BAILIWICK OF GUERNSEY

DATA PROTECTION COMMISSIONER
REPORT FOR 2008

MISSION STATEMENT

The Data Protection Office will encourage respect for the private lives of individuals by:

- *promoting good information handling practice,*
- *enforcing data protection legislation and*
- *seeking to influence national and international thinking on privacy issues.*

Front Cover: Hemisphere of the Council of Europe, venue for the 30th International Conference of Data Protection and Privacy Commissioners, Strasbourg.

CONTENTS

FOREWORD

I am pleased to present my eighth annual report to the States of Guernsey, covering the calendar year 2008.

The succession of high profile data breaches in the UK during the year served to raise the national profile of data protection considerably and, in the words of the UK Commissioner: "Data Protection is being taken seriously at last".

Locally, whilst the breach of security of the States' website provided unwelcome publicity for the States, it did provide additional publicity for the work of this office; however, the investigation of the breach itself took up a considerable amount of time and resources during the year with further follow-up activities continuing during 2009.

As a consequence, expenditure for 2008 exceeded budget, but the eventual outcome was beneficial in that the level of technical security and the awareness of data protection within the States have both increased.

Privacy considerations for users of social networking continued to cause concern and those concerns were justified as social networking sites themselves began to be targeted by identity thieves. The privacy risks of social networking have received both local and international publicity.

In April, the UK Commissioner initiated a review of the 1995 European Union Data Protection Directive; this report will be published in 2009 and be covered in my next annual report. The ICO review was followed by an announcement of a similar review by the European Commission. Any proposed changes to the Directive are likely to take a number of years to come to fruition, but could well influence the future direction of legislation within the Bailiwick. I will keep the situation under review and advise the States accordingly.

Internationally, moves were initiated at the 30th Commissioners' conference to establish a set of data protection and privacy standards for universal application.

The objectives of such standards, and of the more extensive standards being developed by the International Standards Organisation, to which my office is contributing, are to bridge the gaps that exist between the diverse approaches to privacy protection adopted in different parts of the world, thereby facilitating international transfers of personal data.

Data Protection Commissioner, May 2009.

DATA PROTECTION ISSUES

Amendments to the Law

The amendments to the Law that were approved by the States on 27th September 2006 have yet to be enacted. These amendments mirrored changes to UK legislation; subsequently, further amendments to the UK legislation have been made, including a strengthening of the powers of the Information Commissioner. Consequently, it is possible that a follow-up report with proposals for additional amendments to the Law may be submitted to the States during 2009.

States Website Data Breach

In March, 2008, the Guernsey Press published an article claiming that, as a result of an alleged vulnerability of the States of Guernsey website, personal data of care home residents and applicants for enrolment on the Electoral Roll were accessible on the Internet.

The existence of such vulnerability could have constituted a breach of the data protection principles, specifically principle 7, which requires data controllers to have adequate security in place.

The Commissioner engaged the assistance of PwC in conducting a thorough investigation of the allegation. His report[1] concluded that there had been a breach of the seventh data protection principle, in that insufficient security measures had been in place to protect the personal data of some care home residents and online Electoral Roll registrants.

The Commissioner concluded that, whilst technical responsibility for the breach lay with the Treasury and Resources Department, the Policy Council should share some of the responsibility by having failed to provide effective corporate guidance to departments on the management of confidential and personal information.

As a consequence, both the Council and the Department embarked on programmes to rectify the deficiencies that had been identified and agreed to advise the Commissioner of their progress on a regular basis.

The Treasury and Resources Department appointed an Information Security Officer and its Information Technology Unit embarked on a number of technical projects to improve the security and management of confidential and personal information. Funding restraints meant that some of these projects were not able to commence until 2009.

[1] http://www.gov.gg/ccm/home-department/data-protection/press-release/2008/commissioner-publishes-his-assessment-of-the-breach-of-the-states-website.en

The Policy Council advised the Commissioner that work had started on the development of corporate information management strategies in line with recommendations in the report.

The Commissioner will continue to liaise with the relevant States departments over the implementation of the recommendations arising from his report.

Data Subject Access to Health Records

Representatives of the medical profession contacted the Commissioner to enquire if anything could be done to address the problem of the high cost of responding to requests from patients to access their medical history.

It appeared that the information sought by a "subject access request" was often required in connection with litigation. In such circumstances it was often an individual's entire medical record that was requested.

The Law states quite clearly that an individual is entitled to be given a copy of information relating to him [or her] and regulations provide that a maximum fee of £10 may be charged for the provision of such information.

The level of fee was set at a level that would not deter genuine requests, but, in the case of medical records, quite clearly does not approach the cost of provision of an entire medical record.

In responding to this enquiry, the Commissioner researched the wording of the European Directive 95/46/EC, with which the Law is intended to be compliant. The 41st recital to the Directive states:

"… any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; …"

Article 12 of the Directive provides that subject access: "… *shall be without constraint and at reasonable intervals and without excessive delay or expense".*

The Commissioner concluded that the principal purposes of the subject information provisions in the Law were to enable the applicant to check the accuracy of their personal data and that the processing was compliant with the Law.

In the Commissioner's opinion, the exploitation of the subject information provisions of the Law in connection with litigation is contrary to the primary purpose for which those provisions of the Law were drafted; hence, applicants for information which is required to support prospective legal action would be better advised to use document

discovery and to pay the actual costs incurred in the provision of the information.

Section 7(9) of the Law provides that it is ultimately for a court to order compliance where it is found that a data controller has failed to comply with a subject access request.

Accordingly, whilst he would always aim to act in support of genuine requests by individuals for information, he would be unlikely to use his enforcement powers in support of a subject access request, where the motivation of the request appeared to be concerned with fuelling separate legal action.

A guidance note on this topic was been prepared and discussed with the medical profession with a view to publication on the Commissioner's web site in 2009.

Surveillance by public bodies

Surveillance is now an inescapable fact of life. Each time we walk down the street, make a telephone call or surf the Internet, we are liable to be monitored, even if our actions are entirely lawful.

Governments around the world have gradually constructed elaborate surveillance régimes that would have been the envy of the former communist bloc countries of Eastern Europe. These actions, justified as necessary in the fight against terror, risk eroding those basic rights and freedoms that they are intended to protect.

Continued vigilance is needed to ensure that surveillance and monitoring is proportionate and necessary and that the data collected by these methods are not used for other unrelated purposes by government agencies.

A prime example is the use of CCTV for crime prevention purposes. Whilst it is true that many people feel safer if they know that the streets are protected by CCTV surveillance, others feel that their privacy is threatened. It is essential that the use of CCTV images is strictly controlled to ensure that it is limited to cases where the gathering of evidence in relation to criminal acts is required.

This topic remains under active consideration by data protection and privacy commissioners worldwide and in January 2009 the House of Lords Select Committee on the Constitution published a report entitled: "Surveillance: Citizens and the State"[2] , which detailed its concerns over the increasing use of surveillance by public bodies.

[2] Volume 1 : Report http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/18.pdf and

Privacy Protection in Social networking

The popularity of social networking has continued to grow. Many people find that it offers a convenient way of keeping in touch with friends and publishing interesting family news amongst a closed networking community.

However, not everyone understands the privacy risks that are inherent in this use of this technology. Unless great care is taken to limit the scope of the sharing of information, personal and private facts, which were meant to be of limited circulation, could be published far and wide; once published, it can be virtually impossible to withdraw such information from the public domain.

In October, the Commissioner published guidance for individuals on how to protect their privacy on social networking sites such as Facebook.

The International Working Group on Data Protection in Telecommunications adopted a report on Social networking at its 43rd meeting in Rome on 3-4 March 2008, ("the Rome Memorandum")[3].

