

erdu

**ENTERPRISE
RESEARCH and
DEVELOPMENT
unit**



Data Protection and Small and Medium Enterprises

Report prepared for the Information Commissioner's Office

FINAL REPORT

September 2004

Prepared and submitted by
Enterprise Research and Development Unit (ERDU)
Lincoln Business School
University of Lincoln
Brayford Pool
Lincoln LN6 7TS

Project Team:
Kirk Frith, Research
Charlotte McClelland, Research
John McManus, Project Manager
Liz Price, Analysis
Jenny Reynolds, Research

Contact:
Professor Andrew Atherton
01522 886927
aatherton@lincoln.ac.uk

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
1. INTRODUCTION AND OVERVIEW OF THE STUDY	4
2. RESEARCH OBJECTIVES and OUTPUTS	5
3. RESEARCH APPROACH	5
4. THE TELEPHONE SURVEY SAMPLE	7
5. AWARENESS AND LEVELS OF ENGAGEMENT	8
6. RESPONDENTS' VIEWS ON DATA PROTECTION	9
7. KEY TERMS AND CONCEPTS	10
Table 1: Key Terms Ranked by Respondents	10
Table 2: Terms Ranked as Most Significant	12
8. COMPLIANCE WITH THE ACT: REQUIREMENTS, ISSUES AND DEMANDS	14
Table 3: Ranking of 'Compliance Requirements' for the Data Protection Act	15
9. BEST PRACTICE PATTERNS AND TRENDS IN DATA PROTECTION	17
10. IS THERE A CASE FOR ADOPTING DATA PROTECTION PRINCIPLES?	19
11. ANALYSIS OF POSSIBLE RELATIONSHIPS AND ASSOCIATIONS	20
Table 4: Summary Statements derived from Annex 4 Cross-Tabulations	22
12. IMPLICATIONS 1: ATTITUDES AS A KEY DETERMINANT OF PRACTICE	22
13. IMPLICATIONS 2: SEGMENTING THE SME MARKET BY RESPONSE	23
14. IMPLICATIONS 3: IDENTIFYING GOOD PRACTICE IN DATA PROTECTION	26
15. IMPLICATIONS 4: THE PROFILE OF THE ICO	27
16. CONCLUSIONS AND OBSERVATIONS	28
Conclusions	28
Observations	29
 ANNEXES	 30
 ANNEX 1: AWARENESS AND LEVELS OF ENGAGEMENT WITH THE ACT	 31
ANNEX 2: ANALYSIS OF THE TELEPHONE SAMPLE	40
ANNEX 3: CATEGORISATION BY INDUSTRY CATEGORY	43
ANNEX 4: CROSS-TABULATIONS WITH COMMENTARY	45
ANNEX 5: ANALYSIS OF SCENARIOS FOR SMEs AND DATA PROTECTION	67
ANNEX 6: THE ENTERPRISE RESEARCH AND DEVELOPMENT UNIT	72

Note:

This study has been undertaken by the Enterprise Research and Development Unit, University of Lincoln, on behalf of the Information Commissioner's Office. Although ERDU has taken every step to ensure that the data acquired and used for the study are accurate and robust, we cannot be held responsible for the responses made by those interviewed during the study. Data collected during the study has been handled confidentially by ERDU and cannot be made available to any third party without permission from the original source of data.

EXECUTIVE SUMMARY

- 1 There is a high level of awareness of data protection and the Data Protection Act.
- 2 There is broad acceptance of the values and principles of data protection, although opinions appear divided as to the benefits of compliance.
- 3 Awareness and acceptance of principles in broad terms does not necessarily translate into specific knowledge of registration/notification.
- 4 The compliance or 'red tape' burden associated with government regulation does not appear to be a major issue for the Data Protection Act for most of the business, although there is a small 'vocal minority' who consider this an issue.
- 5 Two key terms registered most strongly with the businesses (1) Security of Data and Information, and (2) Confidentiality. Privacy also figured as a significant term, but not to the same extent.
- 6 Effective practice in data protection was closely associated with wider information management and data control within the business – those enterprises that deployed information for business benefit tended to be actively supportive of data protection principles and found it easy to comply with the Act.
- 7 Individual and shared attitudes towards data protection and information are key influences on business approaches to this issue, and so constitute a primary influence on compliance and engagement with the Act and the ICO.
- 8 Different approaches to data protection and information can be identified, and used to identify distinctive segments – each with different requirements and approaches.
- 9 There was some indication that respondents were considering effective practice in information and data management and handling, with data protection being seen as a 'sub-set' of these considerations. Good practice in data protection, in other words, appears to be part of and to stem from wider approaches to information.
- 10 Although the Act itself had a high profile, the ICO was less well known and some businesses thought that it would be useful for the ICO to engage more with SMEs.

1. INTRODUCTION AND OVERVIEW OF THE STUDY

- 1.1 This report is the final output of the study '**Encouraging Small and Medium sized Enterprises to Adopt the Values of Data Protection**'. The project was commissioned by the Information Commissioner's Office in December, 2003, and was completed in March, 2004.
- 1.2 The research has been undertaken by the Enterprise Research and Development Unit (ERDU) at the University of Lincoln. ERDU is the focus for the University's activities related to small and medium businesses and entrepreneurship. The project team has extensive knowledge and experience of commissioned research relating to SMEs as well as an understanding of and previous engagement with information management and with regulatory compliance issues and the Data Protection Act. Details of the team and ERDU are provided in Annex 6 of this report.
- 1.3 As indicated in the tender invitation, the overall aim of the project is to: "investigate small and medium sized businesses' attitude to privacy, to look at their practical compliance measures and to evaluate their concerns about this area of the law." Primary objectives are to assess:
- (1) The attitudes of SMEs to the values of data protection
 - (2) Their concerns about the impact of data protection compliance on the business.
- 1.4 The research examined data protection and information handling issues, including but not restricted to the Data Protection Act, within the context of and from the perspective of the small and medium enterprise (SME). Our focus has been on understanding current practice relating to information and data in SMEs, and to relate this insight to data protection practice.
- 1.5 As well as generating real insight into the views and experiences of SMEs, the project has involved direct, ongoing and 'hands-on' engagement of the ICO as commissioning body. This extended beyond reporting on actions undertaken and progress to include direct inputs into the direction of the research. The aim has been to involve the Information Commissioner's Office in the research process and in active engagement with the data and findings. Successive meetings and face-to-face discussions have been incorporated into the work programme along with weekly progress reporting, in order to provide a detailed and up-to-date profile of research activities.
- 1.6 The main sections of the report highlight key findings and patterns. Data presentation and analysis has been placed within a series of Annexes (*see Table of Contents*). The Annexes have been designed as an information 'resource' that provides detailed feedback on the results of the research. The focus of the main report, therefore, is on the meaning and significance of the findings, with supporting data analysis contained in Annexes 1 to 5 of this document.

2. RESEARCH OBJECTIVES and OUTPUTS

2.1 The objectives of this project were:

- (1) To develop an in-depth understanding as to SME experiences of and views on data protection and the Data Protection Act
- (2) To feed back to the Information Commissioner the findings from consultations with SMEs
- (3) To consider the implications of these findings for the Information Commissioner and for the pursuit of compliance with and acceptance of legislation in this area
- (4) To identify and examine strategies and options for the Information Commissioner related to data protection compliance amongst SMEs
- (5) To consider the case for compliance, with an eye to the Commissioner developing and promulgating such a case to SMEs.

2.2 As well as the final report, the project team has produced additional outputs for the Information Commissioner:

- (1) Weekly progress reports summarising activities undertaken and work in progress
- (2) An initial discussion document based on the face-to-face interviews and the first 23 telephone interviews (“Data Protection and Small and Medium Enterprises: Points for Discussion from the Preliminary Face-to-Face Interviews”, February 5th, 2004)
- (3) An interim report providing an initial summary of analysis of the first 103 telephone interviews (“Data Protection and Small and Medium Businesses: Summary Report of Preliminary Findings from the First 103 Interviews”, March 8, 2004).

2.3 The final report addresses the aims and objectives laid out in the tender and tender specification. It also explicitly considers and addresses the three identified outcomes listed in 2.2 above.

3. RESEARCH APPROACH: PRINCIPLES, STRATEGIES & FRAMEWORKS

3.1 The research was based on three linked and sequential stages of research activity:

- (1) **Consultation** with SMEs and stakeholders in order to:
 - Understand in detail the issues and nature of perceptions and practices relating to data protection
 - Identify key questions and points to address
 - Build a preliminary insight into the SME context
 - Identify drivers and reasons for adoption of data protection practices
 - Identify potential barriers, hurdles and challenges to data protection compliance and good practice

- Identify and formulate questions to include in the survey
- Test and pilot the survey questionnaire.

(2) **Telephone survey** of a representative sample of SMEs, so as to:

- Develop a profile and representative cross-section of SME views on and attitudes to data protection and compliance
- Identify key issues to address, identified needs and priorities, and problems and barriers related to data protection
- Identify levels of intensity of application of and engagement in data protection practices
- Identify the perceived impacts and costs of data protection and compliance
- Identify positive drivers to engage in data protection.

(3) Focus groups and **consultation** with the Information Commissioner's Office in order to:

- Discuss the findings and their implications for adoption of data protection practices
- Consider and develop responses to key issues identified in the survey
- Identify strategies for compliance with data protection legislation
- Identify and formulate good practice in SME data protection activities and approaches.

3.2 **Initial consultation with SMEs and stakeholders.** The primary goal of these consultations was to develop a clear agenda, including the identification of (1) 'need-to-know' issues, (2) critical questions to address, and (3) a practitioner 'context' within which to consider the data and findings from the study.

3.3 **Telephone survey.** The telephone survey used a structured questionnaire mainly consisting of closed pre-set questions, i.e. questions where the responses have already been identified and are presented to the interviewee. The questionnaire was validated via: (1) follow-up with the businesses interviewed face-to-face; (2) its piloting with three businesses, and; (3) consultation with and feedback from the ICO. The questionnaire has four key sections:

1. Information About Your Business: basic data about the business and the respondent
2. Awareness of Data Protection and the Data Protection Act: awareness of the Act and data protection principles and how they might relate to the business
3. Your Views on Data Protection and the Data Protection Act: relevance of data protection principles, ease of compliance
4. Key Issues related to Data Protection: broader concepts and terms relating to data and information in SMEs, compliance issues and requirements.

3.4 **Consultations with the ICO.** Involvement of the ICO has been sought during the study, in order to ensure that the research related to identified concerns and questions.

3.5 **Data Analysis.** Quantitative data were analysed by coding through data entry into the SPSS data analysis software package, and then through the summary of (1) frequencies of response, i.e. overall levels of reply to questions, and (2) comparisons between responses. Comparative

'cross-tabulations' between responses were undertaken and only those with apparent significance or potential meaning are highlighted. Qualitative data were analysed via extraction of (1) quotations, (2) key themes and emergent issues, and (3) cross-referencing against frameworks and hypotheses identified in the original tender and via consultation interviews. Examples of extracted quotations appear as text boxes, interspersed throughout the report. Overall, the report combines quantitative and qualitative data and incorporates multiple forms of analysis in order to develop a clear and comprehensive account of the research and data analysis.

4. THE TELEPHONE SURVEY SAMPLE

- 4.1 The telephone survey involved interviews with 250 businesses in 9 English regions and in Scotland. The majority of interviews were undertaken with businesses in England.
- 4.2 The geographical distribution of the survey is broad (*see Annex 2*), ensuring that results are not based on particular regional characteristics or localised practices. However, the sample was not intended or designed to represent the overall geographical distribution of SMEs across either England or the UK for. The objective of the survey was to explore issues related to data protection and SMEs, and their implications for the ICO. The focus, as a result, has been on ensuring diversity and range in responses, rather than on developing a representative cross-section. The profile of surveyed businesses indicates sufficient breadth and coverage, based on multiple criteria, to demonstrate that a wide cross-section of SMEs is included and, as such, the results reflect broader trends across this size-group.
- 4.3 Particular geographic features of the sample are: (1) it has a high representation of businesses, compared to the overall population, in the Eastern region; (2) the South-East, including London, has a lower proportion of respondents than its respective share of the SME population; (3) there are no interviews with businesses located in Wales or Northern Ireland, and only two with businesses in Scotland. This reflected the nature of responses to the telephone survey, in particular regional response patterns. There is no discernible or identified reason not to expect results from the English regions to be relevant to conditions in Scotland and Wales.
- 4.4 In terms of sector (*see Annex 3 for categorisation method used*), there is a relative under-representation of public and other non-commercial businesses in the sample. This reflects the search criteria for businesses, which was based on identification of independent companies. The sample, as a result, is heavily dominated by the private sector. It also has a greater proportion of manufacturing and related businesses (around 35%, compared with a national average of just over 20%).

- 4.5 The reliance on Companies House data can also be seen in employee and turnover figures, both of which are relatively high for the SME sector as a whole. Employee size ranged from 4 to 300 (with some significantly larger 'outliers'), with the median lying at 80 staff and the mean at 95. Turnover ranged from £235,00 to £136 million with the median being £6 million and the mean just over £13 million (reflecting the 'upwards pull' of the outlying turnover figures at the top of the range). It should be noted that when the small number of 'outliers' are removed, i.e. businesses close to the top of the range in terms of employees and sales figures, average staff and turnover levels fell closer to (although still above) means across the population.
- 4.6 A particular feature of the sample is that there appears to be a relatively high-representation of businesses with a turnover of between £20 and £26 million and with 100 to 125 employees when compared with the UK population of SMEs.
- 4.7 Roles of respondents were spread across directors, managers and administrators. Most job functions of respondents were in finance or HR/personnel, reflecting the tendency for these two functional areas to manage data that is sensitive and requires protection.

5. AWARENESS AND LEVELS OF ENGAGEMENT WITH DATA PROTECTION

- 5.1 Virtually **all** respondents (248 of 250, i.e. 99.2%) had heard of the Data Protection Act (see *Annex 1 for a detailed analysis of the results relating to this section of the report*).
- 5.2 Most of the businesses thought that the Data Protection Act was relevant to their business (205, or 80.2%). Around 1 in 7(13.6%) thought it was not relevant.

"I knew about it when it first came out in the 1980s. There was a lot of publicity surrounding it then."

"It's common knowledge and there is a high profile attached to it within the company."

"I'm not sure where at first, but there's a lot of media publicity surrounding it at the moment."

- 5.2 However, actual levels of notification were significantly lower than overall awareness, with less than half (109 or 44%) indicating that the business had to notify/register.¹ Under half of all respondents (106 or 42.4%) indicated that their business had actually notified the Information Commissioner's Office.

- 5.3 There appear to be several reasons for this divergence between awareness and recognition on the one hand, and actual notification on the other. Some respondents indicated a need to check records to confirm whether the business had actually notified. In these cases, the company may have notified, but the respondent was not actively aware of this or had not done it themselves. Others expressed confusion about the meaning of the terms '*notification*' and '*registration*' in terms of compliance with the Data Protection Act.

¹ Note: Most respondents used the term *registration* rather than *notification* when discussing the Data Protection Act. Wherever this was the case, we have used both terms to highlight this finding.

6. RESPONDENTS' VIEWS ON DATA PROTECTION

6.1 Most respondents agreed that 'data protection principles are a good thing when doing business' (182/250, i.e. 73%).

Even more (80%) agreed 'absolutely' that their business should protect data and personal information. Only 8 of the respondents (3.2%) thought the principles were not a 'good thing'.

6.2 However, responses demonstrated some ambivalence about the Act, with respondents expressing concerns about: (i) the implementability of the Act, (ii) how to interpret it, and (iii) whether the Act actually encouraged businesses to fully embrace the underpinning principles (i.e. whether the

process of compliance took the business focus away from the principles and placed it on the mechanics of notification).

6.3 Responses were mixed as to whether data protection principles could 'help or hinder' the business. Around one-third of respondents indicated that the principles would help, and overall more than half saw them as beneficial (56% reported they would "help" or "a bit of both, but more help than hinder"). Just over a third (34.4%) indicated that data principles both helped and hindered, i.e. a "bit of both".

6.4 There was little indication by the respondents that they saw the Data Protection Act as constituting a major compliance 'burden' for their businesses. Most indicated that compliance was not a major effort or challenge for the business: almost one in four (24%) considered it "very easy" and more than half (51.6%) either "quite easy" or "a small effort". Most respondents, therefore, did not consider compliance a "large effort." In fact, only around 10% considered it "a large effort" or "almost impossible".

"I think that private and personal things should always be kept confidential and be available only to certain people."

"Most people are concerned about information that organisations have about them. It is appalling that this information is sellable. Many application forms do not take the Act into account."

"It is important that personal and private information is maintained in confidence. Therefore, I fully agree with the principles. Now that compliance has been sorted within this company, it is easily workable."

7. KEY TERMS AND CONCEPTS

“It is the company’s duty and mine to maintain confidentiality at all times. This would happen irrespective of the Data Protection Act.”

“The security of data is like a safety net – confidentiality puts people at ease, especially if they know information about them is secure.”

“If we are handling sensitive data then I would be duty bound to protect it. I wouldn’t want my personal info in the hands of the wrong people, and I wouldn’t want my staff’s either.”

7.1 Three key terms registered most strongly with the respondents: (1) Confidentiality, (2) Security of Data and Information, and (3) Privacy. All three terms were frequently ranked as ‘most appropriate or familiar’ (on a scale of 1 to 4, with 1 being most important). Information handling and information risk – terms that were identified in the face-to-face interviews – were not deemed of particular

significance by the telephone respondents. To some extent, information handling and information risk were perceived as more abstract concepts that were more difficult to apply to a business context.

