Annual Report 2007

THE OFFICE OF THE
Data Protection Commissioner

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;

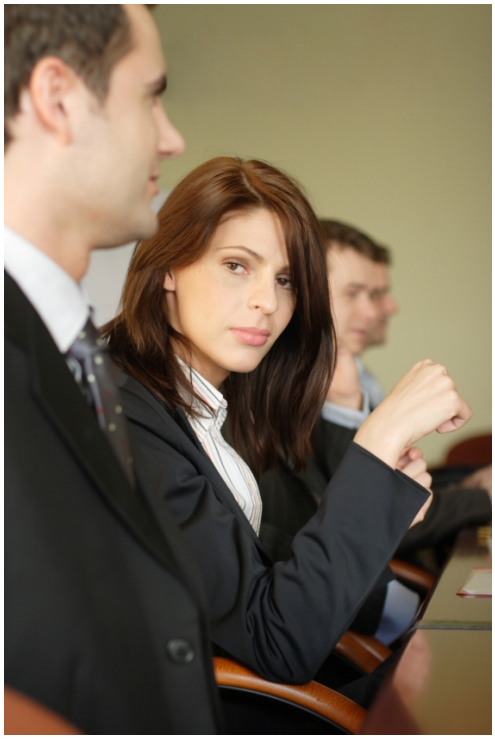
Right to seek compensation
You can claim compensation from a data controller for damage or distress caused by any breach of the Law;

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 fourth report as Data Protection Commissioner for the Bailiwick of Jersey. It covers the year 2007 which was the second full year of the Data Protection (Jersey) Law 2005 being in force.

Following on from the successful first year of implementation of the Law, we continue to see a significant number of data controllers utilising our on-line notification and secure payments system. Whilst not eliminating the administrative burden for data controllers completely, the new system has certainly reduced it.

One of the most significant developments for Jersey's data protection regime in 2007 was the continued work towards 'adequacy'. One of the driving forces behind implementation of the 2005 Law was the desire to attain the high standards of protection of personal data within the European Economic Area. For jurisdictions outside of that area, the importing of data can prove problematic. Being such a jurisdiction, Jersey implemented the Law in line with the European standards. The European Commission has been assessing Jersey for 'adequacy' since 2006 looking critically and in detail at the regulatory regime in place. It has proved a challenging and protracted process, culminating in a meeting in Brussels in mid-2007. I am very optimistic that the outcome will be positive but am also aware that we cannot afford to rest on our laurels.

"...I am aware that we cannot afford to rest on our laurels."

The field of data protection is challenging and constantly evolving and we must, as a regulatory authority and as an Island, ensure we are responsive and proactive.

Certainly 2007 saw challenges from within as well as without the shores of Jersey. Work continued on the population register project. This will see every Islander registered on a central database which will be used for specific government functions, such as health screening and population control, strictly controlled by legislation.

The state protection of personal data of its citizens has been a hot topic in itself with the security breaches in the UK involving HMRC. Such breaches serve to remind us that with the collection and processing of personal data increasingly ubiquitous, the obligations of individuals and organisations to comply with the data protection legislation has never been so critical.

"The significant challenges for government result from its unique relationship with the citizen."

The significant challenges for government result from its unique relationship with the citizen. Public policy making carries a very special responsibility in that it applies to everyone and it is compulsory. Everyone working in the public sector should be cognisant of that fact – with such powerful rights come equally important obligations to act fairly, lawfully, proportionally and transparently.

Of course, the public sector is not the only arena where large amounts of personal data are processed. The private sector in Jersey processes vast amounts of data every day. Our office works closely with both sectors to encourage the high levels of compliance expected in a well regulated jurisdiction - compliance which is important for the citizens of Jersey as well as individuals who trust their data to the Island.

Whilst we consider the 2005 Law to be proving a success, there is no room for complacency. There is a lot of work still to do. With complaints rising from residents concerned about the way their information is handled by credit reference agencies, we propose to publish a code of practice to cover such organisations recognising the risk that poor handling practices poses to individuals.

In addition, we have very real concerns about the unprecedented increase in the amount of personal data being placed into the public arena on social websites and chat rooms.

Not only does this expose individuals, largely children, to the obvious personal security risks, it also runs the risk of adversely affecting future employment prospects. We have clear evidence that some employers are trawling such sites before recruiting. It is notoriously difficult, if not impossible, to ensure that data is deleted from such sites. We are therefore working closely with the appropriate organisations and agencies to examine ways of improving awareness in this area.

