process or general obligation. This is coupled with a right to use third parties to assist with incident mitigation and remediation at the cost of the data processor;
- *termination* - should remediation fail, specific termination rights for personal data security breaches are proposed, such as termination rights for breach of data protection and data security warranties (being a contractual extension of the rights otherwise available for breach of warranty);
- *assistance* - even if a data processor has agreed to the Seventh Principle obligations, the data controller remains responsible for DPA breaches and so must require the data processor to comply with its contractual security obligations, which assists the data controller with its liabilities;
- *confidentiality* – confidentiality provisions should inclusively refer to the personal data that is to be processed by the data processor under the contract and protect it as confidential; and
- *indemnity* –particular losses resulting from a personal data security breach incident should be recoverable on an indemnity basis.

The OGC contracts are intended to cover specific supply to the public sector. However, an examination of the terms deemed mandatory is useful for private sector organisations as an insight into what the Government believes is required of data processors providing services to bring about compliance with the Seventh Principle through its contracting.

---

<sup>15</sup> see - [http://www.ogc.gov.uk/documents/PPN\\_Data\\_Handling\\_Review.pdf](http://www.ogc.gov.uk/documents/PPN_Data_Handling_Review.pdf)

## 6. Third Parties and Security of Personal Data

Where processing of personal data is carried out by a third party data processor on behalf of a data controller, such as in a situation of an outsourced service provision, the DPA places specific obligations on the data controller if this processing is to comply with the Seventh Principle. The data controller must<sup>16</sup>:—

- choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the data processing;
- take reasonable steps to ensure compliance with those measures; and
- ensure there is a written contract between the data controller and the data processor under which:
  - the processing is carried out;
  - the data processor is to act only on instructions from the data controller; and
  - the data processor is bound to comply with obligations equivalent to those imposed on a data controller by the Seventh Principle.

It is essential that the data controller makes every effort to choose the right data processor because as with all DPA requirements, the responsibility for compliance rests with data controllers and not data processors. Even if a data processor causes a breach of the Seventh Principle, its instructing data controller will primarily be liable for that breach under the DPA.

Similar security measures are also required where a data controller will pass information to another data controller. Therefore any organisation sharing personal data has an obligation to ensure that all intended recipients have appropriate security in place.

Practical and contractual measures which a data controller could take in order to evaluate a data processor and keep the data processor's security measures under review include:

- carrying out appropriate due diligence – for example visiting suppliers' premises, ensuring that they maintain clean desk policies, that computer screens cannot be viewed externally, etc.
- incorporating suitable controls on sub-contracting – for example preventing sub-contracting or sub-contracting without the data controller's consent and ensuring that any sub-contractor maintains at least the same security measures as the data processor;
- ensuring that audit rights are in place and are regularly exercised;
- requiring the prompt reporting of any data which is lost or destroyed or becomes damaged, corrupted or unusable to the data controller;
- ensuring that suppliers are fully trained, follow best practice and keep up to date with any developments in security precautions, for instance installing security patches on servers and routers; and
- requiring service providers to co-operate with investigations and notifications.

## 7. Model Clauses

One means for data controllers to ensure compliance with the requirements of the DPA when using a third party service provider to process personal data is to use the applicable set of the three sets of

---

<sup>16</sup> see paragraphs 11 and 12, Part II, Schedule 1, DP Act – see [http://www.opsi.gov.uk/acts/acts1998/ukpga\\_19980029\\_en\\_9](http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_9)

model contractual clauses (“**Model Clauses**”) which the European Commission (the ‘**Commission**’) has approved under Articles 26(2) and (4) of the Directive as offering adequate safeguards for the protection of personal data and data subjects’ rights. More often considered in the context of exporting personal data from the UK<sup>17</sup>, the Model Clauses require the recipient of personal data to provide adequate safeguards in respect of the personal data. These three sets of Model Clauses are set out as an annex to the relevant Commission decision which approves them:

- the first set is for use by EU-based data controllers when transferring personal data to **data controllers** outside the EEA (“**Data Exporter Clauses**”)<sup>18</sup>;
- the second set is for use by EU-based data controllers when transferring personal data to **data processors** outside the EEA<sup>19</sup> (“**Data Processor Clauses**”); and
- the third set, like the first set, is for use by EU-based data controllers when transferring personal data to **data controllers** outside the EEA<sup>20</sup> (“**New Model Clauses**”).

