THE OFFICE OF THE
Data Protection Commissioner

2010 ANNUAL REPORT

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;

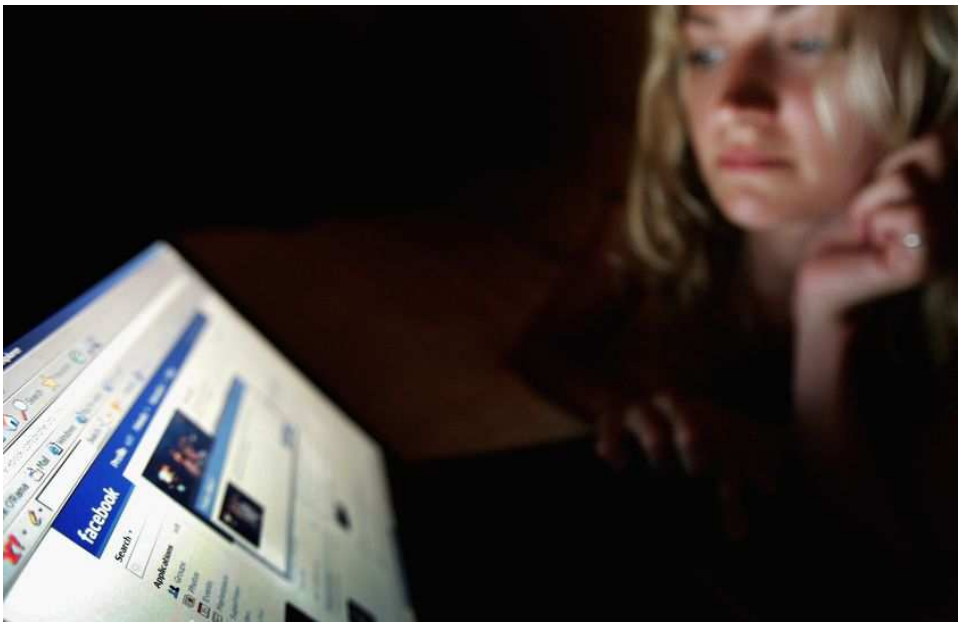
Right to seek compensation
You can claim compensation from a data controller for damage or distress caused by any breach of the Law;

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

"Personal information is the single most valuable non-consumable asset possessed by any business."
Masons, into the Data Protection Act 1998.

Foreword

This is my sixth report as Data Protection Commissioner for the Bailiwick of Jersey. It covers the year 2010. The Data Protection (Jersey) Law 2005 has been in force for five years. The Law is now fully operational and covers a very wide range of data and processing.

2010 was another challenging year. We have seen a significant rise in the number of enquiries and complaints made to the department. The increasingly complex nature of the investigations now undertaken 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. New technologies and the ease with which data can be collected, stored and disclosed had further added to this challenge.

All of the immediate communication through Twitter, blogs and wikis etc. is looking, on the face of it, as if it is encouraging freedom – freedom of speech and the free flow of information. However, the trend for using these in place of traditional sources of information which require more review and confirmation, amounts ironically to an unintentional censorship of opinions. The accountability which is part of traditional media is easily sidestepped by individuals posting information online – people become more likely to rely on these sources for information, news and opinions. Thus, the impact extends way beyond questions of privacy.

It would appear that we have four possible approaches to internet usage –

1) the state you live in decides what you can and can't see;
2) the big companies you rely on (Yahoo, Apple, Microsoft etc) select what you see;
3) you want to be free to see whatever you want – uncensored news from anywhere, all world literature, manifestos from all parties, jihadist propaganda, bomb-making instructions, intimate details of other peoples private lives, child pornography – all should be freely available. It's then up to you to decide what you'll look at;
4) everyone should be free to see everything, except for that limited set of things which clear, explicit global rules specify should not be available.

At the moment we have mostly 1) and 2) and with developments in technology we are seeing more of 3). My view is that we should look seriously at 4).

I admit that that may seem utopian. But utopian ideals are of value. Of course, they don't help us deal with specific problems, but they provide us with a fixed point by which to navigate through these choppy waters. Ideals can help us take stock of where we are, where we're going and whether we really want to head further in that direction. In the absence of that dialogue – we will be taken somewhere we haven't decided we want to go.

In 1864, Lincoln stated – "*the world has never had a good definition of the word 'liberty'; we are much in need of one. We all declare for liberty but in using the same word we do not mean the same thing. The shepherd drives the wolf from the sheep's throat, for which the sheep thanks the shepherd as his liberator, while the wolf denounces him for the same act as the destroyer of liberty".*

Much like the concept of liberty, privacy is notoriously difficult to articulate and it means different things to different people. Governments try and work through such challenges by creating 'social contracts' with citizens whereby it agrees to protect the natural rights of the people, to act as arbiter in disputes and to establish just laws. In return, all who live in the jurisdiction agree to accept the authority of government and laws as are established.