This serves to highlight the fact that whilst the principles that underpin data protection are not new, the environment often is. That, in essence, is where the challenge of our job lies. It is a challenge that my staff and I enjoy and I owe them much credit for dealing with significant workloads and complex problems in a professional way with integrity and enthusiasm. Whilst it is undeniably a daunting challenge for such a small team, it is one which we all take extremely seriously. The ultimate aim is to ensure all those who handle our personal information understand and adhere to their obligations, whilst all of us who provide our information to ever increasing number of organisations understand our rights and demand that they are respected.

Emma Martins
Data Protection Commissioner

Part 1 – Activities in 2007

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. Very few Enforcement Notices have been served upon local organisations since the implementation of the 2005 Law which is indicative of the successful proactive compliance work undertaken by the Commissioner and her staff in bringing data protection to the fore and the recognition of the required standards by Jersey-based entities.

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. In 2007, the Commissioner was caused to exercise her powers on a small number of data controllers. Four Information Notices and two Enforcement Notices were issued, and two search warrants were executed under the Law.

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 2007, especially having regard for the overall approach of the Office as a regulatory body.

Promoting general awareness in Data Protection has resulted in a dramatic increase in the number of complaints received by the Commissioner. As more people become aware of their rights under the Law, more people are beginning to realise the benefits.

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 one of the most important parts of our work.

During 2007, the Office continued to respond 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 and the recording of telephone calls;
- Importation of personal data to Jersey
- 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 and personal information on the internet.

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

As with 2006, some of those queries, such as those in relation to notification and internet issues have prompted the review of existing guidance or the development of new guidance and good practice notes. These are currently in development and will be made available on the Commissioner's website.

Whilst no specific need for additional guidance was identified during 2007, there are plans to add to the existing guidance during 2008.

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 possible 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. It remains its most important communication and information tool. The website is reviewed on a regular basis to ensure that the public has access to accurate and up to date information. During 2007, the website averaged 2107 visits per month, which calculates to an average of 69 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 23 presentations to a wide variety of organisations between them during 2007, 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 important power 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.

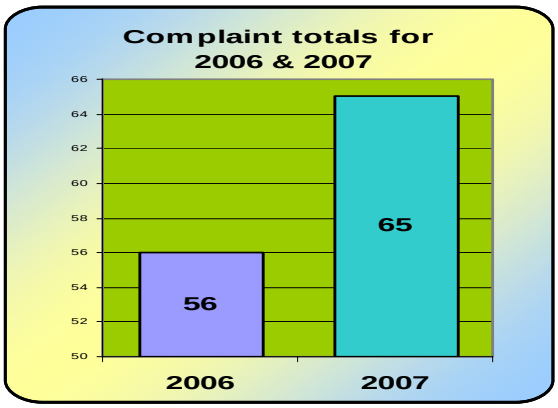
As yet, no Jersey data controller has been subject of prosecution through the Island's courts as a result of a complaint made to the Commissioner. The vast majority of complaints have been resolved before the need to invoke any significant enforcement measures such as those described. However, four Information Notices and two Enforcement Notices were issued, and two search warrants were executed under the Law during the year.

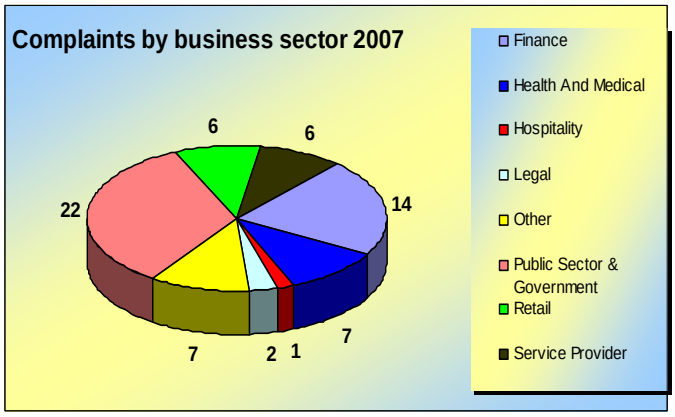
In a significant number of cases investigated during 2007, complaints found to be substantiated were resolved by the respective data controller updating and improving their policies and procedures, or improving the controls over their data handling.