Table 1: Key Terms Ranked by Respondents (prompted)

Key Word	1	2	3	4	# Responses	‘Score’ ²
Confidentiality	185	37	7	8	237	1.32
Data/Information Security	181	39	14	7	241	1.37
Privacy	175	45	12	6	238	1.37
Data Protection	120	67	29	19	235	1.77
Data Sensitivity	129	44	32	29	234	1.83
Information Handling	89	60	42	44	235	2.17
Information Risk	67	55	44	56	222	2.40

7.2 Data protection as a term received a relatively high score indicating the high level of overall importance placed on it by the respondents (an average of 1.77 out of 4, with 1 being the highest). However, the number of respondents allocating the highest level of importance to this term (a ranking of 1) was significantly lower than overall rankings of the three ‘most important’ terms.

“I think the principles behind it are very sound, but as with many things the difficult part is putting the theory into practice.”

“Due to the nature of the business we hold data sensitive information.”

Overall, less than half of the sample ranked the term ‘data protection’ as most important, and

² ‘Score’ = a weighted mean. For example, where responses of 1, i.e. considered most important, this answer was rated a value of 1 also. Where a rating of 4 was given in interview, this answer was rated a value of 4. This rated value is multiplied by the number of responses to the question. The results are added together, and score figure is calculated which shows the mean of these values. Thus the lower the answer, the higher the rating of importance of the term.

almost one-fifth ranked it as relatively unimportant (a 3 or 4 ranking). There appear, therefore, to be two types of response to the term Data Protection: (1) recognition of the term as significant, by just under half of the sample, (2) a lack of recognition or high ranking of the term by a minority of

“We hold a lot of data sensitive information about customers. They need to know this information is secure and confidential. From a marketing perspective, being a trustworthy company is at the heart of a business’s branding.”

the respondents
(around 23%).

- 7.3 Assessments and considerations of key terms focused on, and were defined by, business drivers and priorities - i.e. by the use and application of information and data for the business and by the business.
- 7.4 Key terms such as confidentiality and data and information security were defined in terms of how they can help the business to compete and secure competitive advantage (see text box above, which sees confidentiality as an important means of gaining customer trust and loyalty).
- 7.5 Data protection was seen in terms of security and protection of records and data needed by the business in order to function, rather than as an issue or concern relating to individual rights. Although a business-focused view held across most of the sample, there were some exceptions: “It is a good moral thing which I am happy to comply with and guide others...but, a freedom of information act would help society too.”
- 7.6 Two terms were singled out as particularly significant: Confidentiality, and Security of Data and Information. Both terms were associated with: (1) how the business protects the data it needs to manage itself and to operate, and (2) how the business treats information and data to gain competitive advantage, in particular in terms of overall reputation and in securing new clients and continued loyalty. Considerations of data and information are not only influenced by but also are fundamentally determined by the needs and concerns of the business itself. Indeed, this is the key driver for most of the interviewed businesses, rather than a concern with personal rights.
- 7.7 It should be noted that very few respondents from the total interviewed actually identified a significant Issue (only 70, or 28% of the 250). The figures in the table below under *Most Significant* indicate the number of responses. The % figures are percentages of the 70 responses to the question, not of the 250 total (*See Table on following page*).

“We have to be very careful with the databases that we use and ensure that they are kept confidential at all times – it would be damaging to our company if they fell into the wrong hands.”

“We hold a lot of information. We have to ensure confidentiality and maintenance of this information.”

“If applied in the correct way, the DPA leads to added security and confidentiality of information. This is becoming more important now that computers are being used so much more and such a vast amount of information is being held electronically.”

Table 2: Terms Ranked as Most Significant

<i>Key Word</i>	<i>Most Significant</i>	<i>%</i>
Confidentiality	27	38.6%
Data/Information Security	21	30.0%
Information Handling	6	8.6%
Privacy	5	7.1%
Information Risk	5	7.1%
Data Protection	4	5.7%
Data Sensitivity	2	2.9%
Total	70	28.0%

7.8 **Information Risk** relates to the management of information and data during the creation, processing, transport and storage of data within the information lifecycle. Risks include the physical and electronic security of data maintained by the company or other third parties.

“I don’t think effective information and data management would benefit business – I think it would help boost the confidence of the people working in that business and that’s more important.”

“I guess the benefits of effective information and data management would help keep things secure, and stop the risk of leaking information.”

“Info should be accurate, up-to-date and secure.”

Although half of the SMEs interviewed acknowledged the importance of information risk (when prompted), 41.7% felt that information risk was a moderate or low consideration in managing data. A small number of SMEs (7.2 %) suggested that information risk was not meaningful to their business or operations. When questioned in more detail some respondents suggested that information risk was hard to quantify due to a lack of

performance measures and means of monitoring risk. There is some indication that there is a low awareness of what risk means in relation to managing data and information within SMEs: “I’m sorry I need 5 minutes to think about this question - what’s the next one?”

7.9 **Information Handling** involves receiving, transmitting, disseminating and distributing

“Information is key to business – so handling it is vital. As is improved communication and productivity through having effective systems.”

information and data between organisations and systems. The results show a high level of procedural awareness, with 61.8 % of survey participants indicating that information handling was a critical factor within their

respective businesses. Little evidence could be found to support the statement that information handling was not meaningful, although there are indications that information handling was not deemed particularly important. It also appears that some SMEs made value judgements on what constitutes primary and secondary business data. One respondent said: “...for primary data we have good procedures and systems.” A key issue around information handling is the amount of data that is collected and the means by which those data are stored and retrieved.

The majority of SMEs that participated in the study had invested in IT systems, which made data management easier.

7.10 **Data Protection:** A small minority (3.3%) felt that data protection was not meaningful. However, 77 % agreed that data protection was important to their business and that the practice provided them with credibility to their customers: “...being able to manage customer information is paramount to the operation of the business and also maintains the appearance of being professional.”

“It’s part of our day-to-day business practice. We’ve always applied data protection principles.”

“The principles are always needed to a degree and they work in favour of the business, though they can hinder in some instances.”

“I don’t actually understand what it [DPA] is supposed to do – what is data? Can they accurately define it for me? Who cares? Bureaucratic nonsense.”

7.11 **Data Sensitivity:** There is a strong correlation between those SMEs that responded positively to the key words Data Protection and Data Sensitivity. In reviewing the responses, there is

“The information that is protected under the DPA is sensitive, and our business depends on us keeping that kind of information confidential.”

evidence to suggest that many SMEs subscribe to the idea of data sensitivity, and that this awareness is more prevalent within those business sectors associated with financial services, legal, car dealerships and travel

services. A small minority (3.7%) considered data sensitivity not meaningful. It could be argued that the function of data sensitivity is to some extent encapsulated within the policies and procedures employed within individual SMEs. The smaller the SME, the more likely that these policies and procedures are less developed: “it would help if we had supporting policies and procedures.”

7.12 **Security of Data and Information.** Data integrity exists when data is handled as intended and is not exposed to accidental or malicious modification, destruction, or disclosure. Data is entered using formal business rules, and accuracy is checked using automated edits and manual reviews.

Of the 250 SMEs interviewed, 225 (90.5 %) believed that security of data and information was important to their business operations. Those ranking this attribute lower at 3 or 4 accounted for 8.7 %. There appears to be a strong bias to protecting data and this is reinforced through the qualitative statements of respondents.

Irrespective of the type of business there is a strong awareness amongst SMEs of personal information, although respondents’ definitions did vary. Key issues around security were focused on accidental loss, abuse, disclosure and ethical use of personal

“Ensuring that all the data we hold is secure is quite time-consuming.”

“It is important in maintaining the security of information – both computerised and paper-based.”

information. Some of the respondents acknowledged that data does go missing and abuse is some times difficult to police: "...Databases can be misused if they fall into the wrong hands – people can appropriate information from their companies and use it illegally."

- 7.13 **Privacy and Confidentiality** are defined as the legal rights of the subject (that is person) to be protected from malicious damage and to preserve their statutory rights under the DPA.

There is an identifiable relationship between security, privacy and confidentiality – so not surprisingly the results for privacy and confidentiality are strongly correlated. Of the 250 SMEs interviewed, an average of 228 respondents (91.2 %) agreed that privacy and confidentiality were important to their clients and business operations.

Based on the qualitative statements, two issues dominate: (1) invasion of privacy and (2) violation of the individual rights under the act. Although the majority of SMEs acknowledged the importance of confidentiality a very small number of respondents felt that privacy was not meaningful.

8. COMPLIANCE WITH THE ACT: REQUIREMENTS, ISSUES AND DEMANDS

- 8.1 Respondents, on the whole, did not consider that compliance with the Act constituted a heavy or major 'regulatory burden'. Overall scores for compliance requirements were relatively low, i.e. no compliance requirements 'relevant to the Data Protection Act' were considered of great importance (with most around a value of 3, i.e. not particularly important).
- 8.2 The level of response was sufficiently high to reinforce the finding that compliance is not a major issue for the Data Protection Act (216 of 250 interviews did not consider compliance requirements to be an issue).
- 8.3 None of the compliance requirements were identified as a 'burning issue', i.e. as a significant concern or problem by a large proportion of the respondents. Indeed, only 36 of the 250 interviewees identified a 'burning issue' related to compliance. Amongst those that responded, moreover, only one issue, namely 'Identification of Data Held, appeared to be significant (21/36 responses, or 8.4% of all respondents).

Table 3: Ranking of ‘Compliance Requirements’ for the Data Protection Act

Key Word	1	2	3	4	#Responses	‘Score’ ³
Identification of data held	52	47	39	92	230	2.74
Effort to modify existing systems	41	51	55	88	235	2.81
Time to find out how to comply	33	52	42	89	216	2.87
Need to create new systems	27	49	44	107	227	3.02
Monetary cost to comply	31	43	45	116	235	3.05
Time to register/notify	15	33	42	103	193	3.21

8.4 Although the majority of respondents did not associate the Act with a high level of ‘red tape’ and ‘regulatory burden’, there was a small group of businesses that viewed compliance as a major issue. This ‘vocal minority’ associated adherence to the Act with concerns over government intervention and compliance burdens. These contrasting views can be summarised in the quotations in the following two text boxes:

Against Compliance

“It is something like a ‘necessary evil’ – so a bit of both, but not one more than the other. It’s the same with all legislation.”

“Again, it’s a government body. Useful in parts, but you’re forced to abide by it, so I’m sure it hinders too.”

“It’s major bureaucracy. It’s like a sledgehammer to crack a nut. What is data?”

Not Concerned About Compliance

“It encourages us to operate at high standards which in turn attracts customers and improves their confidence in us.”

“It ensures data is maintained and managed correctly. This has a positive effect on the company’s reputation.”

“It helps to define the guidelines within which we can operate.”

8.5 **Monetary Cost to Comply.** When asked to rank the importance of cost to comply, 166

“Costs are unnecessary if you’re careful. It’s a matter of balance.”

“It’s not costs you should think about – it’s more of an investment [DPA compliance].”

“There are minimal costs as the procedures are in place. There is a small registration fee”.

respondents (66.5 %) suggested that the monetary cost of compliance was “not significant” to their business. Some 77 (30.6%) SMEs considered the cost of compliance significant, but only one SME considered it to be a burning issue. Those SMEs that considered the cost significant were in the main removed from the financial operations of the business and to some extent they associated the cost of

compliance with the volume of paper work they were processing during the day-to-day operations of the business.

³ Refer to footnote 1, page 9

- 8.6 **Time to Register/Notify the ICO:** 152 respondents (60.7 %) said that the time taken to notify the ICO was “not” an issue. Fifty respondents (20.1 %) did, however, feel it was. When asked why, a number felt that the notification process was complicated and that the “Help-Line” could be more helpful. Some respondents had difficulty understanding the process, and 15.1% felt that the process was not meaningful to their business operations.

“Once registered it is no problem at all. When you’ve established the DPA in your business then it’s easy – but it’s hard at first.”

“The principle is fine – it’s the registration that’s horrendous. Have you ever seen the registration document?”

- 8.7 **Time to Find Out How to Comply.** Just over half (54.6 %) felt that the ICO publicised its services well and that its web site was informative. A number of SMEs (35.4%) held the view that there was an issue in finding out how to comply. This opinion tended to be held by participants working in smaller businesses with fewer than 20 employees.

“Data protection is a good idea – absolutely essential. But I have 1½ inches of paper on my desk about the latest edition. What a waste of trees and time.”

“It is time consuming.”

- 8.8 **Effort to Modify Existing Systems.** Some 59.1% of respondents suggested that little or no effort was required to modify their business systems to accommodate the compliance aspects of the Act. In fact only 2 of the SMEs that participated considered it a burning issue. Although 38% of respondents did suggest some effort was required, when asked to qualify their response most of them were hard pressed to say why. Many of the qualitative statements by interviewees support the view that many SMEs have adequate systems and better than average policies and procedures for satisfying the compliance aspects of the Act (*see text box below*).

- 8.9 **Need to Create New Systems.** Many of the SMEs interviewed (62.9%) felt that their existing systems were more than adequate to cope with the information processing demands placed on them in their day-to-day business operations. Those that didn’t (31.7% or 79/250) operated a number of manual and electronic systems, which tended to be work-intensive and to some degree involved tasks outside the immediate scope of compliance. As such, having user-responsive information systems is a key factor in managing the audit requirements for compliance.

“We are registered, the systems are in place. Hopefully we can’t go wrong!”

“Well to comply, we had to put more things under lock and key – create passwords, new files, new access rules etc. It was sensible and relatively easy.”

“We have our routines in place – it should be part of your working practice.”

Having appropriate policies and procedures to support the information processes helps to improve perception and productivity. The more sophisticated SMEs used web technology to offer online assistance to their staff and customers: car dealerships, for example, seemed to have sophisticated online data and information systems.

8.10 **Identification of Data Held** was ranked as the most “burning issue” by SMEs. Responses

“Nobody is clear what we can and can’t use our base information for. We are afraid to ring up and ask for guidance in case we may be doing something wrong.”

“The company holds much personal data and financial information about employees and customers – there are vast amounts of this kind of data.”

“[*The DPA tells us that*] We have to destroy documents after 6 years.”

from the interviewees indicated that this related to the wider challenge of effective data management. The high volume of personal data generated and held over long periods (up to 30 years in some instances) is a problem for many. More than half (53.3%) of the sample said that they have problems in identifying what data to retain.

For many responding SME managers, compliance with the Act appeared to mean finding a balance between providing easy access to the right information, and

establishing the necessary preventative measures to maintain the integrity of the data held.

9. BEST PRACTICE PATTERNS AND TRENDS IN CURRENT DATA PROTECTION

9.1 Best practice in data protection and in information management, as well as in terms of compliance with the Data Protection Act, was identified in many of the businesses interviewed (both face-to-face and by telephone). In particular, three primary themes or areas of effective practice can be identified:

1. Company activities and systems enable data and information handling and management, in multiple and reinforcing formats.
2. Management and handling of information is seen as central to the business and its competitiveness, i.e. data sits at the ‘heart’ of business activities and processes.
3. There are shared values that recognise and promote data and information as central to the business and to effective management.

9.2 ***Company activities and systems enable data and information handling and management, in multiple and reinforcing formats.*** To a great extent, this aspect of effective practice focused on the formalisation of particular activities to support data handling and information management. Examples cited by the respondents included:

- The provision and availability of training that covered the Data Protection Act (specifically) or information and data management (more broadly). The training was both ‘in-house’, i.e. offered to company staff only, and external. In-house courses tended to focus on managers in some companies, but extended to all staff in certain cases – often in businesses that were particularly reliant on data or that operated in a sector, profession or business that had specific data handling practices and regulations.

“I need to know more about the DPA. As it happens though, I am going to a seminar on this very topic next week.”

External training typically consisted of programmes related to accreditation such as CIPD awards, and so included data protection as a component or module within a wider course.

- The business circulated documentation, typically in the form of circulars or newsletters, to staff reminding them of their Data Protection obligations. These communications were internally produced or were received from external sources and then disseminated within the company. In both instances, there tended to be a focus on ensuring regular distribution and dissemination of news and information to staff that extended beyond data protection issues, i.e. there was a general pre-occupation with circulating information within the business that incorporated this issue.

“Various sources, including the staff handbook. A handout from this explaining how personal information is to be handled is given to all staff. Also, websites – ACAS, CIPD. An academic course I am studying on (CIPD degree).”

“There has been a great awareness within the company for many years. We were one of the first to register with the ICO.”

- Clear and available procedures and policies were shared and understood by staff. In these businesses, there was explicit guidance on data protection that was available. This guidance was either actively circulated to staff or there was clear indication as to where to find it (and in some cases who to contact).
- There was a high level of embedded and accumulated knowledge, based on experience, within the business. In many of these cases, compliance with the Data Protection Act was considered an automatic and typical business activity, i.e. there was no confusion as to how to perform this task. There were also cases where the responsibilities of the respondent who was interviewed were based on data handling and so protection and related issues were an integral part of their job and role.

9.3 **Management and handling of information is seen as central to the business and its competitiveness.** Businesses that identified data protection as a positive contribution to

“Because as we stand we are protecting information anyway. The Data Protection Act shadows and backs this up.”

“All it involves is filling out a form and sending a cheque once a year. Quite easy, really!”

business practice and that did not associate it with a compliance burden tended to be effective and systematic managers and handlers of information and data.

