THE OFFICE OF THE

Data Protection Commissioner

2009

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;

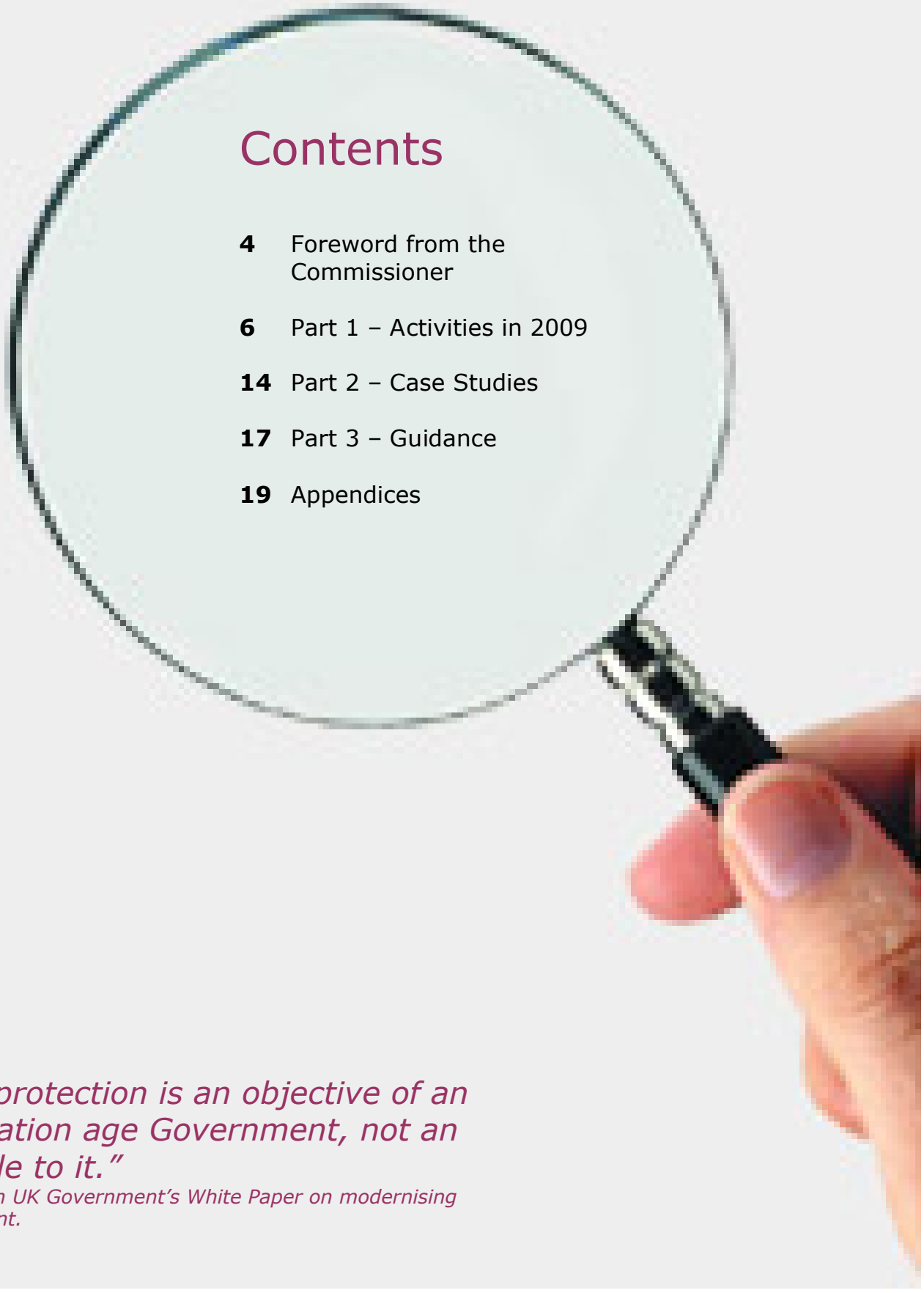
Rights to have inaccurate information corrected
You can demand that an organisation corrects or destroys inaccurate information held about you;

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



"Data protection is an objective of an information age Government, not an obstacle to it."

Quote from UK Government's White Paper on modernising Government.

Foreword

This is my sixth report as Data Protection Commissioner for the Bailiwick of Jersey and covers the year 2009.