The number of complaints received during 2007 continued to increase to 65, a rise of 16% from 2006. This is only a fraction of the massive increase from the previous year but still indicates a growing awareness in data protection by the general public.

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.

2007 saw a 16% rise in the number of complaints received by the Commissioner.

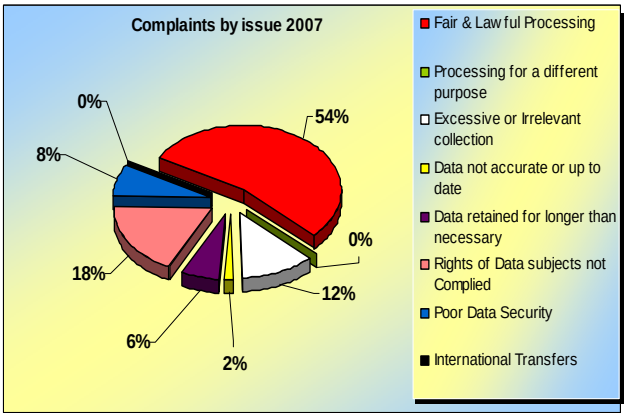




The largest number of complaints received in 2007 was in relation to public sector and government organisations.

Most complaints received during 2007 were in relation to allegations of unfair processing.

18% were alleged to have failed to allow individuals to exercise their rights under the Law, specifically in relation to subject access.



The Public Register

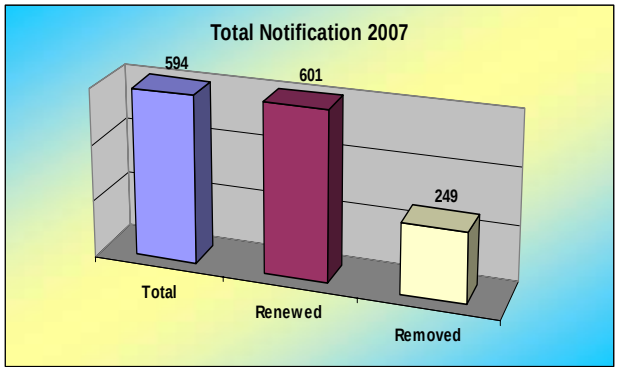
2007 saw the second year of the operation of the on-line notification system and on-line public register. The system underwent some important enhancements during the year and in most cases, users have had no complaints.

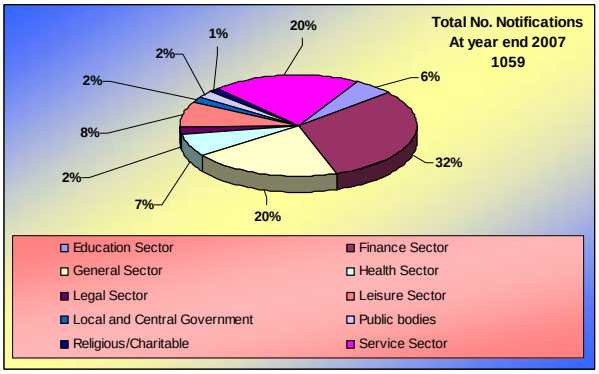
A final phase of development and enhancement to the notification system is planned for 2008 in order to further streamline the process.

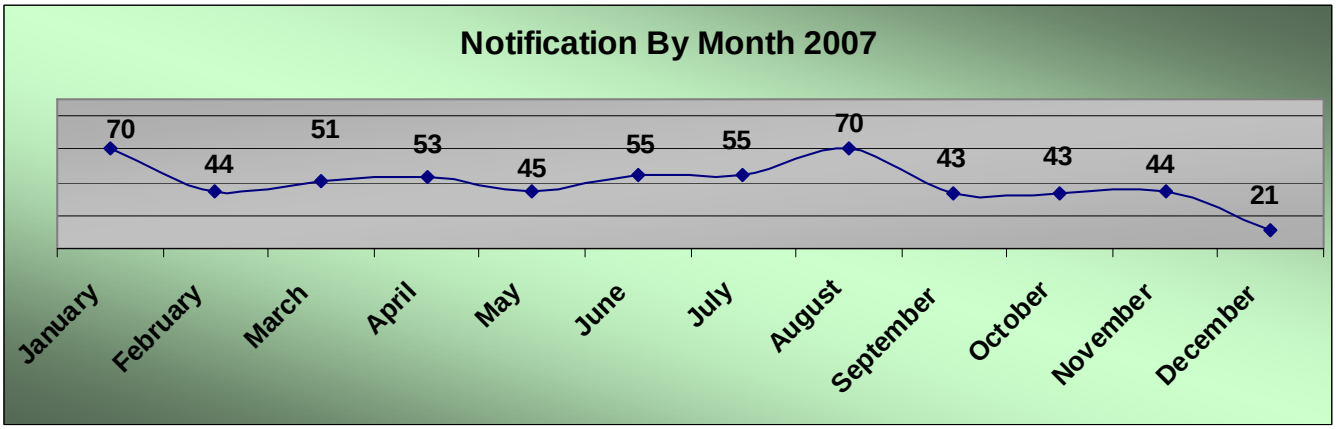
The transitional period between the former 1987 Law and the 2005 Law, particularly in relation to the registration process, makes it extremely difficult to draw any kind of comparative statistics.