So whilst some may have differing view on what concepts such as liberty and privacy mean, we have to accept that the legislation has been implemented in a democratic manner. Democratic states seek to provide the individual with liberty, allowing him/her to do anything as long as no harm is done to others in the process. Such an approach is at the heart of modern democracies and the link between democracy and privacy is not accidental. Limits on privacy intrusions are justified on the grounds of preventing harm to others. Breaching privacy, now more than ever, has the potential to do very real harm to individuals, groups and society as a whole. A breach of privacy can severely inhibit a person's autonomy and self development and the effect can be profound. Thus protecting privacy can promote peoples autonomy as much as free speech can. We do not live in an anarchic state, so such questions are political in their nature.

We have put deterrence and punishment for unlawful acts into the hands of government because the social and individual costs of vigilantism are too high.

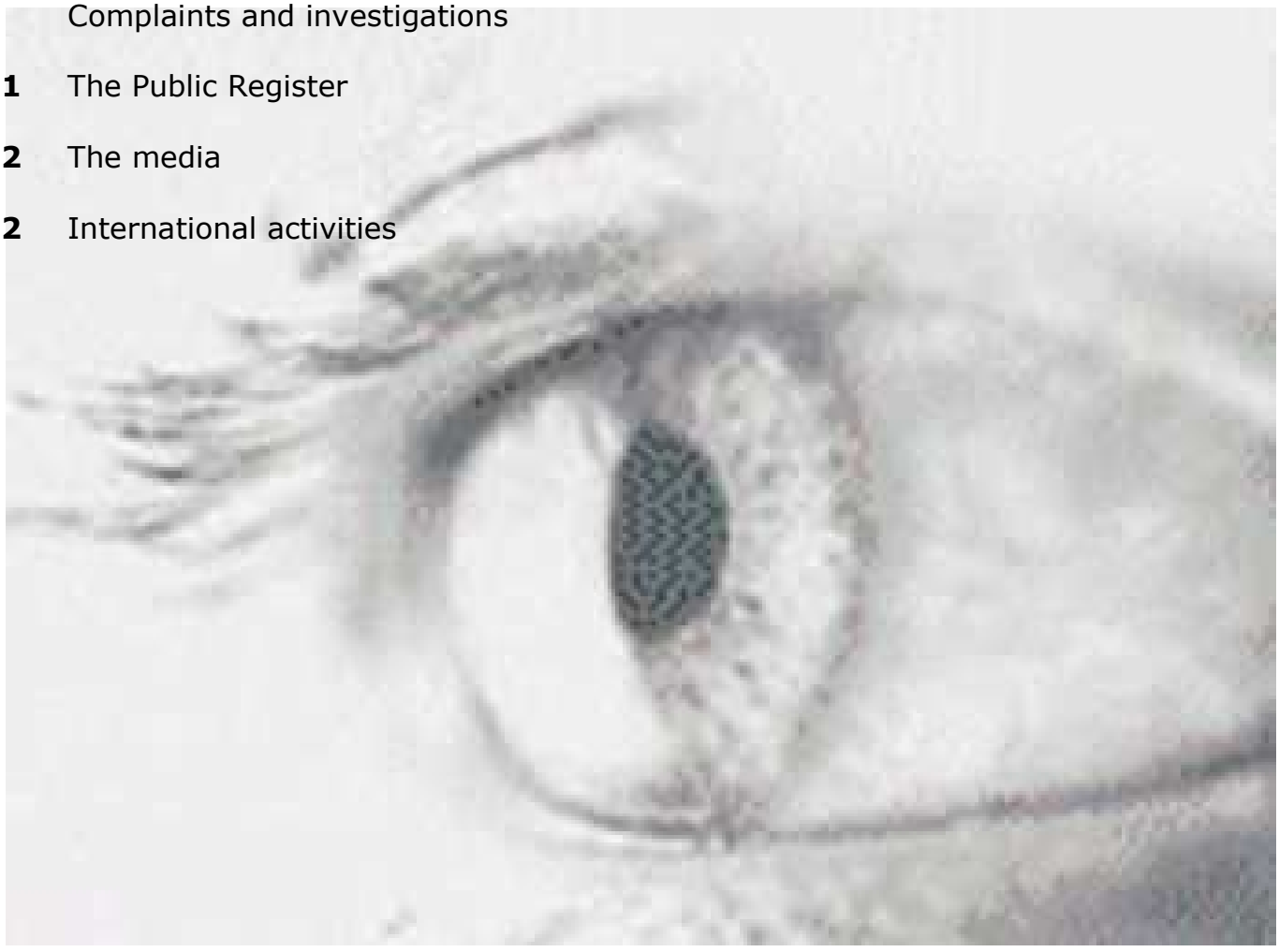
Importantly, I am of the firm belief that looking towards 'legislation' of global civil society should not be viewed as a zero sum relationship. Lincoln articulated this over a century ago, but it resonates today - *"We must avoid the common fallacy of supposing that freedom and discipline are inconsistent. Such discipline does not take the form of a compulsory obedience to a higher authority, but is based upon an intelligent understanding of the fact that order and sanity are essential if the liberty of the individual is to be reconciled with the rights of other individuals….the responsible individual, not the irresponsible individual, is the real basis of a truly free society".*