These businesses tended to be compliant with the Act as a result of their internal systems and management approach,

i.e. notification occurred and was made easy as a result of how the business used data and information. These businesses, in other words, saw effective information management (which includes data protection), as good for profile and reputation, as well as a source of greater efficiency and capability.

9.4 **Shared values that recognise and promote data and information as central to the business and to effective management.** Businesses demonstrating good practice in data protection and adherence to associated principles, articulated explicit and strong values towards the role and use of data and information in and by businesses, including:

- A general acceptance of the need and benefits of data and information management
- Sympathy with the concepts of personal confidentiality and privacy (and to a lesser extent broader notions such as freedom of information and human rights)
- Associating data protection with the self as well as the business
- Responding to the Act in a pragmatic way
- Open-minded about the Act as legislation
- Able to relate compliance and use of data protection principles to benefits for the business.

9.5 Many of the businesses involved in the interviews demonstrated aspects or degrees of best practice (as outlined above). There appears to be some engagement with data protection by businesses. However, few businesses demonstrated effective practice ‘across the board’, suggesting that most businesses – even those with good practice – can develop and improve. Good practice, as such, appears to be a development framework and spectrum that can apply to most, if not all SMEs.

“Although the context of the DPA isn’t relevant to us, I would say that good practice in organisations has got to be beneficial, especially in terms of operating.”

“Effective data and information management is a prerequisite of all good businesses.”

“The DPA helps maintain good working practices.”

10. IS THERE A ‘BUSINESS CASE’ FOR ADOPTING DATA PROTECTION PRINCIPLES AND COMPLYING WITH THE ACT: EVIDENCE FROM THE BUSINESSES

“Effective data and information handling and management are critical to businesses. We have spent a lot of money on updating systems recently. The benefits are improved efficiency in order to operate better.”

10.1 Many respondents associated data protection and information handling practices with effective management of the business, and so agreed that there is a broad ‘business case’ to adopt these principles.

10.2 However, the responses were general rather than specific, and related to the overall implications and outcomes for the business.

10.3 Most of these broad affirmations focused on the benefits of improved and effective information and data management to the business, and considered data protection principles as an aspect or ‘sub-set’ of this wider notion.

10.4 Some respondents identified specific benefits and these can be summarised as follows:

- Able to identify data held by the business
- Ease of access to data held
- Ease of retrieval of data
- Improved organisation and 'house keeping' of information
- Removes or reduces duplication of data
- Ensures and enables data consistency and integrity
- Ensures data accuracy and/or reduces data error
- Generates dependable historical records
- Identifies levels of confidentiality and security of data
- Identifies means of improving data confidentiality and security
- Identifies communication needs and requirements
- Enables improved communication of organised and accurate data
- Identifies means of improving 'handling and processing' efficiency
- Enhanced data quality and availability enables and supports decision-making and management judgement.

10.5 There was some indication that presenting the business case was, for many of the respondents, 'teaching to the converted', in that businesses that embraced data and information saw the benefits clearly and could relate them to competitiveness and performance. Businesses that did not see the value of data and information were less likely to accept the broader business case.

11. ANALYSIS OF POSSIBLE RELATIONSHIPS AND ASSOCIATIONS

11.1 Responses to the survey were first compared using frequency tabulations (see Annex 1) and then via the 'cross-tabulation' of different questions. By comparing questions using cross-tabulation, more detailed breakdowns and distributions of responses were identified. From this, relations and causal relationships could be identified as well as unexpected or unusual findings. A detailed analysis of relevant and significant cross-tabulations is attached as Annex 4 to this report. Table 4 (*next page*) summarises the key findings from the cross-tabulation analysis.

11.2 Overall there is strong support for the principles of data protection. There is also some acceptance of the Data Protection Act as a credible and necessary form of legislation. The data protection principles were still considered good by those who did not view the Act as relevant to their business (*see statement 2, Table 4*). The 'case' for data protection practices to be adopted appears therefore to be accepted by the interviewed SMEs, suggesting that there is 'buy-in' to the underpinning concepts.

Those who accepted the 'case', tended to suggest that data protection helped their business, that businesses should protect data and personal information and compliance requirements were fairly effortless. "Making the case" for Data Protection, therefore, would not appear to be of great importance to those respondents who embraced the importance of information and data management and use in the business.

11.3 Respondents that agreed with and considered data protection relevant to the business tended not to consider the Act as a major piece of legislation that is difficult to comply with. Instead, acceptance of data protection principles appears to reflect a perception that compliance is either easy or not a major concern (see *statement 6, Table 4*). This may be a reflection of a belief or view within these businesses that systems are already established that support the notions of data protection principles.

11.4 There appears to be some evidence for the reverse: respondents who did not accept the relevance of data protection tended to consider it a greater compliance 'burden'. In these (far fewer) cases, considerations such as 'time', 'cost', 'establishing systems' and 'effort' were valued as more important.

11.5 There is some indication that respondents who were positively aligned with or towards data protection did not see information management and the development and modification of systems and approaches as a major concern or constraint. The telephone responses and the face-to-face interviews identified a group of 'information embracers', i.e. businesses that see information and data as key to the management and development of the venture. These are businesses that have effective and adaptable information management and control systems do not have difficulty with compliance and tend to accept the data protection principles and values.

11.6 Overall, the cross-tabulations supported the broad conclusion that 'data protection' is, on the whole, seen as positive - particularly when couched in business terms. They also suggest that

"I don't wish to be constrained by the Act. I know how to use data already. But saying that, I can see its value"

the relationship between actual business compliance and perceived 'regulatory burden' was not fully established, and that decisions to notify were not based on perceptions of the ease or difficulty of meeting the requirements for notification.

The principal finding supported from the cross-tabulation is that acceptance of the principles does not lead inevitably to notification, i.e. to compliance with the legislation. As such, the analysis suggests that for many of the respondents "*data protection is fine in theory but not always in practice.*"

Table 4: Summary Statements derived from Annex 4 Cross-Tabulations

1. Of those who said they believed they had to register with the ICO as regards to DP, 94% also said that they actually were registered.
2. Of those who said they believed they had to register with the ICO as regards to DP, 81% believed that the DP principles were a good thing when doing business. Of those who did not believe that they had to register, 74% still believed that the DP principles were a good thing.
3. Of those who said they believed they had to register with the ICO as regards to DP, 88% believed that they should 'absolutely' protect data and personal information.
4. Of those who considered the DPA as relevant to their business, 78% also considered the DP principles as a good thing when doing business.
5. Of those who considered the DP principles as a good thing when doing business, 92% also said that their business should 'absolutely' protect data and personal information.
6. Of those who considered the DP principles as a good thing when doing business, 50% considered the monetary cost to comply as of very little importance.
7. Of those who said that the 'effort to modify existing systems' in order to comply was of little importance to them, 76% also said the same of the 'monetary cost to comply'.
8. Of those who considered the 'time to find out how to comply' with the DPA as of little importance, 70% also placed very little importance on the 'effort to modify existing systems' and 76% also considered similarly the 'need to create new systems', in order to comply.
9. Of those who considered the 'security of data and information' was very important to them, the term 'information risk' had little overall value, with 36% saying it was very important, and 25% saying it had very little importance.
10. Of those who considered the term 'data protection' as very important to them, 95% also rated the term 'privacy' as of equal importance.
11. Of those who considered that the 'security of data and information' was very important to them, approximately 90% also considered both the terms 'privacy' and 'confidentiality' as very important too.
12. Of those who said confidentiality was of significant importance to them, 89% also said that they believed that their business should protect data and personal information.

12. IMPLICATIONS 1: BEHAVIOURAL AND ATTITUDINAL RESPONSES TO DATA PROTECTION AS A KEY DETERMINANT OF PRACTICE

12.1 How respondents perceived the use of information within their business correlated with views on data protection and the Data Protection Act. Where respondents reported a high level of understanding and use of information and data in the business, awareness

"The company has an 'open-book' policy: it is very open with the ICO about the data it holds, and is likely to hold in the future. This makes compliance very easy."

"As far as the Act is concerned, the company has no problem in terms of data storage. The computer systems are very capable as the company has a great deal of IT expertise."

"All our systems are 'in-house' and established. The public cannot access the information on them, so it is easy to comply with the DPA."

of data protection principles and techniques tended to be high. Typically, these businesses did not consider notification to be a major regulatory burden and often noted that they were essentially compliant without notification because of their own systems and procedures.

“I believe it’s a waste of time, as no company will ever truly comply.”

“I haven’t had the chance to consider the Act and it’s implications yet. Too busy dealing with other legislation more relevant to the business, e.g. in relation to weighing and measuring.”

12.2 Conversely, businesses that were not aware of the Act or did not believe that it related to their business tended to view it more as ‘red tape’ and were less likely to place information management and data at the heart of the business.

12.3 As such, approaches to data protection, and the Data Protection Act, appear to be linked with broader attitudes towards how the business is managed, and in particular, the role and function of information and data. In cases where this correlation exists, data protection practice as well as compliance with the Data Protection Act can and do arise because of management approaches and attitudes.

12.4 Compliance and engagement with the principles therefore, do not necessarily or always occur because of or as a result of interaction with the Act or with the ICO per se. Instead, such interactions can be seen as an aspect of the business’ attitudes towards using and managing information and data.

12.5 A key conclusion arising from this observation is that the ICO can enable data protection by engaging with and focusing on broader behaviours and attitudes relating to how the business is managed and, in particular, how it deploys and uses data and information.

13. IMPLICATIONS 2: SEGMENTING THE SME MARKET BY RESPONSE PATTERN

13.1 One way of engaging with SMEs in terms of their approach to data and information management is to segment by apparent or revealed behaviour, much as consumer market research develops distinctive customer profiles based on purchasing patterns and preferences.

13.2 **Information Embracers.** Our findings indicate that there is a group of businesses that embrace information and consider it as fundamental. This category is made up of two segments, each with their own distinctive characteristics:

“The company needs to ensure that there is no inappropriate disclosure of information relating to it’s employees / suppliers / subcontractors / customers. Much of this is very sensitive information that would give other businesses competitive advantage”

Information ‘Champions’: businesses that develop and adopt innovative and leading edge approaches to data management as a matter of course. Information champions have well-

established and intensively-used information and data management and handling systems and strategies, and tend to view information as of central importance and a primary source of competitiveness. Businesses like this made up a small proportion of our sample.

Information Consumers, i.e. businesses that operate in environments that are information-rich or that demand that businesses are information-aware. Information consumers understand and

“We hold a lot of confidential information: personnel records, customer and supplier information. Without confidentiality of this information the business could not function, as electronic transfer of information is key to this business.”

engage in information management and data protection because it is intrinsic to or necessary for the operation of the business.

Examples of information workers are businesses that: (1) manipulate information and data (e.g. research companies, information and data processors); (2) base their ‘offer’ on information that is generally confidential or sensitive (e.g. accountants, solicitors); (3) generate and base themselves on proprietary knowledge or information (e.g. technology-based businesses).

- 13.3 Businesses that notified the ICO (42.9%) tended to display some or many of the characteristics of either *Information Champions* or *Information Consumers*, that is they were information sharers that demonstrated the following attributes: forward thinking management; able to plan for change; good IS strategies; good internal channels of communication; well publicised policies and procedures; good staff relationships; champions or appointees to notify.

From the qualitative statements made by respondents, there is strong evidence to suggest that this group has very positive attitudes to legislation and its impact on business performance and plans accordingly for change. This group also sees business opportunities in compliance and promotes registration positively with its customers, clients and other stakeholders.

“The DPA is relevant to all businesses in terms of information held about employees and customers.”

“We work with data constantly – we need to abide by the DPA.”

- 13.4 **Reluctant compliers.** The ‘vocal minority’ of businesses that perceived the Data Protection

“I think that it’s a lot of rubbish really – it just gets in the way.”

“I have no problem with the Act itself, but I do have a problem with the bumf connected to it. It is just too much to comply with easily.”

Act as regulation and hence as ‘red tape’ tended to be less positive about data protection, in part because they associated the principles with the legislation. These businesses complied, but tended to see compliance as an additional business cost and, for some at least, as a distraction or unnecessary allocation of time and effort. Often, reluctant compliers appeared to have preconceptions and fixed views as to the Data Protection Act and its relevance.

13.5 **Reluctant compliers** tend to do only what is necessary in terms of compliance. They are often less developed in terms of their management and information systems and tend to have some or all of the following characteristics: as ad-hoc processes, few formalised procedures, no data champion, few or no information tracking procedures, no formalised information strategy. This group sees the ICO as ‘another’ government department with a remit to raise money or to impose restrictions on business practices. This group also places reliance on individual knowledge and often does not share knowledge explicitly within the business.

13.6 **‘Users in principle, but not in practice.’** A group of businesses agreed with data protection in principle and had heard of the Act, but did not see a need to comply and had not notified the

“The Act doesn’t really have much impact on the way the business is run, as we are already adhering to guidelines and principles irrespective of the Act.”

“It is a waste of time – people would be better off using their common sense.”

“The principles are good – there’s merit in the arguments for the DPA, (from my limited understanding) but how widespread do you throw the net? The application to all businesses of the DPA is questionable too. It’s the whole Big Brother thing.”

ICO. These businesses appear to accept the principles associated with data protection and information use in the business, but do not appear to have complied with the legislation.

13.7 SMEs that fall within this group are aware of and often appreciate their obligations under the act and in the main are information aware and information literate. However, they have not translated this into active engagement with

either the Act or, to a lesser extent, with data protection principles. A sub-set of this group see compliance with the Act as of little relevance or importance and tend not to know about the ICO.

13.8 **The ‘Unaware’.** A small group of respondents either indicated that they were not aware that they had to comply with the Act or believed that their business did not need to notify the ICO. Some of these businesses lacked information or knowledge about the Act (*see text box*). Others recognised the importance of the Data Protection Act, but indicated that it was not relevant to their own business (*see text box*).

“Is it going to be legislation eventually? What I mean is, I know it exists, but the requirements aren’t forced upon us at the moment. I think it will affect us in 2007 or something.”

“We don’t hold the relevant range of information in order to qualify for registration.”

“We have no data that we store or keep hold of! No personal information here.”

13.9 SMEs falling into this category employed small numbers of people and did not have sophisticated management and control systems. Employees typically covered more than one role or area of responsibility. Few SMEs within this group seemed conscious of what information was available and in some cases lacked the ability or motivation to gain such information. Characteristics displayed by this group include: poor quality systems, little access to external sources of information and a tendency to be reactive to situations.

13.10 The identification of segments differentiated by attitudes and behaviours provides an opportunity to develop tailored strategies for engaging with different segments. Awareness-raising documentation and communications can be designed and developed to attract and focus on specific segments, as can support documents and guidance. Here then, there may be an opportunity to develop a portfolio of documentation, guidance and marketing activities that are distinguished by segment.

14. IMPLICATIONS 3: IDENTIFYING AND FORMULATING GOOD AND BEST PRACTICE IN DATA PROTECTION

14.1 Respondents were able to (1) associate adoption of data protection principles with best practice, and (2) identify broad benefits from effective management and handling of data and information. However, there was only partial indication of the actual practices and strategies developed and adopted in order to follow these principles and achieve such benefits. This suggests a 'need-to-know' more about the actual practices undertaken by businesses that constitute good and best practice.

Some businesses were also keen to find out more about good and best practice in *other* businesses, in order to 'learn' from the experiences of others (See *text box*).

"Basically, once you're registered and paid, why do you have to pay again annually? I'd be interested to know what cases of prosecution and contravention existed"

"It is a good moral thing which I'm happy to comply with and guide others. I ask others to consider it with a 'common sense approach' in the context of 'how would I like my data to be handled and used?'"

14.2 The attitudes of those within the business, and how they translate into actions and behaviours, appear to drive and reflect good practice. Businesses that believe in and support data and information management as a priority tend to be effective in these practices (and so can provide benchmarks for the SME 'sector').

14.3 In addition, the 'entry point' or 'lever' in terms of encouraging businesses to develop good and best practice around data protection appears to focus on information management and the extent to which it is deployed and harnessed for business advantage. A broad implication is that the articulation of the case for data protection, typically incorporated into wider concerns with data management and information handling, can be made effectively by demonstrating advantage to and benefits in other businesses.

15. IMPLICATIONS 4: THE PROFILE OF THE ICO

15.1 Many respondents indicated that the ICO did not have a strong profile with SMEs and that there may be advantages in taking a more active role of public leadership in promoting and articulating the importance of data protection and how to comply with the Act.

These businesses suggested additional and wider awareness-raising and information dissemination, and

indicated that there were four primary areas where more communication may be useful or beneficial:

1. Enhancing the profile of the ICO itself, so as to provide greater awareness of data protection and information issues as a whole and also in order to offer businesses a contact point that is known to them.
2. Develop useable and user-friendly documents that can be made widely available to businesses, including 'how-to' guides, examples, and templates to complete.
3. Raising awareness with businesses of data protection issues and principles, mainly by 'establishing a dialogue' with businesses directly.

"I think the Information Commission should provide a straightforward booklet or CD that would cover typical business scenarios and have simple tick box flows."

"By raising awareness, particularly with smaller companies, about compliance requirements. Information is available if you look for it, but many companies don't know where and how to access it."

15.2 **Should the ICO develop a stronger profile?** Although explicit suggestions were made to

"The ICO should advertise better. You should have the ICO as the top hit when you do a Data Protection Act search on the Internet. This may reduce the risk of falling for scams."

raise the profile of the ICO, there was no clear consensus from a majority of respondents that this was desirable or advisable (nor was there indication that it was not). Given the broad nature of the comments on the profile of the ICO, the feedback probably does not constitute sufficient grounds

in themselves for action. They do, however, suggest that the public profile and hence 'market positioning' of the ICO in relation to SMEs may be a point for future consideration.