In addition, the streamlining and mergers of many large private sector organisations has had an impact on the number of registrations and notifications held. At the end of 2007, there were still 575 active registrations under the 1987 Law, which are due to renew under the new system during 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 and 2007. Overall, there were a total of 594 new notifications received during 2007, 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 previous 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, 2006 and 2007.

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 2 years.

The Media

Data protection all too often hits the headlines for 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 2007, data protection was the subject of coverage in the local media a total of 59 times. Of those reports, only 4 portrayed data protection in a negative light.

International Activities

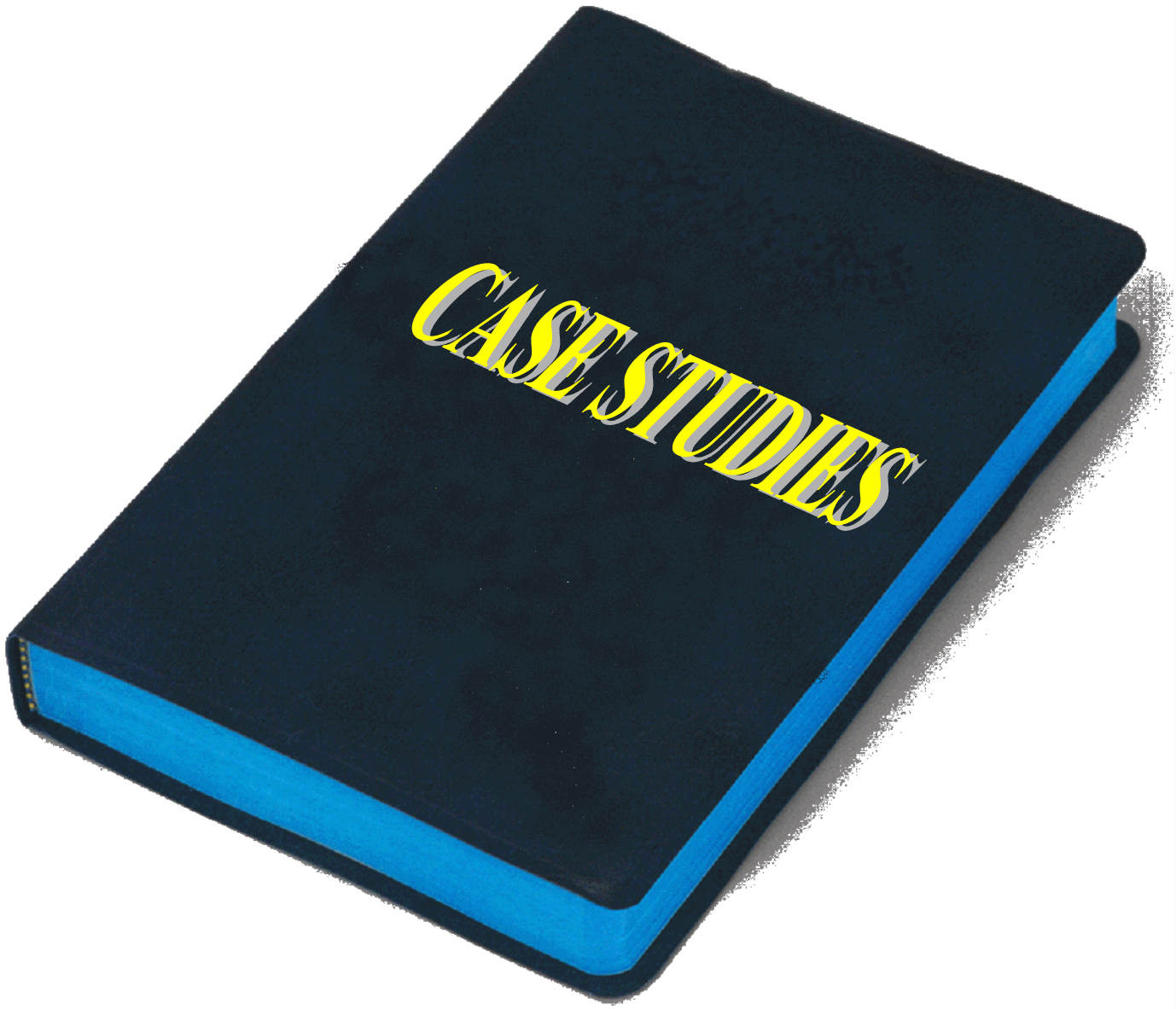
In April, the Deputy Commissioner attended the 41st meeting of the International Working Group on Data Protection in Telecommunications, held in Guernsey, while both the Commissioner and her Deputy attended the annual meeting of British and Irish Data Protection Authorities in the July. This meeting has now been extended to also include the authorities from Cyprus and Gibraltar as well as the three Crown Dependencies.

