



THE OFFICE OF THE
Data Protection Commissioner



Annual Report **2008**

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

- 4 Foreword from the Commissioner
- 6 Part 1 – Activities in 2008
- 14 Part 2 – Case Studies
- 17 Part 3 – Guidance
- 19 Appendices

“Privacy is at the heart of freedom in the modern state.”

Professor Alan Westin, ‘Privacy & Freedom’

Foreword



This is my fifth report as Data Protection Commissioner for the Bailiwick of Jersey and covers the year 2008.

"2008 continued to be a challenging year for the department in respect of resources."

Emma Martins, Commissioner

The Data Protection (Jersey) Law 2005 has been in force for three years and 2008 saw the end of the 'transitional period' which allowed organisations an opportunity to incorporate the substantial new legal requirements contained within the Law into their processes. The Law is now fully operational and covers a very wide range of data and processing.

The annual report for 2007 highlighted the continued efforts in seeking to achieve 'adequacy'. One of the driving forces behind 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, such as Jersey, the free flow of data can be hindered. In seeking 'adequacy', Jersey was seeking confirmation from the European Commission that our legislation reached their high and exacting standards – thus protecting the substantial flows of data to and from the Island. I am delighted to confirm that in 2008 we received confirmation that we had achieved 'adequacy' status. Jersey is now on the list of jurisdictions formally recognised as having the highest standards of data protection throughout the globe.

This significant development is clearly good news for all those who are in some way involved and interact with businesses located outside of Jersey, of which there is a significant number.

2008 continued to be a challenging year for the department in respect of resources. The increasing national and international political dialogue concerning rights to privacy, high profile data security breaches and our own awareness campaigns all serve to increase the profile of data protection. In turn, this helps to enhance individuals' awareness of their rights and gives them confidence to address situations where those rights may have been breached. As a result, we have seen an increase in the number and seriousness of enquiries and complaints made to the department and these are increasingly requiring protracted and lengthy investigation. Striking a balance between our proactive, educational objectives and our reactive, enforcement responsibilities has proved more challenging than ever.

"...in 2008 we received confirmation that we had achieved 'adequacy' status." *Emma Martins, Commissioner*

The increasing prevalence of technology and the ease with which personal information can be collected, stored and disclosed had further added to this challenge.

We are, indisputably, living in a globalized world in respect of our personal data. This provides us with unprecedented opportunities but also unprecedented risks. We have an entire generation growing up with the minutia of their personal lives forever digitally stored on the internet, often impossible to remove. How that 'digital baggage' may affect them in their future is a very serious question. As a regulator we clearly have our part to play, but the discussion extends beyond one regulator in one jurisdiction. Wider society has its part to play; the way children are educated; the way the media handle related issues; the way governments decide to apply local standards and the way the international community respond to the global risks. Clearly such issues go to the heart of the way modern politics is conducted and I do not pretend to have all the answers, but I do seek to encourage dialogue.

However, it is true to say that robust data protection legislation responds in a significant way to risks posed by ubiquitous processing of personal data but it only goes as far as the shores of our Island. In respect of the manner in which we are all engaging with the wider world, we all need to understand the risks that necessarily accompany that; risks not only for us as individuals, but also to our society, because harm to individuals is harm to society at large.

In essence, this is not a question of new principles, but of a new environment. Technology means that it is easier than ever before to unlawfully collect, misuse, and inappropriately disclose very private information about all of us. We take our role in this very seriously and are committed to ensuring organisations are aware of their responsibilities and individuals are aware of their rights. Data protection cannot and should not be seen as a trivial 'add-on', or unnecessary bureaucracy for any civilised society. Privacy is a key value which underpins human dignity and other important values. The responsibilities shouldered by all regulators should not be underestimated and I am proud to work in a team that not only recognises the importance of their role but rise to the challenge with enthusiasm and integrity.

"A man without privacy is a man without dignity; the fear that Big Brother is watching and listening threatens the freedom of the individual no less than the prison bars"
(**Professor Cohen, 1969**).

Emma Martins
Data Protection Commissioner

"Data protection cannot and should not be seen as a trivial 'add-on'..."
Emma Martins, Commissioner



Part 1 – Activities in 2008

- 7 Introduction
- 8 Promoting public awareness
- 9 Customer services and advice given
- 9 Complaints and investigations
- 11 The Public Register
- 13 The media
- 13 International activities

“The basis of a democratic state is liberty.”

Aristotle

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. This 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.

However, 2008 saw an increase in the number of information and enforcement notices issued by the Commissioner. Of even greater concern was the increase in the number of criminal investigations undertaken for alleged offences under Article 55 of the Law, which deals with the unlawful obtaining or disclosure of personal data. These investigations are continuing into 2009.

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 2008.