16. CONCLUSIONS AND OBSERVATIONS

Conclusions

16.1 Primary findings from the study have been highlighted throughout the report, and can be summarised as follows:

- There is a high level of awareness of data protection and the Data Protection Act
- There is broad acceptance of the values and principles of data protection, although opinions appear divided as to the benefits of compliance
- Awareness and acceptance of principles in broad terms does not necessarily translate into specific knowledge of registration/notification
- The compliance or 'red tape' burden associated with government regulation does not appear to be a major issue for the Data Protection Act for most of the business, although there is a small 'vocal minority' who consider this an issue
- Two key terms registered most strongly with the businesses (1) Security of Data and Information, and (2) Confidentiality. Privacy also figured as a significant term, but not to the same extent
- Effective practice in data protection was closely associated with wider information management and data control within the business – those enterprises that deployed information for business benefit tended to be actively supportive of data protection principles and found it easy to comply with the Act
- Individual and shared attitudes towards data protection and information are key influences on business approaches to this issue, and so constitute a primary influence on compliance and engagement with the Act and the ICO
- Different approaches to data protection and information can be identified, and used to identify distinctive segments – each with different requirements and approaches
- There was some indication that respondents were considering effective practice in information and data management and handling, with data protection being seen as a 'subset' of these considerations. Good practice in data protection, in other words, appears to be part of and to stem from wider approaches to information
- Although the Act itself had a high profile, the ICO was less well known and some businesses thought that it would be useful for the ICO to engage more with SMEs.

Observations

16.2 ***The ICO and its role as a regulator.*** There appears to be some ambiguity and a lack of awareness not only of the ICO itself, but also of its role. Several respondents indicated that a clearer and more articulated public role for the ICO might help promote data protection practices amongst small and medium enterprises. This does not necessarily mean that these businesses are recommending a high-level or major publicity campaign, however. Instead, one emergent view was that SMEs that are facing difficulties or problems relating to data protection and the Act would benefit from understanding what the ICO does, and whether it can assist or enable the business to resolve any issues (either directly or indirectly).

“The ICO should provide simplified guidance for business that is easy to understand”

“We need more advice and guidance”

16.3 ***The ICO as Data and Information ‘Kitemark’ Body?*** One possibility would be to develop a form of quality accreditation, or ‘kitemark’ for businesses that would embrace and adhere to data protection principles and practices. Such a kitemark would be awarded to businesses undergoing some form of accreditation process, perhaps similar to Investors in People or ISO, and would be formally recognised if successful. Developing this type of profile may offer the ICO a direct and positive means of engaging with SMEs at all stages of the information ‘life-cycle’.

“I fully agree with the spirit of the Act. Complying with the Act would give business advantage. However, the Act doesn’t ‘sell itself’ unlike Investors in People and other quality standards which do gain companies more business”

16.4 ***Opportunities for businesses to learn from each other – a role for the ICO as an experience exchange facilitator and disseminator?***

Businesses that identified and recounted instances of good practice in data protection tended to work closely with and learn from other enterprises. There may, as such, be opportunity to encourage various forms of ‘experience exchange’ and ‘peer learning’ in order to raise awareness of, as well as improve practices in, data protection.

“I think the ICO should communicate in broad terms – they should let us know of the breaches that other businesses have made in order to warn us and stop us from falling into the same trap”

Data Protection and Small and Medium Businesses

Report prepared for the Information Commissioner's Office

ANNEXES

**ANNEX 1: AWARENESS AND LEVELS OF ENGAGEMENT WITH THE DATA
PROTECTION ACT**

ICO Survey Frequencies

Region

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	East Midlands	31	12.4	12.4	12.4
	West Midlands	28	11.2	11.2	23.6
	North West	26	10.4	10.4	34.0
	Yorkshire and Humberside	21	8.4	8.4	42.4
	Eastern	50	20.0	20.0	62.4
	Northern	30	12.0	12.0	74.4
	South Western	29	11.6	11.6	86.0
	Southern	16	6.4	6.4	92.4
	Scotland	2	.8	.8	93.2
	South Eastern	17	6.8	6.8	100.0
	Total	250	100.0	100.0	

2.1 Have you heard of the Data Protection Act?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	248	99.2	99.2	99.2
	no	2	.8	.8	100.0
	Total	250	100.0	100.0	

2.3 Do you think the DPA is relevant to your business?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	205	82.0	82.3	82.3
	no	34	13.6	13.7	96.0
	don't know	10	4.0	4.0	100.0
	Total	249	99.6	100.0	
Missing	99.00	1	.4		
Total		250	100.0		

2.5 Does your business have to register with the ICO with regard to Protection?

		Frequenc	Percen	Valid	Cumulativ Percen
Valid	yes	109	43.6	43.8	43.8
	no	34	13.6	13.7	57.4
	don't	106	42.4	42.6	100.0
	Total	249	99.6	100.0	
Missin	99.00	1	.4		
Total		250	100.0		

2.6 Is your business registered with the ICO?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	106	42.4	42.9	42.9
	no	44	17.6	17.8	60.7
	don't know	97	38.8	39.3	100.0
	Total	247	98.8	100.0	
Missing	99.00	3	1.2		
Total		250	100.0		

3.1 Are data protection principles a good thing when doing business?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	182	72.8	73.4	73.4
	no	8	3.2	3.2	76.6
	sometimes	33	13.2	13.3	89.9
	possibly	15	6.0	6.0	96.0
	don't know	10	4.0	4.0	100.0
	Total	248	99.2	100.0	
Missing	99.00	2	.8		
Total		250	100.0		

3.2 Do you think that your business should protect data and personal information?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	absolutely	201	80.4	81.7	81.7
	mostly	25	10.0	10.2	91.9
	sometimes	11	4.4	4.5	96.3
	no	4	1.6	1.6	98.0
	not relevant	3	1.2	1.2	99.2
	don't know	2	.8	.8	100.0
	Total	246	98.4	100.0	
Missing	99.00	4	1.6		
Total		250	100.0		

3.3 Do you think the principles of data protection could help or hinder your business?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	help	82	32.8	33.2	33.2
	hinder	32	12.8	13.0	46.2
	bit of both (more help)	58	23.2	23.5	69.6
	bit of both (more hinder)	28	11.2	11.3	81.0
	neither	31	12.4	12.6	93.5
	don't know	16	6.4	6.5	100.0
	Total	247	98.8	100.0	
Missing	99.00	3	1.2		
Total		250	100.0		

3.5 How easy do you feel it is to comply with the DPA?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	very easy	59	23.6	24.0	24.0
	quite easy	78	31.2	31.7	55.7
	a small effort	51	20.4	20.7	76.4
	a large effort	22	8.8	8.9	85.4
	almost impossible	4	1.6	1.6	87.0
	don't know	32	12.8	13.0	100.0
	Total	246	98.4	100.0	
Missing	99.00	4	1.6		
Total		250	100.0		

How important is the term Information Risk?

		Frequenc	Percen	Valid	Cumulativ Percen
Valid	1.00	67	26.8	27.9	27.9
	2.00	55	22.0	22.9	50.8
	3.00	44	17.6	18.3	69.2
	4.00	56	22.4	23.3	92.5
	not	18	7.2	7.5	100.0
	Total	240	96.0	100.0	
Missin	99.00	9	3.6		
	Syste	1	.4		
	Total	10	4.0		
Total		250	100.0		

How important is the term Information Handling?

		Frequenc	Percen	Valid	Cumulativ Percen
Valid	1.00	89	35.6	36.9	36.9
	2.00	60	24.0	24.9	61.8
	3.00	42	16.8	17.4	79.3
	4.00	44	17.6	18.3	97.5
	not	6	2.4	2.5	100.0
	Total	241	96.4	100.0	
Missin	99.00	8	3.2		
	Syste	1	.4		
	Total	9	3.6		
Total		250	100.0		

How important is the term Data Protection?

		Frequenc	Percen	Valid	Cumulativ Percen
Valid	1.00	120	48.0	49.4	49.4
	2.00	67	26.8	27.6	77.0
	3.00	29	11.6	11.9	88.9
	4.00	19	7.6	7.8	96.7
	not	8	3.2	3.3	100.0
	Total	243	97.2	100.0	
Missin	99.00	6	2.4		
	Syste	1	.4		
	Total	7	2.8		
Total		250	100.0		

How important is the term Data Sensitivity?

		Frequenc	Percen	Valid	Cumulativ Percen
Valid	1.00	129	51.6	53.1	53.1
	2.00	44	17.6	18.1	71.2
	3.00	32	12.8	13.2	84.4
	4.00	29	11.6	11.9	96.3
	not	9	3.6	3.7	100.0
	Total	243	97.2	100.0	
Missin	99.00	6	2.4		
	Syste	1	.4		
	Total	7	2.8		
Total		250	100.0		

How important is the Security of Data/ Info?

		Frequenc	Percen	Valid	Cumulativ Percen
Valid	1.00	181	72.4	74.5	74.5
	2.00	39	15.6	16.0	90.5
	3.00	14	5.6	5.8	96.3
	4.00	7	2.8	2.9	99.2
	not	2	.8	.8	100.0
	Total		243	97.2	100.0
Missin	99.00	6	2.4		
	Syste	1	.4		
	Total	7	2.8		
Total		250	100.0		

How important is the term Privacy?

		Frequenc	Percen	Valid	Cumulativ Percen
Valid	1.00	175	70.0	72.0	72.0
	2.00	45	18.0	18.5	90.5
	3.00	12	4.8	4.9	95.5
	4.00	6	2.4	2.5	97.9
	not	5	2.0	2.1	100.0
	Total		243	97.2	100.0
Missin	99.00	6	2.4		
	Syste	1	.4		
	Total	7	2.8		
Total		250	100.0		

How important is the term Confidentiality?

		Frequenc	Percen	Valid	Cumulativ Percen
Valid	1.00	185	74.0	77.4	77.4
	2.00	37	14.8	15.5	92.9
	3.00	7	2.8	2.9	95.8
	4.00	8	3.2	3.3	99.2
	not	2	.8	.8	100.0
	Total		239	95.6	100.0
Missin	99.00	8	3.2		
	Syste	3	1.2		
	Total	11	4.4		
Total		250	100.0		

Most Significant Term from 4.1

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	information risk	5	2.0	7.0	7.0
	information handling	6	2.4	8.5	15.5
	data protection	4	1.6	5.6	21.1
	data sensitivity	2	.8	2.8	23.9
	security of data/info	21	8.4	29.6	53.5
	privacy	5	2.0	7.0	60.6
	confidentiality	27	10.8	38.0	98.6
	other	1	.4	1.4	100.0
	Total	71	28.4	100.0	
Missing	99.00	178	71.2		
	System	1	.4		
	Total	179	71.6		
Total		250	100.0		

How important would be the Monetary cost to comply?

		Frequenc	Percen	Valid	Cumulativ Percen
Valid	1.00	31	12.4	12.8	12.8
	2.00	43	17.2	17.8	30.6
	3.00	45	18.0	18.6	49.2
	4.00	116	46.4	47.9	97.1
	not	6	2.4	2.5	99.6
	don't	1	.4	.4	100.0
	Total	242	96.8	100.0	
	Missin	99.00	7	2.8	
Syste		1	.4		
Total		8	3.2		
Total		250	100.0		

How important would be the Time to register/notify the ICO?

		Frequenc	Percen	Valid	Cumulativ Percen
Valid	1.00	15	6.0	6.3	6.3
	2.00	33	13.2	13.8	20.1
	3.00	42	16.8	17.6	37.7
	4.00	103	41.2	43.1	80.8
	not	36	14.4	15.1	95.8
	don't	10	4.0	4.2	100.0
	Total	239	95.6	100.0	
	Missin	99.00	10	4.0	
Syste		1	.4		
Total		11	4.4		
Total		250	100.0		

How important would be the Time to find out how to comply?

		Frequenc	Percen	Valid	Cumulativ Percen
Valid	1.00	33	13.2	13.8	13.8
	2.00	52	20.8	21.7	35.4
	3.00	42	16.8	17.5	52.9
	4.00	89	35.6	37.1	90.0
	not	20	8.0	8.3	98.3
	don't	4	1.6	1.7	100.0
	Total	240	96.0	100.0	
Missin	99.00	9	3.6		
	Syste	1	.4		
	Total	10	4.0		
Total		250	100.0		

How important would be the Effort to modify existing systems?

		Frequenc	Percen	Valid	Cumulativ Percen
Valid	1.00	41	16.4	16.9	16.9
	2.00	51	20.4	21.1	38.0
	3.00	55	22.0	22.7	60.7
	4.00	88	35.2	36.4	97.1
	not	6	2.4	2.5	99.6
	don't	1	.4	.4	100.0
	Total	242	96.8	100.0	
Missin	99.00	7	2.8		
	Syste	1	.4		
	Total	8	3.2		
Total		250	100.0		

How important would be the Need to create new systems?

		Frequenc	Percen	Valid	Cumulativ Percen
Valid	1.00	27	10.8	11.3	11.3
	2.00	49	19.6	20.4	31.7
	3.00	44	17.6	18.3	50.0
	4.00	107	42.8	44.6	94.6
	not	12	4.8	5.0	99.6
	don't	1	.4	.4	100.0
	Total	240	96.0	100.0	
Missin	99.00	9	3.6		
	Syste	1	.4		
	Total	10	4.0		
Total		250	100.0		

How important would be the Identification of data held?

		Frequenc	Percen	Valid	Cumulativ Percen
Valid	1.00	52	20.8	21.9	21.9
	2.00	47	18.8	19.8	41.8
	3.00	39	15.6	16.5	58.2
	4.00	92	36.8	38.8	97.0
	not	7	2.8	3.0	100.0
	Total	237	94.8	100.0	
Missin	99.00	12	4.8		
	Syste	1	.4		
	Total	13	5.2		
Total		250	100.0		

'Burning' Issue

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	monetary cost to comply	7	2.8	19.4	19.4
	time to register/notify the ICO	2	.8	5.6	25.0
	time to find out how to comply	2	.8	5.6	30.6
	effort to modify existing systems	2	.8	5.6	36.1
	need to create new systems	2	.8	5.6	41.7
	identification of data held	21	8.4	58.3	100.0
	Total	36	14.4	100.0	
Missing	99.00	213	85.2		
	System	1	.4		
	Total	214	85.6		
Total		250	100.0		

ANNEX 2: ANALYSIS OF THE TELEPHONE SAMPLE

SUMMARY ANALYSIS OF FEATURES OF THE TELEPHONE SURVEY SAMPLE

Table 1: Regional Distribution of Interviews Undertaken

		Region			
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	East Midlands	31	12.4	12.4	12.4
	West Midlands	28	11.2	11.2	23.6
	North West	26	10.4	10.4	34.0
	Yorkshire and Humberside	21	8.4	8.4	42.4
	Eastern	50	20.0	20.0	62.4
	Northern	30	12.0	12.0	74.4
	South Western	29	11.6	11.6	86.0
	Southern	16	6.4	6.4	92.4
	Scotland	2	.8	.8	93.2
	South Eastern	17	6.8	6.8	100.0
	Total	250	100.0	100.0	

Table 2: Distribution of the Sample by Broad Sector Category

		Business Sector			
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agriculture and extraction	6	2.4	2.4	2.4
	Materials processing and basic manufacturing	54	21.6	21.9	24.3
	Advanced manufacturing	35	14.0	14.2	38.5
	Basic and personal services	100	40.0	40.5	78.9
	High value services	48	19.2	19.4	98.4
	Public and other	4	1.6	1.6	100.0
	Total	247	98.8	100.0	
	Missing	System	3	1.2	
Total		250	100.0		

Table 3: Statistics for Number of Employees and Turnover

	Current FTE Employees	Turnover Last Financial Year
Mean	94.9	£13,424,118
Median	80	£6,000,000
Range	296	£135,765,000
Minimum	4	£235,000
Maximum	300	£136,000,000

Table 4: Job Roles of Respondents

Job Role	Frequency	Percent
Manager	57	42.9
MD/Chief Executive	20	15.0
Company Secretary	11	8.3
Finance Director	15	11.3
Administrator	30	22.6
Total	133	100.0

Table 5: Job Functions of Respondents

Function	Frequency	Percent
Finance	39	38.2
HR/Personnel	30	29.4
IT	10	9.8
Administration	13	12.7
Marketing/Customer Relations	10	9.8
Total	102	100.0

ANNEX 3: CATERGORISATION BY INDUSTRY CATEGORY

CATEGORISATION BY INDUSTRY CATEGORY

Business Sector Group	Standard Industrial Classification (2003) Division
Agriculture and Extraction	<ul style="list-style-type: none"> • Agriculture, Hunting and Forestry • Fishing • Mining and Quarrying
Materials Processing and Basic Manufacturing	<ul style="list-style-type: none"> • Manufacture of Food Products, Beverages and Tobacco • Manufacture of Textiles and Textile Products • Manufacture of Leather and Leather Products • Manufacture of Wood and Wood Products • Manufacture of Pulp, Paper and Paper Products • Publishing and Printing • Manufacture of Coke, Refined Petroleum Products and Nuclear Fuel • Manufacture of Chemicals, Chemical Products and Man-made Fibres • Manufacture of Rubber and Plastic Products • Manufacture of Other Non-metallic Mineral Products • Manufacture of Basic Metals and Fabricated Metal Products
Advanced Manufacturing	<ul style="list-style-type: none"> • Manufacture of Machinery and Equipment Not Elsewhere Classified • Manufacture of Electrical and Optical Equipment • Manufacture of Transport Equipment • Manufacturing Not Classified Elsewhere • Electricity, Gas and Water Supply
Basic and Personal Services	<ul style="list-style-type: none"> • Construction • Wholesale and Retail Trade; Repair of Motor Vehicles and Personal and Household Goods • Hotels and Restaurants • Transport, Storage and Communication
High Value Services	<ul style="list-style-type: none"> • Financial Intermediation • Real Estate, Renting and Business Activities
Public and Other	<ul style="list-style-type: none"> • Public Administration and Defence; Compulsory Social Security • Education • Health and Social Work • Other Community, Social and Personal Service Activities • Private Households Employing Staff and Undifferentiated Production Activities of Households for Own Use

ANNEX 4: CROSS-TABULATIONS WITH COMMENTARY

Those who consider the DPA relevant to their business are more likely to see data protection principles as a good thing.

