STATES OF JERSEY

DATA PROTECTION (JERSEY) LAW 2005: ANNUAL REPORT FOR 2006

Presented to the States on 9th July 2007
by the Chief Minister

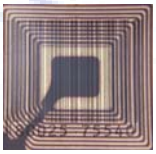
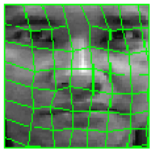
STATES GREFFE

2007 Price code: C R.66

THE OFFICE OF THE
Data Protection Commissioner

Annual Report 2006




Data Protection

A Quick Guide

What is the Data Protection Law (DPL)?

The Data Protection (Jersey) Law 2005 seeks to strike a balance between the rights of individuals and the sometimes competing interests of those with legitimate reasons for using personal information.

The Law gives individuals certain rights regarding information held about them. It places obligations on those who process information (data controllers) while giving rights to those who are the subject of that data (data subjects). Personal information covers both facts and opinions about the individual.

Anyone processing personal information must notify the Data Protection Commissioner's Office that they are doing so, unless their processing is exempt. Notification costs £50 per year.

The eight principles of good practice

Anyone processing personal information must comply with eight enforceable principles of good information handling practice.

These say that data must be:

1. fairly and lawfully processed;
2. processed for one or more specified and lawful purposes;
3. adequate, relevant and not excessive;
4. accurate and up to date;
5. not kept longer than necessary;
6. processed in accordance with the individual's rights;
7. kept safe and secure;
8. not transferred to countries outside European Economic area unless country has adequate protection for the individual.

Individuals can exercise a number of rights under data protection law.

Rights of access
Allows you to find out what information is held about you;

Rights to prevent processing
Information relating to you that causes substantial unwarranted damage or distress;

Rights to prevent processing for direct marketing
You can ask a data controller not to process information for direct marketing purposes;

Rights in relation to automated decision-taking
You can object to decisions made only by automatic means e.g. there is no human involvement;

Right to seek compensation
You can claim compensation from a data controller for damage or distress caused by any breach of the Law;

Rights to have inaccurate information corrected
You can demand that an organisation corrects or destroys inaccurate information held about you;

Right to complain to the Commissioner
If you believe your information has not been handled in accordance with the Law, you can ask the Commissioner to make an assessment.

What is data protection?

Data protection is the safeguarding of the privacy rights of individuals in relation to the processing of personal information. The Data Protection (Jersey) Law 2005 places responsibilities on those persons processing personal information, and confers rights upon the individuals who are the subject of that information.

Contents

Foreword

This is my third report as Data Protection Commissioner for the Bailiwick of Jersey. It covers the year 2006, the first full year since the implementation of the Data Protection (Jersey) Law 2005.

The Data Protection (Jersey) Law 2005 came into force in December 2005 making 2006 the first full year of operation. Despite being a huge leap forward for the Island in terms of data protection regulation, the new Law celebrated its first birthday with very little fuss. A lot of effort had been put into ensuring the local community were well informed of the imminent changes and that certainly paid off.

The first full year of implementation saw continued success of the new website and online notification system. 50% of data controllers have now notified online. Feedback we are getting suggests that this streamlined notification system has helped data controllers understand their legal obligations and see compliance with the Law as less of an administrative burden. As one of our primary objectives is to improve awareness and compliance level, this is welcome news.

Whilst the implementation of the new Law has been relatively trouble-free, the year was not without its challenges.

As technology advances it is certainly true to say that personal information collection is fast becoming ubiquitous.

"A lot of effort had been put into ensuring the local community were well informed of the imminent changes and that certainly paid off."

Both the private and public sector are seeing exponential growth in this area.

In the private realm we have vast amounts of our information being collected and used for things like loyalty cards, marketing and profiling. In government too we can see developments in areas such as the population register, health screening and welfare payments – all of which are demanding ever more information from us all. This is exactly why we need a robust piece of legislation to ensure that a sensible balance is struck to allow for legitimate data collection without compromising our basic rights to have that information protected and our privacy respected.

"Individual liberty is a valuable asset and may be one which all of us are at risk of taking for granted but is certainly something worth fighting for."

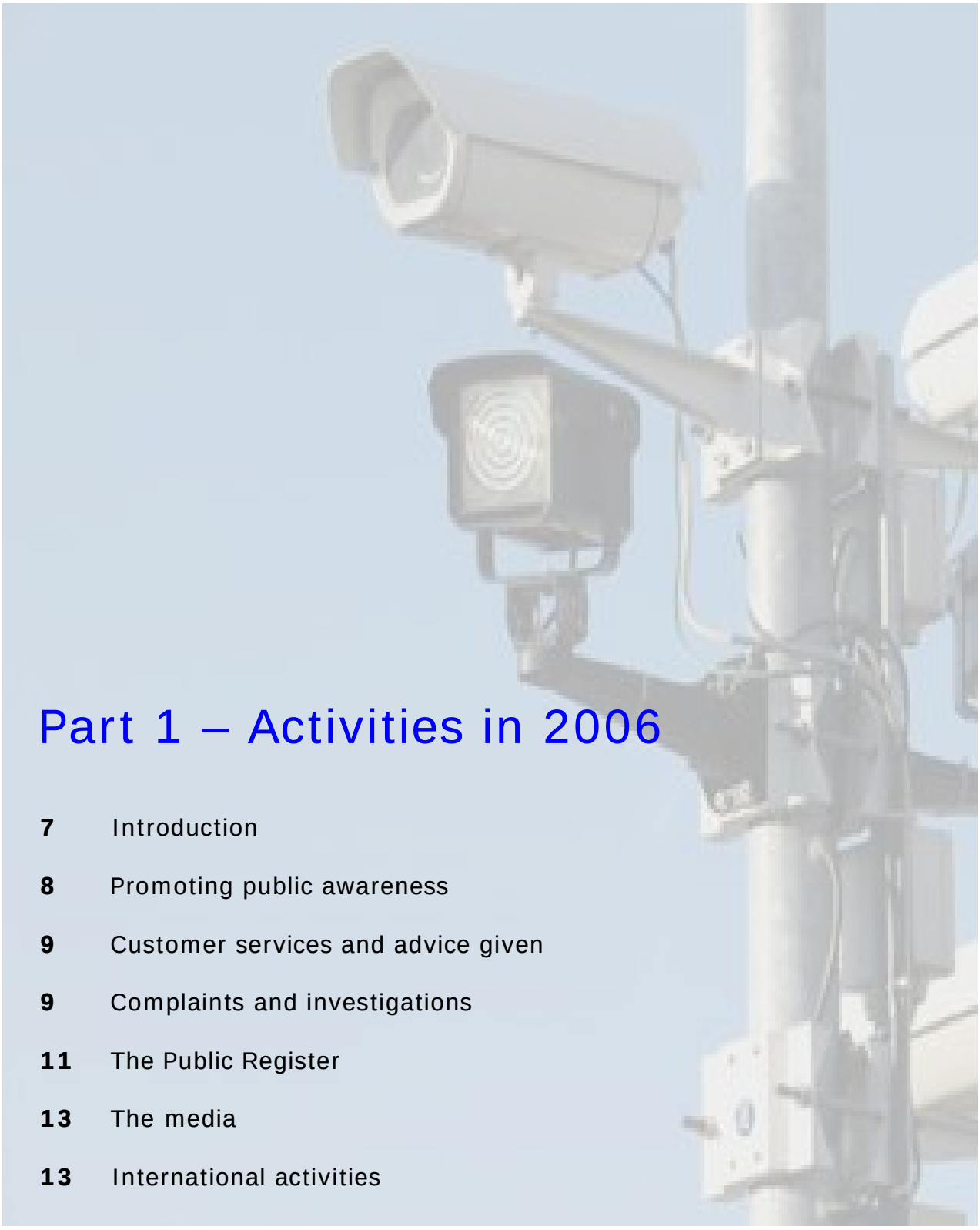
It is not always an easy balance to strike – never more so than in this age of emotive debate on security verses liberty. It is therefore vital that discussions surrounding these important areas are carried out in a public and informed way. We all have a right to know what the issues are and how our rights are to be safeguarded.