Jersey has chosen to implement legislation that sets out the basic standards to ensure privacy and security of personal data. 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 continue to work hard to make it work in a complex and fast-evolving environment.

Emma Martins
Data Protection Commissioner

"The accountability which is part of traditional media is easily sidestepped by individuals posting information online."
Emma Martins – Data Protection Commissioner

Part 1 – Activities in 2010



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.

Notwithstanding, 2010 saw a significant rise in the number of complaints made to the Commissioner. Of particular note was the number of complaints relating to alleged failures by data controllers to comply with the rights of individuals under the Law.

By far the most significant event of the year however was the conclusion of Jersey's first conviction under the Data Protection (Jersey) Law 2005 for the Article 55 offence of unlawful processing of personal data. A former States Member was found guilty of having obtained a confidential Police report and then subsequently publishing the report on a 'blog'. This case was an historic landmark in the international world of data protection, as it is the first of its kind relating to the publication of personal data via an internet blog.

A number of other cases were also referred to Jersey's Crown Prosecutors for consideration of prosecution for data protection offences, further emphasising the Commissioner's strategy to clamp down on poor data processing practices.

2010 also saw the execution of a search warrant at a local General Practitioners offices, following numerous complaints from individuals who could not access their records. The resulting search in conjunction with the States of Jersey Police recovered over 3000 abandoned medical records, many of which were later reunited with their owners.

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 2010, 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;
- The impact of emerging technologies on data processing, such as cloud computing.

- 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 2009, 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.

Once again, Data Protection Day was celebrated on 28th January 2010, with a number of local radio broadcasts arranged to highlight topical areas of data protection.

Unless we establish a balance between privacy and free speech, we may discover that the freedom of the Internet makes us less free.

Daniel J Solove – The Future of Reputation

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. The website was visited a total of 12,961 times during 2010, averaging 35 visits per day, a slight decrease in the number for 2009. 42% of those visits were direct, whereas 36% were referrals through the Google search engine.

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 19 presentations to a wide variety of organisations between them during 2010, 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 and 2009 with regard to allegations of criminal offences under the Law continued into 2010.

In a significant number of cases investigated during 2010, 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.

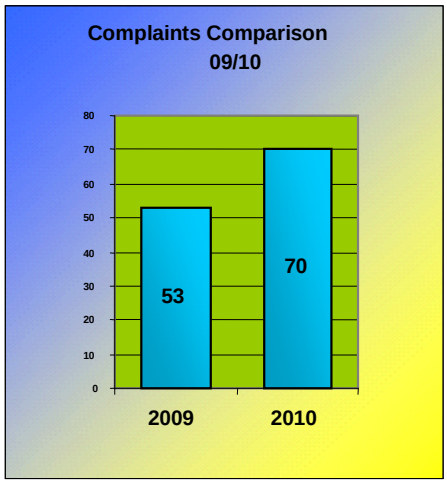
2010 saw the number of complaints received increase significantly on the previous year. 36% of these were in relation to the rights of data subjects not having been complied with. Coupled with the fact that 36% of complaints were against the retail sector, further pro-active work is to be undertaken with retailers during 2011 to ensure compliance with the Law and Principles.

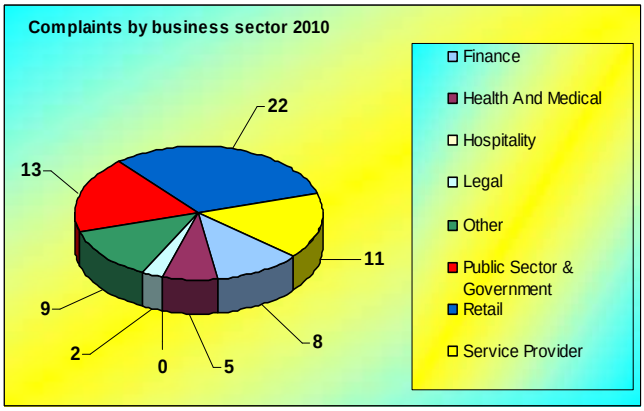
In addition, a total of three enforcement notices were served and one formal undertaking issued during 2010.