“Of even greater concern was the increase in the number of criminal investigations undertaken”

Paul Vane, Deputy Commissioner

Promoting Public Awareness

Of the many functions the Office undertakes on a daily basis, promoting the general awareness of data protection both to the public and to organisations forms the largest and arguably one of the most important aspects of our work.

During 2008, 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;
- ☞ Sharing data between public sector organisations;
- ☞ Human resources issues, including the provision of employment references and data retention;
- ☞ Workplace monitoring; such as e-mail and the recording of telephone calls;
- ☞ The inclusion of fair processing statements on data collection forms;
- ☞ Notification queries;
- ☞ Internet security and safety, particularly in respect of protecting children's privacy;



- ☞ 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 2007, some of the 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 ongoing and completed guidance is made available on the Commissioner's website.

Towards the end of the year, attention turned to planning Jersey's first Data Protection Day on 28th January 2009. This would undoubtedly provide an excellent opportunity to run an awareness campaign for the general public to bring issues surrounding the protection of personal information to the fore.

"The fantastic advances in the field of communication constitute a grave danger to the privacy of the individual"

Earl Warren (1891 – 1974)

Chief Justice of the US Supreme Court

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. The website is an important communication and information tool which is reviewed on a regular basis to ensure that the public has access to accurate and up to date information. During 2008, the website averaged 1983 visits per month, which calculates to an average of 65 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 due to the other commitments and activities of the staff involved. That said, the Commissioner and her Deputy delivered a total of 28 presentations to a wide variety of organisations between them during 2008, with the subject matter ranging from a general overview of the Law and Principles to more focused topics such as data security and internet data processing issues. Further details of the presentations are provided in Appendix 1.

Complaints and Investigations undertaken

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 criminal prosecution.

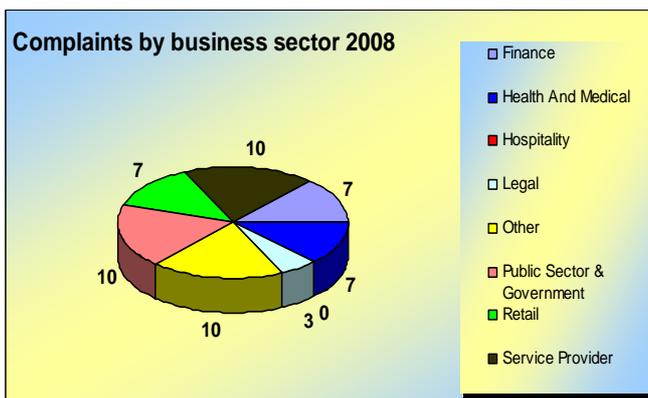
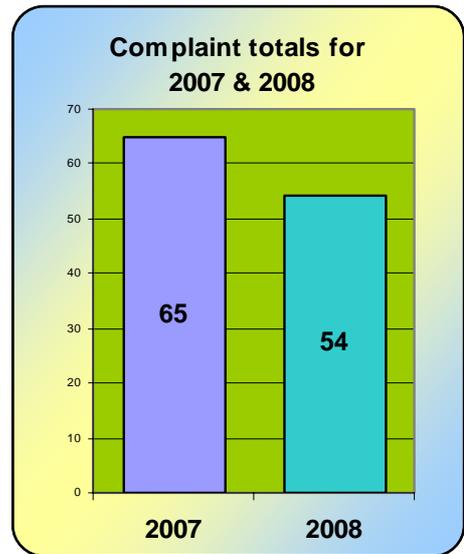
The vast majority of complaints are resolved before the need to invoke any significant enforcement measures such as those described. However, four significant investigations were undertaken during 2008 with regard to allegations of criminal offences under the Law. These investigations are still ongoing.

In a significant number of cases investigated during 2008, 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.

2008 saw an overall decline by 16% in the number of complaints received, although many were of a more serious nature than in previous years requiring more lengthy investigation. Another reason for the decline is as a result of a policy decision whereby complainants must have exhausted the complaints process of the relevant data controller before seeking redress with the Commissioner. Again, this has proved necessary in the light of increasing strain on the resources of the office.

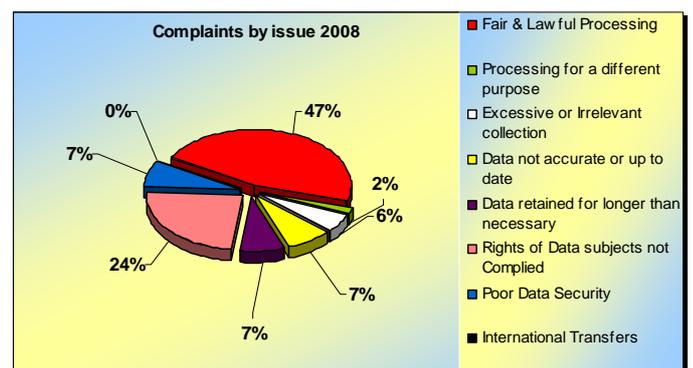
Our experiences show that in the main, data controllers are extremely co-operative and willing to assist where individuals have made complaints about the way in which their personal information has been handled.