This report was adopted, in an amended form by the 30th International Conference of Data Protection and Privacy Commissioners at its meeting in Strasbourg in October.

More recently, it has come to light that social networking sites are facing the kinds of security attacks previously associated with email accounts. Accordingly, the adoption of precautions is becoming even more important.

A summarised version of the guidance published by the International Conference[4] is given below:

Volume 2 : Evidence
http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/18ii.pdf

[3] Report and Guidance on Privacy in Social Network Services – "Rome Memorandum"
http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491

[4] http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_social_networks_en.pdf

Users of Social Network Services

1. Publication of information

Users of social network services should consider carefully which personal data – if any – they publish in a social network profile. They should keep in mind that they may be confronted with any information or pictures at a later stage, e.g. in a job application situation. In particular, minors should avoid revealing their home address or telephone number. Individuals should consider the usefulness of using a pseudonym instead of their real name in a profile. However, they should keep in mind that the use of pseudonyms offers limited protection, as third parties may be able to lift such a pseudonym.

2. Privacy of other individuals

Users should also respect the privacy of others. They should be especially careful with publishing personal information about somebody else (including pictures or even tagged pictures) without that other person's consent.

Providers of Social Network Services

1. Privacy regulations and standards

Providers operating in different countries or even globally should respect the privacy standards of the countries where they operate their services. To that end, providers should consult with data protection authorities as necessary.

2. User information

Providers of social network services should inform their users about the processing of their personal data in a transparent and open manner. Candid and intelligible information should also be given about possible consequences of publishing personal data in a profile and about remaining security risks, as well as about possible legal access by third parties (including e.g. law enforcement). Such information should also comprise guidance on how users should handle personal information about others contained in their profiles.

3. User control

Providers should further improve user control over the use of their profile data by community members. They should allow for restriction of visibility of entire profiles, and of data contained in profiles, and in community search functions.

Providers should also allow for user control over secondary use of profile and traffic data*;* e.g. for targeted marketing purposes. As a minimum, opt-out for general profile data, and opt-in for sensitive profile data (e.g. political opinion, sexual orientation) and traffic data should be offered.

4. Privacy-friendly default settings

Furthermore, providers should offer privacy-friendly default settings for user profile information. Default settings play a key role in protecting user privacy: It is known that only a minority of users signing up to a service will make any changes. Such settings must be specifically restrictive when a social network service is directed at minors.

5. Security

Providers should continue to improve and maintain security of their information systems and protect users against fraudulent access to their profile, using recognised best practices in planning, developing, and running their applications, including independent auditing and certification.

6. Access rights

Providers should grant individuals (regardless of whether they are members of the social network service or not), the right to access and, if necessary, correct all their personal data held by the Provider.

7. Deletion of user profiles

Providers should allow users to easily terminate their membership, delete their profile and any content or information that they have published on the social network.

8. Pseudonymous use of the service

Providers should enable the creation and use of pseudonymous profiles as an option, and encourage the use of that option.

NOTIFICATION

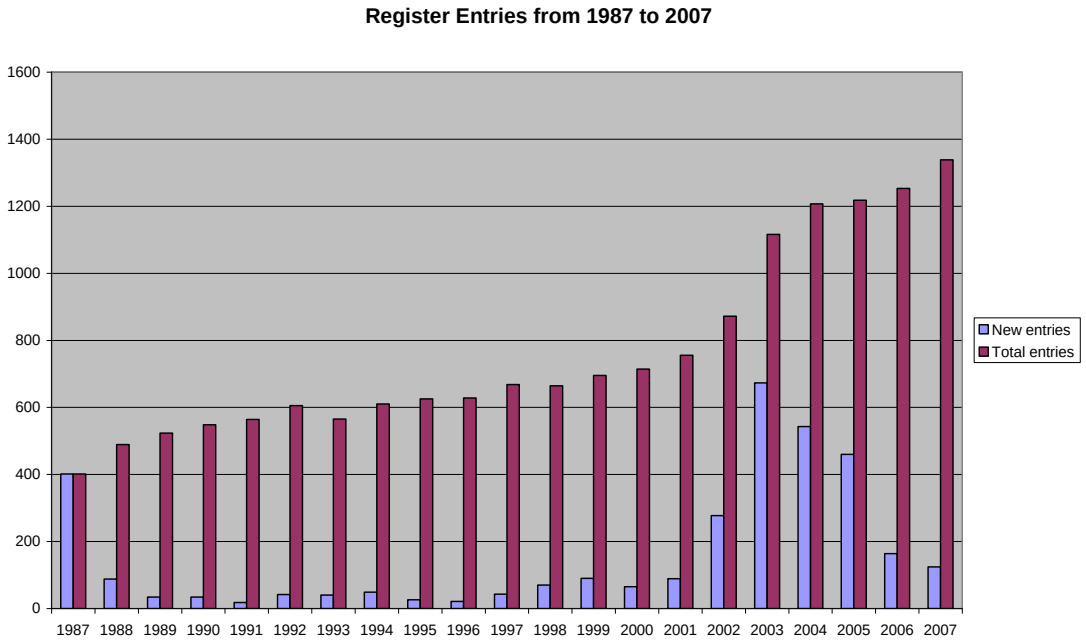
Section 17 of the Law requires Data Controllers to "Notify" the Commissioner of their processing of personal data. This Notification is on an annually renewable basis and covers all processing that is not exempt.

Exemptions from Notification exist for manual data, certain charitable and not-for-profit organisations and for the processing of data associated with the core business purposes of accounts, staff administration and marketing. However, exemption from Notification does not relieve a data controller from the requirement to conform to the data protection principles and the remainder of the Law.

The annual fee for Notification remained at £35 throughout the year, as the legislation increasing the fee to £50 was not enacted during 2008.

Register Entries

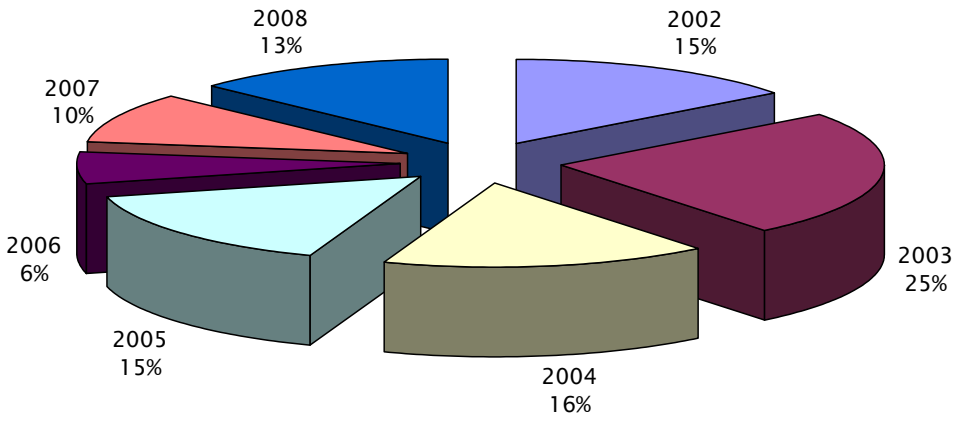
The chart below shows that the number of Register entries has continued to increase slowly.



By the end of December 2008, there were 1479 Notifications on the register, compared with 1356 at the end of 2007.

There were 208 new Notifications and 85 closures during 2008 - a net increase of 123, (compared with 158 new and 55 closures in 2006 - a net increase of 103). This increased number reflects the culmination of the Notification campaign which was begun in 2007.