"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 Cowen*

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.

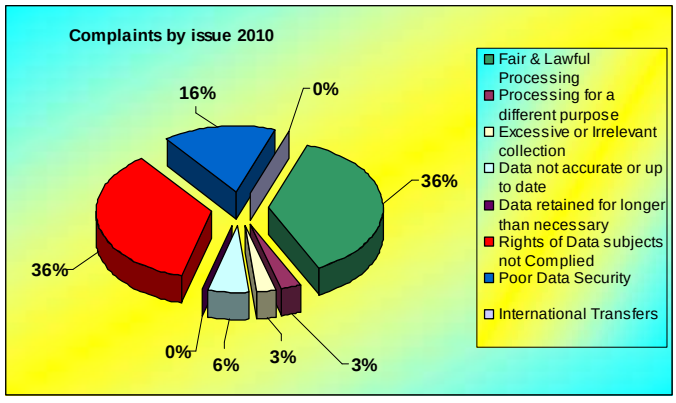
There were a total of 70 complaints, an increase of 32% from 2009. This is more likely due to more individuals becoming increasingly aware of the rights available to them under the Law.





The majority of complaints received were in relation to alleged breaches by retailers. There was a significant rise in the number of complaints against online retailers in particular.

2010 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. In addition, there was also a 12% increase in complaints relating to poor data security.



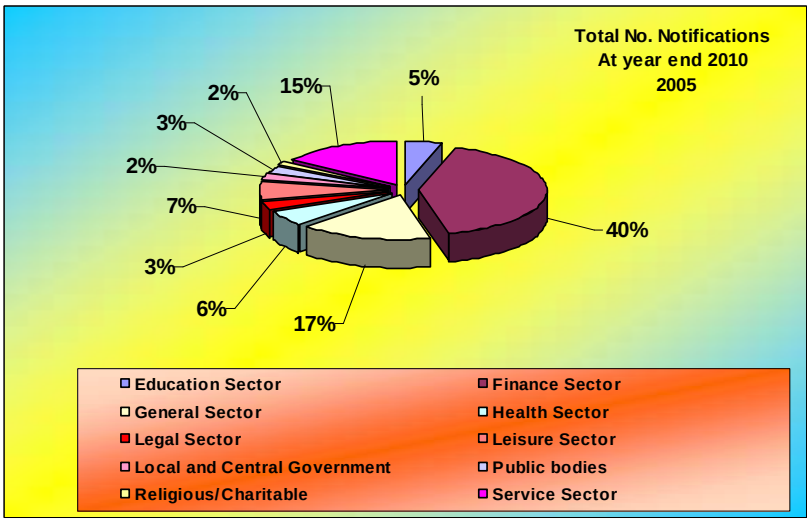
"Processes of control, regulation and surveillance are further intensified by the rapid spread of new technologies." *Paul Lewis*

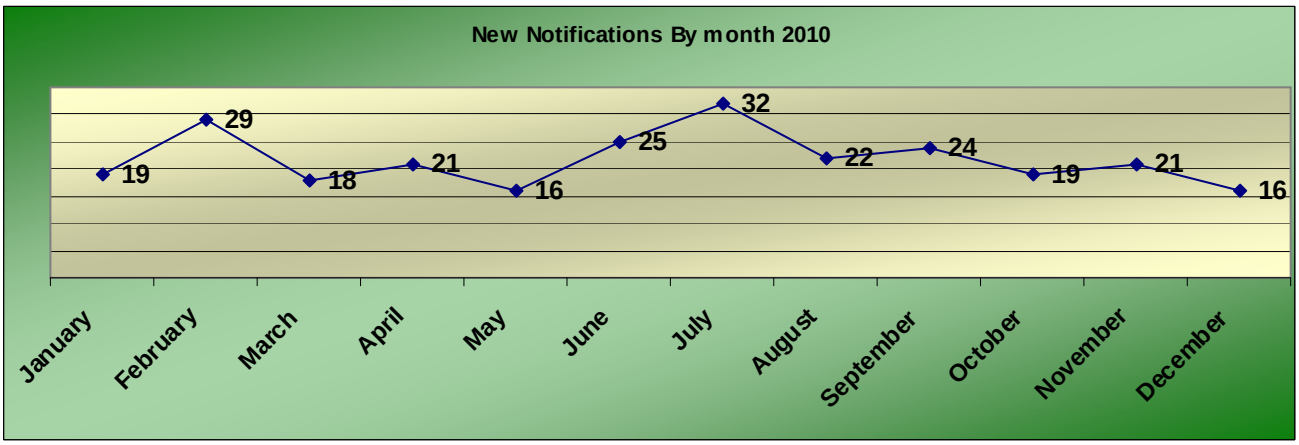
The Public Register

2010 saw the broad spread of notifications remain much the same as it did for 2009, with only a slight rise shown for the finance sector.