2.3 Do you think the DPA is relevant to your business? * 3.1 Are data protection principles a good thing when doing business? Crosstabulation

			3.1 Are data protection principles a good thing when doing business?					Total
			yes	no	sometimes	possibly	don't know	
2.3 Do you think the DPA is relevant to your business?	yes	Count % within 2.3 Do you think the DPA is relevant to your business?	159 77.9%	3 1.5%	27 13.2%	12 5.9%	3 1.5%	204 100.0%
	no	Count % within 2.3 Do you think the DPA is relevant to your business?	18 52.9%	4 11.8%	5 14.7%	2 5.9%	5 14.7%	34 100.0%
	don't know	Count % within 2.3 Do you think the DPA is relevant to your business?	5 50.0%	1 10.0%	1 10.0%	1 10.0%	2 20.0%	10 100.0%
Total		Count % within 2.3 Do you think the DPA is relevant to your business?	182 73.4%	8 3.2%	33 13.3%	15 6.0%	10 4.0%	248 100.0%

Those who consider the DPA relevant are only slightly more likely to consider that businesses should protect data than those who do not see the DPA as relevant.

2.3 Do you think the DPA is relevant to your business? * 3.2 Do you think that your business should protect data and personal information? Crosstabulation

			3.2 Do you think that your business should protect data and personal information?					Total
			absolutely	mostly	sometimes	no	not relevant	
2.3 Do you think the DPA is relevant to your business?	yes	Count % within 2.3 Do you think the DPA is relevant to your business?	170 84.2%	22 10.9%	7 3.5%	1 .5%	1 .5%	202 100.0%
	no	Count % within 2.3 Do you think the DPA is relevant to your business?	24 70.6%	3 8.8%	2 5.9%	3 8.8%	2 5.9%	34 100.0%
	don't know	Count % within 2.3 Do you think the DPA is relevant to your business?	7 70.0%		2 20.0%		1 10.0%	10 100.0%
Total		Count % within 2.3 Do you think the DPA is relevant to your business?	201 81.7%	25 10.2%	11 4.5%	4 1.6%	3 1.2%	246 100.0%

Those who consider the DPA relevant are more likely to view the data protection principles as helpful.

Do you think the DPA is relevant to your business? * 3.3 Do you think the principles of data protection could help or hinder your business? Crosstabulation

			3.3 Do you think the principles of data protection could help or hinder your business?					Total	
			help	hinder	bit of both (more help)	bit of both (more hinder)	neither		don't know
2.3 Do you think the DPA is relevant to your business?	yes	Count % within 2.3 Do you think the DPA is relevant to your business?	75 36.9%	19 9.4%	50 24.6%	26 12.8%	24 11.8%	9 4.4%	203 100.0%
	no	Count % within 2.3 Do you think the DPA is relevant to your business?	2 5.9%	13 38.2%	7 20.6%	1 2.9%	6 17.6%	5 14.7%	34 100.0%
	don't know	Count % within 2.3 Do you think the DPA is relevant to your business?	5 50.0%		1 10.0%	1 10.0%	1 10.0%	2 20.0%	10 100.0%
Total		Count % within 2.3 Do you think the DPA is relevant to your business?	82 33.2%	32 13.0%	58 23.5%	28 11.3%	31 12.6%	16 6.5%	247 100.0%

Those who consider the DPA relevant are more likely to view it as ‘easy to comply’ with.

2.3 Do you think the DPA is relevant to your business? * 3.5 How easy do you feel it is to comply with the DPA? Crosstabulation

			3.5 How easy do you feel it is to comply with the DPA?					Total	
			very easy	quite easy	a small effort	a large effort	almost impossible		don't know
2.3 Do you think the DPA is relevant to your business?	yes	Count	51	71	42	19	2	18	203
		% within 2.3 Do you think the DPA is relevant to your business?	25.1%	35.0%	20.7%	9.4%	1.0%	8.9%	100.0%
	no	Count	7	5	9	3	2	8	34
		% within 2.3 Do you think the DPA is relevant to your business?	20.6%	14.7%	26.5%	8.8%	5.9%	23.5%	100.0%
	don't know	Count	1	2				6	9
		% within 2.3 Do you think the DPA is relevant to your business?	11.1%	22.2%				66.7%	100.0%
Total		Count	59	78	51	22	4	32	246
		% within 2.3 Do you think the DPA is relevant to your business?	24.0%	31.7%	20.7%	8.9%	1.6%	13.0%	100.0%

Those who consider the DPA as relevant are more likely to rate ‘information risk’, ‘data protection’ ‘data sensitivity’, ‘security of data’ ‘privacy’ and ‘confidentiality’ as important as well.

2.3 Do you think the DPA is relevant to your business? * Security of Data/ Info Crosstabulation

			Security of Data/ Info					Total
			1.00	2.00	3.00	4.00	not meaningful	
2.3 Do you think the DPA is relevant to your business?	yes	Count	159	29	10	2	1	201
		% within 2.3 Do you think the DPA is relevant to your business?	79.1%	14.4%	5.0%	1.0%	.5%	100.0%
	no	Count	17	6	3	5	1	32
		% within 2.3 Do you think the DPA is relevant to your business?	53.1%	18.8%	9.4%	15.6%	3.1%	100.0%
	don't know	Count	5	4	1			10
		% within 2.3 Do you think the DPA is relevant to your business?	50.0%	40.0%	10.0%			100.0%
Total		Count	181	39	14	7	2	243
		% within 2.3 Do you think the DPA is relevant to your business?	74.5%	16.0%	5.8%	2.9%	.8%	100.0%

Within the following three cross tabulations, a higher proportion of those who don't consider the DPA relevant rate these compliance requirements highly – a perception of burden rather than as a result of direct experience?

2.3 Do you think the DPA is relevant to your business? * Time to register/notify the ICO Crosstabulation

			Time to register/notify the ICO						Total
			1.00	2.00	3.00	4.00	not meaningful	don't know	
2.3 Do you think the DPA is relevant to your business?	yes	Count % within 2.3 Do you think the DPA is relevant to your business?	9 4.6%	27 13.7%	35 17.8%	86 43.7%	31 15.7%	9 4.6%	197 100.0%
	no	Count % within 2.3 Do you think the DPA is relevant to your business?	5 15.6%	3 9.4%	6 18.8%	14 43.8%	3 9.4%	1 3.1%	32 100.0%
	don't know	Count % within 2.3 Do you think the DPA is relevant to your business?	1 10.0%	3 30.0%	1 10.0%	3 30.0%	2 20.0%		10 100.0%
Total		Count % within 2.3 Do you think the DPA is relevant to your business?	15 6.3%	33 13.8%	42 17.6%	103 43.1%	36 15.1%	10 4.2%	239 100.0%

2.3 Do you think the DPA is relevant to your business? * Effort to modify existing systems Crosstabulation

			Effort to modify existing systems						Total
			1.00	2.00	3.00	4.00	not meaningful	don't know	
2.3 Do you think the DPA is relevant to your business?	yes	Count % within 2.3 Do you think the DPA is relevant to your business?	31 15.5%	43 21.5%	51 25.5%	69 34.5%	5 2.5%	1 .5%	200 100.0%
	no	Count % within 2.3 Do you think the DPA is relevant to your business?	7 21.9%	7 21.9%	2 6.3%	15 46.9%	1 3.1%		32 100.0%
	don't know	Count % within 2.3 Do you think the DPA is relevant to your business?	3 30.0%	1 10.0%	2 20.0%	4 40.0%			10 100.0%
Total		Count % within 2.3 Do you think the DPA is relevant to your business?	41 16.9%	51 21.1%	55 22.7%	88 36.4%	6 2.5%	1 .4%	242 100.0%

2.3 Do you think the DPA is relevant to your business? * Time to find out how to comply Crosstabulation

			Time to find out how to comply						Total
			1.00	2.00	3.00	4.00	not meaningful	don't know	
2.3 Do you think the DPA is relevant to your business?	yes	Count % within 2.3 Do you think the DPA is relevant to your business?	23 11.6%	42 21.2%	40 20.2%	73 36.9%	16 8.1%	4 2.0%	198 100.0%
	no	Count % within 2.3 Do you think the DPA is relevant to your business?	7 21.9%	8 25.0%	2 6.3%	13 40.6%	2 6.3%		32 100.0%
	don't know	Count % within 2.3 Do you think the DPA is relevant to your business?	3 30.0%	2 20.0%		3 30.0%	2 20.0%		10 100.0%
Total		Count % within 2.3 Do you think the DPA is relevant to your business?	33 13.8%	52 21.7%	42 17.5%	89 37.1%	20 8.3%	4 1.7%	240 100.0%

If the respondents agree that the data protection is a good thing they are more likely to agree that their business should protect data and personal information.

3.1 Are data protection principles a good thing when doing business? * 3.3 Do you think the principles of data protection could help or hinder your business?
Crosstabulation

			3.3 Do you think the principles of data protection could help or hinder your business?					Total	
			help	hinder	bit of both (more help)	bit of both (more hinder)	neither		don't know
3.1 Are data protection principles a good thing when doing business?	yes	Count % within 3.1 Are data protection principles a good thing when doing business?	76 42.0%	21 11.6%	43 23.8%	17 9.4%	18 9.9%	6 3.3%	181 100.0%
	no	Count % within 3.1 Are data protection principles a good thing when doing business?	1 12.5%	4 50.0%	1 12.5%		1 12.5%	1 12.5%	8 100.0%
	sometimes	Count % within 3.1 Are data protection principles a good thing when doing business?	4 12.1%	4 12.1%	11 33.3%	5 15.2%	6 18.2%	3 9.1%	33 100.0%
	possibly	Count % within 3.1 Are data protection principles a good thing when doing business?	1 6.7%	2 13.3%	2 13.3%	5 33.3%	5 33.3%		15 100.0%
	don't know	Count % within 3.1 Are data protection principles a good thing when doing business?		1 10.0%	1 10.0%	1 10.0%	1 10.0%	6 60.0%	10 100.0%
Total		Count % within 3.1 Are data protection principles a good thing when doing business?	82 33.2%	32 13.0%	58 23.5%	28 11.3%	31 12.6%	16 6.5%	247 100.0%

If the respondents agree that data protection is a good thing, they are more likely to say that the principle will 'help' or a 'bit of both – more help' their business.

3.1 Are data protection principles a good thing when doing business? * 3.2 Do you think that your business should protect data and personal information?
Crosstabulation

			3.2 Do you think that your business should protect data and personal information?					Total	
			absolutely	mostly	sometimes	no	not relevant		don't know
3.1 Are data protection principles a good thing when doing business?	yes	Count % within 3.1 Are data protection principles a good thing when doing business?	165 91.7%	9 5.0%	3 1.7%	1 .6%	1 .6%	1 .6%	180 100.0%
	no	Count % within 3.1 Are data protection principles a good thing when doing business?	2 25.0%	1 12.5%	2 25.0%	2 25.0%		1 12.5%	8 100.0%
	sometimes	Count % within 3.1 Are data protection principles a good thing when doing business?	18 54.5%	11 33.3%	4 12.1%				33 100.0%
	possibly	Count % within 3.1 Are data protection principles a good thing when doing business?	8 53.3%	4 26.7%	1 6.7%	1 6.7%	1 6.7%		15 100.0%
	don't know	Count % within 3.1 Are data protection principles a good thing when doing business?		8 80.0%		1 10.0%		1 10.0%	10 100.0%
Total		Count % within 3.1 Are data protection principles a good thing when doing business?	201 81.7%	25 10.2%	11 4.5%	4 1.6%	3 1.2%	2 .8%	246 100.0%

If the respondents say that data protection is a good thing then it is maybe perceived that it is less of an effort to comply with it (although not strongly conclusive).

3.1 Are data protection principles a good thing when doing business? * 3.5 How easy do you feel it is to comply with the DPA? Crosstabulation

			3.5 How easy do you feel it is to comply with the DPA?					Total	
			very easy	quite easy	a small effort	a large effort	almost impossible		don't know
3.1 Are data protection principles a good thing when doing business?	yes	Count % within 3.1 Are data protection principles a good thing when doing business?	51 28.2%	64 35.4%	39 21.5%	14 7.7%	2 1.1%	11 6.1%	181 100.0%
	no	Count % within 3.1 Are data protection principles a good thing when doing business?	1 14.3%		1 14.3%	1 14.3%	1 14.3%	3 42.9%	7 100.0%
	sometimes	Count % within 3.1 Are data protection principles a good thing when doing business?	4 12.1%	10 30.3%	7 21.2%	5 15.2%	1 3.0%	6 18.2%	33 100.0%
	possibly	Count % within 3.1 Are data protection principles a good thing when doing business?	1 6.7%	3 20.0%	2 13.3%	2 13.3%		7 46.7%	15 100.0%
	don't know	Count % within 3.1 Are data protection principles a good thing when doing business?	2 20.0%	1 10.0%	2 20.0%			5 50.0%	10 100.0%
	Total	Count % within 3.1 Are data protection principles a good thing when doing business?	59 24.0%	78 31.7%	51 20.7%	22 8.9%	4 1.6%	32 13.0%	246 100.0%

If the respondents say that data protection is a good thing then a higher proportion ranked the importance of data protection as 'high' (1 or 2).

3.1 Are data protection principles a good thing when doing business? * Data Protection Crosstabulation

			Data Protection					Total
			1.00	2.00	3.00	4.00	not meaningful	
3.1 Are data protection principles a good thing when doing business?	yes	Count % within 3.1 Are data protection principles a good thing when doing business?	107 59.4%	46 25.6%	15 8.3%	9 5.0%	3 1.7%	180 100.0%
	no	Count % within 3.1 Are data protection principles a good thing when doing business?	1 16.7%	2 33.3%	1 16.7%	2 33.3%		6 100.0%
	sometimes	Count % within 3.1 Are data protection principles a good thing when doing business?	6 18.2%	14 42.4%	9 27.3%	3 9.1%	1 3.0%	33 100.0%
	possibly	Count % within 3.1 Are data protection principles a good thing when doing business?	1 6.7%	3 20.0%	4 26.7%	3 20.0%	4 26.7%	15 100.0%
	don't know	Count % within 3.1 Are data protection principles a good thing when doing business?	5 55.6%	2 22.2%		2 22.2%		9 100.0%
	Total	Count % within 3.1 Are data protection principles a good thing when doing business?	120 49.4%	67 27.6%	29 11.9%	19 7.8%	8 3.3%	243 100.0%

Those who consider data protection a good thing were ‘sometimes’ or ‘possibly’ likely to see that the monetary cost to comply as important.

3.1 Are data protection principles a good thing when doing business? * Monetary cost to comply Crosstabulation

			Monetary cost to comply					Total	
			1.00	2.00	3.00	4.00	not meaningful		don't know
3.1 Are data protection principles a good thing when doing business?	yes	Count % within 3.1 Are data protection principles a good thing when doing business?	20 11.2%	26 14.5%	41 22.9%	90 50.3%	2 1.1%	179 100.0%	
	no	Count % within 3.1 Are data protection principles a good thing when doing business?	1 16.7%			5 83.3%		6 100.0%	
	sometimes	Count % within 3.1 Are data protection principles a good thing when doing business?	5 15.2%	12 36.4%	3 9.1%	12 36.4%	1 3.0%	33 100.0%	
	possibly	Count % within 3.1 Are data protection principles a good thing when doing business?	5 33.3%	3 20.0%	1 6.7%	4 26.7%	1 6.7%	1 6.7%	15 100.0%
	don't know	Count % within 3.1 Are data protection principles a good thing when doing business?		2 22.2%		5 55.6%	2 22.2%		9 100.0%
Total		Count % within 3.1 Are data protection principles a good thing when doing business?	31 12.8%	43 17.8%	45 18.6%	116 47.9%	6 2.5%	1 .4%	242 100.0%

Note: those who are less convinced about whether the DPA is a good thing are more inclined to consider compliance issues such as cost, time, systems etc as important.

Those who ranked ‘the time to find out how to comply’ as being low in importance also ranked similarly ‘the effort to modify existing systems.’