We are a small but dedicated team that work tirelessly to raise awareness of individuals' rights, and organisations responsibilities. We focus heavily on communicating these rights and responsibilities throughout the Island but also have a significant workload relating to enquiries and complaints. This too is an area of our work which is increasing at a noticeable rate – a fact which on the face of it may appear to evidence poor compliance levels, but in reality I consider to be a reflection of increasing awareness of individuals.

Firstly in understanding that they have rights enshrined in Law to have their personal information protected, and secondly to know that they have a route for redress should things go wrong. We must acknowledge some of the very good work being done in both the private and public sector to ensure compliance with the legal requirements. That does not mean we are complacent and it must be said that there is still significant room for improvement of compliance levels across Jersey.

Individual liberty is a valuable asset and may be one which all of us are at risk of taking for granted but is certainly something worth fighting for.

Emma Martins
Data Protection Commissioner



Part 1 – Activities in 2006

Introduction

The Data Protection (Jersey) Law 2005 creates a framework for the handling of personal information across all areas of society. But what is personal data? It is information about us as individual people, which can sometimes be of a sensitive nature. The real issue is how this information about us is handled by the people to whom we entrust it.

Organisations across the Island are tasked with protecting the information they hold about individuals and are legally obliged to apply certain standards which enable them to handle that information in the correct manner. Those organisations which choose to act outside that framework do so at the risk of legal action being taken against them by the individual affected, as well as the possibility of enforcement action by the Commissioner or the Courts.

The Data Protection (Jersey) Law 2005 provides a legal basis upon which the Commissioner can exercise her powers of enforcement. Nonetheless, the Commissioner and her team pride themselves on the fact that as yet, no Enforcement Notices have been served upon a local organisation since the implementation of the 2005 Law and see this as indicative of the successful proactive compliance work undertaken by the Commissioner and her staff in bringing data protection to the fore.

There will, however, be occasions where the issuing of an Information or Enforcement Notice will be the appropriate measure to be taken to ensure compliance by a data controller.

The Eight Data Protection Principles are easy to understand and make for a common sense approach to the handling of personal data by organisations. The Principles are rules which should be respected if data controllers are to ensure the trust of their customers and this applies equally in the public sector where more often than not, the public do not have a choice but to surrender their information.

The following pages give an insight into the work carried out by the Commissioner and her team during 2006, especially having regard for the overall approach of the Office as a regulatory body.

Of all the many functions the Office undertakes on a daily basis, promoting the general awareness of Data Protection both to the public and to data controllers forms the largest and arguably the most important part of our work.

Paul Vane, Deputy Commissioner

Promoting Public Awareness

Of all the many functions the Office undertakes on a daily basis, promoting the general awareness of Data Protection both to the public and to data controllers forms the largest and arguably the most important part of our work.

During 2006, the Office responded to a large volume of general enquiries via telephone, e-mail and post from the business sector and individuals alike. The nature of the calls varied considerably, but included enquiries such as:

- How to make, and how to deal with a subject access request;
- The formulation of data processing contracts and data sharing protocols;
- Disclosures of personal data to other countries outside the European Economic Area;
- Workplace monitoring; such as e-mail monitoring and the recording of telephone calls;
- Human resources issues, particularly data retention and the storage of HR files;
- The inclusion of fair processing statements on data collection forms;
- Notification queries;
- Publication of photographs on the internet.

The above list is not exhaustive and is merely an indication of the variation in the enquiries received.

Some of those queries, such as those in relation to outsourcing issues and employee references, have triggered the publication of focused guidance or good practice notes on the Commissioner's website.

Formal guidance was also published in relation to charities and non-profit making organisations as well as guidance for the inclusion of privacy statements on websites.

Customer Service and Advice Given

The Office of the Data Protection Commissioner is a public office serving the Island's community. It is therefore vital that it maintains a high standard of customer service and is in a position to provide the best service at all times to the general public.

To many, the 'front face' of the Office is through the Commissioner's website (www.dataprotection.gov.je) which details all the latest information and guidance published. The website is reviewed on a regular basis to ensure that the public has access to accurate and up to date information. During 2006, the website averaged 4363 visits per month, which calculates to an average of 143 visits per day.