Montreal, September 2007

Later in the year in September, the Deputy Commissioner also represented the Island at the 29th Annual International Conference of Data Protection and Privacy Commissioners. The conference took place in Montreal, Canada and was hosted by Privacy Commissioner of Canada. It was attended by a large number of delegates from over 60 countries around the world.

The theme of the conference ('Privacy Horizons: Terra Incognita') focused on the many challenging issues data protection and privacy Commissioners deal with. The main challenges, identified as 'dragons' were: Public safety, globalisation, law meets technology, ubiquitous computing, next generation and body data. Possible answers ('dragon slayers') were discussed, such as children's privacy education, audits and privacy impact assessments.

In December, the UK Information Commissioner hosted a workshop in London focusing on effective strategies for data protection authorities. The Commissioner attended this workshop which discussed relevant issues for strategic planning and how to determine priorities for effective actions. ('Selective to be more effective').



Part 2 – Case Studies

Case Study:

Subject Access Requests – How much will it cost?

1

A man had to leave his job because of an injury at work. In order to claim on his company's health insurance he made a subject access request to the hospital for a copy of his medical records. He became concerned when he received a response from the hospital stating he would be charged £50 for the request, and £1 per page provided.

Subject Access Request fees are set in Law. The Data Protection (Subject Access Miscellaneous)(Jersey) Regulations 2005 set out the maximum fee which can be charged by a data controller in response to a Subject Access Request.

- The standard maximum fee for a Subject Access Request is £10.
- Access requests for data held on the Police National Computer can expect a maximum fee of £20.
- An access request for information held by a school will cost a maximum of £30.
- Certain Subject Access Requests for health records will cost a maximum of £50.
- No additional 'administration' fee can be charged.

Case Study:

Recognising a Subject Access Request

2

A woman was in dispute with her bank regarding a loan. After exhausting the bank's complaints procedure, she submitted a subject access request to obtain personal data held about herself, as she believed this information would help her to resolve the matter. Mrs X submitted her request in writing on more than one occasion but the bank did not respond.

Having made reasonable attempts to resolve the matter herself, the woman complained to us. After taking the matter up with the bank, it became clear that their staff had failed to recognise a subject access request.

The bank made arrangements to handle the subject access request in full. As a result, the bank identified an internal training need and provided all their existing staff with data protection refresher courses and all new staff with specific data protection training.

Case Study:

Unsolicited marketing

3

A man who had ordered some CD's from an online music retailer attempted to 'unsubscribe' from receiving the company's newsletter via e-mail. Despite several attempts, the man continued to receive the newsletter at his e-mail address.

One of the rights available to individuals under the Data Protection (Jersey) Law 2005 is the right to object to direct marketing. If a data controller receives a request from a customer to remove his name from a marketing database, the company must suppress its records.

In this instance, staff at the company had failed to ensure that unsubscribe requests were carried out properly, thus ensuring the customer continued to receive newsletters. Additional training was provided and the company updated its policies and procedures for dealing with such requests.