"The affects of living in a globalised world continue to ripple through the world of data protection."
Emma Martins, Commissioner

The Data Protection (Jersey) Law 2005 has been in force for four years. 2009 was the first year of full implementation of the Law after 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 2008 highlighted the successful efforts made 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. 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 and the news has impacted on business in a positive way. This has been reflected in the nature and volume of enquiries received at the office regarding international transfers.

2009 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. 2009 saw the department involved in its first Data Protection Day which was a huge success. As a result, we are continuing to see an increase in the number of enquiries and complaints made to the department. The complexity of the investigations now undertaken by the office is testament to the evolving nature of privacy rights and expectations both locally and further afield. Striking a balance between our proactive, educational objectives and our reactive, enforcement responsibilities continues to prove challenging. The increasing prevalence of technology and the ease with which personal information can be collected, stored and disclosed had further added to this challenge.

The affects of living in a globalised world continue to ripple through the world of data protection. More and more discussion is being had about personal boundaries and expectations of privacy. Few weeks go by without a news story concerning a social networking site or a data security breach. The technology that is associated with globalisation by its very nature creates greater risk as well as greater benefit. To what extent we have to compromise with regards to that risk is a question for society as a whole. Regulators like ourselves have our part to play and whilst clearly that means ensuring the law is properly and robustly upheld it also involves stimulating debate and discussion about what the future holds. Is privacy dead as some big names in technology have claimed, or are the boundaries being redefined? My view is that whilst privacy is, and always has been, a fundamental and important right, it is nonetheless challenging to articulate. It means different things to different people. We should think carefully before assuming that openness in all things is a desirable social goal. I hear all too often the mantra of 'nothing to hide, nothing to fear'. To suggest that individuals are allowed nothing which they legitimately want to keep private is astonishingly ignorant or incredibly callous. It is a paradox that the freedoms of new technologies such as the internet may in fact make us less free. Rather than being 'dead', the subject of privacy is, in my view, more alive than ever before.

Jersey has chosen to implement legislation that sets out the basic standards to ensure privacy and security of personal data. Such standards are inextricably linked to preventing the reappearance of an oppressive bureaucracy seen during the Nazi years. Born from this historical backdrop, data protection now faces entirely new challenges of technology and increasing generational divides. But whilst the technologies have changed, the basic principles have not. For a law to work, the standards must be universal. Ultimately it is up to each state to establish the legal protection it wants to provide for its citizens. The Data Protection (Jersey) Law 2005 is a robust piece of legislation that, largely behind the scenes, protects our information from misuse. It is a small but significant piece in the puzzle that makes up parliamentary democracies in the civilised world. Both my team and I remain proud to have responsibility for the Law and we are committed to making it work in an increasingly complex and challenging environment.

Emma Martins
Data Protection Commissioner

"Rather than being 'dead', the challenge of privacy is, in my view, more alive than ever before."
Emma Martins, Commissioner

Part 1 – Activities in 2009

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.

2009 was very much a repeat of 2008 in respect of the number of complaints received, with a similar number recorded. The pattern of complaints by business sector also remained consistent with previous years.

The Commissioner also exercised a new enforcement tool in the shape of an "undertaking".

It was recognised that in many circumstances, there was little to be gained from issuing an enforcement notice to an organisation that had taken significant steps already to remedy the breach and achieve compliance with the Law. The issue of an enforcement notice to a data controller who had already complied with most if not all of the provisions of that notice, would also in effect de-value the notice as an enforcement measure. However, it was felt important to be able to issue some degree of official warning to the data controller to recognise the level of the breach on a more formal level. Undertakings have been used successfully in the UK for some time and so the concept has been adopted for Jersey.

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 2009.

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 2009, 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;
- Social networking sites and internet blogs;
- The inclusion of fair processing statements on data collection forms;
- Notification queries;
- Internet security and safety, particularly in respect of protecting children's privacy;