Another valuable method of increasing awareness of data protection has been through presentations given by the Commissioner and her Deputy. The Office receives many requests for speaking engagements however it would be impossible to accept all invitations made due to the other commitments and activities of the staff involved. That said, the Commissioner and her Deputy delivered a total of 36 presentations to a wide variety of organisations between them during 2006, with the subject matter ranging from a general overview of the Law and Principles to more focused topics such as human resources and health data processing issues. Further details of the presentations are provided in Appendix 1.

Complaints and Investigations undertaken

One of the most significant powers conferred upon the Commissioner is the power of investigation of alleged breaches of the Law or Principles.

Complaints received by the Commissioner are extremely varied in their nature and the Commissioner can exercise a number of powers including the issuing of an Information Notice, Special Information Notice or an Enforcement Notice, as well as seeking a prosecution through the Island's Attorney General.

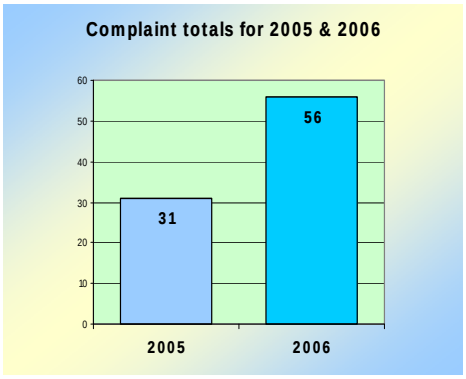
As yet, no Jersey data controller has been subject of prosecution through the Island's courts as a result of a copmplaint made to the Commissioner, and the vast majority of complaints have been resolved before the need to invoke any significant enforcement measures such as those described.

In the majority of cases investigated during 2006, complaints found to be substantiated were resolved by the respective data controller updating and improving their policies and procedures.

Where a breach of the data protection principles is identified, individuals may decide to use that decision when taking forward claims for compensation for damage or distress suffered as a direct result of the breach. In one specific case involving two data controllers, an individual was successful in claiming £500 compensation from each organisation.

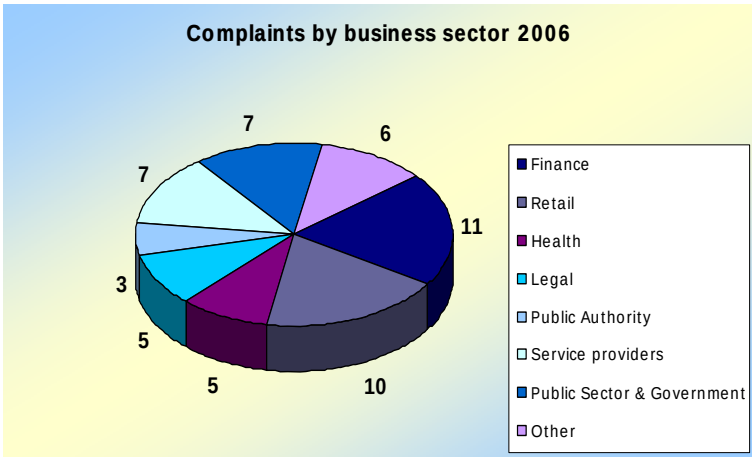
The number of complaints received during 2006 increased to 56, a rise of 84% from 2005. This was wholly expected as the public's general awareness of data protection increases.

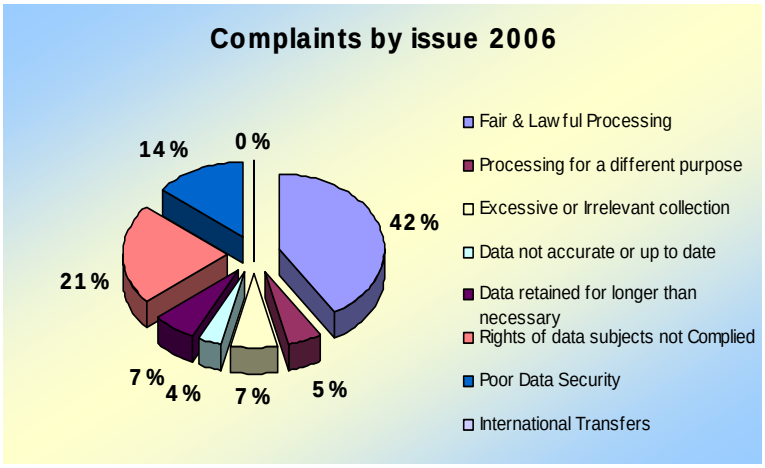
The illustrations below demonstrate how those complaints are spread across different sectors of business and also detail the general nature of the complaint by Principle.



2006 saw an 84% rise in the number of complaints received by the Commissioner.

37% of complaints received were in relation to the processing activities of the finance and retail industries.





42% of complaints were in relation to allegations of unfair processing.

21% were alleged to have failed to allow individuals to exercise their rights under the Law, specifically in relation to subject access.

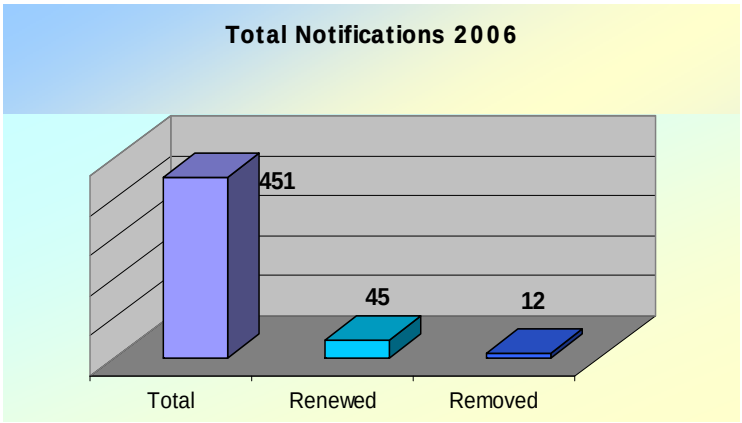
The Public Register

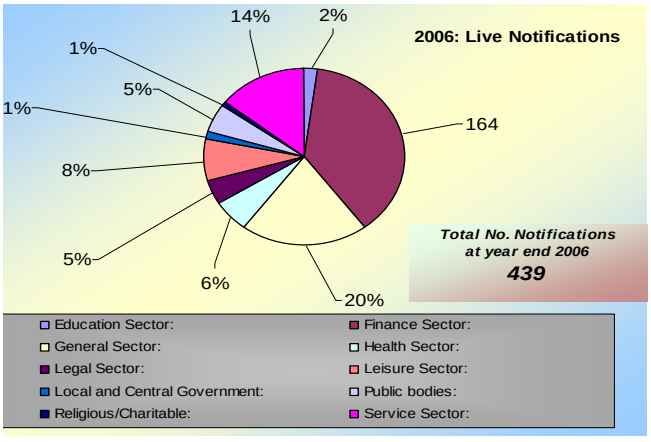
2006 saw the first full year of the operation of the new on-line notification system and on-line public register. Whilst the inevitable teething problems were evident on the administration side of the system, the majority of users had no complaints and many complemented the Office on the ease of notification when compared to the previous method of registration under the former 1987 Law.