Case Study:

Subject Access and Employment References

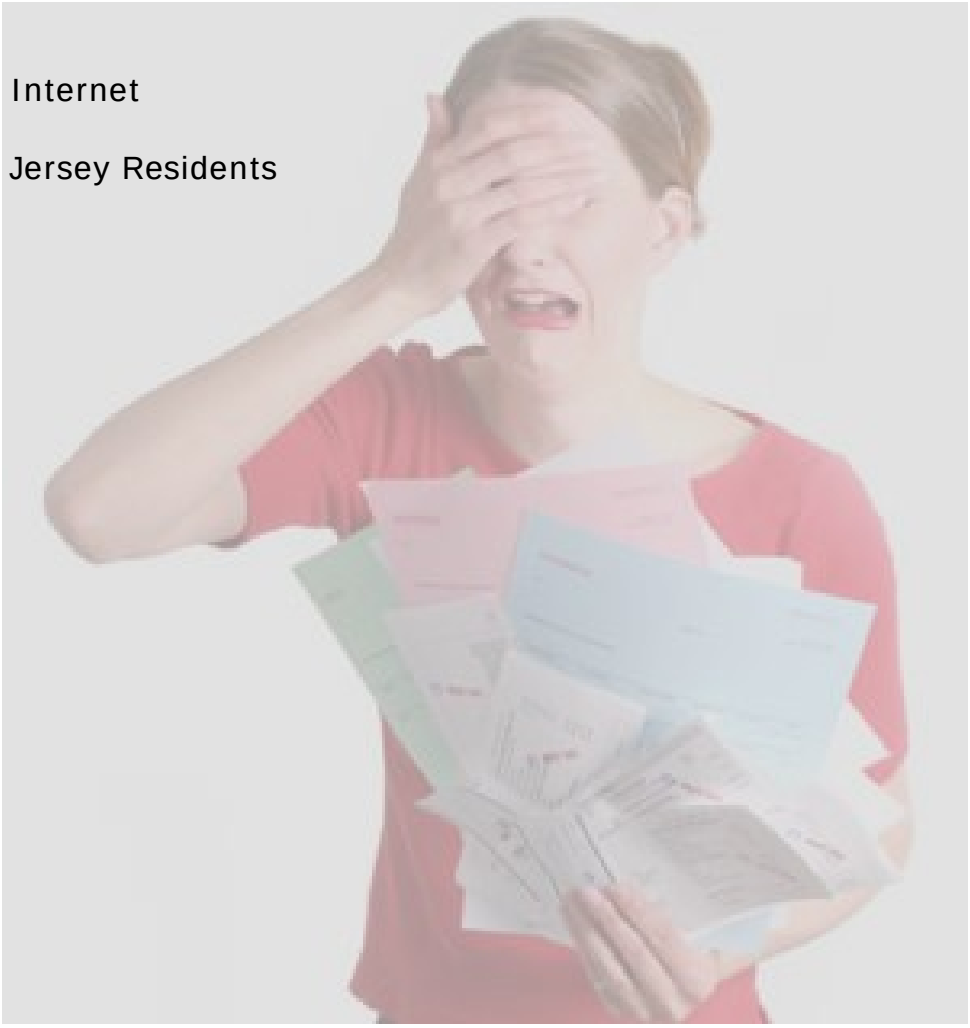
4

A woman made a subject access request to her former employer for a copy of a reference he had written about her. He refused to provide her with a copy, saying the reference was 'confidential'.

Schedule 7 of the Data Protection (Jersey) Law 2005 provides a data controller giving a reference with an exemption from having to comply with such a request provided the reference was written in confidence. However, this does not prevent the referee from providing a copy of the reference if its content was either factual in nature, or the individual would be aware of the content in any case.

The exemption does not apply to the receiver of a reference, however all the facts must be considered before releasing the information to the individual. For example: Does a duty of confidentiality exist to the referee? What is the potential effect upon the individual? Is the reference accurate in its content? Is there any risk to the referee by disclosing it? The Commissioner's Good Practice Note on this subject gives more information.

Part 3 – Guidance



Guidance

Guidance notes

One of the important functions of the Commissioner is to produce guidance for 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. During 2006, further documents were added to the already comprehensive list of guidance. As such, it was not considered necessary to add to the guidance already issued during 2007, although steps commenced to review all guidance with a view to making any amendments or updates as required.