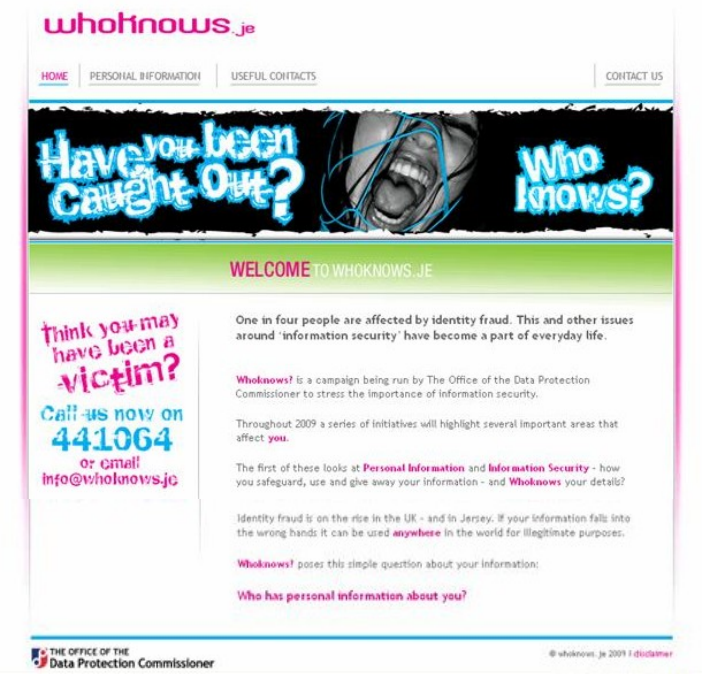
- Publication of photographs and personal information on the internet.

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

As with 2008, 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.

The most notable event in the diary however was Jersey's first Data Protection Day on 28th January 2009. This was an excellent opportunity to run an awareness campaign for the general public to bring issues surrounding the protection of personal information to the fore, and the WhoKnows? Campaign and accompanying website was launched.

Data Protection Day
29th January 2009



2009 saw Jersey's first Data Protection Day on 29th January. The day was deliberately picked as it reflected both European Data Protection Day, and International Privacy Day, celebrated across western jurisdictions such as Canada and the United States. The day itself was picked by a group European Data Protection Commissioners as it represented the anniversary of the signing of the Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data.

Whilst many ideas were put forward as to how Jersey should celebrate its first Data Protection Day, the WhoKnows? website campaign was chosen as the most appropriate way of getting the message across to the general public, in conjunction with a series of radio interviews leading up to and including the day.

The campaign focused on security of personal information; how to safeguard, use and give away information about you in a safe and secure way. The main object of the initiative was to provide the knowledge and tools to the general public, and empower them to ask questions such as, 'Why do you need my information?', 'What are you going to do with it?', and 'Who are you going to give my information to?'

As well as the launch of the WhoKnows.je website, the Commissioner's Office also produced an information leaflet which was handed out to the public through the town centre on Data Protection Day itself, and placed in a number of advisory agencies, including the Citizen's Advice Bureau.

The day was a huge success and the Commissioner hopes to continue to use the day each year to launch some form of privacy and data protection-related initiative.

"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."
Prof. Zelman Caven, "The Private Man" – 1969 – ABC Boyer Lectures

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 2009, the website received 14,375 visits for the year, averaging 1198 visits per month, which calculates to an average of 39 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 24 presentations to a wide variety of organisations between them during 2009, 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, Enforcement Notice, or an Undertaking as well as seeking a criminal prosecution.

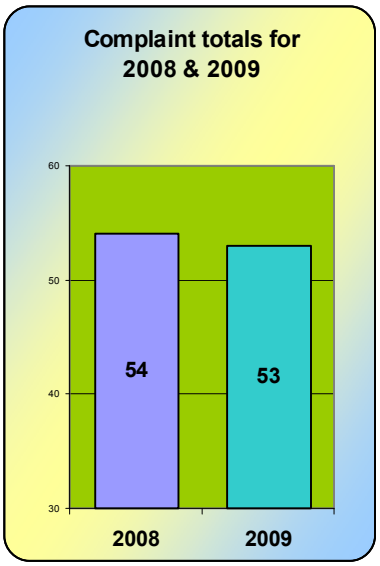
The vast majority of complaints are resolved before the need to invoke any significant enforcement measures such as those described. However, work on a number of significant investigations undertaken during 2008 with regard to allegations of criminal offences under the Law continued into 2009.

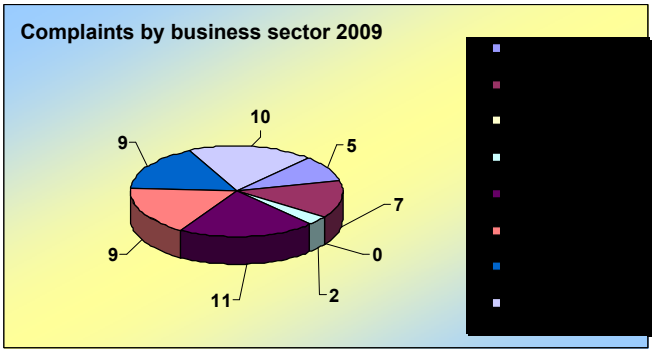
In a significant number of cases investigated during 2009, complaints found to be substantiated were resolved by the respective data controller updating and improving their policies and procedures, or improving the controls over their data handling.