The number of complaints received during 2008 fell to 54, a decrease of 16% from 2007. This small decline was expected in light of complainant's attempting to resolve issues directly with data controllers, much of the time with successful outcomes.



It was also encouraging to see a steep decline in the number of complaints made against public sector organisations during 2008.

As with 2007, most complaints received during 2008 were in relation to allegations of unfair processing and alleged failures of organisations in allowing individuals to exercise their rights under the Law, specifically in relation to subject access.



“Privacy invasions are socially constructed, not randomly or evenly distributed.”

Charles Raab & Colin Bennett

The Public Register

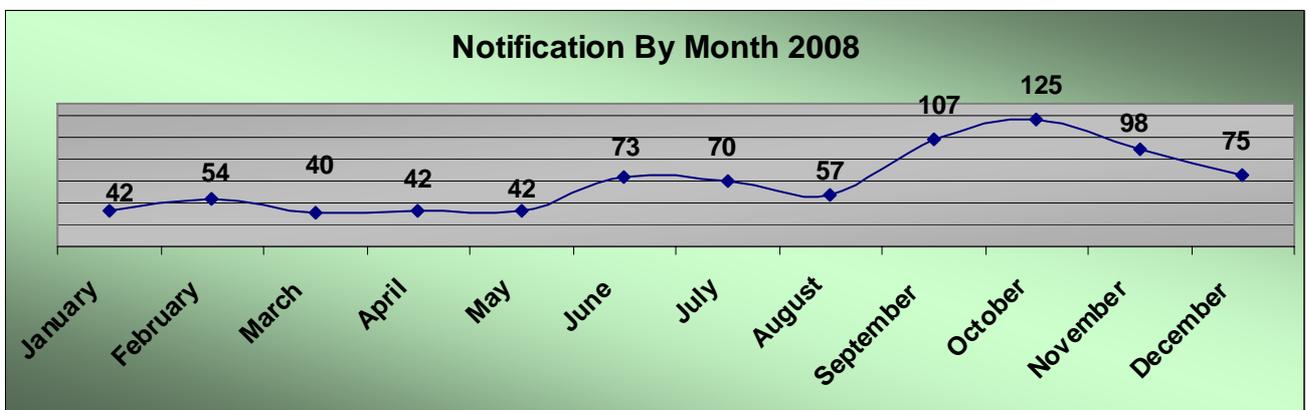
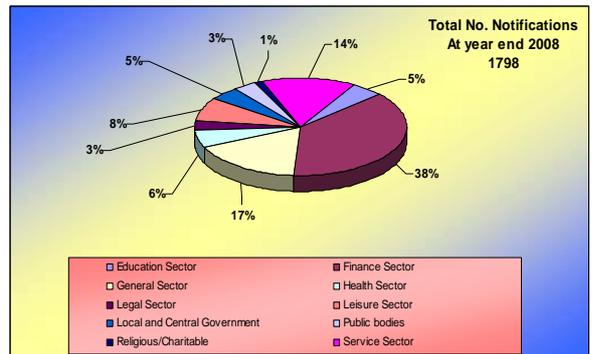
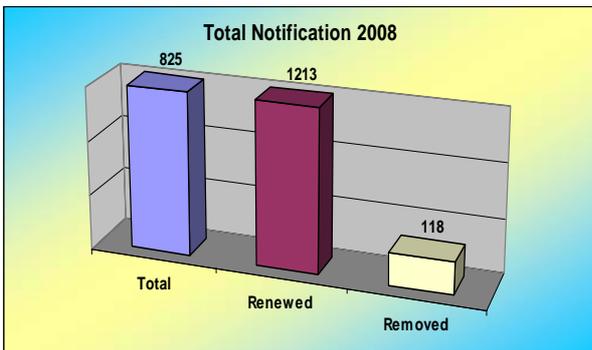
2008 saw the final year of the transitional period, with most of the remaining data controllers registered under the former 1987 Law coming into line with the new requirements.

Technological difficulties with the administrative functions of the on-line notification system resulted in provisions being made for a full assessment of the system in 2009 as part of a wider States Information Services Website project.

Work is ongoing to ensure the system is robust and user-friendly.

The transitional period between the former 1987 Law and the 2005 Law, particularly in relation to the registration process, made it extremely difficult to draw any kind of comparative statistics. However, it is possible to see that during 2008, a total of 825 new notifications were made. This was far in excess of the anticipated figure, demonstrating that more data controllers are becoming aware of their obligations to notify under the Law.

At the end of 2008, a project was undertaken by the Commissioner's Office to identify any additional data controllers based in Jersey that may be required to Notify under the Law.



“Personal information is the single most valuable non-consumable asset possessed by any business.”