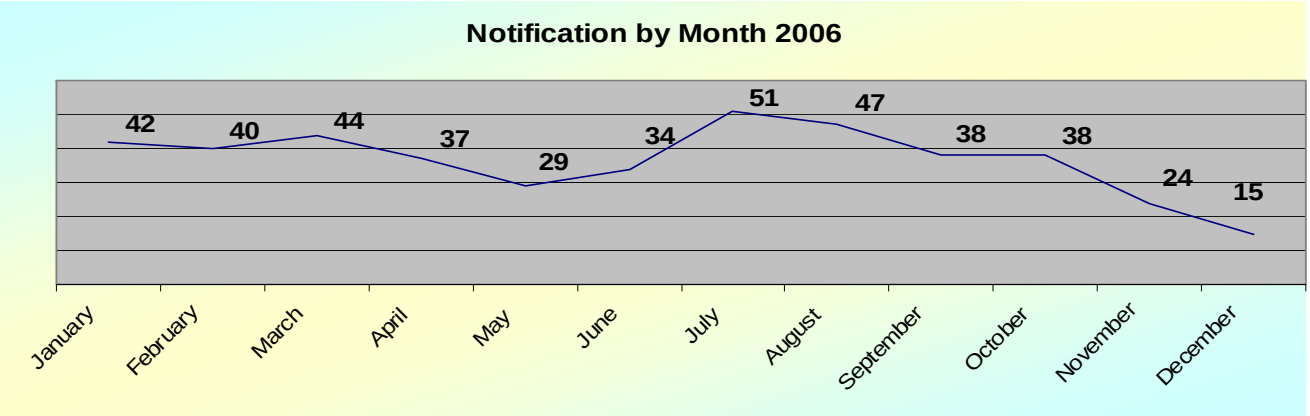
A second phase of development and enhancement to the notification system was undertaken during the summer months in order to further streamline the process, and a third phase of additional enhancements is planned for the second half of 2007.

The transitional period between the former 1987 Law and the new 2005 Law, particularly in relation to the registration process, makes it extremely difficult to draw any kind of comparative statistics. In addition, the streamlining and mergers of many large private sector organisations has had an impact on the number of registrations or notifications held. At the end of 2006, there were still 837 active registrations under the 1987 Law, which are due to renew under the new system either during 2007 or 2008.

The new process of annual notification started on 1st December 2005. As such there is no comparative data for the number of new notifications received during 2006. Overall, there were a total of 451 new notifications received during 2006, which can be illustrated by sector as shown below.







For this annual report, no statistics have been published in relation to registrations under the former 1987 Law. The main reason for this is due to the difficulty in making comparisons between the old-style registration process and the new notification facility. The two systems are entirely different and it would be impossible to draw any useful conclusions from comparison between the registration or notification figures for 2005 and 2006.

In addition, the streamlined effect of the new system has led to many data controllers being able to consolidate several registrations into one single notification.

Also of important note is the fact that a number of data controllers previously required to register under the 1987 Law can now benefit from an exemption from notification under the 2005 Law. This however does not exempt these data controllers from having to comply with the requirements of the Law and the Principles of data protection.

Another factor which has resulted in the consolidation of registrations is mergers and acquisitions. A number of data controllers have either merged or have been subject of commercial takeover by another data controller. This has resulted in the submission of one new umbrella notification replacing a number of registrations.

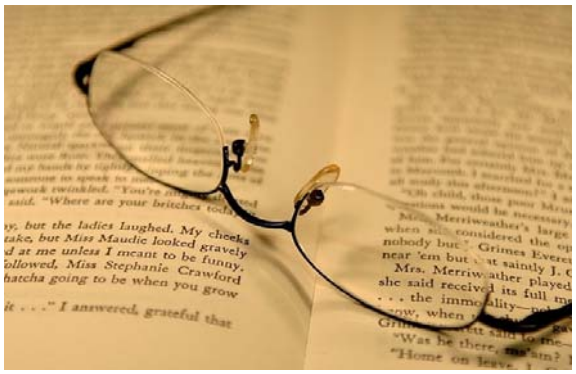
Despite all of the above, the number of new notifications received under the 2005 Law since its implementation in December 2005 has increased steadily. Whilst the projected figure for the total number of notifications received by the end of the transitional period is in the region of 1600, this figure is expected to be higher if the trend of new notifications continues as it has done over the past 18 months.

The Media

Data protection all too often hits the headlines for all the wrong reasons. It is true to say that in the main, such coverage is purely as a result of either a misinterpretation of the Law or a lack of awareness or appreciation of surrounding issues.

Jersey is no different in this respect, however we are fortunate in such a small jurisdiction that misleading or mis-informed articles are few and far between. The vast majority of local press coverage reflects the work of the Commissioner and the requirements of the Law in a positive light and in such a way that it further enhances the public awareness of data protection requirements and current issues.

During 2006, data protection was the subject of coverage in the local media a total of 46 times. Of those reports, only 1 portrayed data protection in a negative light.