2009 saw the number of complaints received nearly equal that of the previous year, a total of 53 in all. Similarly to 2008, many were of a more serious and complex nature than in previous years requiring more lengthy investigation. The Commissioner's policy on complaint handling, whereby complainants must have exhausted the complaints process of the relevant data controller before seeking redress with the Commissioner, worked well although many complainants still eventually resorted to contacting the Commissioner having failed to seek an adequate level of resolution to their complaint from the data controller.

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.

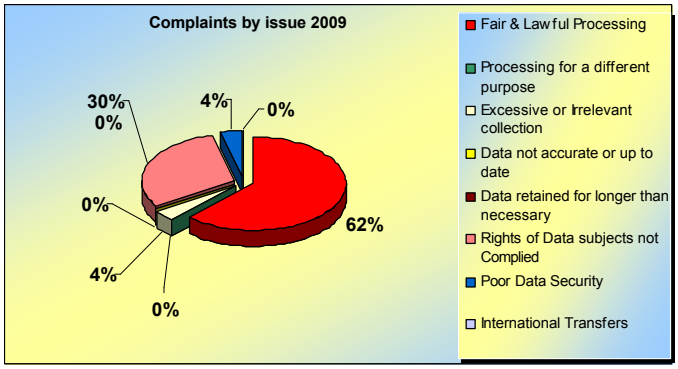
There was a total of 53 complaints, a decrease of less than 2% from 2008. This small decline was expected in light of complainant's attempting to resolve issues directly with data controllers, much of the time with successful outcomes.





The spread of complaints by business sector was consistent with previous year's statistics.

2009 saw a sharp increase in complaints relating to allegations of unfair processing, as well as a slight rise in complaints where individuals' rights under the Law had not been complied with. However, it was encouraging to see a slight fall in complaints relating to poor data security.



"The link between democracy and privacy is not all accidental; without a private zone, public life is impossible."
Charles J Sykes

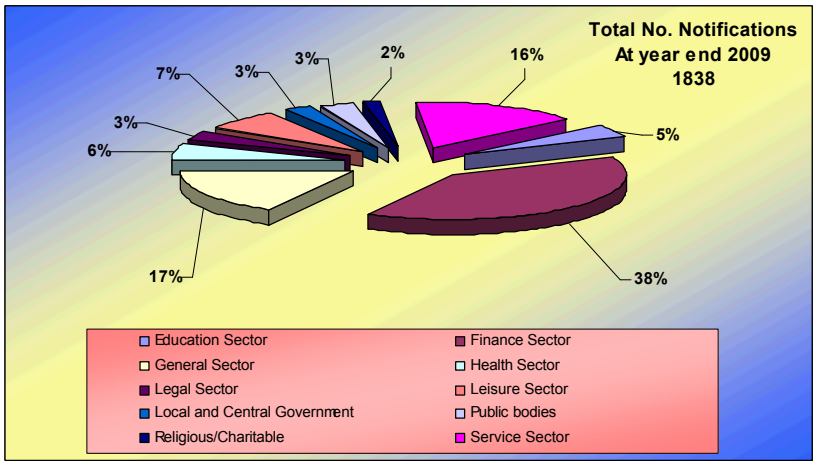
The Public Register

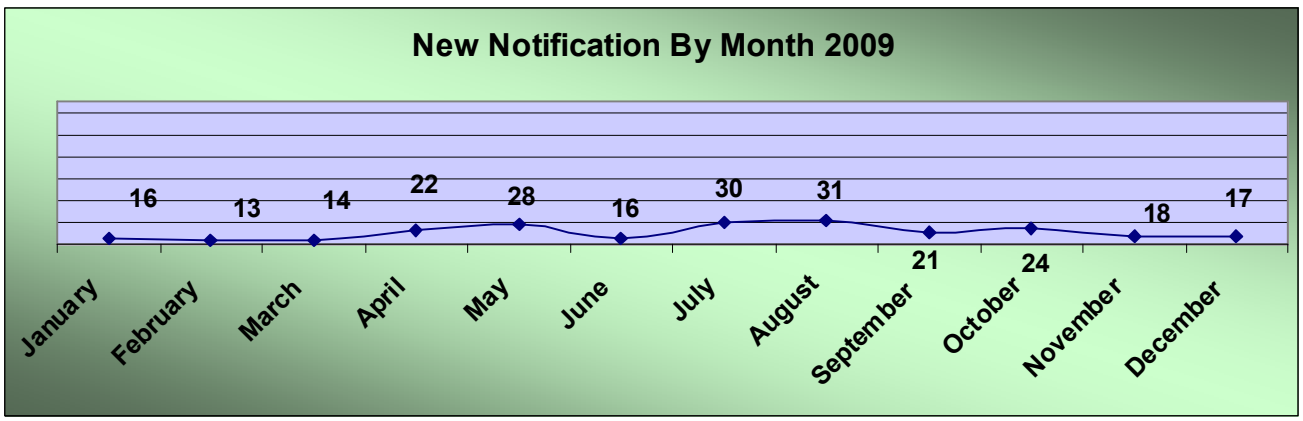
2009 saw the first full year out of the transitional period, with all data controllers being required to comply in full with the 2005 Law requirements.