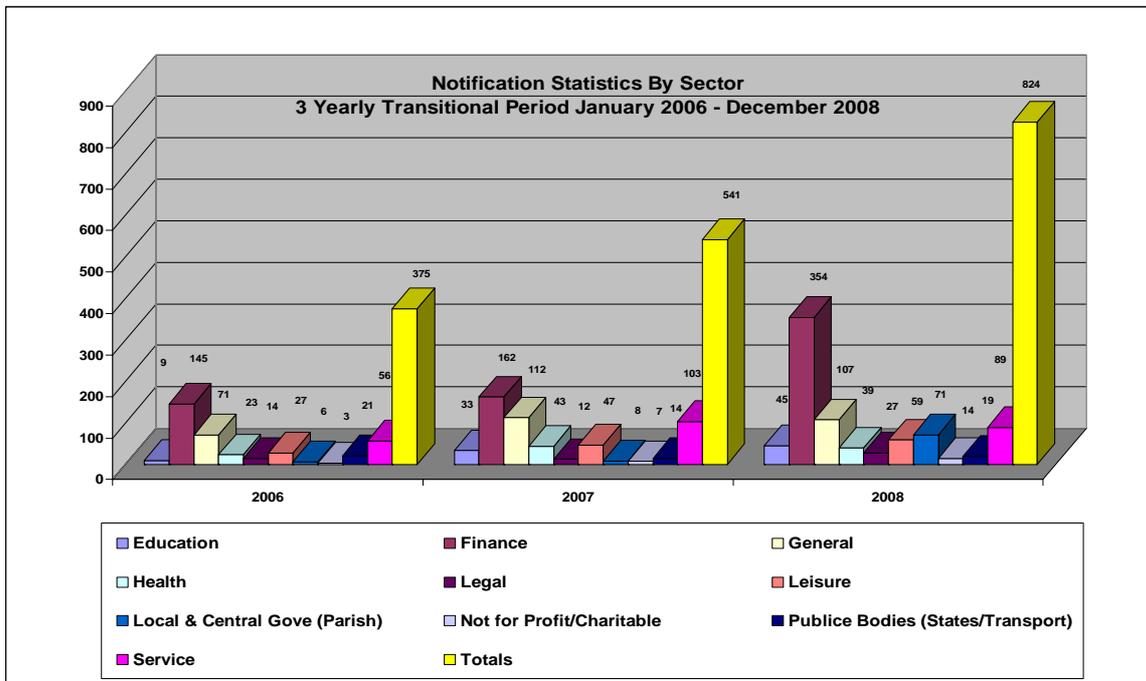
Pincet Masons, UK Law firm – Introduction to the Data Protection Act 1998

For the last few years, 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 requirements. 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 these years.

It has been possible however to examine the notification figures for 2006, 2007 and 2008 in more detail to establish where the main increases and decreases have occurred. It was expected that the overall numbers would increase over the three-year period as more data controllers fell within the scope of the 2005 Law. The figures for the full three-year transitional period are illustrated below.

The figures show that 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 was in the region of 1600, this figure has been significantly exceeded with 1798 notifications recorded by the end of 2008.

It is also encouraging to note that the secure on-line payments facility for new and renewal of notifications is becoming more popular, thus increasing the speed of turnaround for notification applications.



“Our job is to articulate the privacy interests of the public. It is up to the government to legislate, taking these interests into account.” David Flaherty

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 fair and positive light and in such a way that it further enhances the public awareness of data protection requirements and current issues.

During 2008, data protection was the subject of coverage in the local media a total of 28 times. Of those reports, only 1 portrayed data protection in a negative light.

International Activities

In April, the Commissioner and her Deputy attended the European Conference of Data Protection Authorities in Rome. The annual meeting of British and Irish Data Protection Authorities took place in Gibraltar in the July, however work commitments resulted in Jersey missing this particular meeting. This meeting has now been extended to also include the authorities from Cyprus and Gibraltar as well as the three Crown Dependencies.