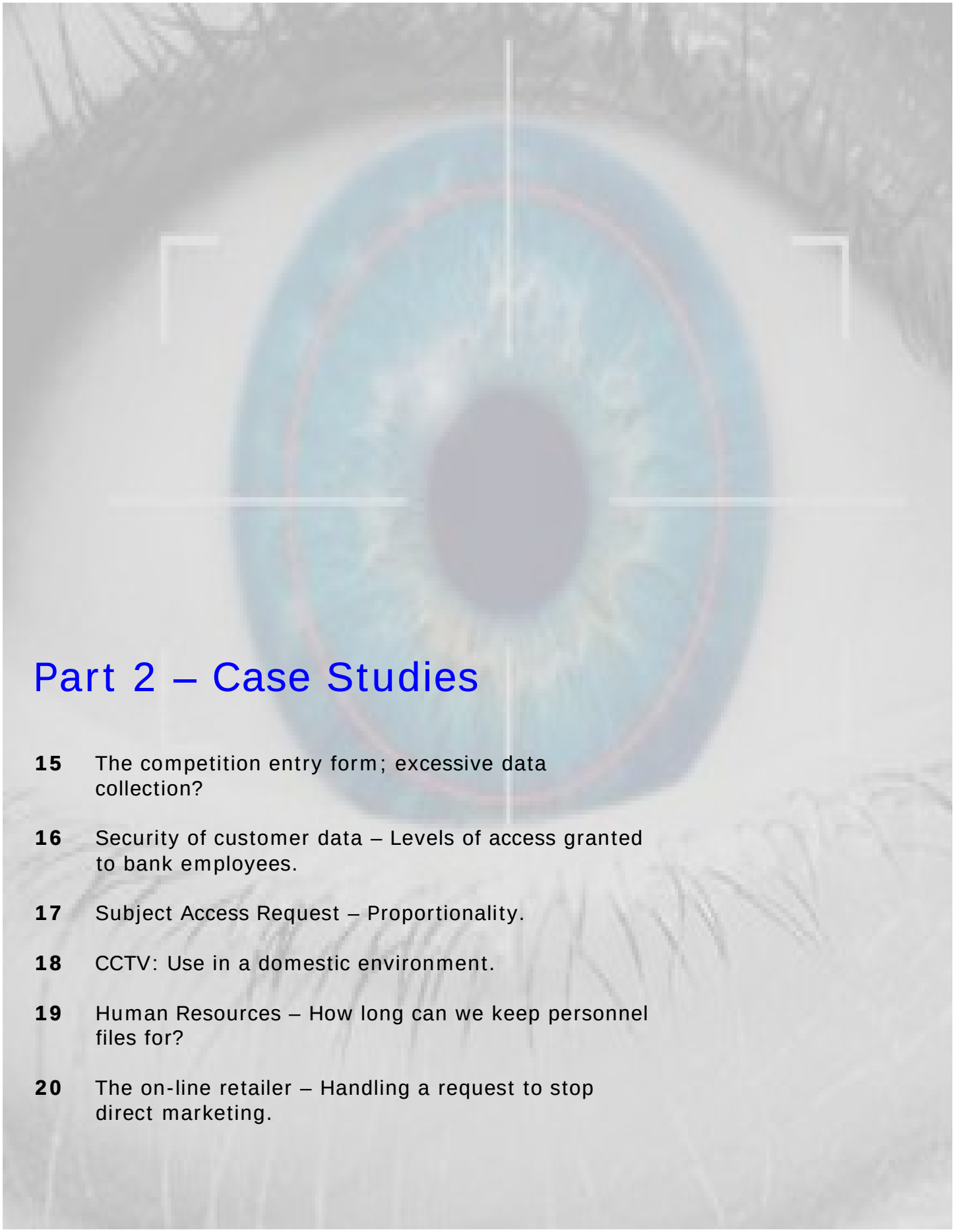


International Activities

April 2006 saw the Island represented at the European Spring Conference of Data Protection Commissioners for the first time. The Commissioner and her Deputy attended the 2-day conference, which took place in the beautiful city of Budapest in Hungary.

In the July, the Commissioner attended the annual meeting of British and Irish Data Protection Authorities, held in the Isle of Man, whilst the Deputy Commissioner attended the 19th Annual International Data Protection Conference hosted by Privacy Laws & Business in Cambridge.

Later in the year in November, the Deputy Commissioner also represented the Island at the annual International Conference of Data Protection and Privacy Commissioners held in London. This was a change in venue form the originally planned conference due to be held in Argentina, and followed the theme of a 'Surveillance Society', based on a recently commissioned report on the subject by the Information Commissioner's Office in the UK.



Part 2 – Case Studies

Case Study:

The competition entry form – Excessive data collection?

1

An airline conducted a customer satisfaction survey, with the added incentive of entering a competition to win a pair of flights to a European destination of the winners' choice.

Customer satisfaction surveys are a popular way of identifying customer trends and weaknesses in an organisation. However the main motivation behind such a survey is often to identify the best people to market a product to. The addition of a competition to the survey is purely to attract more people to complete it.

It is thus very easy to ask a number of questions which are not directly relevant for the purposes of establishing the level of satisfaction of your customers with regard to the service you are providing, or to enable entry to a competition.

The First and Third Data Protection Principles talk about informing individuals of the nature of the processing and ensuring that only adequate and relevant information is collected for specific purposes. There are therefore several key areas that should be addressed when considering such a scheme:

- Decide precisely what you want to achieve from the outset. Is this a marketing campaign? Are you genuinely just offering an opportunity for your customers to provide you with feedback on your service?
- Tell your customers who is collecting the information and who it might be shared with, if anybody. Is it your company, or is it another company higher up the chain, or another part of your group or third parties? This will assist towards compliance with the first data protection Principle.
- How are you going to advise your customers as to the reasons why you are collecting their information? Have you considered how your fair processing statement will be worded?
- What questions are you going to ask? Do they fit with the purposes for which you are requesting the information? Do they fit with what you have told your customers you are collecting it for?
- Make sure the questions are relevant. Do not turn your survey into a lifestyle questionnaire if you don't need one.
- If you are considering using the information for marketing purposes, have you made that clear and given the customer the opportunity to opt out of receiving marketing information from you or third parties?

Case Study:

Security of customer data – Levels of access granted to bank employees.

2

A couple worked together at a bank and both had accounts held there. The couple separated. One left the bank whilst the other remained in their position, which was one that enabled legitimate access to customer accounts.

Employing any person for a role which carries with it responsibility is always going to amount to a certain element of trust between you and the employee.

When that trust is broken, there is often only one outcome – dismissal of the employee. But it can also result in regulatory issues for the institution concerned.

In this case study, the separation of the two employees concerned was not amicable. The partner who remained at the bank was in a position which permitted access to all customer accounts. That individual extracted information from the ex-partner's account and sent it to the other partners' ex-spouse in an attempt to exact some kind of revenge.