## **D. RESPONDING TO A PERSONAL DATA SECURITY BREACH**

### **1. ICO and Security Breach Management**

In April 2008, the ICO published two Good Practice Notes on responding to personal data security breaches. The first of these notes addressed how data controllers should manage breaches of personal data security<sup>21</sup>. The second note considers when data controllers should notify the ICO of personal data security breaches<sup>22</sup>.

The ICO considers data controllers should have plans in place in the event that such a security breach occurs. The ICO has set out four key elements to any breach management plan which data controllers should consider:

- *containment and recovery* –
  - who needs to be made aware of the breach and how such persons can provide assistance in any containment activities; and
  - are any losses recoverable and whether the damage caused by the breach could be limited;

---

<sup>17</sup> see - [http://www.kemplittle.com/PDFs/Article\\_NoteOnExportingPersonalDataFromTheUK.pdf](http://www.kemplittle.com/PDFs/Article_NoteOnExportingPersonalDataFromTheUK.pdf)

<sup>18</sup> Commission Decision 2001/497/EC15 of 15 June 2001 – see [http://eur-lex.europa.eu/pri/en/oj/dat/2001/l\\_181/l\\_18120010704en00190031.pdf](http://eur-lex.europa.eu/pri/en/oj/dat/2001/l_181/l_18120010704en00190031.pdf)

<sup>19</sup> Commission Decision 2002/16/EC16 of 27 December 2001 – see [http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l\\_006/l\\_00620020110en00520062.pdf](http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_006/l_00620020110en00520062.pdf)

<sup>20</sup> Commission Decision 2004/915/EC17 of 27 December 2004 – see [http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l\\_385/l\\_38520041229en00740084.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_385/l_38520041229en00740084.pdf)

<sup>21</sup> see - [http://www.ico.gov.uk/upload/documents/library/data\\_protection/practical\\_application/guidance\\_on\\_data\\_security\\_breach\\_management.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/guidance_on_data_security_breach_management.pdf)

<sup>22</sup> see - [http://www.ico.gov.uk/upload/documents/library/data\\_protection/practical\\_application/breach\\_reporting.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/breach_reporting.pdf)

- *assessment and risk* – assess the seriousness of the risks or how substantial these are as a result of the breach. Factors to consider in risk assessment include:
  - the type of personal data concerned, to whom it relates and how sensitive it is;
  - a consideration of what has happened to the personal data;
  - whether the personal data was encrypted;
  - what information a third party could learn from the personal data;
  - how many individuals are affected by the breach; and
  - what harm could come about as a result of the breach
- *evaluation and response* –
  - assess the causes of the breach;
  - analyse the effectiveness of the response to the breach;
  - risks should be assessed, improvements identified; and
  - the ICO recommends that as a minimum, a group of people should be responsible for responding to security breaches
- *notification of breaches* – this is specifically addressed in the second Good Practice Note which is discussed in **Section D2** below.

## 2. ICO and Security Breach Notification

For public sector organisations the fallout from the HMRC/Child Benefit matter has lead the Commissioner to require Government departments to notify data breaches to the ICO. There is currently no specific legal obligation in the UK requiring other data controllers to notify a breach of personal data security. However, the ICO is of the view that serious breaches of security which result in loss, release or corruption of personal data should be reported to the ICO. Indeed, as we have seen in Section A above, the number of personal data security breach notifications has risen to 277 in the space of approximately a year at the end of October 2008<sup>23</sup>.

Whether a breach is serious enough to warrant notification will depend on a matrix of:

- the potential harm to data subjects;
- the volume of personal data lost, released or corrupted; and
- the sensitivity of the personal data lost, released or corrupted.

The second Good Practice Note issued by the ICO<sup>24</sup> provides that where there is significant actual or potential harm as a result of the breach, whether because of the volume of personal data, its sensitivity or a combination of the two, there should be a presumption to report.

In some cases it may be appropriate for data controller to notify data subjects and third parties of a personal data security breach which affects them. Some of the factors highlighted by the ICO which data controllers should consider when deciding whether to notify include whether, for instance:

- they are required to notify any breach contractually, or as a result of any sector specific regulations or voluntary codes (see for example **Section D3** below);
- notifying data subjects may enable those individuals to mitigate any risks brought about by a breach;

---

<sup>23</sup> see note 2

<sup>24</sup> see [http://www.ico.gov.uk/upload/documents/library/data\\_protection/practical\\_application/breach\\_reporting.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/breach_reporting.pdf)

- whether a large number of people are affected and/or the consequences are particularly serious; and
- whether disproportionate enquiries and work would be caused by notifying a large number of data subjects when only a small number are affected by the breach.