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, by looking at the monthly figures it is possible to see that during 2009 a total of 250 new notifications were received.

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. However, the global recession saw a number of businesses merging and ceasing trading, resulting in a net increase of 40 notifications on the total for 2008.

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. This project has continued throughout 2009.





"Privacy invasions are socially constructed…not randomly or evenly distributed."
Raab & Bennett

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 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 2009, data protection was the subject of coverage in the local media a total of 65 times, more than doubling the figures for 2008. Of those reports, only a handful portrayed data protection in a negative light.

International Activities

In April, the Deputy Commissioner attended the European Conference of Data Protection Authorities in Edinburgh. The annual meeting of British and Irish Data Protection Authorities took place in Dublin 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.

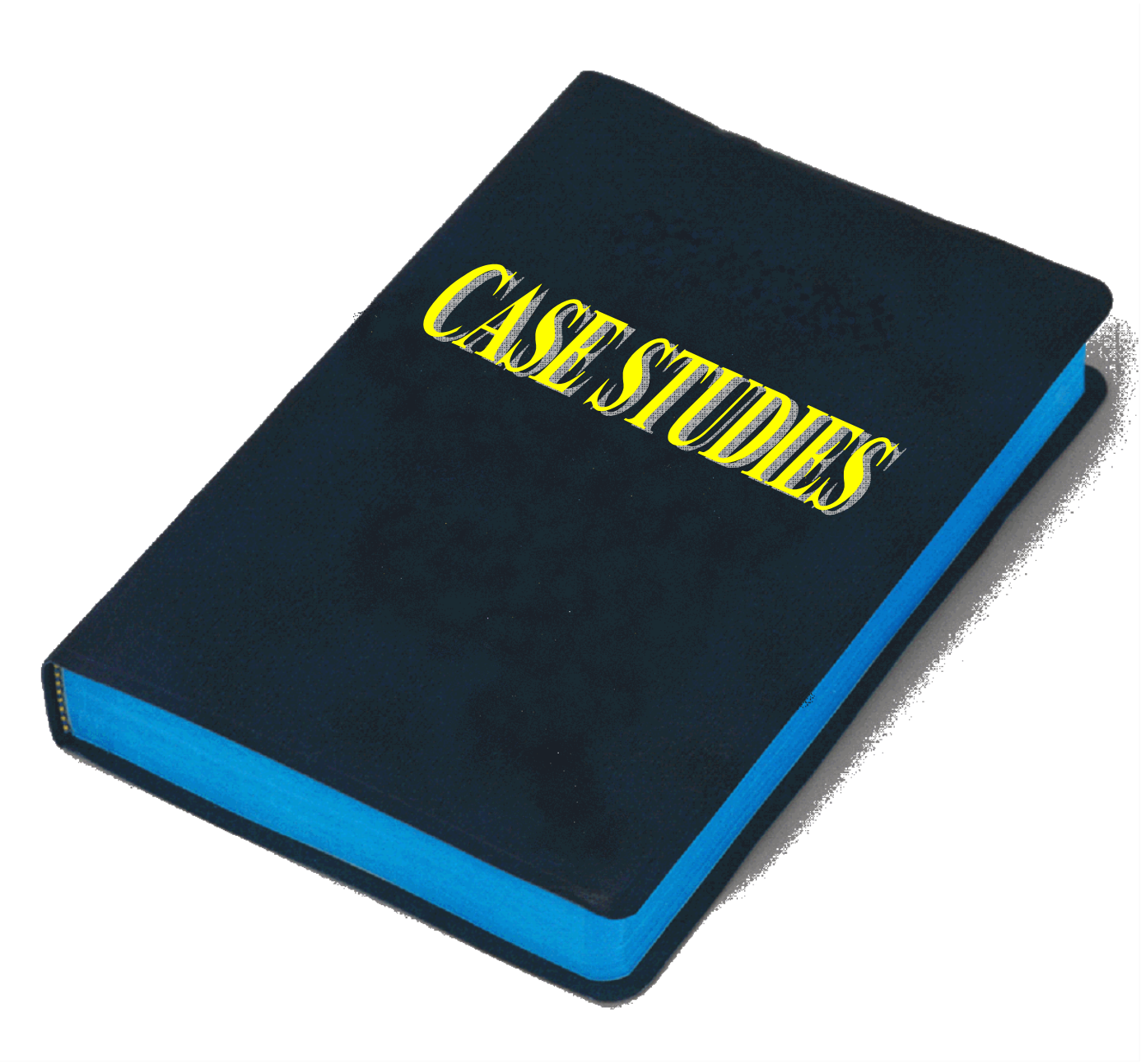
Edinburgh, April 2009

Later in the year in November, the Commissioner and her Deputy represented the Island at the 30[1st] Annual International Conference of Data Protection and Privacy Commissioners. The conference took place in Madrid and was hosted by the Spanish Data Protection Authority.

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 "Privacy: Today is Tomorrow", concentrating on the increasing threats to privacy in the shape of new technologies designed to counter terrorism and internet crime.

"Privacy is like freedom: The less you have of it, the easier it is to recognise."
Simon Davies – Director, Privacy International



Part 2 – Case Studies

Case Study:

Data retention: How long must I hold records for?

1

A man made a complaint to a company about the length of time they had retained his records. He was a former employee of the company and he had discovered that they still held a copy of his contract of employment 7 years after he had left. The man considered that this was excessive and complained to the Commissioner.

The 5th Data Protection Principle requires that personal information is not retained for longer than is necessary. The complainant claimed that it was not necessary for the company to still be holding his contract of employment. However, there are many external factors which determine how long a company can retain data, and therefore justify retention.

Jersey contract law states that a contract is challengeable for up to 10 years following its termination. It is therefore considered reasonable that a contract of employment can be retained for a 10 year period following the termination of employment. As a result, the complaint was not upheld. It is therefore important to know what external factors may influence how long data is retained for, but clearly such data should be held securely and only authorised access allowed.

Case Study:

Client databases

2