Time to find out how to comply * Effort to modify existing systems Crosstabulation

			Effort to modify existing systems							Total
			1.00	2.00	3.00	4.00	not meaningful			
Time to find out how to comply	1.00	Count	15	10	4	3	1		33	
		% within Time to find out how to comply	45.5%	30.3%	12.1%	9.1%	3.0%		100.0%	
	2.00	Count	15	20	10	6	1		52	
		% within Time to find out how to comply	28.8%	38.5%	19.2%	11.5%	1.9%		100.0%	
	3.00	Count	4	11	16	9	2		42	
		% within Time to find out how to comply	9.5%	26.2%	38.1%	21.4%	4.8%		100.0%	
	4.00	Count	4	4	19	62			89	
% within Time to find out how to comply		4.5%	4.5%	21.3%	69.7%			100.0%		
not meaningful	Count	3	5	4	6	2		20		
	% within Time to find out how to comply	15.0%	25.0%	20.0%	30.0%	10.0%		100.0%		
don't know	Count			1	2		1	4		
	% within Time to find out how to comply			25.0%	50.0%		25.0%	100.0%		
Total	Count	41	50	54	88	6	1	240		
	% within Time to find out how to comply	17.1%	20.8%	22.5%	36.7%	2.5%	.4%	100.0%		

Those who ranked ‘the time to find out how to comply’ as being low in importance, also ranked the following terms as being low in importance (a 4 rating): ‘the need to create new systems’, ‘identification of data held’, monetary cost’ and the ‘time to register’.

Time to find out how to comply * Need to create new systems Crosstabulation

			Need to create new systems							Total
			1.00	2.00	3.00	4.00	not meaningful			
Time to find out how to comply	1.00	Count	10	12	3	5	3		33	
		% within Time to find out how to comply	30.3%	36.4%	9.1%	15.2%	9.1%		100.0%	
	2.00	Count	12	16	12	7	5		52	
		% within Time to find out how to comply	23.1%	30.8%	23.1%	13.5%	9.6%		100.0%	
	3.00	Count	3	12	9	15	2		41	
		% within Time to find out how to comply	7.3%	29.3%	22.0%	36.6%	4.9%		100.0%	
	4.00	Count	1	6	14	67			88	
% within Time to find out how to comply		1.1%	6.8%	15.9%	76.1%			100.0%		
not meaningful	Count	1	2	5	10	2		20		
	% within Time to find out how to comply	5.0%	10.0%	25.0%	50.0%	10.0%		100.0%		
don't know	Count			1	2		1	4		
	% within Time to find out how to comply			25.0%	50.0%		25.0%	100.0%		
Total	Count	27	48	44	106	12	1	238		
	% within Time to find out how to comply	11.3%	20.2%	18.5%	44.5%	5.0%	.4%	100.0%		

A higher proportion of those who rank ‘time to find out how to comply’ as being low importance (3 or 4) also say that they believe the data protection principles are a good thing. Time is therefore less important to those who view the principles as a good thing?

Time to find out how to comply * 3.1 Are data protection principles a good thing when doing business? Crosstabulation

			3.1 Are data protection principles a good thing when doing business?					Total
			yes	no	sometimes	possibly	don't know	
Time to find out how to comply	1.00	Count % within Time to find out how to comply	22 66.7%	1 3.0%	5 15.2%	5 15.2%		33 100.0%
	2.00	Count % within Time to find out how to comply	31 59.6%	1 1.9%	15 28.8%	3 5.8%	2 3.8%	52 100.0%
	3.00	Count % within Time to find out how to comply	37 88.1%		3 7.1%	2 4.8%		42 100.0%
	4.00	Count % within Time to find out how to comply	71 79.8%	4 4.5%	9 10.1%	1 1.1%	4 4.5%	89 100.0%
	not meaningful	Count % within Time to find out how to comply	14 70.0%		1 5.0%	2 10.0%	3 15.0%	20 100.0%
	don't know	Count % within Time to find out how to comply	2 50.0%			2 50.0%		4 100.0%
Total	Count % within Time to find out how to comply	177 73.8%	6 2.5%	33 13.8%	15 6.3%	9 3.8%	240 100.0%	

Those who viewed the principles of data protection as more positively also saw compliance with the DPA as very easy or quite easy. The negative relationship is less obvious.

3.3 Do you think the principles of data protection could help or hinder your business? * 3.5 How easy do you feel it is to comply with the DPA? Crosstabulation

			3.5 How easy do you feel it is to comply with the DPA?					Total	
			very easy	quite easy	a small effort	a large effort	almost impossible		don't know
3.3 Do you think the principles of data protection could help or hinder your business?	help	Count % within 3.3 Do you think the principles of data protection could help or hinder your business?	32 39.5%	27 33.3%	8 9.9%	6 7.4%		8 9.9%	81 100.0%
	hinder	Count % within 3.3 Do you think the principles of data protection could help or hinder your business?	4 12.5%	7 21.9%	9 28.1%	6 18.8%	1 3.1%	5 15.6%	32 100.0%
	bit of both (more help)	Count % within 3.3 Do you think the principles of data protection could help or hinder your business?	6 10.5%	26 45.6%	17 29.8%	4 7.0%		4 7.0%	57 100.0%
	bit of both (more hinder)	Count % within 3.3 Do you think the principles of data protection could help or hinder your business?	5 17.9%	6 21.4%	7 25.0%	4 14.3%	2 7.1%	4 14.3%	28 100.0%
	neither	Count % within 3.3 Do you think the principles of data protection could help or hinder your business?	12 38.7%	6 19.4%	6 19.4%	2 6.5%	1 3.2%	4 12.9%	31 100.0%
	don't know	Count % within 3.3 Do you think the principles of data protection could help or hinder your business?		5 31.3%	4 25.0%			7 43.8%	16 100.0%
Total	Count % within 3.3 Do you think the principles of data protection could help or hinder your business?	59 24.1%	77 31.4%	51 20.8%	22 9.0%	4 1.6%	32 13.1%	245 100.0%	

The majority of all who responded – regardless of whether they considered the principles of data protection as a help or hindrance – considered ‘data protection’ as important to them and their businesses.

3.3 Do you think the principles of data protection could help or hinder your business? * Data Protection Crosstabulation

			Data Protection					Total
			1.00	2.00	3.00	4.00	not meaningful	
3.3 Do you think the principles of data protection could help or hinder your business?	help	Count % within 3.3 Do you think the principles of data protection could help or hinder your business?	52 65.0%	18 22.5%	6 7.5%	4 5.0%		80 100.0%
	hinder	Count % within 3.3 Do you think the principles of data protection could help or hinder your business?	15 50.0%	8 26.7%	3 10.0%	3 10.0%	1 3.3%	30 100.0%
	bit of both (more help)	Count % within 3.3 Do you think the principles of data protection could help or hinder your business?	27 46.6%	19 32.8%	8 13.8%	2 3.4%	2 3.4%	58 100.0%
	bit of both (more hinder)	Count % within 3.3 Do you think the principles of data protection could help or hinder your business?	10 35.7%	12 42.9%	5 17.9%	1 3.6%		28 100.0%
	neither	Count % within 3.3 Do you think the principles of data protection could help or hinder your business?	7 22.6%	8 25.8%	6 19.4%	6 19.4%	4 12.9%	31 100.0%
	don't know	Count % within 3.3 Do you think the principles of data protection could help or hinder your business?	8 53.3%	2 13.3%	1 6.7%	3 20.0%	1 6.7%	15 100.0%
	Total	Count % within 3.3 Do you think the principles of data protection could help or hinder your business?	119 49.2%	67 27.7%	29 12.0%	19 7.9%	8 3.3%	242 100.0%

Those who thought the time to register or notify was important also thought the time to find out how to comply was important. The converse was also the case, i.e. those seeing one as unimportant also saw the other as unimportant.

Time to register/notify the ICO * Time to find out how to comply Crosstabulation

			Time to find out how to comply					Total
			1.00	2.00	3.00	4.00	not meaningful	
Time to register/notify the ICO	1.00	Count % within Time to register/notify the ICO	12 80.0%	2 13.3%	1 6.7%			15 100.0%
	2.00	Count % within Time to register/notify the ICO	5 15.2%	24 72.7%	3 9.1%	1 3.0%		33 100.0%
	3.00	Count % within Time to register/notify the ICO	3 7.1%	15 35.7%	17 40.5%	7 16.7%		42 100.0%
	4.00	Count % within Time to register/notify the ICO	5 4.9%	6 5.8%	13 12.6%	76 73.8%	3 2.9%	103 100.0%
	not meaningful	Count % within Time to register/notify the ICO	7 19.4%	3 8.3%	6 16.7%	3 8.3%	17 47.2%	36 100.0%
	don't know	Count % within Time to register/notify the ICO	1 10.0%	2 20.0%	1 10.0%	2 20.0%		10 100.0%
	Total	Count % within Time to register/notify the ICO	33 13.8%	52 21.8%	41 17.2%	89 37.2%	20 8.4%	4 1.7%

‘Does the registration time affect whether the business is actually registered or not?’ Apparently not significantly so from the cross-tabulation below...

Time to register/notify the ICO * 2.6 Is your business registered with the ICO? Crosstabulation

			2.6 Is your business registered with the ICO?			Total
			yes	no	don't know	
Time to register/notify the ICO	1.00	Count	7	3	4	14
		% within Time to register/notify the ICO	50.0%	21.4%	28.6%	100.0%
	2.00	Count	15	5	13	33
		% within Time to register/notify the ICO	45.5%	15.2%	39.4%	100.0%
	3.00	Count	24	7	11	42
		% within Time to register/notify the ICO	57.1%	16.7%	26.2%	100.0%
	4.00	Count	55	19	29	103
		% within Time to register/notify the ICO	53.4%	18.4%	28.2%	100.0%
	not meaningful	Count	3	4	28	35
		% within Time to register/notify the ICO	8.6%	11.4%	80.0%	100.0%
	don't know	Count		3	7	10
		% within Time to register/notify the ICO		30.0%	70.0%	100.0%
Total		Count	104	41	92	237
		% within Time to register/notify the ICO	43.9%	17.3%	38.8%	100.0%

Of those who considered that the term ‘data protection’ was very important to, a high proportion also considered ‘time to register’ as least important to them.

Time to register/notify the ICO * Data Protection Crosstabulation

			Data Protection					Total
			1.00	2.00	3.00	4.00	not meaningful	
Time to register/notify the ICO	1.00	Count	6	6	1	2		15
		% within Time to register/notify the ICO	40.0%	40.0%	6.7%	13.3%		100.0%
	2.00	Count	11	9	8	3	2	33
		% within Time to register/notify the ICO	33.3%	27.3%	24.2%	9.1%	6.1%	100.0%
	3.00	Count	20	11	5	4	2	42
		% within Time to register/notify the ICO	47.6%	26.2%	11.9%	9.5%	4.8%	100.0%
	4.00	Count	64	24	6	8	1	103
		% within Time to register/notify the ICO	62.1%	23.3%	5.8%	7.8%	1.0%	100.0%
	not meaningful	Count	15	10	8	1	2	36
		% within Time to register/notify the ICO	41.7%	27.8%	22.2%	2.8%	5.6%	100.0%
	don't know	Count	1	6	1	1	1	10
		% within Time to register/notify the ICO	10.0%	60.0%	10.0%	10.0%	10.0%	100.0%
Total		Count	117	66	29	19	8	239
		% within Time to register/notify the ICO	49.0%	27.6%	12.1%	7.9%	3.3%	100.0%

Compliance requirements show a positive correlation trend here: those who considered ‘time’ as being important to them also considered ‘monetary cost’ as important. Those who viewed one requirement as being of low importance also considered the other as of low importance.

Time to register/notify the ICO * Monetary cost to comply Crosstabulation

			Monetary cost to comply					Total
			1.00	2.00	3.00	4.00	not meaningful	
Time to register/notify the ICO	1.00	Count	9	3	2	1		15
		% within Time to register/notify the ICO	60.0%	20.0%	13.3%	6.7%		100.0%
	2.00	Count	10	14	3	6		33
		% within Time to register/notify the ICO	30.3%	42.4%	9.1%	18.2%		100.0%
	3.00	Count	2	7	19	14		42
		% within Time to register/notify the ICO	4.8%	16.7%	45.2%	33.3%		100.0%
	4.00	Count	2	9	15	77		103
	% within Time to register/notify the ICO	1.9%	8.7%	14.6%	74.8%		100.0%	
	not meaningful	Count	6	9	3	13	5	36
	% within Time to register/notify the ICO	16.7%	25.0%	8.3%	36.1%	13.9%		100.0%
	don't know	Count	1	1	1	5	1	10
	% within Time to register/notify the ICO	10.0%	10.0%	10.0%	50.0%	10.0%	10.0%	100.0%
Total	Count	30	43	43	116	6	1	239
	% within Time to register/notify the ICO	12.6%	18.0%	18.0%	48.5%	2.5%	.4%	100.0%

Those who considered the ‘security of data and information’ quite important also felt that privacy and confidentiality were quite important too.

Security of Data/ Info * Privacy Crosstabulation

			Privacy					Total
			1.00	2.00	3.00	4.00	not meaningful	
Security of Data/ Info	1.00	Count	157	19	3		2	181
		% within Security of Data/ Info	86.7%	10.5%	1.7%		1.1%	100.0%
	2.00	Count	17	18	3	1		39
		% within Security of Data/ Info	43.6%	46.2%	7.7%	2.6%		100.0%
	3.00	Count		6	6	1	1	14
	% within Security of Data/ Info		42.9%	42.9%	7.1%	7.1%	100.0%	
	4.00	Count	1	2		4		7
	% within Security of Data/ Info	14.3%	28.6%		57.1%		100.0%	
	not meaningful	Count					2	2
	% within Security of Data/ Info					100.0%		100.0%
Total	Count	175	45	12	6	5	243	
	% within Security of Data/ Info	72.0%	18.5%	4.9%	2.5%	2.1%	100.0%	

Security of Data/ Info * Confidentiality Crosstabulation

			Confidentiality					Total
			1.00	2.00	3.00	4.00	not meaningful	
Security of Data/ Info	1.00	Count	160	14	2	1		177
		% within Security of Data/ Info	90.4%	7.9%	1.1%	.6%		100.0%
	2.00	Count	21	15	1	2		39
		% within Security of Data/ Info	53.8%	38.5%	2.6%	5.1%		100.0%
	3.00	Count	3	6	4	1		14
	% within Security of Data/ Info	21.4%	42.9%	28.6%	7.1%		100.0%	
	4.00	Count	1	2		4		7
	% within Security of Data/ Info	14.3%	28.6%		57.1%		100.0%	
	not meaningful	Count					2	2
	% within Security of Data/ Info					100.0%		100.0%
Total	Count	185	37	7	8	2	239	
	% within Security of Data/ Info	77.4%	15.5%	2.9%	3.3%	.8%	100.0%	

Where one may have expected a strong correlation between ‘security of data’ issues and ‘information risk’ issues, there is none.

Security of Data/ Info * Information Risk Crosstabulation

			Information Risk					Total
			1.00	2.00	3.00	4.00	not meaningful	
Security of Data/ Info	1.00	Count	64	38	27	43	7	179
		% within Security of Data/ Info	35.8%	21.2%	15.1%	24.0%	3.9%	100.0%
	2.00	Count	3	14	10	7	5	39
		% within Security of Data/ Info	7.7%	35.9%	25.6%	17.9%	12.8%	100.0%
	3.00	Count		3	5	4	2	14
		% within Security of Data/ Info		21.4%	35.7%	28.6%	14.3%	100.0%
4.00	Count			2	2	2	6	
	% within Security of Data/ Info			33.3%	33.3%	33.3%	100.0%	
not meaningful	Count					2	2	
	% within Security of Data/ Info					100.0%	100.0%	
Total	Count	67	55	44	56	18	240	
	% within Security of Data/ Info	27.9%	22.9%	18.3%	23.3%	7.5%	100.0%	

There was a marginal positive correlation between ‘security of data and information’ and both ‘data protection’ and ‘data sensitivity’ issues.

Security of Data/ Info * Data Protection Crosstabulation

			Data Protection					Total
			1.00	2.00	3.00	4.00	not meaningful	
Security of Data/ Info	1.00	Count	112	41	16	7	5	181
		% within Security of Data/ Info	61.9%	22.7%	8.8%	3.9%	2.8%	100.0%
	2.00	Count	7	20	7	5		39
		% within Security of Data/ Info	17.9%	51.3%	17.9%	12.8%		100.0%
	3.00	Count	1	6	5	1	1	14
		% within Security of Data/ Info	7.1%	42.9%	35.7%	7.1%	7.1%	100.0%
4.00	Count			1	6		7	
	% within Security of Data/ Info			14.3%	85.7%		100.0%	
not meaningful	Count					2	2	
	% within Security of Data/ Info					100.0%	100.0%	
Total	Count	120	67	29	19	8	243	
	% within Security of Data/ Info	49.4%	27.6%	11.9%	7.8%	3.3%	100.0%	

Security of Data/ Info * Data Sensitivity Crosstabulation

			Data Sensitivity					Total
			1.00	2.00	3.00	4.00	not meaningful	
Security of Data/ Info	1.00	Count	125	29	11	11	5	181
		% within Security of Data/ Info	69.1%	16.0%	6.1%	6.1%	2.8%	100.0%
	2.00	Count	4	11	13	9	2	39
		% within Security of Data/ Info	10.3%	28.2%	33.3%	23.1%	5.1%	100.0%
	3.00	Count		4	6	4		14
		% within Security of Data/ Info		28.6%	42.9%	28.6%		100.0%
4.00	Count			2	5		7	
	% within Security of Data/ Info			28.6%	71.4%		100.0%	
not meaningful	Count					2	2	
	% within Security of Data/ Info					100.0%	100.0%	
Total	Count	129	44	32	29	9	243	
	% within Security of Data/ Info	53.1%	18.1%	13.2%	11.9%	3.7%	100.0%	

Respondents linked having to register with or notify the ICO with actually registering – and they also linked not having to notify with not actually doing so (although a smaller number).