Age of Current Notifications



It is interesting to note the spread of age of current Notifications over the seven year period since Notification commenced in 2002. An even spread would be represented by about 14.5% for each of the seven years. The spread is indeed fairly even, except for an above average number of Notifications originating in 2003, the first full year of Notification, and somewhat below average numbers originating in 2006 and 2007.

The scanning of the paper records of Notifications continued and by the end of 2008 over half of the current Notifications and associated correspondence had been scanned into the document management system. It has been possible to destroy the paper records of all closed Notifications, as scanned images of all of that data had been captured in the computer system in 2007.

It is planned to complete the electronic storage of historical Notifications during 2009.

Internet Statistics

This Notification site[5] is used both by those wishing to create and maintain their own Notification entries and by the staff of the Data Protection Office for administration.

Continuous statistics have been gathered over the past five years by the hosting service Eduserv; these show that approximately 38% of the Notification site accesses were for downloads of manuals and

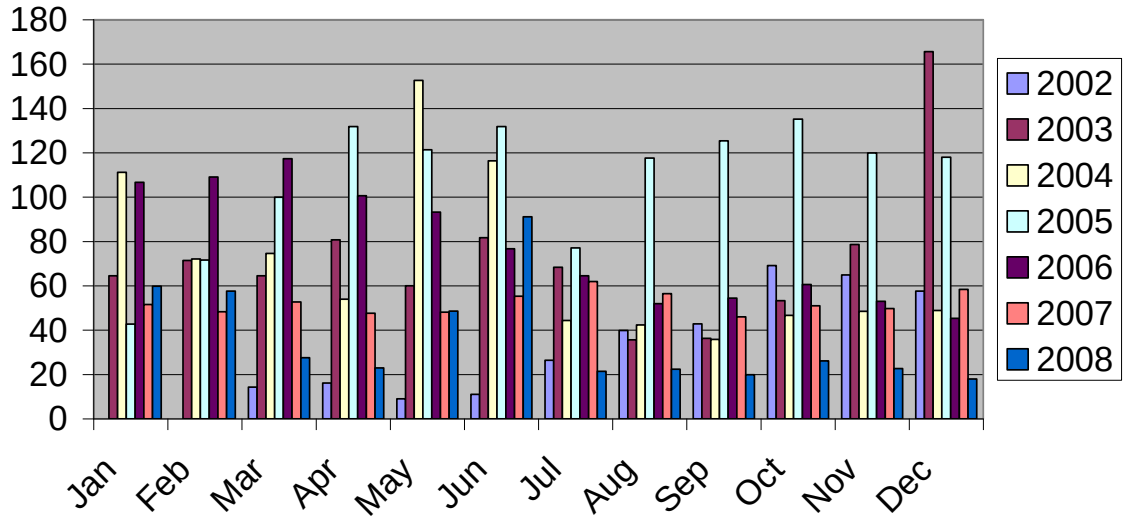
[5] http://www.dpr.gov.gg

information, 20% for administration purposes and the remainder (42%) for online notification activities and enquiries.

The chart below shows the variation in the average daily activity on the Notification site between the commencement of Notification in 2002 and December 2008; the vertical axis represents the average daily rate of successful requests for pages of data from the site each month.

The activity has settled at a lower level for the past two years by comparison with the peak years of 2003-2006, when the 800 historical Registrations under the 1986 Law were replaced by Notifications under the 2001 Law.

Notification Site Activity between 2002 and 2008



There were two significant maintenance incidents in 2008; the first was a fault in the automatic reminders facility and the second slow running due to the implementation of additional security features. Both of these incidents were resolved promptly by Eduserv.

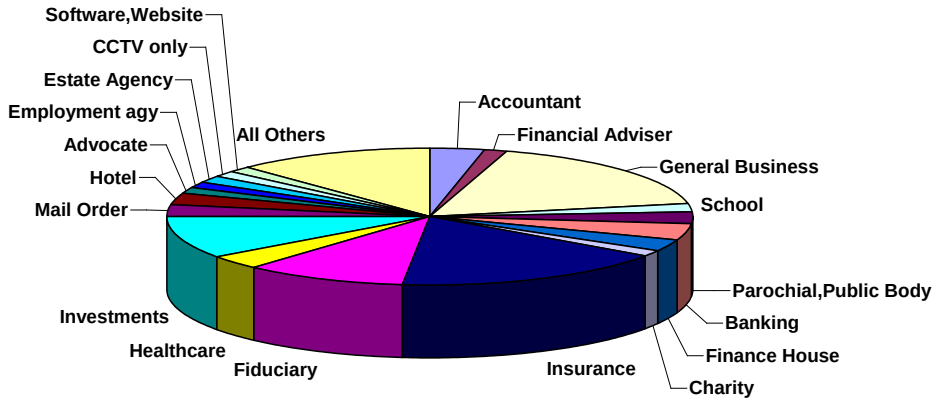
Notifications by Sector

The Notification process requires data controllers to indicate the nature of their business activity. This requirement not only simplifies the process, as it allows for the generation of a standardised draft Notification based on a template, but also enables an indicative record to be maintained of the number of Notifications by industry sector.

The chart represents the breakdown of notification templates for 2008 by industry sector and shows little change from 2007.

There was a small growth in the investments category, reflecting the fact that more organisations have responded to the clarification from the Commissioner that, whilst in certain circumstances a management organisation may notify on behalf of its subsidiaries, each individual entity that is separately licensed by the Financial Services Commission should be separately notified.

Notifications by sector in 2008



Exemptions

Exemptions from the need to Notify may be claimed by those whose processing is limited to the core business purposes of accounts & records, staff administration and a limited amount of marketing to existing clients.

An exemption is also available to most voluntary organisations, charities and to those whose processing is limited to manual data. However, once CCTV is used by an organisation for the prevention and detection of crime, these exemptions from Notification are lost.

Organisations that are exempt may choose to Notify voluntarily, thereby relieving themselves of a responsibility to provide information on request under section 24 of the Law. The number of voluntary Notifications rose to 42 (3% of the total). Under current legislation, those who Notify voluntarily are liable to pay the fee, but this situation would change for Charitable organisations, under the amendments that have been approved by the States but not yet enacted.

In 2003, the Data Protection Office commenced the compilation of a list of those organisations that had informed the Commissioner that they were exempt from Notification and by the end of that year 303 organisations were so listed. The exempt list was primarily designed to assist in monitoring compliance and to avoid pestering those who had previously advised the Office that they were exempt.

During 2004, the exempt total rose to 447; in 2005, it fell to 441, in 2006 it rose to 446 and in 2007 the number fell to 384 representing 22% of the overall total [of 1722 exempt and notified organisations]. In 2008 it stood at 381. The decrease in the number of exempt organisations is due to some previously exempt organisations having subsequently notified and because some others are no longer trading.

The exempt list has not yet been published. It is currently under review by the Assistant Commissioner to eliminate some inaccurate and historical information and should be published on the Commissioner's website during 2009 when that review has been completed.