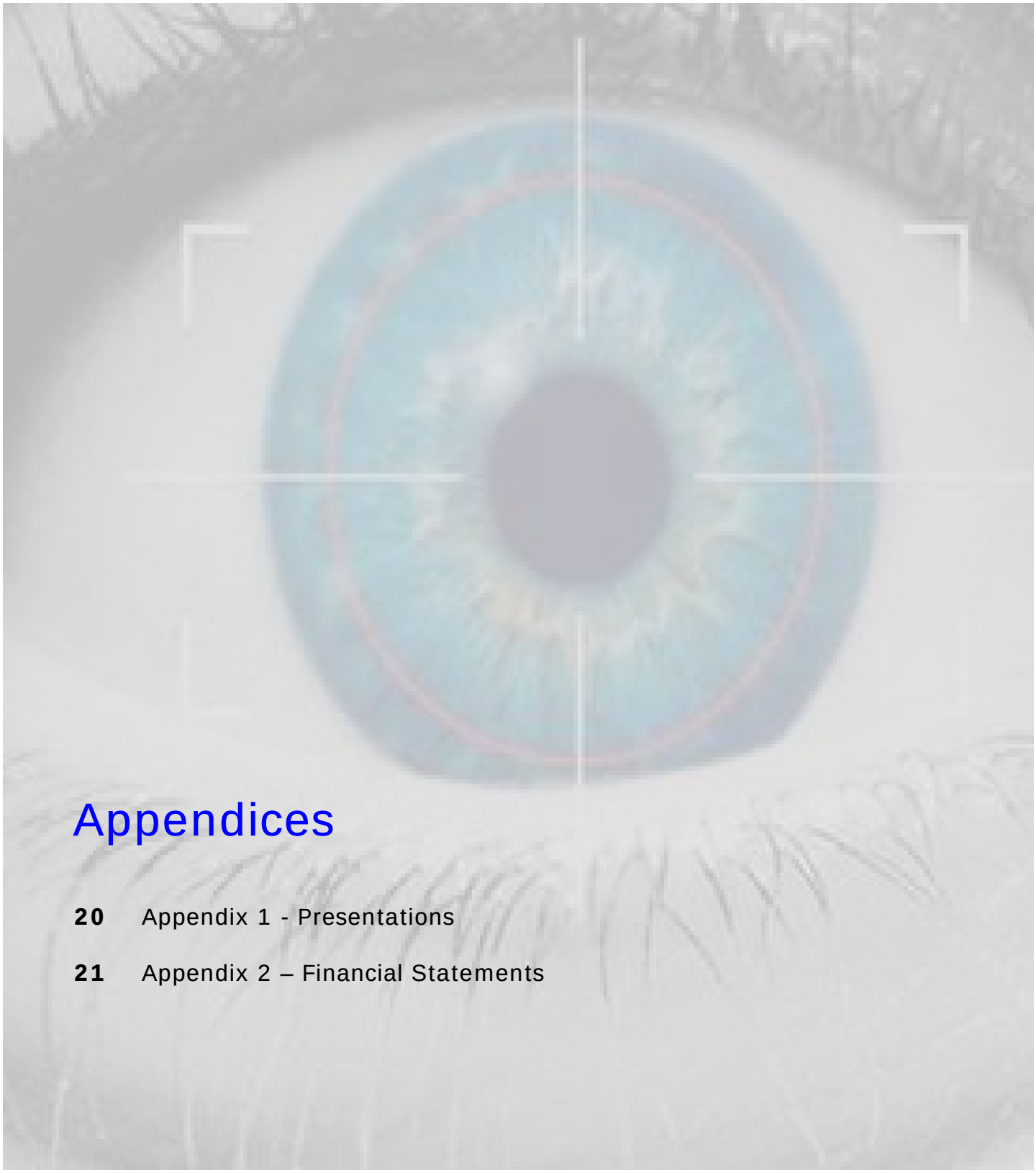
In addition to the above, the Commissioner is also consulted frequently with regard to the data protection implications of new legislation and associated industry matters. One example for 2007 was the Commissioners response to the proposed amendment to the Regulation of Investigatory Powers (Jersey) Law 2005.

Whilst no specific guidance documents were published during 2007, the Commissioner's staff continued to give advice and guidance to both individuals and businesses in relation to a wide range of topics.