An employee decided to copy the company's client database and start a rival business by using the database to contact the clients and sell his new company's services to them.

The 1st and 7th Data Protection Principles would apply with regards the use of, and the security of that data. The employee did not have permission from the company to use the database for his own gain and he did not have consent from the clients to use their data for his own marketing purposes. The company had taken sufficient steps to safeguard client data through their own security policies and procedures, which the employee had chosen to ignore. The employee was required to return all the data to the data controller and sign an undertaking not to contact any clients on the data controller's database.

It is also possible in these circumstances that there may be evidence of a criminal offence of unlawful obtaining of personal data under Article 55 of the Law, in addition to the two Principle breaches highlighted.

Case Study: 3

Loss of data

Many organisations allow staff to take work home with them on removable storage devices such as memory sticks, laptops or Smart devices such as Blackberries and other media.

This is often a convenient way to transport vast amounts of data but can however lead to significant security risks if that device is lost or stolen. One such incident reported to the Commissioner involved the loss of a memory stick containing a large quantity of client data. The employee concerned had taken the data home, but had lost the memory stick during their journey home.

Organisations must have robust processes in place to protect data which may be removed in this manner. Failure to do so could result in the organisation being found in breach of the 7th Data Protection Principle. How the organisation handles the security breach is key, and whilst notification to the regulator or the clients affected is not compulsory, it is an option. In this scenario, the memory stick was later recovered from the employee's vehicle.

Case Study: 4

Excessive data collection

How much information do you ask for? That is the question posed by many organisations who are trying to maximise their marketing potential. One such organisation ran a competition and customer satisfaction survey in an attempt to draw in more customers.

Whilst this is one common marketing method, care must be taken with regard to how much information is sought about the customer. In this instance, the company gave the impression that the data collection was for two purposes: Assessing the satisfaction of the service they provided to their customers, and entry into a competition. No mention was made on the survey forms that the data was also being used for marketing purposes, and no opt-out was given to participants, thus making it unclear exactly what was going to happen to that information.

The survey itself asked many questions relating to customer satisfaction, but also went on to ask many lifestyle questions in order to build a customer profile. The vast majority of these questions were not relevant to the survey itself, or entry into a competition and could be considered excessive, and in breach of the 3rd Data Protection Principle.