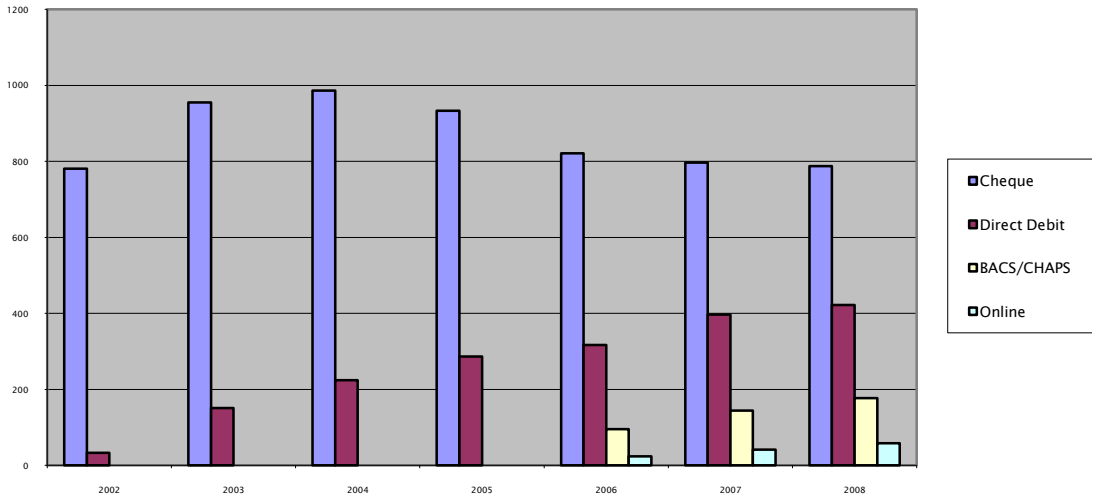
Payment and communications methods

Renewal reminders advised data controllers of the introduction of alternative means for the payment of fees.

The number paying by these various means in 2008 is shown below:

Payment by Direct Debit and BACS continued to show a small increase. Online payment also increased from 3% to 4%, whilst cheque payment continued to decline, but still represented over 50% of the payments received.

Payment methods 2002 to 2008



1256 organisations (85%) provided an email address for communication purposes, compared with 1161 (85%) in 2007; this address was used for the issue of automatic renewal reminders to those who did not renew by Direct Debit; of those, 252 (229 in 2007) required a second reminder to be sent by post. Second reminders were also issued to 29 (16) organisations whose first reminder had been sent by post. It was necessary to resort to final reminders in 39 (34) cases; this resulted in some payments being overdue.

It appears that some data controllers do habitually ignore final reminders resulting in the need for follow-up action. In 2008 there were three referrals to the Law Officers which resulted in two police cautions being issued for late submission of renewal fees. No action was taken in the third case where a data controller was very late in submitting the fee for a new notification.

The most common reason for the issue of second and final reminders was that the data controller's address or the email address of the administrative contact had changed since Notification. It is the responsibility of data controllers to advise the office of any changes to their particulars and in fact an offence for an organisation to fail to keep its registration particulars up to date.

Further administrative savings were made in 2008 by issuing receipts electronically to those who had provided a valid email address.

In addition, some clients with a large number of Notifications have begun to remit consolidated payments, greatly reducing the administrative burden on both sides.

The use of automated email reminders, Direct Debits, consolidated payments and electronic receipts further streamlined the administrative effort involved in the Notification process, freeing up more staff time for education, enforcement and publicity activities.

STAFFING AND STAFF DEVELOPMENT

The Office of the Data Protection Commissioner comprises three people: the Commissioner and Assistant Commissioner, both of whom work full time and the Personal Assistant to the Commissioner, who works part-time.

The Commissioner is a statutory public appointment, but members of his staff are seconded from the Home Department of the Civil Service and are wholly responsible to him.

The Assistant Commissioner devotes the majority of her time to compliance activities, responding to enquiries from individuals and organisations and delivering training to the public and private sectors.

The Personal Assistant undertakes all of the administrative activities for the office including the processing of Notifications, payment of bills and the reconciliation of the accounts.

The Commissioner considers that, whilst his office remains responsible solely for the enforcement of the Data Protection legislation and the associated Privacy Regulations, the current establishment of one full time Assistant and one part time Personal Assistant represents a satisfactory minimum level of staffing resource, which under normal circumstances enables him to discharge his responsibilities adequately under the Law.

The specialist work involved with the assessment of the States Website breach in the early part of the year required additional expert assistance, which was provided under contract by PwC Channel Islands.

The Commissioner is keen to encourage the academic, technical, administrative and professional development of his staff and to that end supports their attendance at training courses, relevant conferences and other forms of personal development.

The Commissioner himself remains a member of the E-commerce and IT Advisory Group of the GTA University Centre and of the Guernsey Digimap Management Board and attends relevant seminars and workshops organised by the GTA University Centre and the Guernsey International Section of the British Computer Society. He has also been invited to become a member of an International Standards Organisation Working Group.

It is pleasing to report that the Assistant Commissioner completed her Open University studies and has been awarded a Bachelor of Laws (Honours) degree, thereby not only advancing her own professional development but also strengthening the legal expertise within the office.

RAISING AWARENESS

There is a continual need to ensure that individuals are made aware of their rights under the Law and organisations that process personal data are made aware of their responsibilities.

The Awareness campaign for 2008 included the following activities:-

- Delivering presentations and training
- Involvement in working groups
- Making use of the media.
- Giving compliance advice
- Developing the Internet web site

Delivering presentations and training

The Commissioner and Assistant Commissioner delivered talks and presentations throughout the year to many professional associations and organisations in the public and private sectors. These included: States departments, nursing homes, finance institutions, retail businesses and voluntary organisations.

The total audience reached in this way was around 380, compared to 579 in 2007. The figures for 2007 had been inflated by the data protection conference that was held in April.

In addition to partaking of formal training, any organisation may obtain a training DVD entitled: "The Lights are On", produced by the UK Information Commissioner.

Copies of this DVD are obtainable free of charge from the Commissioner's Office.

Involvement in Working Groups

The Commissioner and Assistant Commissioner participated in the States Data Guardians Group. The activities of the group have initially been involved with the establishment of data sharing protocols between various departments and sections within the government.

Making use of the media

10 articles or letters relating to Data Protection were published in the local media during 2008, (compared with 25 in 2007), in addition to the extensive coverage of the website data breach. Topics covered included:

- Identity theft;
- Freedom of Information legislation;
- Credit card security;
- Privacy issues with social networking;
- Unsolicited marketing;
- Personal data publicised by HM Greffier;
- European Data Protection Day.

The Commissioner is appreciative of the positive support he receives from all sections of the media to his awareness campaigns.

Guidance Notes

The Commissioner issued two additional Guidance Notes in 2008, one concerned with the disclosure of medical data to the General Medical Council and the other concerning Privacy in Facebook. This brought the number of Guidance Notes published by the Commissioner to 31.

A full list of available publications is given overleaf. These are available as leaflets, in booklet form and are published on the Commissioners website[6].

An estimated 566 hard copies of the literature were distributed to individuals and organisations during 2008, compared with 1096 copies in 2007. The figure for 2007 was inflated due to the number of booklets issued to conference participants.

These figures are in addition to the unknown number of electronic copies of these guidance notes that were viewed or downloaded from the website.