In all of this data controllers should bear in mind that the ICO's overriding consideration in deciding whether a breach should be reported to it is the potential harm to individuals.

### 3. FSA and Security Breach Notification

Data controllers operating in environments subject to additional regulatory controls may encounter sector specific rules with which they must comply if faced with a personal data security breach. For example, data controllers regulated by the Financial Services Authority ("FSA") must comply with the relevant FSA rules. Regulated parties have a general obligation to deal with the FSA in an open and cooperative way and disclose to the FSA appropriately anything relating to the regulated party of which the FSA would reasonably expect notice. This includes giving notice of any significant failure in data controller's systems or controls. In this regard, the FSA expects a firm to discuss relevant matters with it at any early stage, before making any internal or external communications.

In addition to a general obligation to be open and co-operative, a FSA regulated data controller must notify the FSA immediately if it becomes aware of any matter which could have a serious adverse impact on its reputation or its ability to continue to provide adequate services to its customers and which could result in serious detriment to a customer of the firm. In this regard, the FSA expects firms to consider properly all potential consequences of events, including the impact of data security breaches.

Regulated data controllers must also notify the FSA of any significant breach of a FSA rule (including the general principles) or statement of principle. In this regard, 'significance' should be determined having regard to:

- potential financial losses to customers or to the data controller;
- frequency of the breach; and
- implications for data controller's systems and controls and if there were delays in identifying or rectifying the breach.

Lastly in respect of regulated data controllers' communication to customers, the FSA's 'Data Security in Financial Services' guidance<sup>25</sup> states that:

*“When customer data is lost, consumers that are affected have a right to know the enhanced personal risk they face so they can take adequate precautions. Even if there is no evidence of theft or fraud, it is good practice for firms to inform affected customers of a data loss in writing, unless the data is encrypted or there is law enforcement or regulatory advice to the contrary. Firms should consider telling affected consumers exactly what data has been lost, give them an assessment of the risk and give advice and assistance to consumers at a heightened risk of identity fraud”<sup>26</sup>.*

Data controllers should therefore be mindful of regulatory constraints in their industry as well as data protection laws.

---

<sup>25</sup> see - [http://www.fsa.gov.uk/pubs/other/data\\_security.pdf](http://www.fsa.gov.uk/pubs/other/data_security.pdf)

<sup>26</sup> see note 26 at paragraph 99

#### 4. To Notify or Not to Notify?

Absent a legal or contractual obligation to disclose in the UK, whether or not a private sector organisation chooses to notify its customers or the ICO of a breach of personal data security, or to make a breach public, is a balancing act for the data controller. Factors on either side of this weighing up can include:-

- regulatory requirements or voluntary code term implications;
- seriousness of the breach;
- any benefits that might be obtained by disclosure;
- whether notification assists with security and so compliance with the Seventh Principle;
- whether notification will help the individuals whose personal data is leaked in the breach;
- loss of reputation for the data controller; and
- loss of customer goodwill by the data controller.

As evidenced by published statistics to date and discussed in **Section A** above, of 277 notifications in the year to October 2008, only 30 of the most serious are being investigated by the ICO. Therefore regulatory action by the ICO remains a consideration, but one which in reality is only likely to have an impact on notification decisions in circumstances of the most serious breaches of personal data security. In all decisions of whether to notify (as with decisions re any regulatory action by the ICO) the data controller must set the benefits of maintaining public confidence in data sharing (through not disclosing) against operating a transparent business operation.

As the ICO notes in his first Good Practice Note<sup>27</sup>:

*“Informing people and organisations that you have experienced a data security breach... is not an end in itself. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.”*

Consequently any data controller who is faced with a breach must satisfy itself that there is a positive consequence of any notification it proposes to make.

#### 5. Considerations if Notifying of a Breach

Once the decision to notify has been made, the data controller must then consider the direction of any notification and its content. Notification will be made in accordance with the data controller’s obligations (if any):

- contractual requirements will likely necessitate disclosure to the counterparty(ies) at the very least
- sector specific rules may require a notification to be issued to the sector regulator
- voluntary codes will require disclosure in accordance with their terms –often to a central body or other signatories
- the ICO may need to be informed if a large number of people are affected or there are very serious consequences.