Rome, April 2008

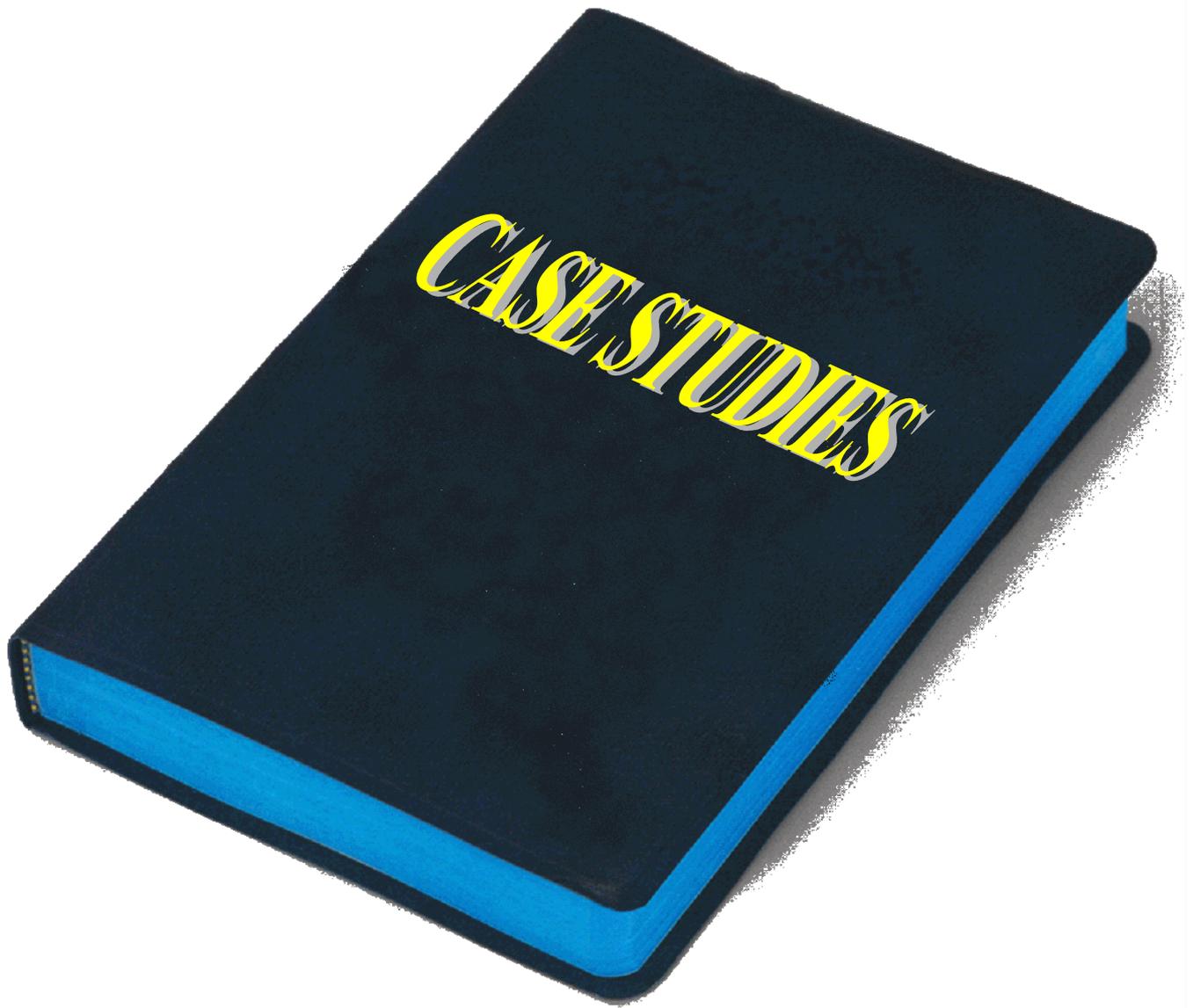
Later in the year in September, the Commissioner and her Deputy represented the Island at the 30th Annual International Conference of Data Protection and Privacy Commissioners. The conference took place in Strasbourg and was jointly hosted by the French and German Data Protection Authorities, who coincidentally were also celebrating their 30th anniversaries.

As always, the conference was attended by a large number of delegates from over 60 countries around the world.

The theme of the conference was "Protecting Privacy in a Borderless World", concentrating on the increasing challenge of data protection regulation in a globalized world. Of particular interest was the issue of cross-jurisdictional investigations and enforcement action where data controllers and data subjects are located in different countries.

"The heart of our liberty is choosing which parts of our lives shall become public and which parts we shall hold close."

Kathleen Blatz, Chief Judge, Minnesota Supreme Court



Part 2 – Case Studies

- 15 Subject Access Requests – How long should it take?
- 15 Keeping your plastic safe.
- 16 Temporary staff: Access to data.
- 16 Self breach reporting.

Case Study:

Subject Access Requests – How long should it take?



A woman made a complaint to a company and in her letter of complaint she requested details of information the company held about her. The company decided to wait the full 40 days before responding to her with the information she requested.

The Law requires that a data controller should respond to a data subject promptly and in any event within the 40 day maximum time limit as prescribed by Regulations.

It is therefore not acceptable for a data controller to unnecessarily withhold the requested information for the full 40-day period in order to inconvenience the data subject.

If the data controller is able to locate the information fairly quickly, then they should respond to the data subject as soon as they are able.

A delay such as that described above would amount to a breach of the 6th Data Protection Principle, in that the data controller has not supplied the information in accordance with the requirements of Article 7.