In respect of new notifications received, once again there was a slight rise in the total number which reached 262 by the year end, an increase of 12 from 2009. The figures do not show any comparable trend with regard to the busiest times of the year, although February saw the biggest rise on a monthly figure compared to the same time in 2009.

A project was undertaken by the Commissioner's Office during 2009 and 2010 in an attempt to identify any additional data controllers based in Jersey that may be required to notify under the Law. It is conceivable that the large number of new notifications received during 2010 could be attributed to this project, however it is also likely that the increase in the profile of data protection through the media and similar publicity combined with our routine proactivity on notification compliance has also played a part.





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 2010, data protection was the subject of coverage in the local media a total of 78 times, another increase on the 2009 figure which more than doubled the figures for the previous year. Of those reports, only six portrayed data protection in a negative light.

International Activities

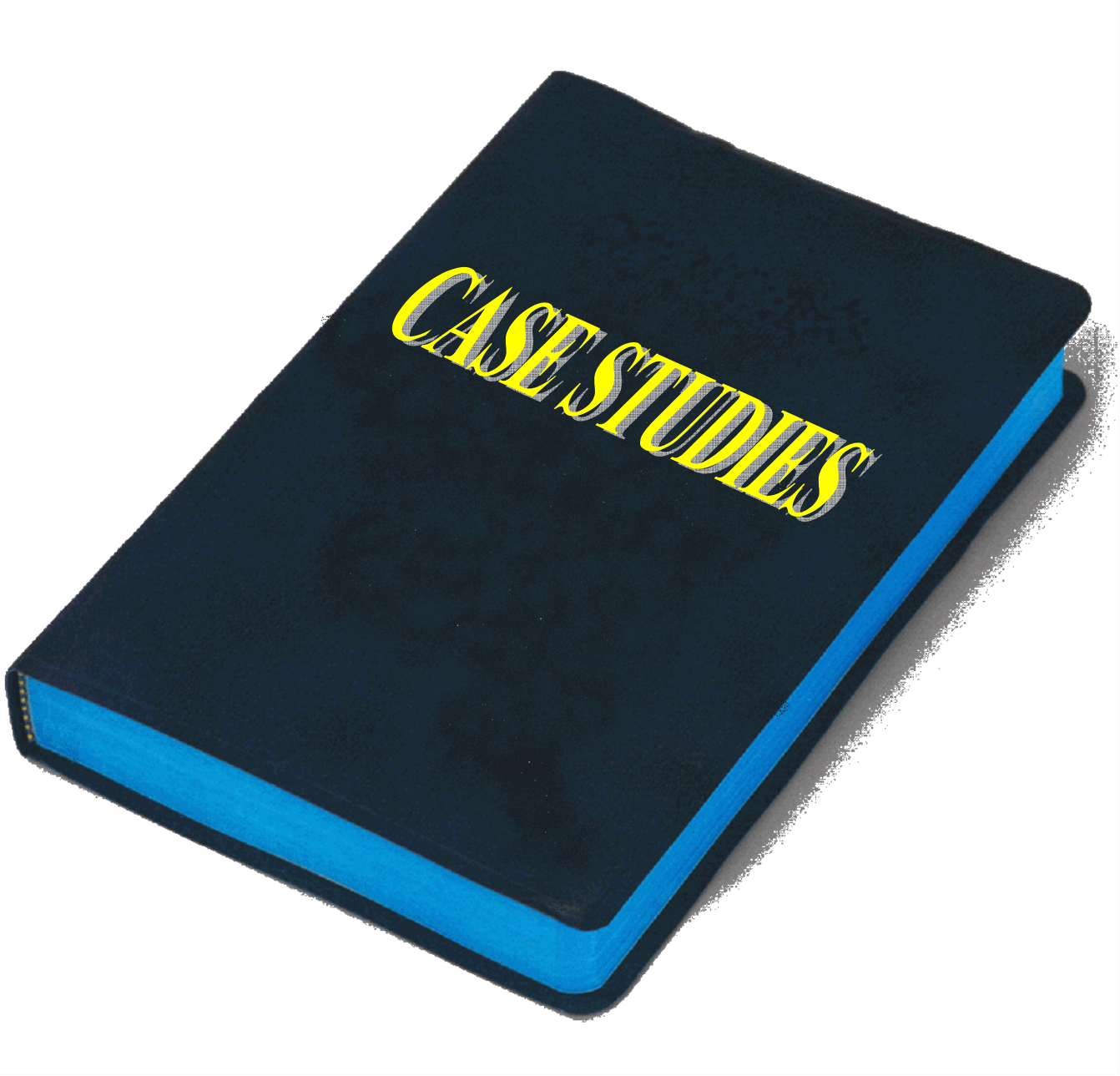
In April, the Deputy Commissioner attended the European Conference of Data Protection Authorities in Prague. In July, we were delighted to host the the annual meeting of British and Irish Data Protection Authorities in Jersey. This meeting has now been extended to also include the authorities from Cyprus and Gibraltar as well as the three Crown Dependencies.