---

<sup>27</sup> see -

[http://www.ico.gov.uk/upload/documents/library/data\\_protection/practical\\_application/guidance\\_on\\_data\\_security\\_breach\\_management.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/guidance_on_data_security_breach_management.pdf)

As to content of any disclosure, the data controller must take time to finalise what information should be in any disclosure, and how this will be communicated. In these considerations the ICO has suggested that data controllers address all of the following factors:-

- medium - use of the most appropriate medium of communication having regard to the security of the medium as well as the urgency of the situation;
- detail - as a minimum, telling the ICO how and when the security breach occurred and what personal data was involved;
- security – again if telling ICO, set out details of the security measures and security procedures in place at the time the breach occurred;
- response - setting out for the ICO full details of what measures have already been taken to respond to the security risks arising from the breach;
- audience needs - consider if the recipients of a notice have specific needs for the notice, for example, vulnerable adults;
- proportionality - do not over-notify, send notification to those who are, or may be, affected only;
- guidance - provide individuals with specific and clear advice on how they may protect themselves;
- assistance - clarify any assistance to be provided to relevant data subjects; and
- support – provide an ongoing point of contact for questions and support.

If notifying the ICO, guidance suggests that data controllers should also inform the ICO if the media has been made aware of the security breach. This allows the ICO to co-ordinate activities so as to cater for a likely upturn in enquiries from members of the public. The ICO has stated that it will not usually inform the media or other parties about a security breach being notified to it. It may, however, advise the data controller to let the media know of the incident. The ICO also suggests that when informing the media of a personal data security breach, a data controller should confirm whether they have contacted the ICO and, if so, what action is being taken.

Finally data controllers should consider whether there are any other third parties who should be notified of the security breach. This will very much be driven by the circumstances of the breach but may include:

- police – if the security breach potentially involves a crime;
- insurers – if the data controller has relevant cover, say for loss of data;
- bank or credit card companies – particularly if customers’ payment details have been breached; and
- trade unions – if workers’ details have been lost in a unionised environment.

## **E. RESPONSES TO DATA SECURITY BREACHES**

### **1. Commissioner’s Initial Response to Notification of a Breach**

When a breach is reported to it, the ICO’s first response is to:

- assess the nature and seriousness of the breach;
- assess the adequacy of any remedial action; and
- determine a course of action.

The ICO may then implement one of the following courses of action:

- record the breach and take no further action; or

- investigate the background to the breach and consider what would be suitable remedial action.

## 2. Commissioner's Investigation of a Notified Breach

If the second course in **Section E1** is plotted by the ICO this can result in:

- a decision of no further action being required;
- the imposition of a requirement on the data controller to undertake a course of action to prevent further breaches; or
- the instigation of formal enforcement action which would have the effect of turning the ICO's requirements into legal binding obligations.

The Commissioner has various powers which enable him to carry out investigations into breaches or suspected breaches of data protection law, including the ability to apply for a warrant to gain entry to premises and carry out inspections; the ability to request information using an Information Notice; the ability to obtain undertakings from the data controller; and the ability to issue an Enforcement Notice specifying action which a data controller must take, or refrain from taking, in order to comply with the DPA. For example, in October 2008, the ICO found Virgin Media Limited ("**Virgin**") to be in breach of the DPA following the loss of an unencrypted CD containing the personal details of over 3,000 customers. Virgin has since been ordered to implement, with immediate effect, a number of security measures to protect customers' personal data more effectively including:-

- encrypting all portable or mobile devices which store and transmit personal information;
- ensuring its third party partners processing personal information on behalf of Virgin must also use encryption software; and
- ensuring this requirement is clearly stated in all contracts with third parties.

Virgin has also signed a formal undertaking to comply with the principles of the DPA. Failure to meet the terms of the undertaking is likely to lead to further enforcement action by the ICO.

## 3. Enforcement by the Commissioner

The ICO has issued guidance on its enforcement strategy<sup>28</sup> where it confirms it will:

- use enforcement action on a selective or targeted basis; and
- combine such action with market forces and damage to reputation by way of an effective regulatory influence.

Where the ICO takes regulatory action, its policy is to publicise this activity, including any formal undertakings provided to the ICO by a data controller, unless there are exceptional reasons not to do so. The ICO is slow to take regulatory action, preferring data controllers to take any ICO recommended remedial action. Regulatory action by the ICO is more likely where the ICO believes future compliance by the data controller is unlikely or the matter is one in which the ICO must provide reassurance to the public, such as where the breach and its origins are public knowledge.