[6] www.gov.gg/dataprotection

Guidance Notes published by the Data Protection Office

Baby Mailing Preference Service: *How to stop the receipt of unwanted mail about baby products*
Be Open…with the way you handle information: *How to obtain information fairly and lawfully*
CCTV Guidance and Checklist *Explains how to comply with the law in relation to the use of CCTV*
Charities / Not-for-Profit Organisations
Data Controllers: *How to comply with the rules of good information handling*
Dealing with Subject Access Requests
Disclosure of medical data to the General Medical Council *and other statutory bodies.*
Disclosures of vehicle keeper details *Explains when vehicle keeper details can be disclosed*
Exporting Personal Data
Financial Institutions
How to Protect your Privacy on Facebook
Mail, telephone, fax and e-mail preference service *How to stop the receipt of unsolicited messages.*
Marketing – A Guidance for Businesses
No Credit: *How to find out what credit references agencies hold about you and how you can correct mistakes*
Notification – *a Simple Guide* *A Full Guide* *Exemptions self assessment*
Personal Data & Filing Systems *(guidance on what makes information "personal" and explains what manual records are covered by the Law)*
Privacy Statements on Websites – a Guidance
Respecting the Privacy of Telephone Subscribers
Rehabilitation of Offenders – *Guidance for applicants – Police Disclosures* *Recommended Disclosure Policy for Guernsey Police* *Code of Practice and Explanatory Guide for Employers*
The Data Protection Law and You: *A Guide for Small Businesses*
Spam – *How to deal with spam*
States Departments – a Guidance
Transparency Policy
Trusts and Wills – a Guidance
Violent warning markers: use in the public sector *How to achieve data protection compliance in setting up and maintaining databases of potentially violent persons*
Work References
Your rights under the Law: *Guidance for Individuals*

Developing the Internet Web Site

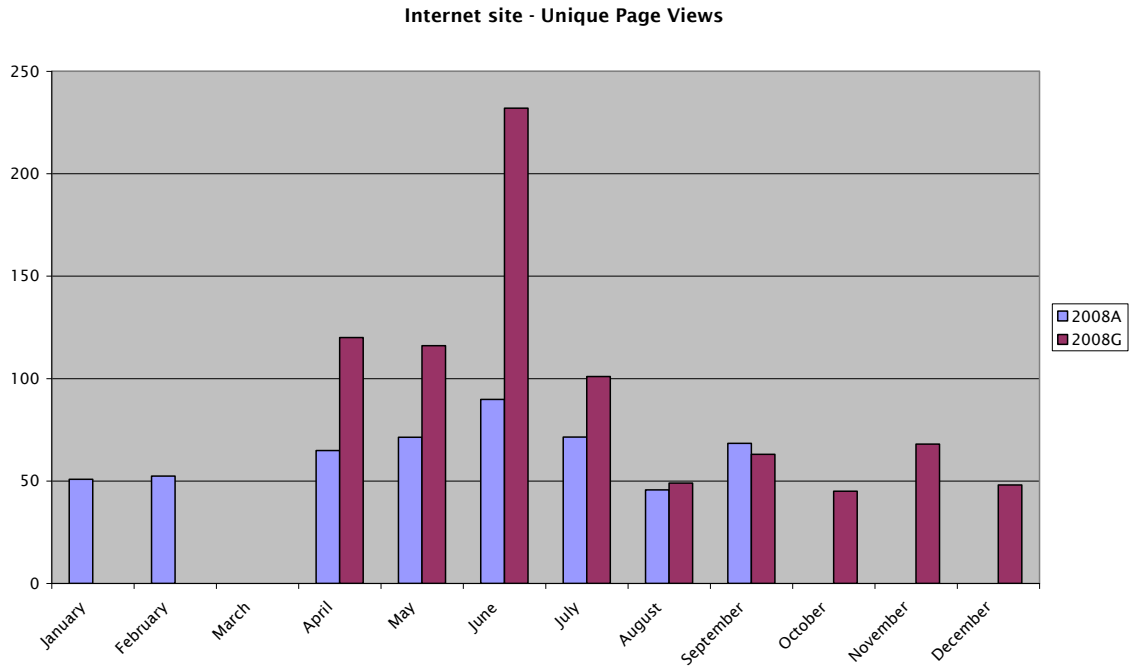
Work continued throughout the year to keep the information on the official website up to date.

Partway through the year, the Information Technology Unit changed the basis of statistics collection from AWS, based on log files (January to September) to Google Analytics, which is based on tagged pages (April to December).

No statistical data were collected for March 2008.

The chart below shows reasonably comparative statistics collected using each of these methods. Future reports will show the data collected using Google Analytics alone.

Currently, it would appear that about 50 unique pages are being accessed each month. The most accessed pages are those relating to the Law and the Guidance Notes.



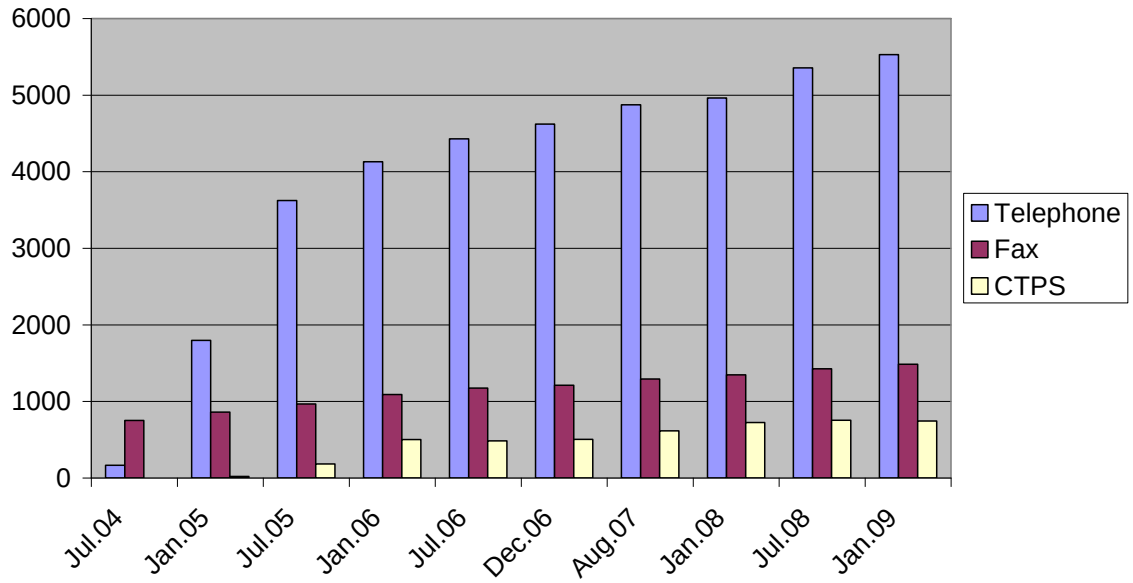
Registrations with the Preference Services

The Telephone Preference Service (TPS)[7] allows individuals to opt-out of the receipt of unsolicited marketing calls. Although the regulations covering the TPS apply only to marketing organisations based in the British Isles, in practice TPS registration appears to reduce, but not eliminate, the receipt of calls originating from overseas, since many reputable overseas telemarketers appear to screen their calls against the TPS database.

The Fax Preference Service (FPS)[8] allows any individual or business with a fax machine to opt out of the receipt of unsolicited marketing faxes whereas the Corporate Telephone Preference Service (CTPS) is for use by organisations wishing to opt out of the receipt of marketing calls.

The chart below, derived from data provided by the Direct Marketing Association, shows that registrations for TPS continue to show a small increase, with 5,527 numbers being registered, compared with 4,961 at the end of 2007 and 4,622 in 2006. Registrations for FPS have increased by 144 to 1,484 and those for CTPS have risen by 19 to 743.

Registrations for Preference Services



[7] www.tpsonline.org.uk
[8] www.fpsonline.org.uk

ENFORCEMENT

The Law provides for a number of offences:-

a) Failure to notify or to notify changes to an entry;

b) Unauthorised disclosure of data, selling of data or obtaining of data;

c) Failure to comply with a Notice issued by the Commissioner.

The Commissioner may serve an Enforcement Notice where he has assessed that a controller is not complying with the principles or an Information Notice where he needs more information in order to complete an assessment. With the advent of the Privacy in Electronic Communications Regulations, the Commissioner's power to issue Notices has been expanded to cover non-compliance with those Regulations.

Notices

No Information or Enforcement Notices were served during 2008. One data controller was served with a Preliminary Enforcement Notice in 2007, and no Notices had been served in 2006.