Prague Castle, April 2010

Due to resource implications, neither the Commissioner nor her Deputy attended the International Conference, which was held in Jerusalem in October. Instead, the Deputy Commissioner attended the Privacy and Data Protection Compliance Conference held in London.

This conference covered numerous privacy-related subjects across the two days, such as social networking and cloud computing. The conference also focused on children's privacy, specifically looking at the changing attitudes to privacy amongst young people compared to adults.

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



Part 2 – Case Studies

Case Study:
Disclosing 'spent' convictions

A lady was applying for a job in a bank, but was concerned as she had a previous conviction for a criminal damage 20 years earlier when she was a teenager. The application form asked for details of all previous criminal convictions. As the conviction was considered 'spent' under the Rehabilitation of Offenders (Jersey) Law 2001, she did not disclose the conviction.

Within the first week of commencing her new employment, the Directors called her into a meeting a questioned her about her previous conviction, having heard about it from another source. The lady declined to offer any information about her previous conviction as it was 'spent'. However, the Directors dismissed her on the grounds that she had not been honest in her application form.

This raises a number of issues:

Firstly, the lady was under no obligation to disclose details of any spent convictions she may have had, and her employers should not have attempted to force her to disclose the information. Furthermore, the employers had obtained the information from another source without the explicit consent of the employee, thus leaving themselves open to a breach of the 1st data protection Principle.

Case Study:
Unsubscribing from marketing activity

A man made a one-off purchase with a Jersey-based online retailer. The following week he began to receive a daily e-mail newsletter from the company, advertising their products and services.

The man clicked on the 'unsubscribe' link at the bottom of the email newsletter, believing that this action would prevent any further emails being received. However, the emails continued to arrive and despite several more attempts to unsubscribe, he continued to receive them.

Like any other data controller, online retailers are expected to comply with the 6th data protection Principle, which requires them to comply with the rights of data subjects under the Law.

One of those is the right to object to receiving direct marketing material. Any individual can exercise this right so long as it is directed personally to you, and a data controller is expected to comply with the subjects wishes within a reasonable time, normally within 28 days. The data controller should have robust processes in place to comply with the unsubscribe request. Should they fail to comply with the request, they risk regulatory action for a failure to comply with the 6th data protection Principle.

Case Study:

Rights of access to personal data

An employee was dismissed from her employment and felt that she had been treated unfairly. She decided to take her case to an employment tribunal, but needed to gain access to her employment personnel file.

An individual has a right of access to information held about themselves by a data controller under Article 7 of the Law. An employee can therefore exercise their rights to gain access to the information held within their employment personnel file by making a 'subject access request'.

The data controller can charge up to £10 for the request and is obliged to respond at the earliest opportunity but no longer than 40 calendar days.

There is however a common perception that the employee is entitled to a copy of the entire file. This is not the case. An individual is entitled to a copy of the **information** held about them, and not necessarily a copy of the original documents. The data controller may also withhold certain information from the file, such as third party data and information not covered by the Law. In this regard, the subject access request may not always be the best source of information if it is to be used for litigation purposes.

Case Study:

Purpose 'jumping'

A company organised a prize draw as part of a publicity campaign, by posting flyers through household letter boxes and handing them out in the street. The application form collected names, addresses and email addresses of entrants.

The form did not however make it clear to the entrants exactly what the information would be used for. The reasonable expectation of the entrant was that the information would be used to contact them in the event that they won the competition. However, the intention of the company was to use the information to compile a marketing database.

After the draw took place, entrants began to receive marketing emails from the company. None of the entrants had consented for their information to be used for this purpose.

Information collected for one purpose and used for something different is known as purpose 'jumping' and could amount to a breach of the 2nd data protection Principle. However this can be easily avoided if data controllers make it clear to consumers from the outset what they are collecting the data for. A good fair processing notice on the form will identify who is collecting the data, what it is to be used for, and who it might be disclosed to. If the data is to be used for marketing activity, then the opportunity to opt out should also be included.