2.5 Does your business have to register with the ICO with regard to Data Protection * 2.6 Is your business registered with the ICO? Crosstabulation

			2.6 Is your business registered with the ICO?			Total
			yes	no	don't know	
2.5 Does your business have to register with the ICO with regard to Data Protection	yes	Count % within 2.5 Does your business have to register with the ICO with regard to Data Protection	101 93.5%	4 3.7%	3 2.8%	108 100.0%
	no	Count % within 2.5 Does your business have to register with the ICO with regard to Data Protection		29 87.9%	4 12.1%	33 100.0%
	don't know	Count % within 2.5 Does your business have to register with the ICO with regard to Data Protection	5 4.7%	11 10.4%	90 84.9%	106 100.0%
Total		Count % within 2.5 Does your business have to register with the ICO with regard to Data Protection	106 42.9%	44 17.8%	97 39.3%	247 100.0%

Regardless of registration status, high proportions considered data protection principles a good thing. This may suggest that the ‘theory’ and moral obligation of the principles is more acceptable and plausible than the status of actually ‘being registered’.

5 Does your business have to register with the ICO with regard to Data Protection * 3.1 Are data protection principles a good thing when doing business? Crosstabulation

			3.1 Are data protection principles a good thing when doing business?					Total
			yes	no	sometimes	possibly	don't know	
2.5 Does your business have to register with the ICO with regard to Data Protection	yes	Count % within 2.5 Does your business have to register with the ICO with regard to Data Protection	87 80.6%	4 3.7%	10 9.3%	4 3.7%	3 2.8%	108 100.0%
	no	Count % within 2.5 Does your business have to register with the ICO with regard to Data Protection	25 73.5%	1 2.9%	6 17.6%	1 2.9%	1 2.9%	34 100.0%
	don't know	Count % within 2.5 Does your business have to register with the ICO with regard to Data Protection	70 66.0%	3 2.8%	17 16.0%	10 9.4%	6 5.7%	106 100.0%
Total		Count % within 2.5 Does your business have to register with the ICO with regard to Data Protection	182 73.4%	8 3.2%	33 13.3%	15 6.0%	10 4.0%	248 100.0%

To those who considered that they ‘have’ to register with the ICO, around half saw the monetary cost to comply as of little significance.

2.5 Does your business have to register with the ICO with regard to Data Protection * Monetary cost to comply Crosstabulation

			Monetary cost to comply						Total
			1.00	2.00	3.00	4.00	not meaningful	don't know	
2.5 Does your business have to register with the ICO with regard to Data Protection	yes	Count	13	21	17	56			107
		% within 2.5 Does your business have to register with the ICO with regard to Data Protection	12.1%	19.6%	15.9%	52.3%			100.0%
	no	Count	6	4	10	13	1		34
		% within 2.5 Does your business have to register with the ICO with regard to Data Protection	17.6%	11.8%	29.4%	38.2%	2.9%		100.0%
	don't know	Count	12	18	18	47	5	1	101
		% within 2.5 Does your business have to register with the ICO with regard to Data Protection	11.9%	17.8%	17.8%	46.5%	5.0%	1.0%	100.0%
Total		Count	31	43	45	116	6	1	242
		% within 2.5 Does your business have to register with the ICO with regard to Data Protection	12.8%	17.8%	18.6%	47.9%	2.5%	.4%	100.0%

Those who are not registered with the ICO still feel that the DPA is relevant to their business.

2.5 Does your business have to register with the ICO with regard to Data Protection * 2.3 Do you think the DPA is relevant to your business? Crosstabulation

			2.3 Do you think the DPA is relevant to your business?			Total
			yes	no	don't know	
2.5 Does your business have to register with the ICO with regard to Data Protection	yes	Count	94	12	3	109
		% within 2.5 Does your business have to register with the ICO with regard to Data Protection	86.2%	11.0%	2.8%	100.0%
	no	Count	25	8	1	34
		% within 2.5 Does your business have to register with the ICO with regard to Data Protection	73.5%	23.5%	2.9%	100.0%
	don't know	Count	86	14	6	106
		% within 2.5 Does your business have to register with the ICO with regard to Data Protection	81.1%	13.2%	5.7%	100.0%
Total		Count	205	34	10	249
		% within 2.5 Does your business have to register with the ICO with regard to Data Protection	82.3%	13.7%	4.0%	100.0%

Regardless of registration status, a high proportion of respondents believed that data protection principles are a good thing.

2.6 Is your business registered with the ICO? * 3.1 Are data protection principles a good thing when doing business? Crosstabulation

			3.1 Are data protection principles a good thing when doing business?					Total
			yes	no	sometimes	possibly	don't know	
2.6 Is your business registered with the ICO?	yes	Count	84	2	12	4	3	105
		% within 2.6 Is your business registered with the ICO?	80.0%	1.9%	11.4%	3.8%	2.9%	100.0%
	no	Count	26	4	9	3	2	44
		% within 2.6 Is your business registered with the ICO?	59.1%	9.1%	20.5%	6.8%	4.5%	100.0%
	don't know	Count	70	2	12	8	5	97
		% within 2.6 Is your business registered with the ICO?	72.2%	2.1%	12.4%	8.2%	5.2%	100.0%
Total		Count	180	8	33	15	10	246
		% within 2.6 Is your business registered with the ICO?	73.2%	3.3%	13.4%	6.1%	4.1%	100.0%

Regardless of registration status, a high proportion of respondents thought they should 'absolutely' protect data and personal information.

2.6 Is your business registered with the ICO? * 3.2 Do you think that your business should protect data and personal information? Crosstabulation

			3.2 Do you think that your business should protect data and personal information?					Total	
			absolutely	mostly	sometimes	no	not relevant		don't know
2.6 Is your business registered with the ICO?	yes	Count	91	8	2		1	2	104
		% within 2.6 Is your business registered with the ICO?	87.5%	7.7%	1.9%		1.0%	1.9%	100.0%
	no	Count	28	5	7	3	1		44
		% within 2.6 Is your business registered with the ICO?	63.6%	11.4%	15.9%	6.8%	2.3%		100.0%
	don't know	Count	80	12	2	1	1		96
		% within 2.6 Is your business registered with the ICO?	83.3%	12.5%	2.1%	1.0%	1.0%		100.0%
Total		Count	199	25	11	4	3	2	244
		% within 2.6 Is your business registered with the ICO?	81.6%	10.2%	4.5%	1.6%	1.2%	.8%	100.0%

Of the respondents who 'didn't know' or 'weren't' registered with the ICO, a high percentage said that the DPA was relevant to their business.

2.6 Is your business registered with the ICO? * 2.3 Do you think the DPA is relevant to your business? Crosstabulation

			2.3 Do you think the DPA is relevant to your business?			Total
			yes	no	don't know	
2.6 Is your business registered with the ICO?	yes	Count	92	11	3	106
		% within 2.6 Is your business registered with the ICO?	86.8%	10.4%	2.8%	100.0%
	no	Count	29	12	3	44
		% within 2.6 Is your business registered with the ICO?	65.9%	27.3%	6.8%	100.0%
	don't know	Count	83	10	4	97
		% within 2.6 Is your business registered with the ICO?	85.6%	10.3%	4.1%	100.0%
Total		Count	204	33	10	247
		% within 2.6 Is your business registered with the ICO?	82.6%	13.4%	4.0%	100.0%

A positive correlation can be seen when cross tabulating the importance of ‘the effort to modify existing systems’ with ‘the need to create new systems’.

Effort to modify existing systems * Need to create new systems Crosstabulation

			Need to create new systems						Total
			1.00	2.00	3.00	4.00	not meaningful	don't know	
Effort to modify existing systems	1.00	Count	19	13	4	3	2	41	
		% within Effort to modify existing systems	46.3%	31.7%	9.8%	7.3%	4.9%	100.0%	
	2.00	Count	6	29	7	7	1	50	
		% within Effort to modify existing systems	12.0%	58.0%	14.0%	14.0%	2.0%	100.0%	
	3.00	Count	1	7	26	18	3	55	
		% within Effort to modify existing systems	1.8%	12.7%	47.3%	32.7%	5.5%	100.0%	
	4.00	Count	1		7	77	2	87	
	% within Effort to modify existing systems	1.1%		8.0%	88.5%	2.3%	100.0%		
	not meaningful	Count				2	4	6	
	% within Effort to modify existing systems				33.3%	66.7%		100.0%	
	don't know	Count					1	1	
	% within Effort to modify existing systems						100.0%	100.0%	
Total	Count	27	49	44	107	12	1	240	
	% within Effort to modify existing systems	11.3%	20.4%	18.3%	44.6%	5.0%	.4%	100.0%	

Paradoxically, a significant proportion of those who placed least importance on ‘the effort to modify existing systems’ rated the term ‘data protection’ most highly.

Effort to modify existing systems * Data Protection Crosstabulation

			Data Protection					Total
			1.00	2.00	3.00	4.00	not meaningful	
Effort to modify existing systems	1.00	Count	16	11	5	6	3	41
		% within Effort to modify existing systems	39.0%	26.8%	12.2%	14.6%	7.3%	100.0%
	2.00	Count	17	21	11	1	1	51
		% within Effort to modify existing systems	33.3%	41.2%	21.6%	2.0%	2.0%	100.0%
	3.00	Count	24	21	5	5		55
		% within Effort to modify existing systems	43.6%	38.2%	9.1%	9.1%		100.0%
	4.00	Count	60	12	7	6	3	88
	% within Effort to modify existing systems	68.2%	13.6%	8.0%	6.8%	3.4%	100.0%	
	not meaningful	Count	2	2	1	1		6
	% within Effort to modify existing systems	33.3%	33.3%	16.7%	16.7%		100.0%	
	don't know	Count					1	1
	% within Effort to modify existing systems					100.0%	100.0%	
Total	Count	119	67	29	19	8	242	
	% within Effort to modify existing systems	49.2%	27.7%	12.0%	7.9%	3.3%	100.0%	

Those who said that the 'effort to modify existing systems' was least important to them also said that the 'monetary cost to comply' was least important.

Effort to modify existing systems * Monetary cost to comply Crosstabulation

			Monetary cost to comply						Total
			1.00	2.00	3.00	4.00	not meaningful	don't know	
Effort to modify existing systems	1.00	Count	14	8	6	13			41
		% within Effort to modify existing systems	34.1%	19.5%	14.6%	31.7%			100.0%
	2.00	Count	11	16	14	8	2		51
		% within Effort to modify existing systems	21.6%	31.4%	27.5%	15.7%	3.9%		100.0%
	3.00	Count	3	12	15	25			55
		% within Effort to modify existing systems	5.5%	21.8%	27.3%	45.5%			100.0%
	4.00	Count	2	7	8	67	3	1	88
	% within Effort to modify existing systems	2.3%	8.0%	9.1%	76.1%	3.4%	1.1%	100.0%	
	not meaningful	Count	1		2	3			6
	% within Effort to modify existing systems	16.7%		33.3%	50.0%			100.0%	
	don't know	Count					1		1
	% within Effort to modify existing systems					100.0%		100.0%	
Total	Count	31	43	45	116	6	1	242	
	% within Effort to modify existing systems	12.8%	17.8%	18.6%	47.9%	2.5%	.4%	100.0%	

Of those who thought the process of 'identifying the data held' in their business as being of the least importance, a high percentage also rated 'data sensitivity' as being very important to them.

Identification of data held * Data Sensitivity Crosstabulation

			Data Sensitivity					Total
			1.00	2.00	3.00	4.00	not meaningful	
Identification of data held	1.00	Count	22	13	7	9	1	52
		% within Identification of data held	42.3%	25.0%	13.5%	17.3%	1.9%	100.0%
	2.00	Count	13	16	8	7	3	47
		% within Identification of data held	27.7%	34.0%	17.0%	14.9%	6.4%	100.0%
	3.00	Count	17	7	11	3	1	39
		% within Identification of data held	43.6%	17.9%	28.2%	7.7%	2.6%	100.0%
4.00	Count	69	7	5	8	3	92	
	% within Identification of data held	75.0%	7.6%	5.4%	8.7%	3.3%	100.0%	
	not meaningful	Count	3	1	1	1	1	7
	% within Identification of data held	42.9%	14.3%	14.3%	14.3%	14.3%	100.0%	
Total	Count	124	44	32	28	9	237	
	% within Identification of data held	52.3%	18.6%	13.5%	11.8%	3.8%	100.0%	

The importance of confidentiality is not reflected in the efforts to modify existing systems – this may indicate that businesses already have systems establishes that support confidentiality.

Confidentiality * Effort to modify existing systems Crosstabulation

			Effort to modify existing systems						Total
			1.00	2.00	3.00	4.00	not meaningful	don't know	
Confidentiality	1.00	Count	36	37	36	68	6	1	184
		% within Confidentiality	19.6%	20.1%	19.6%	37.0%	3.3%	.5%	100.0%
	2.00	Count	4	10	14	9			37
		% within Confidentiality	10.8%	27.0%	37.8%	24.3%			100.0%
	3.00	Count		1	3	3			7
		% within Confidentiality		14.3%	42.9%	42.9%			100.0%
	4.00	Count	1	2	1	4			8
		% within Confidentiality	12.5%	25.0%	12.5%	50.0%			100.0%
	not meaningful	Count		1		1			2
		% within Confidentiality		50.0%		50.0%			100.0%
Total	Count	41	51	54	85	6	1	238	
	% within Confidentiality	17.2%	21.4%	22.7%	35.7%	2.5%	.4%	100.0%	

A high percentage of those who considered confidentiality very important, also considered that businesses should ‘absolutely’ protect data and information.

Confidentiality * 3.2 Do you think that your business should protect data and personal information? Crosstabulation

			3.2 Do you think that your business should protect data and personal information?						Total
			absolutely	mostly	sometimes	no	not relevant	don't know	
Confidentiality	1.00	Count	163	13	6		1		183
		% within Confidentiality	89.1%	7.1%	3.3%		.5%		100.0%
	2.00	Count	23	9	3	1		1	37
		% within Confidentiality	62.2%	24.3%	8.1%	2.7%		2.7%	100.0%
	3.00	Count	4	2		1			7
		% within Confidentiality	57.1%	28.6%		14.3%			100.0%
	4.00	Count	6	1	1				8
		% within Confidentiality	75.0%	12.5%	12.5%				100.0%
	not meaningful	Count				1	1		2
		% within Confidentiality				50.0%	50.0%		100.0%
Total	Count	196	25	10	3	2	1	237	
	% within Confidentiality	82.7%	10.5%	4.2%	1.3%	.8%	.4%	100.0%	

Almost 50% of those that ranked ‘privacy’ as being most important to them also felt little need to ‘create new systems’ in their business.

Privacy * Need to create new systems Crosstabulation

			Need to create new systems						Total
			1.00	2.00	3.00	4.00	not meaningful	don't know	
Privacy	1.00	Count	21	32	24	86	9	1	173
		% within Privacy	12.1%	18.5%	13.9%	49.7%	5.2%	.6%	100.0%
	2.00	Count	4	10	13	16	2		45
		% within Privacy	8.9%	22.2%	28.9%	35.6%	4.4%		100.0%
	3.00	Count	1	3	5	2	1		12
		% within Privacy	8.3%	25.0%	41.7%	16.7%	8.3%		100.0%
	4.00	Count	1	2	1	2			6
		% within Privacy	16.7%	33.3%	16.7%	33.3%			100.0%
	not meaningful	Count		2	1	1			4
		% within Privacy		50.0%	25.0%	25.0%			100.0%
Total	Count	27	49	44	107	12	1	240	
	% within Privacy	11.3%	20.4%	18.3%	44.6%	5.0%	.4%	100.0%	

Nearly 100% of respondents who considered the term ‘data protection’ very important to them considered the terms ‘ security of data’, ‘privacy’ and ‘confidentiality’ as very important as well.

Data Protection * Privacy Crosstabulation

			Privacy					Total
			1.00	2.00	3.00	4.00	not meaningful	
Data Protection	1.00	Count	114	5			1	120
		% within Data Protection	95.0%	4.2%			.8%	100.0%
	2.00	Count	34	24	8	1		67
		% within Data Protection	50.7%	35.8%	11.9%	1.5%		100.0%
	3.00	Count	15	9	3	2		29
		% within Data Protection	51.7%	31.0%	10.3%	6.9%		100.0%
	4.00	Count	8	6	1	3	1	19
		% within Data Protection	42.1%	31.6%	5.3%	15.8%	5.3%	100.0%
	not meaningful	Count	4	1			3	8
		% within Data Protection	50.0%	12.5%			37.5%	100.0%
Total	Count	175	45	12	6	5	243	
	% within Data Protection	72.0%	18.5%	4.9%	2.5%	2.1%	100.0%	

Many of those who rated ‘data protection’ highly also rated the ‘identification of data held’ in their business as low.

Data Protection * Identification of data held Crosstabulation

			Identification of data held					Total
			1.00	2.00	3.00	4.00	not meaningful	
Data Protection	1.00	Count	20	13	11	69	2	115
		% within Data Protection	17.4%	11.3%	9.6%	60.0%	1.7%	100.0%
	2.00	Count	18	15	20	12	2	67
		% within Data Protection	26.9%	22.4%	29.9%	17.9%	3.0%	100.0%
	3.00	Count	6	10	5	6	2	29
		% within Data Protection	20.7%	34.5%	17.2%	20.7%	6.9%	100.0%
	4.00	Count	5	6	3	3	1	18
		% within Data Protection	27.8%	33.3%	16.7%	16.7%	5.6%	100.0%
	not meaningful	Count	3	3		2		8
		% within Data Protection	37.5%	37.5%		25.0%		100.0%
Total	Count	52	47	39	92	7	237	
	% within Data Protection	21.9%	19.8%	16.5%	38.8%	3.0%	100.0%	

If ‘information handling’ is considered of low importance, so is the ‘effort’ and ‘need’ to modify and/or create new systems. This may indicate the type of information used by some businesses.