Police Cautions

Some data controllers do habitually ignore final reminders to renew their Notifications, resulting in the need for follow-up action.

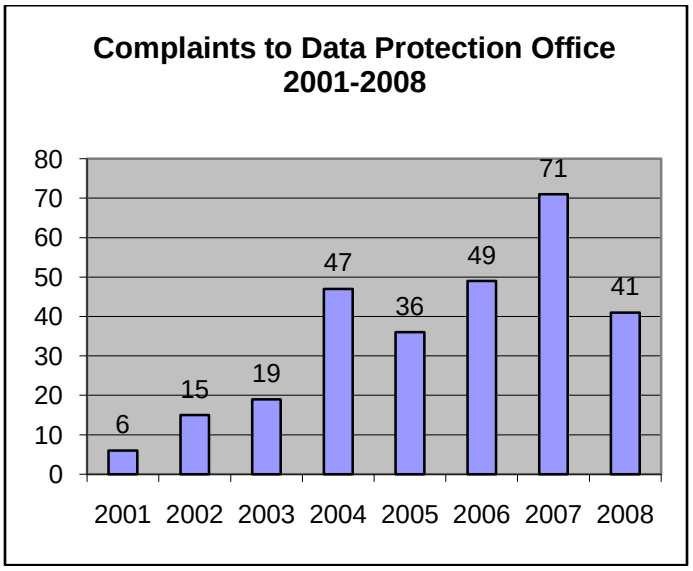
In 2008 two Police Cautions were administered for this reason, the same number as in 2007

A significant amount of administrative time is spent on pursuing late payers and it is recommended that a financial penalty should be imposed in the case of those who are late in renewing their notifications.

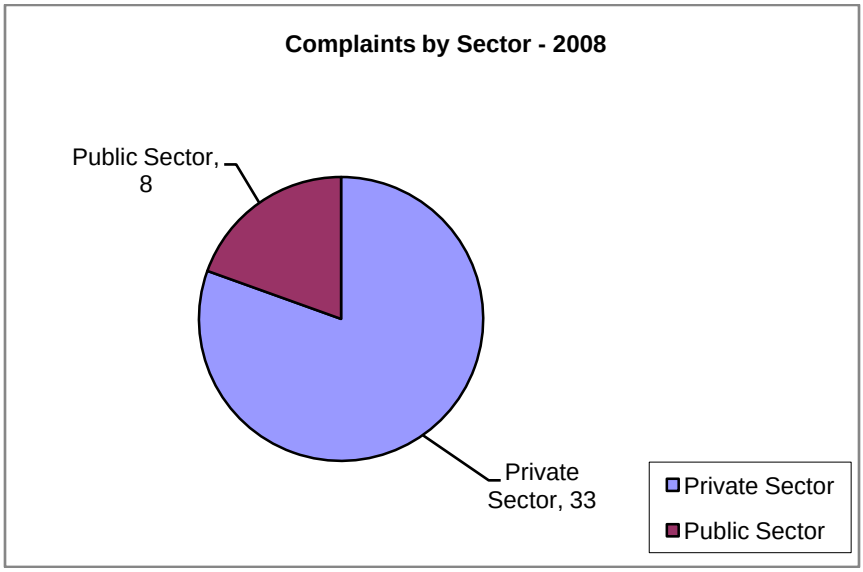
This action would be likely to prevent the need to refer such matters to the Law Officers, thus saving their time as well as the time of the Police.

Complaints

There were a total of 41 complaints received by the Commissioner during 2008, compared with 71 in 2007, 49 in 2006 and 36 in 2005.
The significant increase in 2007 was due to the disclosure of Guernsey residents' personal details by UK banks to the HMRC; these complaints were referred to the UK Commissioner.



The chart depicted below shows that 33 complaints related to the private sector and 8 to the public sector



Of those 33 private sector complaints, 4 were referred to the UK, I to Jersey and 1 to Spain.

19 complaints were upheld, 18 were not upheld, 1 was partially upheld and 2 are ongoing. One complaint was sent to the Jersey Commissioner and at the time of writing it is not known whether or not that particular complaint was upheld.

Case Studies

Case Study 1 –

An individual complained that he had received an inaccurate notice for non-payment of a debt. He claimed that this notice was received despite the account already having been settled. His claim was primarily against the creditor who had instructed a credit reference agency to collect the debt.

If this complaint had substance a breach of the fourth principle would have occurred. The fourth principle states that personal data must be processed accurately and kept up to date if necessary. In addition the sixth data protection principle states that personal data must not be processed in a manner which is likely to cause damage or distress. The complainant was elderly and was very concerned that his name was "blackened" as the notice had stated that the account details had been passed to all major credit reference agencies and that his ability to obtain credit in the future could be affected.

The creditor was contacted and requested to give his side of the story. The facts were: the complainant had purchased goods and paid by credit card but the payment was reclaimed by the bank. The complainant did not respond to the creditor's letters so the matter was referred to a credit reference agency. The day after the referral was made the complainant contacted the creditor but did not settle the account. However the creditor emailed the credit reference agency and instructed that the complainant should not be contacted until further notice.

However a notice was served on the complainant. Further investigation revealed that the complainant paid the outstanding account four days after receiving the notice.

The complaint against the creditor was not upheld. There was no inaccurate processing of personal data and the credit reference agency had been informed to hold off serving any notice.

Attention then turned to the credit reference agency to establish why it had served a notice when instructed not to.

The agency responded that it had moved to new offices, there were not enough telephone lines, an employee had left some days before and there was no-one to use his computer and there was nowhere to plug this computer into. The email from the creditor instructing the agency to defer the serving of the notice was not read as it was addressed to the employee who had left and no other member of staff had been tasked with reading his emails.

The seventh data protection principle states that there must be appropriate organisational and technical measures in place to prevent any unauthorised disclosure of personal information and to prevent against any accidental loss or damage.

The agency clearly breached this principle as there were no measures in place to ensure that staff could access work related messages of an absent colleague. These measures are especially important in a credit reference environment where it is essential that all information is processed accurately.

The agency has now formulated appropriate procedures to ensure that all communications are received and acted upon in a timely manner.

Case Study 2 –

A gentleman and his partner moved into a new house and took over the phone number of the previous occupier and went ex-directory with it. The partner received a call from a local company which was conducting a sales campaign and the caller knew the partner's name. The couple spoke to the manager of this company and learned that the partner's name had been obtained from the Greffe. It had been just a matter of ringing the Greffe and requesting the name of the owner of the house.

What had happened was that a full list of all property transactions is published on a monthly basis and all the company had to do was to match up the property with its old phone list and then telephone the Greffe to get the name of the owner of the property.

This was upsetting for the couple and especially frightening for the partner who had experienced problems which required police intervention and the serving of an injunction. Within a few hours of learning that her name, address and telephone number were in the public domain the house was fitted with an alarm and the phone company changed the telephone number.

The Greffier was contacted and he responded stating that ownership of real property is a matter of public record in Guernsey and the Greffe has a responsibility for maintaining records of all land transactions (the Registry of Deeds) and for making that information available to the public. The Greffier has no power to restrict access to this Registry and he cannot require any searcher to give a reason for their search.

The Cadastre Digimap Search system covers all properties and their ownership in one index and the public was able to access this system via the public terminals in the Greffe Strong-room.

After consultation with the Chief Cadastre Assessor the Cadastre search terminals in the Strong-room became password controlled requiring searchers to log-on and pay a fee.

Staff at the Greffe may no longer provide members of the public with details of property ownership either in writing or over the phone. Anyone seeking such information must search at the Greffe or through an agent.