Case Study:

Keeping your plastic safe



Most people know to keep their credit and debit cards safe. But how many people discard the printed receipts following a purchase without giving it a second thought? One woman was very surprised to see her full account number, card number and name printed on her receipt having that day made a purchase at a well known High Street store.

Most retail outlets now have chip and pin facilities for customers in their stores. The receipts generated should, as a matter of course, now disguise the card number with asterisks or similar, with the exception of the last 4 digits.

Should a data controller operate a system that fails to disguise the number, on

customer receipts, they may find themselves in breach of the 7th Data Protection Principle, having not taken sufficient steps to safeguard against unauthorised access or accidental loss of personal data.

Case Study:

Temporary staff: Access to data



Many organisations utilise temporary staff to carry out administrative tasks on a short term basis. But should these staff have access to all the personal information held by the organisation?

Dependent upon the role in which the temporary staff member is employed, it may not be necessary or desirable for that member of staff to have full access to all available data held by the organisation. Access should be restricted to those staff who have a genuine business need for it. Furthermore, temporary staff may not always be subject to the same level of training or vetting and security checks as

permanent staff. It is therefore crucial to ensure appropriate levels of access to data are considered and the risks of allowing access by temporary staff members are managed accordingly. Data controllers need to be aware that part of their obligations to keep data secure will include appropriate access levels to relevant members of staff, whether temporary or permanent.

Case Study:

Self reporting breaches



A hotly-debated issue across Europe is that of breach reporting, and whether or not a data controller should be compelled to inform the relevant data protection authority that a breach has occurred.

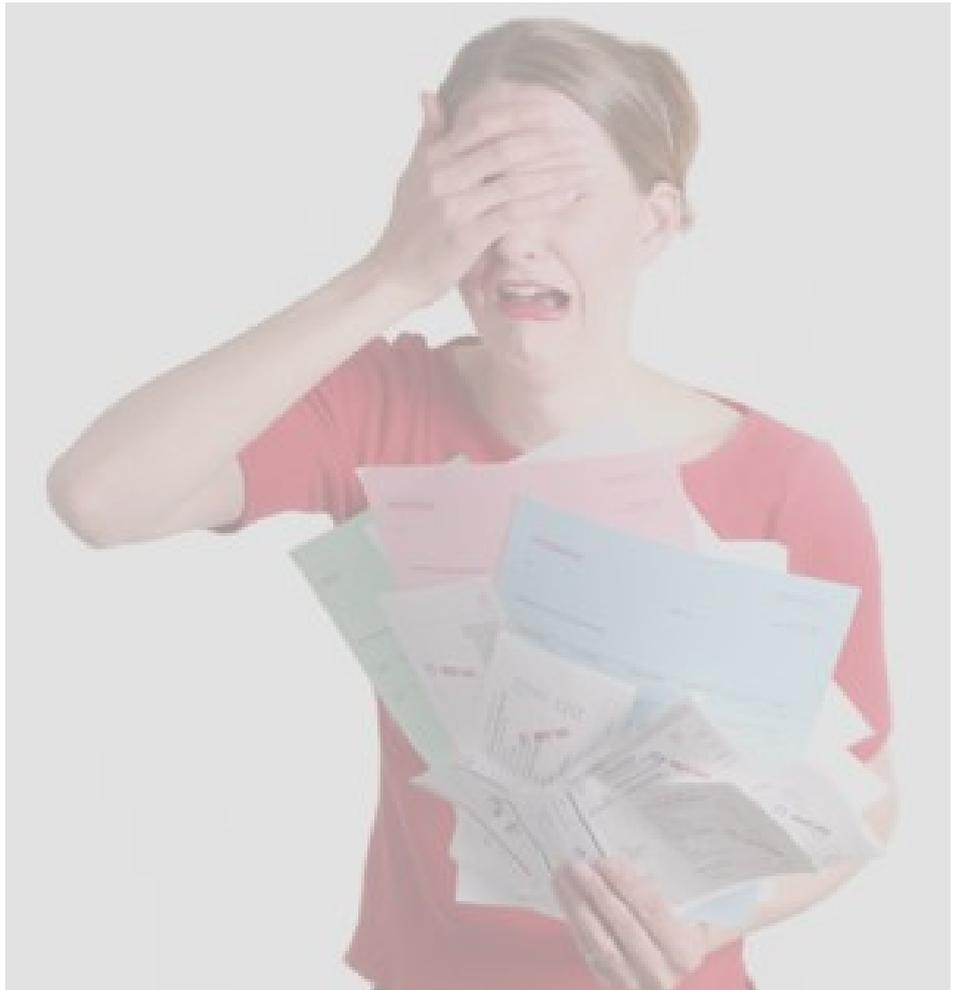
Some States within USA has legislation in place to compel organisations to report data breaches. The intention is to encourage companies to have robust controls in place to avoid the data breach in the first place. However, there has been much dispute over what constitutes a 'data breach' and what information should be given to the relevant authority. As such, there is no requirement in European legislation for compulsory data breach reporting as yet.