Two of the most common queries related to access to employment references, and the use of CCTV cameras, both for business purposes and for domestic use for the purposes of protecting ones own property.

Other issues included children's' privacy on the internet, human resources issues, the proposed population register and questions in relation to data subject's rights under the Law, to name only a few.

Towards the end of the year, the UK announced a large scale data security breach at Her Majesty's Revenue and Customs (HMRC) where two CD's containing millions of pieces of personal data had gone astray in the post. This prompted a dramatic increase in the number of enquiries received by the Commissioner's staff in relation to data security.



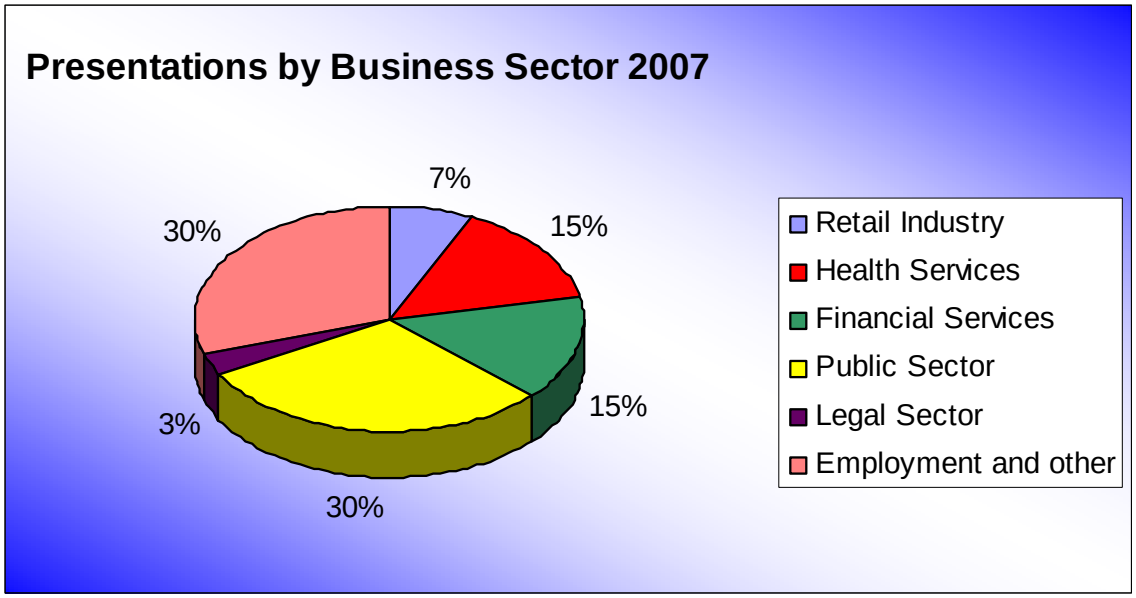
Appendices

Appendix 1

Presentations

During 2007, 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 2007

	Note	£	2007 £	£	2006 £
Income:					
Registry fees	1		56,423		28,388
Total income			56,423		28,388
Contribution from the States of Jersey			208,900		216,539
Net income			265,323		244,927
Operating expenses:					
Manpower costs:					
Staff salaries, social security and pension contributions		244,529		210,410	
Supplies and services:					
Computer system and software costs		3,216		7,703	
Pay Offshore admin fees		368		294	
Administrative costs:					
Printing and stationary		1,587		1,638	
Books and publications		2,330		2,530	
Telephone charges		825		910	
Postage	2	1449		800	
Advertising and publicity		0		0	
Meals and Entertainment		84		0	
Conference and course fees		4,745		5,697	
Bank charges		455		188	
Other administrative costs		2,352		3,889	
Premises and maintenance:					
Utilities (incl. Electricity and water)		8,721		9,284	
Rent		26,372		25,729	
Total operating expenses			297,033		269.072
Excess of income over expenditure			-31,709		-24,145

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 increase in income for 2007 was as a result of more data controllers notifying under the 2005 Law. The decrease 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) Postage

This figure has increased significantly since 2006 and is largely as a result of the fact that notification is now an annual process instead of a 3-yearly process as it was under the 1987 Law. Notification first reminders and renewal notices are sent by post, thus the volume of post generated by the office has increased, together with the cost in postal charges.

Montreal Skyline, September 2007

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