Clearly, this kind of disclosure raises significant questions about the risks posed by staff, as well as the general security of and access to customer account details.

Fortunately, there are a number of measures an organisation can take to help protect the information it holds.

The Seventh Data Protection Principle requires that an organisation has both technical and organisational measures in place to protect against the unlawful processing of data, or against loss or accidental destruction of those data. Some of these measures will include:

- Having comprehensive policies and procedures for staff detailing when they are permitted to access customer data, and for what purposes.
- These policies and procedures should be placed in an area where staff can readily access them, e.g. the staff handbook and/or intranet. Do staff sign to confirm they have read the policies and procedures? Does it form part of their contract of employment?
- Different levels of access for different staff. Do junior staff have restricted access to customer data? Access should be on a need to know basis only.
- Technical measures, eg Password protection? Audit trails?

Case Study:

Subject access requests: Proportionality

3

An individual made a subject access request to a law firm in relation to a case they had been dealing with in which he was involved. The law firm claimed disproportionate effort and refused to comply with his request.

Many individuals utilise their legitimate rights under the Law to access personal information held about them. There are, however, a number of exemptions that the data controller needs to be aware of.

One of these is that responding to the request would involve a 'disproportionate effort' on the part of the data controller. However, this only applies with regard to the supply of the requested information in permanent form and does not preclude the organisation from providing the information via alternative means. Some of those alternatives are described below:

- Could access to the information be granted by allowing the individual to visit your premises and inspect the data for themselves?
- Could the data be provided in another format, for example on CD-Rom?
- Is the individual happy for you to provide the information in an alternative format?

If the above alternatives are not appropriate or the individual does not agree to them, the key issues in deciding whether or not a claim for disproportionate effort can be made are:

- Could the information be provided in an acceptable, understandable form in hard copy?
- How much time and manpower will be required to print the information required?

The Commissioner is able to conduct an assessment of the way in which a data controller has complied with a subject access request. The Law allows for regulatory action if non-compliance is evidenced.

Case Study: 4

CCTV: Use in a domestic environment

An individual had been the victim of vandalism to his property and vehicle parked outside his property. To detect further occurrences, he installed CCTV equipment to monitor his property and vehicle.

The use of CCTV equipment for this purpose is considered to be legitimate. An individual has a right to protect his property against crimes such as vandalism.

The difficulty arises when such monitoring begins to impact upon areas outside of your own property, especially areas to which the general public may have access. In this case study, the individual had CCTV equipment positioned in two places; one located on the corner of the house looking directly down the side of his property to the rear garden, the second from an upstairs front window, overlooking his vehicle parked outside his house, but also covering some the pavement area and an area of grass where children frequently played.

It was the second camera which caused an issue and had been subject of complaint from neighbours concerned that the individual was filming children.

Following investigation, the second camera was relocated to a position where only images of the vehicle were captured.

When considering the installation of CCTV equipment, whether for domestic or business purposes, there are many questions to consider, such as:

- Are the camera's fixed or moveable? Can they zoom in and out on the subject?
- What are the purposes of the CCTV equipment? ie. Crime prevention, general security or monitoring of persons?
- How do you let individuals who may have their images taken know you are using CCTV equipment? Do you have adequate signage on display?
- Will you be recording the images? If so, how long are the tapes kept for and who can have access to them?

Further guidance on the use of CCTV equipment can be found in the Commissioners Code of Practice and Guidance on the Use of CCTV Equipment, which can be found at www.dataprotection.gov.je/guidance.

Case Study: 5

Human Resources – How long can we keep personnel files for?

An organisation recently undertook a data protection audit and was found to be holding personnel files dating back 20 years.

Personnel files contain a wide variety of personal data about an employee, ranging from initial application information, sickness and medical data, absence information, to appraisals, references and much more. The question "How long can we keep personnel files for?" is not, therefore, as straightforward as it may seem.

The Fifth Data Protection Principle states that personal data should not be retained for longer than is necessary to fulfil the purpose for which it was originally obtained. There is, therefore, no specified time for the retention of employee data, as is the case for all types of personal data.

In many cases, there will be additional factors to consider, such as other legal obligations which require that such information be kept for a certain period of time. For example, contract law in Jersey states that a contract can be challengeable by either party up to 10 years after the contract has expired. Thus, it may be prudent for an employer to retain contracts of employment for a 10-year period in the event that such a challenge may occur.

What, if anything, should be destroyed after an employee leaves the company?

The answer is relatively simple: If it is no longer required, then it should not be retained.

Certain records, such as Curriculum Vitae's, go out of date very quickly. A much shorter retention period may therefore be appropriate.

Each organisation will have different requirements, and it is important that they ask themselves questions such as:

- What are we holding this information for?
- Why do we still need it?
- Are there any other legislative obligations affecting retention requirements?
- If necessary, do I have the employee's consent to continue to hold that information?
- Do we have data retention policies? If so, what does the company retention policy say regarding employee data?
- Can we justify keeping it any longer?

Case Study: 6

The on-line retailer – Handling a request to stop direct marketing

An individual purchased a number of CD's from a popular on-line music retailer. Over the next 6 months he received e-mail newsletters from the company advertising new products. Despite unsubscribing from the service on numerous occasions, he continued to receive the newsletters.

One of the most common complaints received at our Office during 2006 was in relation to direct marketing material, and in particular, the failure of some organisations to comply with the customers' request to stop their personal data being used for direct marketing.

One of the rights available to individuals under the Law is the right to stop direct marketing. This is an absolute right and once a formal written request has been made to the data controller, the request must be complied with.

Most on-line retailers who conduct this type of e-mail marketing include some method within the communication via which a consumer can opt out of receiving any further direct marketing material. This may be in the form of a return e-mail to a specific address, or more commonly, it may be through an 'unsubscribe' link which sends an e-mail to the originating company.

The consumer, by selecting the appropriate method of unsubscribing, is then under the impression that their request has been actioned.

But that is not always the case. In our experience, many retailers operating this kind of system do not have an automated process for unsubscribe requests. This process is often carried out manually by an individual who, upon receipt of the request, must remove the consumer's name from the database manually.

In addition, some retailers operate through a number of different trading names, and whilst the consumer makes an unsubscribe request through one company, they may still receive marketing information from one of the other associated companies.