At present, some companies in Jersey have chosen to self-report on a voluntary basis when a breach has occurred. This has worked well in that the data controller demonstrates a pro-active attitude towards dealing with the breach, with the added advantage of seeking appropriate advice from The Commissioner's Office. The first response is critical when dealing with a data breach, and self-reporting can be an effective step in demonstrating compliance.

Part 3 – Guidance

18 Guidance notes

18 Guidance on Social Networking Websites



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 and 2007, further documents were added to the already comprehensive list of guidance.

With the ever-increasing use of social networking websites, such as MySpace, Facebook and now Twitter, guidance was issued for both users and providers of such websites to help ensure the privacy of users is maintained. The guidance is split into two parts, one for users and one for providers.

The users section includes tips on how to take care of your personal information and what to look for when choosing a social networking site to use, while the providers section looks at the regulatory requirements, privacy protection and how to manage inappropriate content or activity.

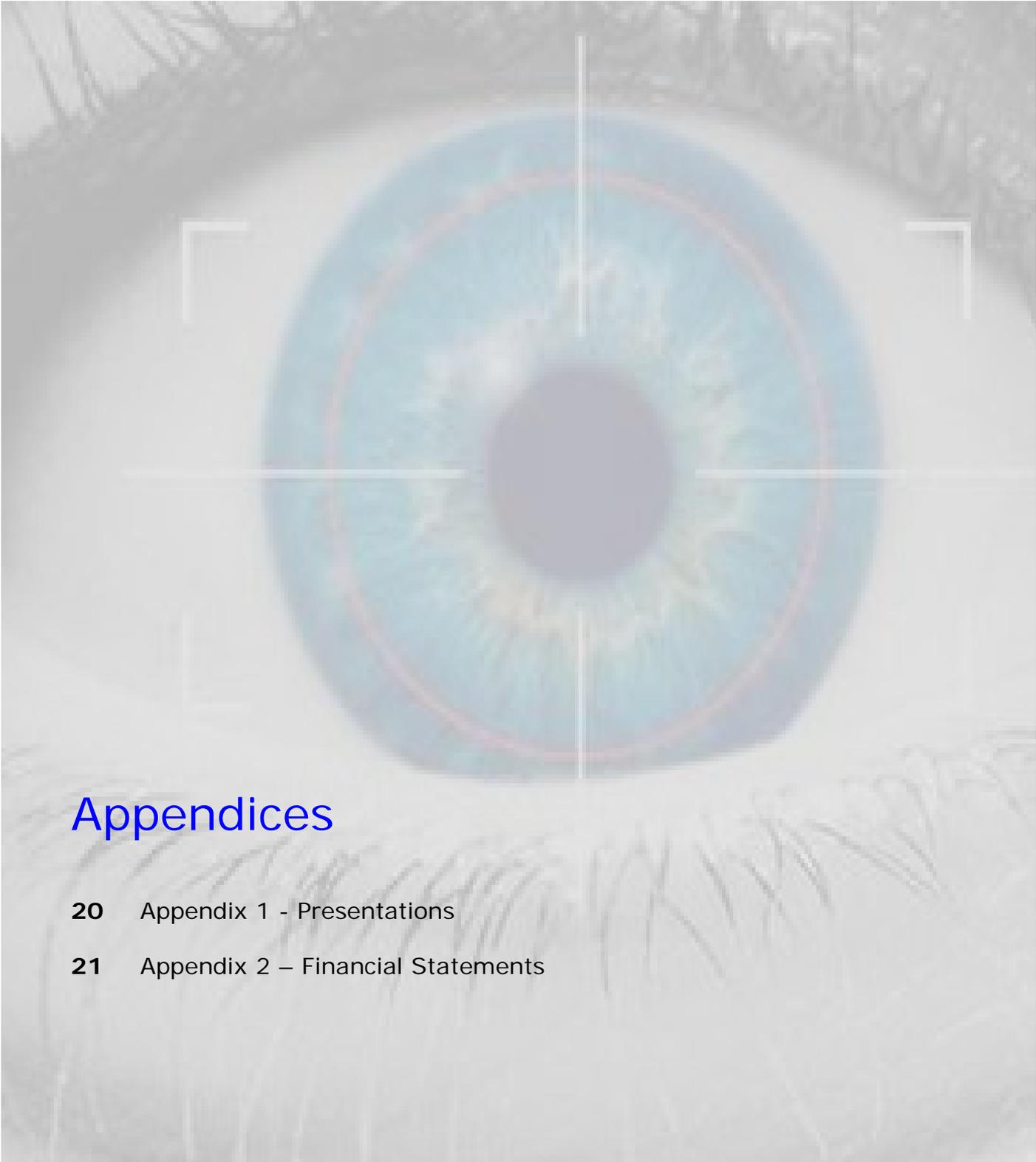
In addition, the Commissioner's staff continued to give advice and guidance to both individuals and businesses in relation to a wide range of topics.