The company concerned were asked to amend their fair processing statement on their forms and make it much clearer to participants as to what their data was to be used for, in line with the 1st Data Protection Principle.

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 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 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.

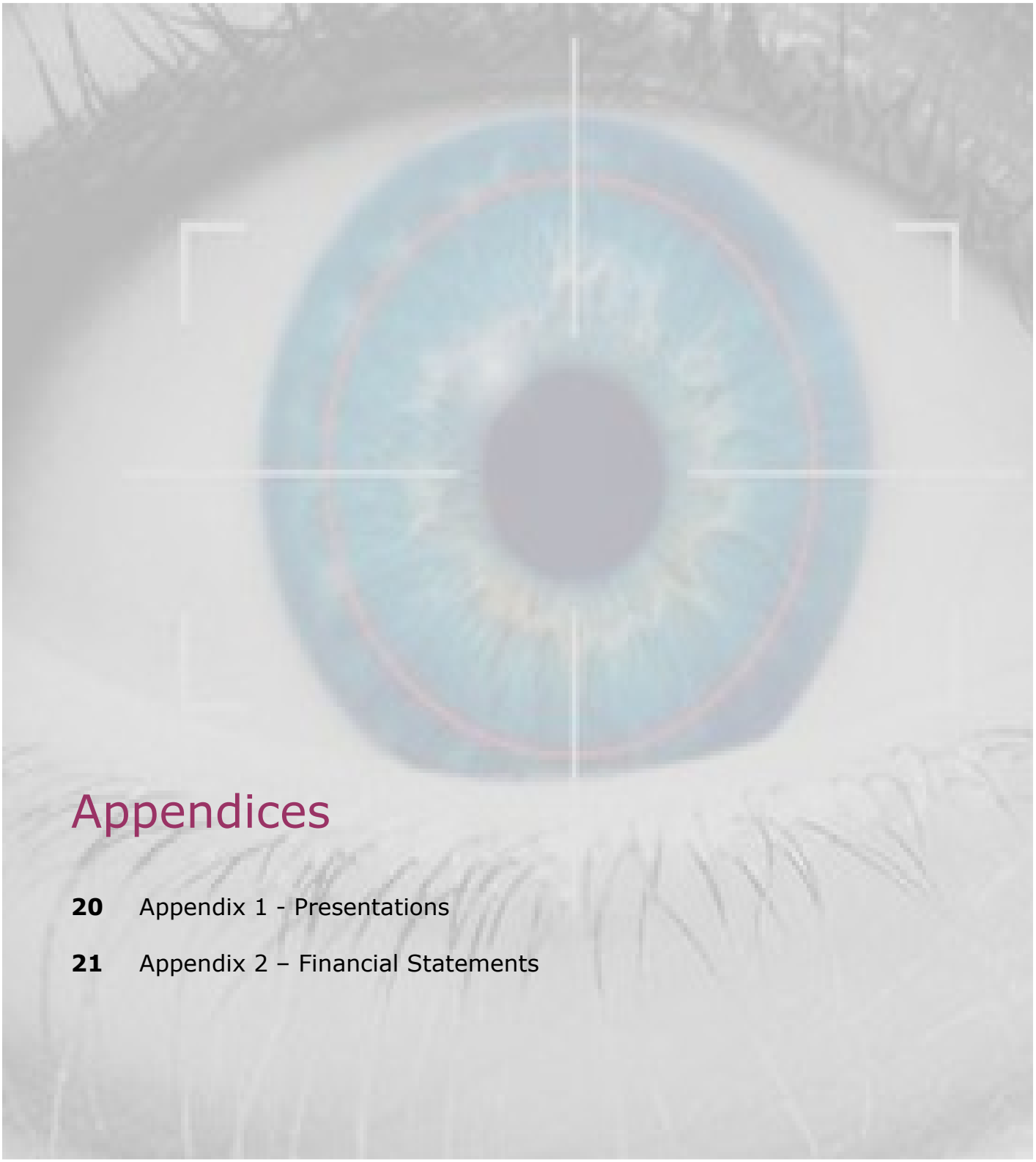
The users section includes tips on how to take care of your personal information and what to look for when choosing a social networking site to use, while the providers section looks at the regulatory requirements, privacy protection and how to manage inappropriate content or activity.

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.