The outcome of this case was that the public still maintained the right to access public information but in imposing certain restrictions on the methods of access individuals have an improved degree of privacy and protection in their homes.

International Conference of Data Protection Authorities

The Commissioner and Assistant Commissioner joined over 650 delegates who attended the 30th International Conference of Data Protection and Privacy Commissioners, which was held in Strasbourg from 15th – 17th October 2008. The conference was hosted jointly by the German and French authorities, both of whom were celebrating their 30th anniversaries.

The conference departed from established practice in being held entirely in plenary sessions, all of which took place in the hemisphere of the Council of Europe. Whilst this location provided an excellent debating chamber with microphones at all seats, the size of the audience limited the scope for debate and there was less of an opportunity to go into subjects to the depth that we had become accustomed to in previous conferences which had featured workshops.

Full details of the conference (including video recordings of the presentations) are available on its website[9]:

The 31st International Conference will be held in Madrid, probably from 11th – 13th November, 2009 but this date is subject to change.

European Spring Conference

The Assistant Commissioner attended the European Spring conference, which was held in Rome from 17th – 18th April 2008. Over 100 representatives from data protection authorities and institutions throughout Europe attended.

The theme of the conference was "What Outlook for Privacy in Europe and Beyond". The three main sessions discussed the balances which must be achieved between -

- Privacy and Security: law enforcement initiatives and surveillance activities impact on individuals' fundamental rights,
- Privacy and Business –globalisation of markets impact on flows of personal information,
- Privacy and New Technologies – are present data protection principles workable and effective in view of new technological developments.

The next European conference will be held in Edinburgh in April, 2009.

[9] http://www.privacyconference2008.org

International Working Group on Data Protection in Telecommunications (IWGDPT)

The Commissioner attended the two meetings of the International Working Group that were held in 2008.

The 43rd meeting was held in Rome on 3rd and 4th March.

The 44th meeting was held in Strasbourg immediately preceding the international conference on 14th October and was itself preceded by a Symposium on 13th October entitled: "Privacy in the Age of Social Network Services".

Both Working Group meetings covered similar topics, mainly concerned with the production of papers addressing the following issues:

- IP Telephony (Voice over IP)
- Voice Analysis Technology
- Privacy and Search Engines
- Trusted Computing and Digital Rights Management
- Privacy and Cross-Border Marketing
- Online Availability of Electronic Health Records
- Spam
- E-Government
- RFID
- Vehicle Event Recorders
- Personal data within WHOIS databases
- Privacy aspects of the World Summit on the Information Society

The 45th meeting of the Working Group will be held in Sofia, Bulgaria in the spring and the 46th meeting will be held in Berlin at the autumn.

British, Irish and Islands' Data Protection Authorities

The Commissioner and Assistant Commissioner joined representatives of the authorities from the UK, Ireland, Cyprus, Jersey, Isle of Man and Bermuda at the "BIIDPA" meeting held on 27th June 2008 in Gibraltar.

These meetings are of particular value to the smaller Island Authorities, which are able to draw on the broader experience of the larger mainland Authorities in dealing with common issues.

The 2009 BIIDPA meeting is expected to be held in July in Ireland.

Meeting with the President of Ireland

In January the Assistant Commissioner along with colleagues from the Irish and UK data protection authorities (which included Belfast, Scotland and Wales) attended a reception hosted by Mary McAleese, the President of Ireland at the Presidential residence in Phoenix Park, Dublin.

The objective of this reception was to recognise the work of the data protection authorities throughout the British Isles and the president thanked them for their work and excellent co-operation with each other.

The President spoke at length with the Assistant Commissioner and referred to the visit which she had recently made to Guernsey.

Following the reception a meeting was held at Farmleigh where the following topics were discussed:

- Audits by data protection authorities;
- Powers of entry and inspection (the Irish authority gave an interesting account of their expertise in this field);
- Security breaches in the UK;
- Greater scrutiny of organisations;
- Civil penalties as opposed to criminalisation;
- Notification fees.

Liaison with the UK Government

Guernsey hosted a meeting between the Crown Dependencies and Ministry of Justice officials, which was held on 9 July.

Prior to the data protection meeting, the Chief Executive and other Policy Council staff met the Ministry of Justice official to discuss information management policies relating to data sharing and freedom of information.

In the afternoon, the liaison meeting with the other Crown Dependencies concentrated on the benefits of facilitating access to Police systems from the islands and on policy developments in the UK and Europe.

The next liaison meeting took place in London in January 2009 and will be covered in the annual report for 2009.

Data Protection Forum

The Assistant Commissioner attended three meetings of the Data Protection Forum that were held in London during 2008; the topics covered in the meetings were:

- *Data Security in Financial Services*
- *The benefits of Privacy Impact Assessments*
- *Interception and its relationship with data protection*
- *Should data breach notifications be compulsory?*
- *How case law has evolved the definition of personal data*
- *How the Freedom of Information Act has impacted on the public sector*
- *Employers and their use of Facebook*
- *The privacy implications of outsourcing personal data*
- *Developments in European data protection*
- *Review of data protection issues during 2008*

The Commissioner was invited to join a panel at a "Commissioners' Question Time" that was held on 4th September, 2008. Other members of the panel were the Irish Data Protection Commissioner and the Deputy Commissioner from Jersey.

The Commissioner presented a paper entitled: "Dealing with Data Breaches in Guernsey". The Irish Commissioner presented a paper on Audit and Enforcement and also read a paper from the UK Commissioner, who unfortunately had to withdraw at the last minute.

Attendance at these meetings provides benefits which include:

- networking with key people involved in data protection, in many cases from parent companies with offices in Guernsey ;
- the opportunity to influence data protection policy-making;
- raising the awareness of pertinent issues and future trends that may affect both the public and private sectors.

Information Privacy Expert Panel

The Commissioner attended the three meetings of the British Computer Society [BCS] Information Privacy Expert Panel [IPEP], which were held in London during the year.

One of the functions of IPEP is to provide expert input to inform official responses by the BCS to UK Government consultations on matters relating to privacy and data protection policy.

The IPEP includes members from academia, the public and private sectors and has considered various topics, including the proposals for increased enforcement powers for the UK Information Commissioner.

The cost of attendance at these meetings of the IPEP and at any related meetings is borne by the BCS.

International Standards Organisation

The Commissioner was invited to join Panel 5 of the SC27 Working Group of the International Standards Organisation, which is developing an international standard on data protection – ISO/IEC 29100, entitled: "Information Technology – Security techniques – privacy framework". This standard, as the name suggests, specifies a privacy framework focusing on specific information and communication technology system-issues from a high-level perspective. It is currently in Committee Draft stage, so has not yet been published.

The majority of the work of the panel is conducted via email and the Commissioner did not attend any meetings in 2008; he is likely to attend two or three meetings in 2009 which will be held under the auspices of the British Standards Institute (BSI) in London.

The BSI is also developing a standard BS10012:2009 entitled: "Specification for the management of personal information in compliance with the Data Protection Act 1998". This standard has been issued in draft form for public comment.[10]

Although directed at compliance with the UK Act, it will of course be of relevance to data controllers established in the Bailiwick, due to the similarity of local legislation with that in the UK.

[10] http://drafts.bsigroup.com/?d=264

OBJECTIVES FOR 2009

The primary objectives for 2009 remain unchanged, encompassing the following areas:-

- ***Legislation***

  Detailed work on the proposed amendments to the Data Protection legislation will continue as and when appropriate.

- ***Adequacy and International Transfers***

  Work will continue to ensure that the European Commission's adequacy finding for the Data Protection régime in the Bailiwick is respected and that international data transfers comply with the eighth Data Protection principle.