Information Handling * Effort to modify existing systems Crosstabulation

			Effort to modify existing systems						Total
			1.00	2.00	3.00	4.00	not meaningful	don't know	
Information Handling	1.00	Count	20	21	23	22	3		89
		% within Information Handling	22.5%	23.6%	25.8%	24.7%	3.4%		100.0%
	2.00	Count	11	19	7	20	2	1	60
		% within Information Handling	18.3%	31.7%	11.7%	33.3%	3.3%	1.7%	100.0%
	3.00	Count	5	7	12	18			42
		% within Information Handling	11.9%	16.7%	28.6%	42.9%			100.0%
	4.00	Count	5	2	10	26	1		44
		% within Information Handling	11.4%	4.5%	22.7%	59.1%	2.3%		100.0%
	not meaningful	Count		2	2	2			6
		% within Information Handling		33.3%	33.3%	33.3%			100.0%
Total	Count	41	51	54	88	6	1	241	
	% within Information Handling	17.0%	21.2%	22.4%	36.5%	2.5%	.4%	100.0%	

There is a strong positive link between ‘information handling’ and ‘information risk’ indicating the connection that respondents make between the two terms.

Information Handling * Information Risk Crosstabulation

			Information Risk					Total
			1.00	2.00	3.00	4.00	not meaningful	
Information Handling	1.00	Count	51	19	6	8	5	89
		% within Information Handling	57.3%	21.3%	6.7%	9.0%	5.6%	100.0%
	2.00	Count	13	24	9	9	5	60
		% within Information Handling	21.7%	40.0%	15.0%	15.0%	8.3%	100.0%
	3.00	Count	2	8	22	10		42
		% within Information Handling	4.8%	19.0%	52.4%	23.8%		100.0%
4.00	Count	1	4	7	28	3	43	
	% within Information Handling	2.3%	9.3%	16.3%	65.1%	7.0%	100.0%	
not meaningful	Count				1	5	6	
	% within Information Handling				16.7%	83.3%	100.0%	
Total	Count	67	55	44	56	18	240	
	% within Information Handling	27.9%	22.9%	18.3%	23.3%	7.5%	100.0%	

Those who found DPA compliance ‘very easy’ also ranked the term ‘data protection’ as very important to them and their business.

3.5 How easy do you feel it is to comply with the DPA? * Data Protection Crosstabulation

			Data Protection					Total
			1.00	2.00	3.00	4.00	not meaningful	
3.5 How easy do you feel it is to comply with the DPA?	very easy	Count	40	7	4	5	1	57
		% within 3.5 How easy do you feel it is to comply with the DPA?	70.2%	12.3%	7.0%	8.8%	1.8%	100.0%
	quite easy	Count	41	20	13	4		78
		% within 3.5 How easy do you feel it is to comply with the DPA?	52.6%	25.6%	16.7%	5.1%		100.0%
	a small effort	Count	23	17	6	3	2	51
		% within 3.5 How easy do you feel it is to comply with the DPA?	45.1%	33.3%	11.8%	5.9%	3.9%	100.0%
	a large effort	Count	9	6	3	2	1	21
	% within 3.5 How easy do you feel it is to comply with the DPA?	42.9%	28.6%	14.3%	9.5%	4.8%	100.0%	
almost impossible	Count	2	1		1		4	
	% within 3.5 How easy do you feel it is to comply with the DPA?	50.0%	25.0%		25.0%		100.0%	
don't know	Count	4	15	3	4	4	30	
	% within 3.5 How easy do you feel it is to comply with the DPA?	13.3%	50.0%	10.0%	13.3%	13.3%	100.0%	
Total	Count	119	66	29	19	8	241	
	% within 3.5 How easy do you feel it is to comply with the DPA?	49.4%	27.4%	12.0%	7.9%	3.3%	100.0%	

Those who considered compliance with the DPA very easy also considered that the 'effort to modify existing systems in order to comply' would be relatively easy (of low importance).

3.5 How easy do you feel it is to comply with the DPA? * Effort to modify existing systems Crosstabulation

			Effort to modify existing systems						Total
			1.00	2.00	3.00	4.00	not meaningful	don't know	
3.5 How easy do you feel it is to comply with the DPA?	very easy	Count	4	4	9	38	1		56
		% within 3.5 How easy do you feel it is to comply with the DPA?	7.1%	7.1%	16.1%	67.9%	1.8%		100.0%
	quite easy	Count	15	23	20	18	2		78
		% within 3.5 How easy do you feel it is to comply with the DPA?	19.2%	29.5%	25.6%	23.1%	2.6%		100.0%
	a small effort	Count	7	11	13	19	1		51
		% within 3.5 How easy do you feel it is to comply with the DPA?	13.7%	21.6%	25.5%	37.3%	2.0%		100.0%
	a large effort	Count	6	7	3	4	1		21
	% within 3.5 How easy do you feel it is to comply with the DPA?	28.6%	33.3%	14.3%	19.0%	4.8%		100.0%	
almost impossible	Count	1	1		2			4	
	% within 3.5 How easy do you feel it is to comply with the DPA?	25.0%	25.0%		50.0%			100.0%	
don't know	Count	8	5	9	6	1	1	30	
	% within 3.5 How easy do you feel it is to comply with the DPA?	26.7%	16.7%	30.0%	20.0%	3.3%	3.3%	100.0%	
Total	Count	41	51	54	87	6	1	240	
	% within 3.5 How easy do you feel it is to comply with the DPA?	17.1%	21.3%	22.5%	36.3%	2.5%	.4%	100.0%	

**ANNEX 5: ANALYSIS OF SCENARIOS FOR SMEs AND DATA PROTECTION
(PEST/SWOT MATRICES)**

Political Impact Analysis of DPA within SMEs		
	Strengths	Weaknesses
Opportunities	<ul style="list-style-type: none"> ▪ Most SMEs able to adapt, and so respond to DPA ▪ In some SMEs, processes can be easily adapted to implement changes specified by the ICO ▪ Opportunity to gain certification – increasing SMEs' profile in wider community, and ability to work with OEMs, larger companies & the public sector 	<ul style="list-style-type: none"> ▪ SMEs left to make difficult and potential litigious decisions without sufficient resource, knowledge or capability ▪ Duplication or reinforcement of legislation in other Acts ▪ May lack ability/knowledge to take up advice and guidelines from ICO
Threats	<ul style="list-style-type: none"> ▪ Compliance by SMEs enforced actively by Government Agencies ▪ Disclosure of competitive and sensitive market information under the law becomes more actively monitored ▪ Guidelines of data protection supervisory authority within ICO office made more explicit, removing interpretive ambiguity ▪ Creation of own privacy codes not congruent with ICO/DPA (opt-out, non-compliance) ▪ Ability by SMEs to undertake trans-border business outwith the legislation of DPA ▪ Negative views of SMEs towards compliance/government 	<ul style="list-style-type: none"> ▪ SMEs don't know about or don't know how to comply with regulation ▪ SMEs may lack ability or resources to respond to prosecution for non-compliance ▪ Integration of international legislation into DP principles and Act
<p>Commentary</p> <p>Prior to the DPA being introduced individual consumers had little protection against abuse of their personal data and as such individuals were open to exploitation. Since the act was introduced evidence would suggest that individuals (and the data held by organisations including SMEs) are better protected under the current legislation. As the commissioner did not create a specific section under the act for SMEs many managers believe that semantic gaps in the current act that could be approved upon in legislation. However, there are a number of issues to consider these issues cover:</p> <ul style="list-style-type: none"> • Cultural differences between SMEs • Ability of SMEs to absorb complex legislative documents • SMEs reliance on 3rd parties to provide legal and managerial support • SMEs ability to enforce and comply with any new legislation 		

Economic Impact Analysis of DPA within SMEs		
	Strengths	Weaknesses
Opportunities	<ul style="list-style-type: none"> ▪ Chance for SMEs to use DP principles & compliance to build up knowledge of consumers and markets ▪ For data-unaware SMEs, driver/stimulus to create & develop information processes and IMS Strategy ▪ For data-aware SMEs, chance to organise and simplify information processes and IMS strategy ▪ Chance for SMEs to obtain free or low cost advice/guidance about DPA (& data) ▪ Efficiency gains through compliance with Act & principles 	<ul style="list-style-type: none"> ▪ Certain SMEs have no data control capability or function ▪ Key decision-makers lack knowledge &/or time to actively address DP issues ▪ Cost to SMEs to process and maintain data and information over time ▪ Purchase cost of systems and applications to manipulate data and other sources of information ▪ Low perceived 'downside' or cost from non-compliance ▪ Ongoing costs of physical and data security to SMEs (SMEs ability to absorb support costs)
Threats	<ul style="list-style-type: none"> ▪ Sharing information and data with other SMEs may reduce competitive position (disincentive to comply) ▪ High costs of investment in electronic data management (disincentive to comply) ▪ Increases in information costs limit potential for investment by SMEs in other areas of operation ▪ Wider costs to SMEs to implement IMS Strategy ▪ Possibility of future changes may reduce incentive to comply 	<ul style="list-style-type: none"> ▪ SMEs unwilling or unable to invest in electronic resource to deal with/manage DP Cost to SMEs to implement future legislative changes to the Act ▪ Cost to compliant SMEs of responding to changes in the legislation ▪ Ability to pay for external advice ▪ Perceived threat of fines is not commensurate with perceptions of ICO response to non-compliance
<p>Commentary</p> <p>Within SMEs conventional information management (including data management and data protection) has been traditionally shepherded through many of its various stages, from initiation to end-user delivery by a handful key management staff, supported by ad-hoc employees without formal or legal training.</p> <p>For many SMEs the exploitation of the digital information economy depends critically on unprecedented numbers of highly qualified managers and others armed with technical degrees, commanding salaries far greater than the average wages and this poses a barrier for many small company's. For those SMEs involved in the digital economy vast quantities of data generated by commercial, government and non-profit institutions consist largely of conventional print documents. In order to acquire, catalogue and disseminate print information, database producers in and out of government must continue to rely on traditional methods or expensive digitizing equipment. As the digital economy emerges, computerized information must be added to existing files, sometimes requiring parallel technologies, staff, and other infrastructure in order to accommodate both print and online documents. What's more, because the digital economy is in its infancy, few common standards have been accepted that a wide variety of non-compatible electronic files must be integrated at great cost.</p>		

Societal Impact Analysis of DPA within SMEs		
	Strengths	Weaknesses
Opportunities	<ul style="list-style-type: none"> ▪ SMEs are considered wealth creators and wealth creation is important to the UK economy and ongoing and new employment (a need to amend/ensure legislation enables/does not prevent this) ▪ Within SMEs, internal awareness about DPA principles and the potential for their adoption 	<ul style="list-style-type: none"> ▪ SME owner-manager views data protection as secondary activity ▪ Data control responsibilities and duties shared across individuals (i.e. shared responsibility towards compliance) ▪ SMEs tend to be considered independent and self-reliant, leading to possible governance issues ▪ Lack of/insufficient control over or management of information systems makes access easier to data
Threats	<ul style="list-style-type: none"> ▪ User empowered information systems make it easier to access information and data ▪ Negative attitudes of the general public to SMEs holding personal data ▪ Perception of ICO as 'social engineer' of DP values by SMEs may discourage engagement ▪ Consumer values towards SMEs ▪ Increased awareness of personal rights by consumers under the act 	<ul style="list-style-type: none"> ▪ DPA implies rather than makes explicit social responsibility implications, i.e. does not directly address these issues ▪ A need to address the extent to which the ICO is empathetic towards and understanding of SMEs ▪ Increased social empowerment will drive consumers to ask for increased access to information ▪ How relevant/tailored is the DPA to virtual, on-line business? ▪ How can the ICO manage or deal with compliance and DP issues in on-line businesses?
<p>Commentary</p> <p>Issues surrounding security of IT systems have become a major concern for UK society and individuals working within the local community. Hence to ensure a conducive and safe electronic environment, the necessary steps in enhancing IT security must be undertaken. In tandem with what the ICO IS doing. SMEs should adopt the following measures:</p> <ul style="list-style-type: none"> ▪ Establishment of internal security guidelines and policy information to protect data ▪ Promoting the positive use of the 8 DPA principles ▪ Harmonizing business procedures to facilitate new ways of transacting through the electronic media ▪ Furthering knowledge transfer between SMEs 		

Technical Impact Analysis of DPA within SMEs		
	Strengths	Weaknesses
Opportunities	<ul style="list-style-type: none"> ▪ Finding new ways of managing information and data with SMEs through technology reengineering ▪ Potential for SMEs to invest in ICT 	<ul style="list-style-type: none"> ▪ Poor technology and lack of technology strategy in SMEs ▪ Many lack technical expertise to protect (1) sensitive personal data (2) confidentiality agreements with 3rd party providers ▪ SMEs' inability to move data between different application data bases ▪ Failure of SMEs to recognise what is company and what is individual data ▪ Failure of SMEs to recognise the value of information has to the organisation
Threats	<ul style="list-style-type: none"> ▪ Many SMEs see information as intellectual property this may be at odds with the views held by the ICO ▪ SMEs' reliance on other 3rd party proprietary technology puts data and information at risk ▪ SMEs' lack strategic skills in technology 	<ul style="list-style-type: none"> ▪ Failure of SMEs to use appropriate information and data protocols, which would prevent systems that share a network corrupting one another's data ▪ SMEs have poor lines of communication to manage issues in information management and leave themselves exposed
<p>Commentary</p> <p>While technological advances offer new hope that broad scale information sharing can become a reality, technology does not operate in a vacuum. Technical, programmatic, and policy issues must be addressed concurrently within a community of shared interests. The ICO Strategic Plan does not appear to address these issues.</p> <ul style="list-style-type: none"> ▪ Recommend for SMEs standards for the collection, collation, storage, analysis, evaluation, and dissemination of information ▪ Recommend for SMEs training standards for all levels of the information sharing ▪ Maintain a Web-based resource for data exchange and information ▪ Adapting appropriate e-commerce technology, harnessing technical and operational standards and striving for sustainable technology transfer. <p>The up take of information technology has resulted in a shortage of skilled knowledge workers to SMEs. There is also a widening gap between IT 'haves' and 'have-nots' across sectors and within regions that is between rural and urban areas and between the younger and older generation. Another challenge is the 'hollowing' of culture that is the erosion of values and ethics through mass global culture pervading the Internet and electronic media.</p>		

**ANNEX 6: THE ENTERPRISE RESEARCH AND DEVELOPMENT UNIT AT THE
UNIVERSITY OF LINCOLN**

RESEARCH UNITS AT LINCOLN BUSINESS SCHOOL

ENTERPRISE RESEARCH AND DEVELOPMENT UNIT (ERDU)

The Enterprise Research and Development Unit was established in October, 2002, as a focus for research and development activity related to small and medium enterprise development and entrepreneurship. The Unit is located within the Business School at the University of Lincoln and is directed by Andrew Atherton, Professor of Enterprise and Entrepreneurship. The Unit has already developed a portfolio of 'R&D' projects and activities related to enterprise and small business, including:



- Consortium partner in the ATHENA European 5th Framework project, undertaking project assessment and policy research to investigate good and best practice in support for business start-ups and new businesses across the EU.
- ATHENA benchmarking study on 'University Spin-Offs and Knowledge Transfer' across the EU member nations.
- Development of municipal SME support and promotion strategies in six pilot cities in China, funded by the Department for International Development.
- Adviser to the Valencia region development agency PRICOVA on the design of a Regional Innovation Strategy for Valencia.
- Development of an innovative portfolio of accredited postgraduate programmes leading to the award of a Masters in Entrepreneurial Management and Entrepreneurship through the University of Lincoln (to be launched Spring 2004).
- Founder and editor of EntreNews, the newsletter for the Entrepreneurship Innovation and Small Business Chapter of the European Foundation for Management Development.
- Adviser and consultant to the Lincoln Media Incubator.

COMMUNITY OPERATIONAL RESEARCH UNIT (CORU)

CORU became part of the University of Lincoln as the result of a successful national bid to become the home of the Community OR Unit. The Unit has an extensive record of working on community development and research projects, locally, regionally and nationally. It has been in operation for more than 5 years and currently has a core staffing of five dedicated researchers and affiliated academics from across the Faculty.

Headed by Dr Rebecca Herron (Senior Research Fellow), its research is focused on assisting community groups and voluntary organisations to become more effective by providing expertise in problem structuring and decision-making. For this purpose it develops and applies management science / operational research/ systems knowledge appropriate in the circumstances of community organisations. The emphasis is on frameworks that support participation, empowerment and transparency. Its method of work is to develop partnerships and networks between stakeholders pursuing personal health, social and economic improvement in local communities.

CORU acts either (1) as lead agency to seek funding from major or minor grant giving sources by designing, implementing and evaluating research or other projects that have the potential to generate useful publications, or (2) as contributor to other agency led projects. CORU has a distinct role within the community taking part in projects within the locality often on a voluntary basis. It also has a facilitating role linking various research and consultancy within the University. The work of CORU has been underpinned by a £20,000 per year contribution from the Lincoln Co-operative Society and £10,000 from Lincolnshire Training & Enterprise Council.