Two of the most common queries related to access to employment files, and the use of social networking sites as described above.

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

Towards the end of 2008, the Commissioner's Office started planning a media campaign for the beginning of 2009 to coincide with International Data Protection and Privacy Day, celebrated on 28th January each year. This was to be the first time that the Jersey Commissioner's Office had promoted the day, and following the numerous data security breach headlines through 2007 and 2008, together with the increase in instances of identity theft, the plan was to try to provide citizens with the necessary tools to help them protect their own personal information.





Appendices

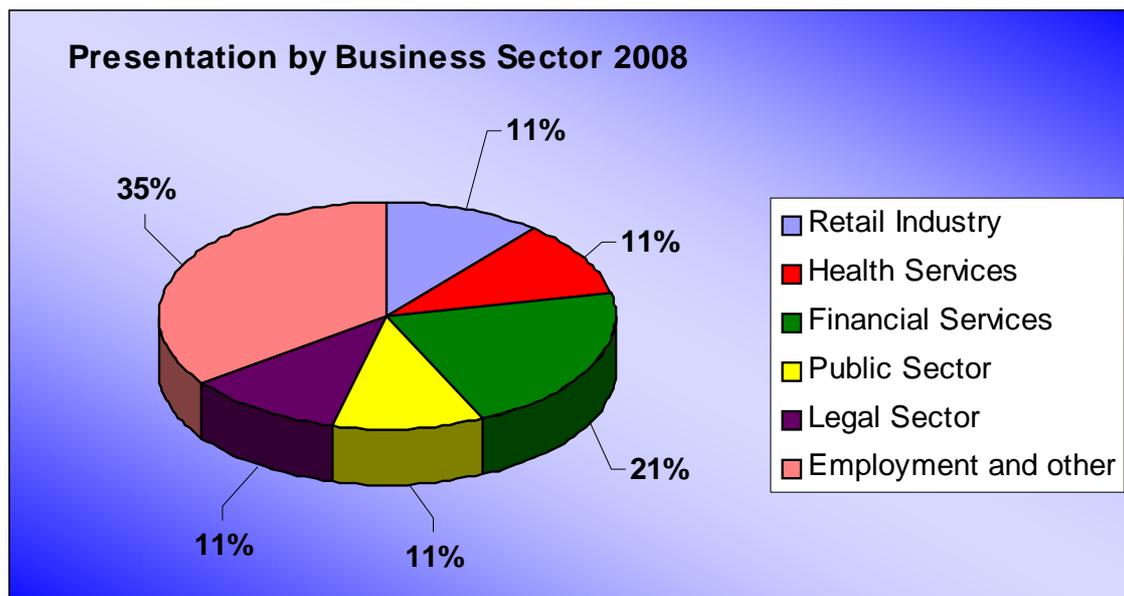
- 20** Appendix 1 - Presentations
- 21** Appendix 2 – Financial Statements

Appendix 1

Presentations

During 2008, a total of 28 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 2008

	Note	£	2008 £	£	2007 £
Income:					
Registry fees	1		<u>93,874</u>		<u>56,423</u>
Total income			93,874		56,423
Contribution from the States of Jersey			<u>239,600</u>		<u>208,900</u>
Net income			333,474		265,323
Operating expenses:					
Manpower costs:					
Staff salaries, social security and pension contributions		239,367		244,529	
Supplies and services:					
Computer system and software costs		2,912		3,216	
Pay Offshore admin fees		399		368	
Administrative costs:					
Printing and stationery		1,722		1,587	
Books and publications		2,690		2,330	
Telephone charges		671		825	
Postage	2	2,538		1,449	
Advertising and publicity	3	3,705		0	
Meals and Entertainment		201		84	
Conference and course fees		6,590		4,745	
Bank charges		130		455	
Other administrative costs	4	13,399		2,352	
Premises and maintenance:					
Utilities (incl. Electricity and water)		8,638		8,721	
Rent		<u>27,031</u>		<u>26,372</u>	
Total operating expenses			<u>309,993</u>		<u>297,033</u>
Excess of income over expenditure			23,481		-31,709

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 2008 was as a result of more data controllers notifying under the 2005 Law. Three main factors had influenced an initial drop in income at the implementation of the 2005 Law. These are detailed as follows:

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 were not 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 because 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.

3) Advertising and Publicity

Planning and preparation for the "WhoKnows" public awareness campaign commenced towards the end of 2008. This figure represents consultancy work undertaken during 2008 as part of that process.

4) Other Administrative Costs

The significant increase in administrative costs is largely attributed to the Notification Research Project commenced during 2008, for which the services of an external consultancy company were engaged.



Council of Europe, Strasbourg, October 2008



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