It is paramount, therefore, that data controllers have appropriate measures in place to effectively and efficiently manage unsubscribe requests if they are to avoid receiving similar complaints.

More details about how to prevent unwanted marketing material can be found on our website at www.dataprotection.gov.je/guidance.

Part 3 – Guidance

Guidance

Guidance notes

One of the primary functions of the Commissioner is to produce guidance to the general public and business community as to how the Law and Principles should be applied. This is often achieved by way of Guidance Notes published on the Commissioner's website.

The vast majority of the Commissioner's guidance was published upon implementation of the 2005 Law in December 2005. However, 2006 saw the need to add to this already comprehensive list of guidance with three additional documents in relation to CCTV use, privacy on the Internet and an further guidance relating to credit referencing.

In addition to the above, the Commissioner is also consulted frequently with regard to the data protection implications of new legislation and associated industry matters. One example for 2006 was the new All Crimes Anti-Money laundering regulations which saw a significant change to the Anti-Money Laundering Guidance Notes and the former Money Laundering (Jersey) Order 1999.

Code of Practice and Guidance on the Use of CCTV Equipment

This was the first Code of Practice issued by the Commissioner and coincided with the topical issue of the use of CCTV cameras in schools.

CCTV surveillance has become an increasing part of our everyday lives, and there is ongoing debate on how effective it is in reducing and preventing crime. One thing is certain however. Its deployment is commonplace in a variety of areas to which the public have free access. For example, we are likely to be caught on camera walking down the High Street, visiting a shop or bank, or walking through an airport.

The Commissioner's Code of Practice and Guidance is split into two parts and aims to address the data protection implications of the use of CCTV equipment. The first part covers the Code of Practice itself and sets out some standard requirements of data controllers. The second part provides some useful guidance and interpretive notes to assist understanding of the Code of Practice.

Protecting privacy on the internet

It is easy to see and understand the benefits the internet can offer individuals, allowing immediate access to global information and markets and facilitating direct global communications. The internet can also be used as a tool for criminals seeking to commit fraud.

Following a number of incidents both in Jersey and in the UK where individuals had suffered at the hands of internet fraudsters, specific guidance was developed to provide some useful assistance to internet users, which will go some way to helping protect users online.

No Credit? An Update for Jersey Residents

Following on from previous guidance about how to ensure that the UK credit reference agencies are aware of individuals who are registered on the Jersey Electoral Register, the Commissioner has developed supplementary guidance with the inclusion of a form for Experian and Equifax in the UK.

If an individual wants to ensure that credit reference agency information relating to them is updated to show that they are registered on the Jersey Electoral Register, they must first apply for a credit report from each of the three agencies in the UK before submitting the form. The individual can then check and confirm the details on the reports.

The purpose of the form is to enable Jersey residents to provide official confirmation that they are on the Jersey Electoral Register to the UK Credit Reference agencies. At present, the Jersey register is not supplied to the UK agencies in the same way that the UK registers are. If an individual has moved address in the last 4 years, then the Electoral Register details will not appear on the credit report. This could have an impact upon the individual's ability to obtain credit and other financial services.

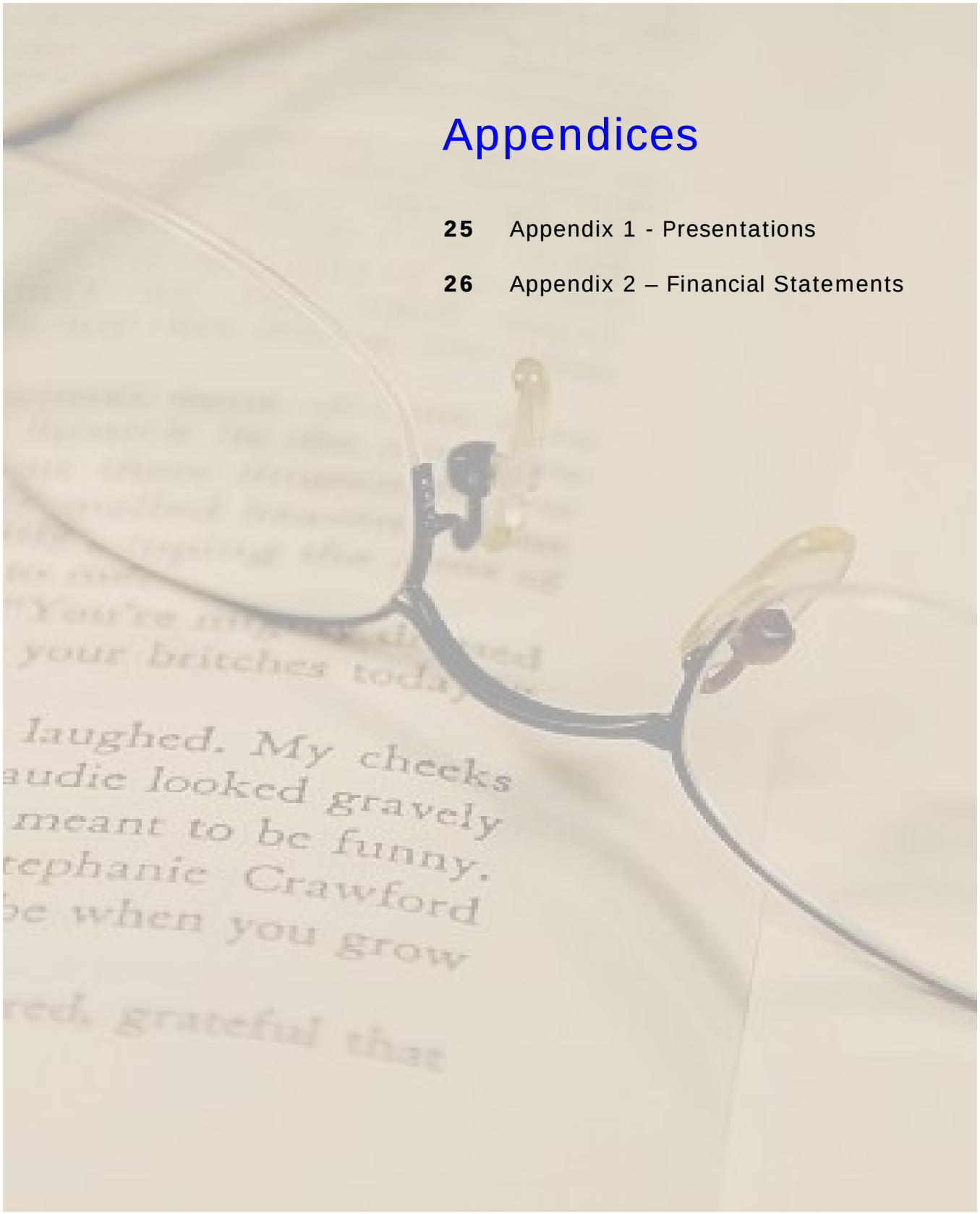
Good Practice Notes

The Commissioner also published 3 Good Practice Notes during 2006 in relation to:

- The buying and selling of customer databases;
- Outsourcing: A guide for small and medium-sized businesses;
- Subject access and employment references.