During 2009, work started on a Code of Practice for the processing of personal data by Credit Reference Agencies. Whilst these organisations are regulated in the UK by the Consumer Credit Act, no such regulation exists in Jersey and it often falls to the Data Protection Law to control what happened to personal data held by them. Such are the differing methods and practices adopted by Credit Reference Agencies in Jersey, it was considered that a Code of Practice is necessary to standardise how such organisations collect, hold, use or disclose personal data that comes into their possession.



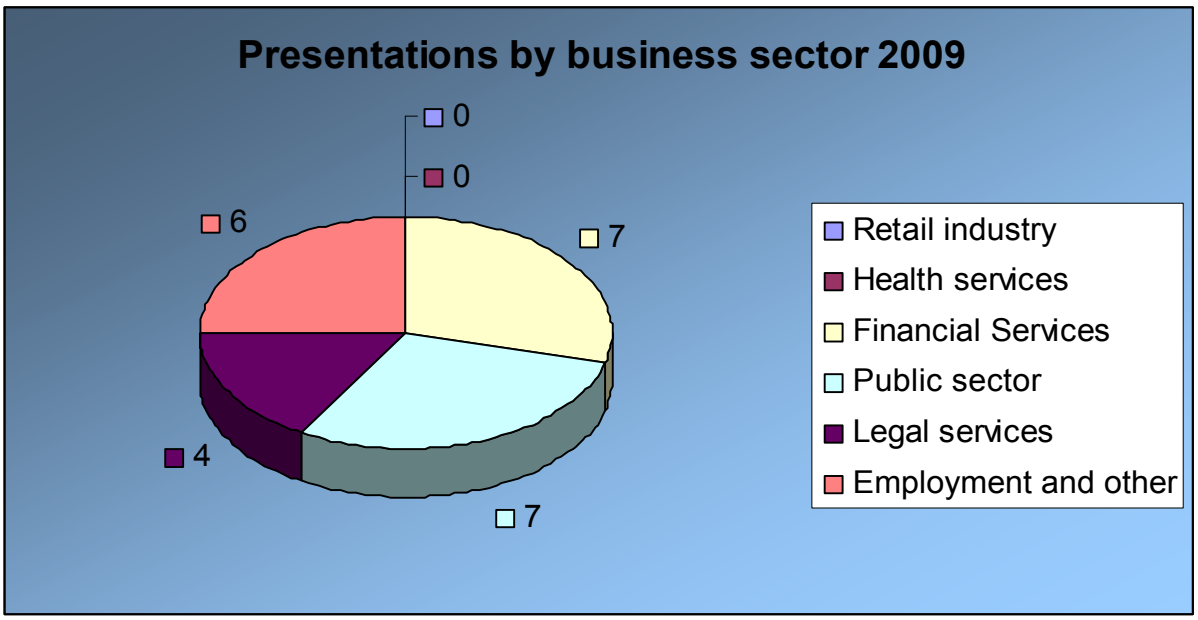
Appendices

Appendix 1

Presentations

During 2009, a total of 24 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 2009

	Note	£	2009 £	£	2008 £
Income:					
Registry fees	1		93,855		93,874
Total income			93,855		93,874
Contribution from the States of Jersey			241,786		239,600
Net income			335,641		333,474
Operating expenses:					
Manpower costs:					
Staff salaries, social security and pension contributions		242,686		239,367	
Supplies and services:					
Computer system and software costs	2	6,675		2,912	
Pay Offshore admin fees		502		399	
Administrative costs:					
Printing and stationery		1,958		1,722	
Books and publications		1,990		2,690	
Telephone charges		689		671	
Postage		2,482		2,538	
Advertising and publicity	3	9,516		3,705	
Meals and Entertainment		176		201	
Conference and course fees		5,477		6,590	
Bank charges		0		130	
Other administrative costs		12,383		13,399	
Premises and maintenance:					
Utilities (incl. Electricity and water)		9,058		8,638	
Rent		27,707		27,031	
Total operating expenses			321,299		309,993
Excess of income over expenditure			14,342		23,481

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

Whilst there would appear to be a slight decrease in notification fees, in real terms the figure represents approximately a 15% increase in the number of notifications estimated at the beginning of 2009.

2) Computer system and software costs

This figure has increased significantly since 2008 and is largely due to the change in contract for development and maintenance of the website and notification system. The Commissioner entered into a contract with C5 Alliance for this purpose at a cost of £3000 per year.

3) Advertising and Publicity

Planning and preparation for the "WhoKnows" public awareness campaign commenced towards the end of 2008 and continued into 2009. This figure represents consultancy work undertaken during 2009 as part of that process.

The Santiago Bernabeu Stadium, Madrid 2009

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