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.

2010 saw the implementation of guidance in respect of subject access requests when connected with legal proceedings. This guidance was introduced following numerous enquiries whereby lawyers acting on behalf of clients were using Article 7 of the Law (rights of access to information) to obtain information for litigation purposes.

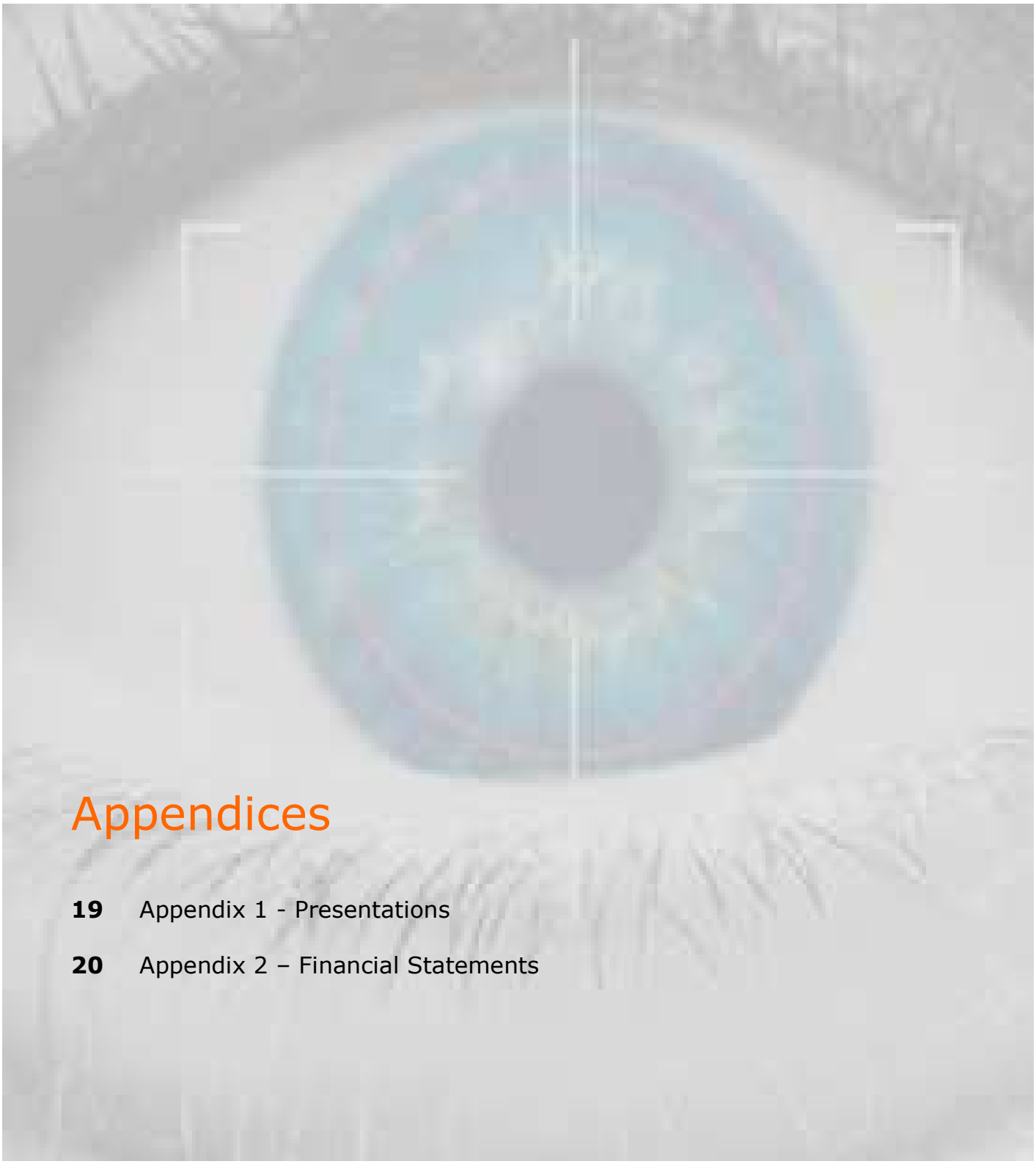
Neither the Law, nor the European Directive on Data Protection (95/46/EC) limit the purposes for which a subject access request can be made. Similarly, there are no exemptions in Law from the right of access where civil legal proceedings are contemplated or ongoing.

The Commissioner's view is that the right of subject access is one of the cornerstones of the Law, and any avoidance of compliance with a request in these circumstances would seriously undermine that fundamental right.

Codes of Practice and guidance on the processing of personal data for credit purposes were also drafted and consulted upon during the course of 2010.