The latter of these has been particularly relevant and the Office continues to receive a large volume of calls in relation to this area.

All of the above Good Practice Notes and the guidance notes detailed on the previous pages are available on the Commissioner's website at: www.dataprotection.gov.je/guidance.



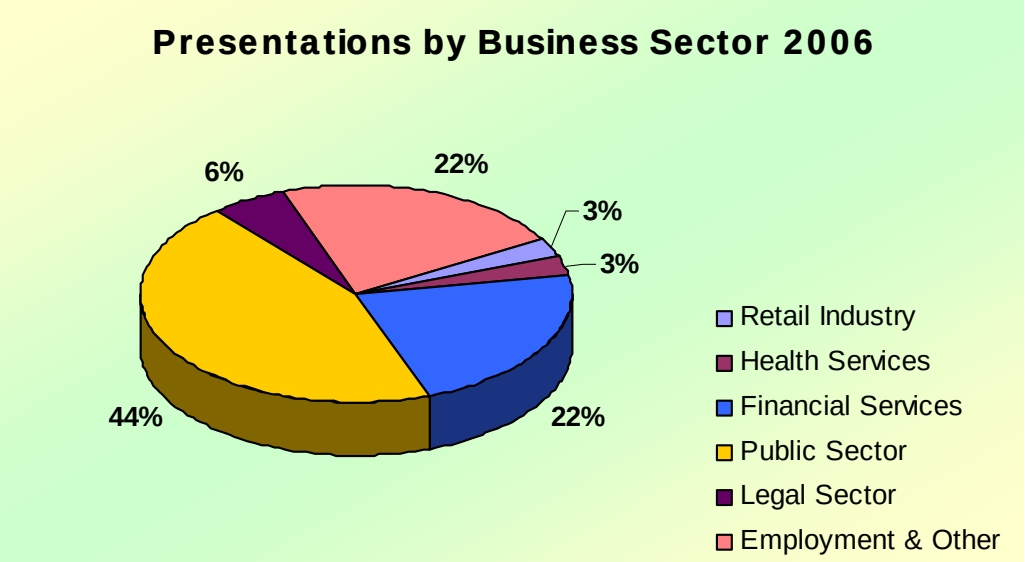
Appendices

Appendix 1

Presentations

During 2006, a total of 36 presentations were delivered to both public and private sector organisations. The subject matter varied depending upon the needs of the particular organisation, and as well as general overview presentations, the Commissioner and Deputy Commissioner also delivered more focused presentations on subjects such as human resources, e-mail and health issues.

The illustration below shows the split of presentations across the varying business sectors and public bodies.



Appendix 2

Financial Statements

Income and Expenditure Account for the year ended 31 December 2006

	Note	£	2006 £	£	2005 £
Income:					
Registry fees	1		28,388		88,044
Total income			28,388		88,044
Contribution from the States of Jersey			216,539		210,393
Net income			244,927		298.437
Operating expenses:					
Manpower costs:					
Staff salaries, social security and pension contributions		210,410		199,163	
Supplies and services:					
Computer system and software costs	2	7,703		3,113	
Pay Offshore admin fees		294		0	
Administrative costs:					
Printing and stationary		1,638		2,440	
Books and publications		2,530		2,267	
Telephone charges		910		982	
Postage		800		1,118	
Advertising and publicity		0		3,264	
Conference and course fees		5,697		5,779	
Bank charges		188		0	
Other administrative costs		3,889		8,432	
Premises and maintenance:					
Utilities (incl. Electricity and water)		9,284		4,358	
Rent		25,729		25,102	
Total operating expenses		269,072	269,072		256,018
Excess of income over expenditure			-24,145		42,419

Statement of recognised gains and losses

There were no recognised gains or losses other than those detailed above.

The notes on the following page form an integral part of this income and expenditure account.

Financial Statements (continued)

Notes to the Financial Statements

1) Income

The large reduction in income for 2006 when compared to 2005 is due to three main factors:

a) The change in the registration process:

Prior to the implementation of the 2005 Law, registration fees were £125 for a 3-year period. These fees now stand at £50 for an annual period, thus a smaller initial fee from each data controller. However, with the process now an annual one, the fees are collected on a more regular basis.

b) The timing of the new 2005 Law:

Many data controllers' registrations under the former 1987 Law reached their expiry date in October and November of 2005 and were renewed under the 1987 Law. As a result, they will not be required to notify under the 2005 Law until October and November 2008.

c) Streamlining of the Notification system:

With the overall approach to notification now far less onerous upon the data controller combined with the legal changes to the notification requirements, it is now possible for a data controller to consolidate several notifications into one single entry, as opposed to the former method of having multiple entries for different trading names and sister companies on the public register. Similarly, some larger organisations have merged or have been acquired by other organisations, resulting in the withdrawal of a significant number of registrations from the public register.

2) Computer system and software costs

This figure has more than doubled since 2005 and is purely as a result of significant enhancement and improvement work carried out on the notification system by States of Jersey Information Services Department. It is envisaged that a similar cost will be incurred in the latter part of 2007 when a third phase of enhancements to the system will be rolled out.

Office of the Data Protection Commissioner
Morier House
Halkett Place
St Helier
Jersey JE1 1DD

Tel: +44 (0) 1534 441064
Fax: +44 (0) 1534 441065
E-Mail: dataprotection@gov.je
Website: www.dataprotection.gov.je