The general practice of the ICO is to issue enforcement notices only in serious cases of breach of the DPA by a data controller. If a data controller fails to follow the terms of any enforcement notice, the ICO may prosecute the data controller, and if successful such prosecutions at summary level can result in fines of up to £5,000 per offence on both the data controller company, and the relevant

---

<sup>28</sup> see -

[http://www.ico.gov.uk/upload/documents/library/data\\_protection/detailed\\_specialist\\_guides/data\\_protection\\_regulatory\\_action\\_strategy.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_regulatory_action_strategy.pdf)

directors or senior managers. Successful prosecutions on indictment can result in fines which have no prescribed limit.

It should be noted that a breach of a data protection principle is not in itself a criminal offence (although the breach of an enforcement or information notice is). Hence the Commissioner's Annual Report for 2007/2008<sup>29</sup> only reported the prosecution of 11 individuals and organizations in the last 12 months. Nevertheless, breach of the DPA can lead to prosecution and the imposition of fines.

#### **4. Market Forces and Reputation**

In any event, as the Commissioner has recognised in its enforcement strategy, the rise in prevalence of crimes such as identity theft and the public's growing awareness and expectation that personal data will be securely maintained, mean the threat of bad publicity arising out of a security breach can incentivise compliance with the DPA. Indeed it is arguable that it is the negative publicity (and the potential loss of business) arising as a result of a security breach, rather than the threat of any sanction under the DPA, which businesses have to fear most. Against that backdrop, it is perhaps surprising that the ICO has not required all breaches of the DPA to be notified to it. At worst it can be argued that those organizations who operate in competitive environments may place themselves at a disadvantage by adhering to current legal provisions for data security.

By way of counter to the above position, it is suggested that though it can be seen as a charter for minor breaches of personal data security to perpetuate, the ICO's stance is a matter of resourcing as much as policy. Furthermore with no legal obligation on data controllers to notify the ICO of a breach, the ICO clearly may often not be sufficiently informed to undertake any activity in respect of a serious breach – the Commissioner cannot be expected to make any recommendations on things he is not aware of.

#### **5. Additional Powers of the Commissioner**

As set out in **Section D2** above, there is currently no specific legal obligation in the UK requiring data controllers to notify a breach of personal data security. In the Ministry of Justice's ("MOJ") response of 24 November 2008<sup>30</sup> to the Data Sharing Review Report<sup>31</sup>, the Government agreed with the Data Sharing Review's recommendation that notification of a data security breach should not be mandatory, although any failure to notify in cases involving substantial damage and distress should be taken into account by the ICO when determining any penalties. The response also confirmed that the Government has decided not to implement data breach notification legislation (similar to that in force in the USA) here.

The ICO has been arguing for some time that its powers, sanctions and resources are inadequate and that it needs stronger powers in order to ensure compliance with the DPA. As a result, section 144 of the Criminal Justice and Immigration Act 2008 introduces a new section 55A-E into the DPA, providing the ICO with the power to impose substantial penalties on data controllers in certain circumstances. In particular, a monetary penalty notice may be served where there is:

- a "*serious contravention*" of the data protection principles;

---

<sup>29</sup> see - [http://www.ico.gov.uk/upload/documents/library/corporate/detailed\\_specialist\\_guides/annual\\_report\\_2007\\_08.pdf](http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/annual_report_2007_08.pdf)

<sup>30</sup> see - <http://www.justice.gov.uk/docs/response-data-sharing-review.pdf>

<sup>31</sup> The Data Sharing Review Report was published on 11 July 2008 and was produced by Dr Mark Walport of the Wellcome Trust and the Information Commissioner, Richard Thomas. The purpose of the report was to independently review the framework for the use of personal information in the public and private sectors: <http://www.justice.gov.uk/reviews/datasharing-intro.htm>

- which is likely to cause substantial damage or substantial distress and either:
  - the contravention was deliberate; or
  - the data controller ought to have known that there was a risk that such a contravention would occur but failed to take reasonable steps to prevent the contravention.

The new provisions also require the Commissioner to prepare and issue guidance on his new powers, including the circumstances in which the Commissioner would consider it appropriate to issue a monetary penalty notice and how the Commissioner will determine the amount of the penalty. Section 55A of the DPA is awaiting Secretary of State sanctioned secondary legislation to bring it into force.