The lack of any Consumer Credit legislation in Jersey has resulted in a largely unregulated credit reference and debt collection industry. Whereas in the UK, the Consumer Credit Act regulates such industry and provides consistency of operation between Credit Agencies, no such framework exists in Jersey. Over time, this has lead to a number of inconsistencies in the operations of Credit and Debt Collection Agencies locally, and the need for a more consistent approach was identified.

Following consultation with industry representatives and the Jersey Consumer Council, Codes of Practice were drafted and these have now been submitted to the States for approval.



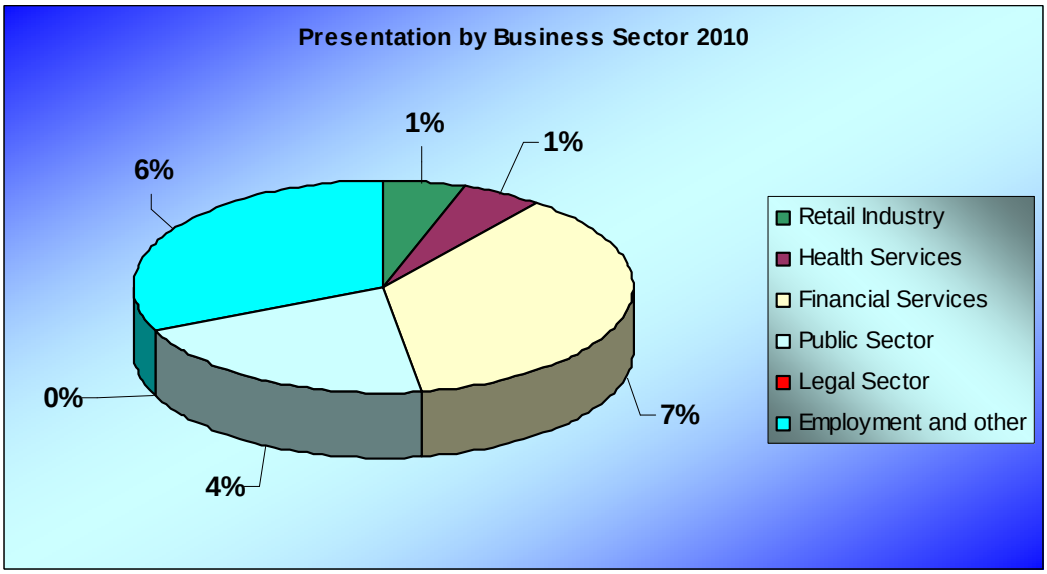
Appendices

Appendix 1

Presentations

During 2010, a total of 19 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 2010

	Note	£	2010 £	£	2009 £
Income:					
Registry fees	1		100,752		93,855
Total income			100,752		93,855
Contribution from the States of Jersey			227,890		241,786
Net income			328,642		335,641
Operating expenses:					
Manpower costs:					
Staff salaries, social security and pension contributions		226,934		242,686	
Supplies and services:					
Computer system and software costs		3,295		6,675	
Pay Offshore admin fees		522		502	
Administrative costs:					
Printing and stationery		2,782		1,958	
Books and publications		2,500		1,990	
Telephone charges	2	1,171		689	
Postage		501		2,482	
Advertising and publicity	3	408		9,516	
Meals and Entertainment		31		176	
Conference and course fees	4	10,604		5,477	
Bank charges		0		0	
Other administrative costs	5	5,369		12,383	
Premises and maintenance:					
Utilities (incl. Electricity and water)		9,408		9,058	
Rent		28,400		27,707	
Total operating expenses			291,925		321,299
Excess of income over expenditure			36,717		14,342

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

2010 saw an unexpected rise in the number of new notifications, thus accounting for an increase in income of just over £7000 on the previous year.

2) Telephone charges

This figure has increased significantly since 2009 and is largely due to the significant increase in communications and work undertaken with UK and international regulators.

3) Advertising and Publicity

Whilst this figure appears to show a significant decrease in the advertising and publicity activities of the office, much of the cost of the campaign for Data Protection Day in 2009 was covered by the Conference and Course Fees budget.

4) Conference and Course Fees

The Commissioner and her Deputy did not attend an International Conference of Data Protection and Privacy Commissioners in 2010, as much of the cost of the campaign for Data Protection Day in 2009, and the hosting of the British and Irish Data Protection Authorities meeting was covered by the Conference and Course Fees budget.

5) Other administrative costs

This figure shows a significant decrease in the additional administrative costs incurred by the Office during 2010. This is largely due to the completion of the Notification Research Project at the end of 2009, which was the primary cause of the higher figure for the previous year.

Elizabeth Marina and Elizabeth Castle, Jersey 2010

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