In relation to the maximum level of the penalty which may be imposed, the Data Sharing Review<sup>32</sup> recommended that this should mirror existing sanctions available to the FSA setting high, but proportionate, maxima related to turnover. The response to the Data Sharing Review Report<sup>33</sup> states that the MOJ is working with the ICO to determine the level of the maximum penalty and that the MOJ is considering the implementation of a model “similar” to that operated by the FSA.

It is open to discussion how much of a deterrent Section 55A will prove to be and how often is it likely to be used by the ICO. Even when it comes into force, the nature of the offence means that the Commissioner will only be able to use his new powers in serious cases where there is essentially a willful disregard for the requirements of the DPA or grossly negligent approach to compliance. In addition, the Government has announced its intention<sup>34</sup> to grant an exemption from the monetary penalty where data controllers consent to a “good practice assessment” (essentially an audit of a data controller’s processing) in order to encourage compliance. Nevertheless, it seems clear that the Commissioner is hoping that the new powers will help to modernize the UK’s data protection regime and send a clear message to data controllers that data protection requirements cannot be ignored or dismissed.

## **6. Other Consequences of a Notification of a Breach**

On 10 September 2008, the Home Secretary announced that the Government had terminated a contractual arrangement with PA Consulting (“PA”), a private sector service supplier. The reason for termination were that PA (which was undertaking research on individuals’ progress through the criminal justice system) had, in the previous month downloaded from a secure website to an unencrypted USB memory stick, the personal data of all 84,000 prison inmates in England and Wales. The memory stick was then misplaced or lost. The contractual ground on which the Home Secretary’s termination of contract relied was PA’s breach of the data security provisions of the contract.

This is an example of what is likely to be a growing trend in contractual based responses to personal data security breaches. Here the Government believed it was entitled to terminate and has now gone further to review all contracts signed by the Government with private companies to ensure that their provisions are appropriate in respect of data security breaches and related rights such as termination. As set out in **Section C6** above, the Government is also obliged to ensure that its contracts provide

---

<sup>32</sup> see - <http://www.justice.gov.uk/reviews/datasharing-intro.htm>

<sup>33</sup> see note 32

<sup>34</sup> See the Ministry of Justice’s response of 24 November 2008 to the consultation paper on the Information Commissioner’s Inspection Powers and Funding Arrangements under the DPA <http://www.justice.gov.uk/docs/information-commissioner-consultation-responses.pdf>

that sufficiently high technical and physical security measures be adopted by the service provider to ensure the integrity of its data.

In addition to termination of the contract, this situation gives rise to a variety of possible compensatory claims:

- subject to the terms of the contract, the Government may claim compensation from PA for any loss or damage suffered by it as a result of PA's breach;
- individuals (prisoners) may have a claim against PA for negligence; and
- individuals (prisoners) can claim against the Government under the DPA.

Whilst to date, awards of compensation under the DPA have been of limited generosity, these facts identify how proactive enforcement of contractual rights when faced with a breach of personal data security can give rise to a range of liabilities.

#### **F. FUTURE LEGISLATION?**

As set out in **Section E5** above, the MOJ confirmed in November 2008<sup>35</sup> that notification of a data security breach by private sector organisations should not be mandatory in the UK. This may however be a 'for now' position.

A new e-Privacy Directive is being debated in the EU Parliament. Among the revisions proposed is an amendment to Article 4 of the e-Privacy Directive to establish a mandatory system in relation to the breach of personal data security. As drafted the Article would require telecommunications providers and ISPs to notify the national regulator, and, in certain circumstances, any user concerned, of any personal data security breaches over their networks, other than where:

- the provider can demonstrate to the national regulator that it has implemented appropriate technological protection measures, and those measures were applied to the data relating to the security breach;
- the technological protection measures render the data in question unintelligible to any person who is not authorised to access them.

The European Council is expected to adopt a common position based on the amendments in early 2009.

While the current proposals for the amendment only capture breach of personal data security by public communication providers, the possibility of a mandatory security breach notification system is already lending encouragement to those who would see its application be more widespread. In particular there are calls to extend the scope of e-Privacy Directive's notification requirements to other organisations with an on-line presence (such as banks and credit card providers). The outcome of this tussle could well result in a widespread mandatory notification scheme being introduced into UK laws.

**Kemp Little LLP (CGM/JMJ)**

**London**

**January 2009**

---

<sup>35</sup> see - <http://www.justice.gov.uk/docs/response-data-sharing-review.pdf>