- ***British Isles and International Liaison***

  Participation in relevant UK, European and international conferences will continue as a means of enhancing the international recognition of the independent status and regulatory prowess of the Bailiwick and ensuring that local knowledge of international developments remains up to date.

- ***Raising Awareness***

  The media will be used to continue the awareness campaign and a further series of seminars and talks for the public and private sectors will be mounted.

  Collaboration with the Training Agency will continue over the organisation of courses leading to formal qualifications in data protection, such as the ISEB Certificate.

  Promotion of relevant training using UK specialists will be done, with training being targeted separately to financial sector organisations, other private sector organisations and the public sector.

  The publication of new literature and the review and revision of existing literature will be undertaken as the need arises.

- ***Compliance***

  Targeted compliance activities will be organised to increase the notification level of local organisations. Rigorous enforcement will continue, including consideration of prosecution of non-compliant organisations.

  The monitoring of websites and periodic surveys to assess compliance with data protection legislation and the privacy regulations will continue.

- ***Government***

  Close liaison with the States of Guernsey Government departments will continue with the aim of promoting data sharing protocols and the further development of subject access procedures.

  Follow up activities related to the implementation of recommendations arising from the website breach report will continue. Opportunities will be taken to promote the use of Privacy Impact Assessments where appropriate.

- ***Administration***

  The process of moving all Notification data onto electronic filing systems will continue, with the aim of dispensing with all manual records of Notifications by the end of 2009.

FINANCIAL REPORT

The Data Protection Office is funded by a grant from the States of Guernsey administered by the Home Department and based on an annual estimate of expenditure prepared by the Commissioner.

In accordance with Section 3 of Schedule 5 of the Law, all fees received are repaid into the General Revenue Account.

The Income and Expenditure, which are included within the published accounts for the Home Department, have been as follows:

INCOME	2008 £	2007 £	2006 £
Data Protection Fees [1]	49,125	46,010	43,382
EXPENDITURE			
Rent	15,526	15,526	15,526
Salaries and Allowances[2]	176,345	147,971	138,328
Travel and Subsistence	10,294	8,926	10,588
Furniture and Equipment[3]	12,761	11,790	13,806
Publications	3,075	2,910	2,886
Post, Stationery, Telephone	4,332	3,977	3,542
Heat Light, Cleaning	6,247	4,681	4,743
TOTAL EXPENDITURE	**£228,580**	**£195,782**	**£189,419**
EXCESS OF EXPENDITURE OVER INCOME	**£179,455**	**£149,771**	**£146,037**

NOTES

[1] Fees remained at £35 per notification or renewal of a notification.

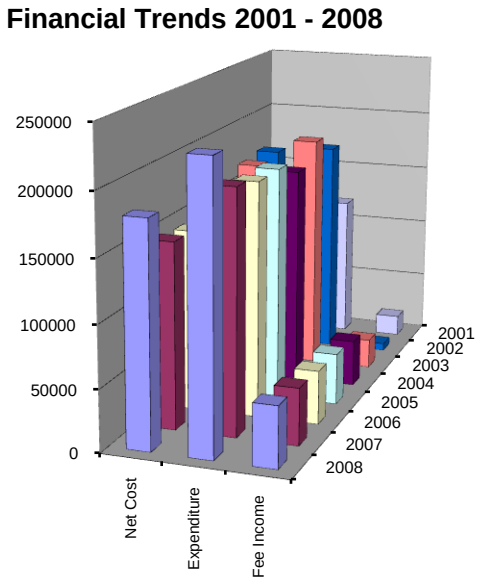
Income from fees is accrued on a monthly basis.

The cash received for notifications in 2008 was £50,750 (£47,810 in 2007 and £43,505 in 2006) representing the 1,450 annual notifications and renewals that were processed during the year.

[2] This includes an amount of £25,520 (£5,510 in 2007 and £1,662 in 2006) for consultancy fees.

[3] This includes the annual fee of £11,000 payable to Eduserv for maintenance and hosting of the Notification website.

The financial trends in income and expenditure since 2001 are shown graphically below.



Expenditure for 2008 rose by £32,798 (16.7%); of that sum £25,000 was due to consultancy fees associated with the investigation of the security breach of the States website.

The cost of an investigation such as this would normally be paid by the data controller, but since the controller in this case was a States Department, the investigation was funded by a supplementary grant of £20,000 from the Treasury.

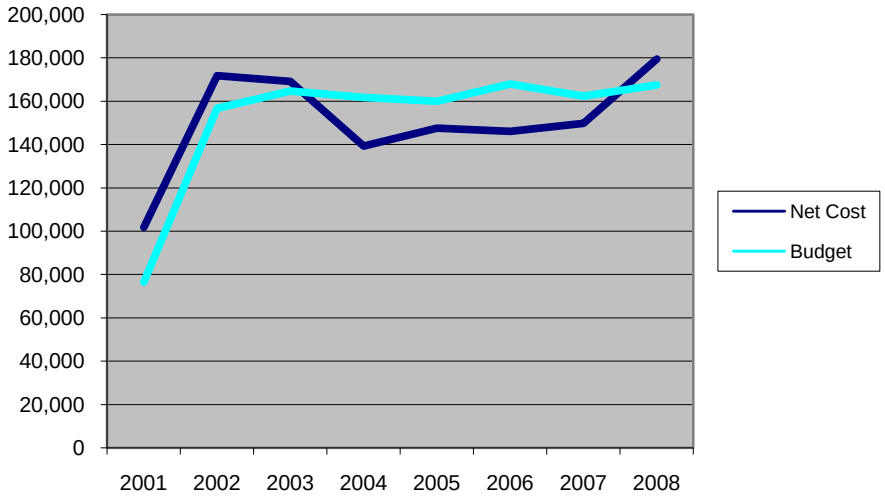
Income from fees rose by £2,628 (6.8%) based on an unchanged notification fee of £35.

Hence, the net cost of the Office to the taxpayer increased by £29,684 (19.8%). In the absence of the exceptional item, the cost would have increased by a more modest £4,684 (3.1%). Another major contribution to this increase was an unexpected 60% increase in heat, light and service charges levied by the landlord, up from £2,672 in 2007 to £4,297 in 2008.

Detailed accounts were submitted to the Home Department in accordance with established practice and as required by paragraph 3 of Schedule 5 to the Law.

The chart below depicts the net cost against budget for the years from 2001 to 2008. It can be seen that the cost exceeded budget in 2008, primarily on account of the costs of the investigation of the website breach.

Net cost vs budget 2001 - 2008



It is anticipated that the costs for 2009 will once more be contained within budget on the assumption that there are no exceptional events such as occurred in 2008.

The Commissioner appreciates the continued administrative support that has been forthcoming from the Home Department and is grateful for the continued technical support provided by the ITU.

In accordance with the standards contained within the Internal Audit report, the Commissioner hereby confirms that no gifts or hospitality were received by him or his staff during 2008.

APPENDIX

THE DATA PROTECTION PRINCIPLES

1. Personal data shall be processed fairly and lawfully and special conditions apply to the processing of sensitive personal data.

2. Personal data shall be obtained for one or more specified and lawful purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed.

4. Personal data shall be accurate and kept up to date.

5. Personal data shall not be kept for longer than necessary.

6. Personal data shall be processed in accordance with the rights of data subjects.

7. Technical and organisational measures shall be taken against unauthorised or unlawful processing and against accidental loss or damage to personal data.

8. Personal data shall not be transferred to a country or territory outside the Bailiwick unless the destination ensures an adequate level of protection for the data.

THE PRIVACY AND ELECTRONIC COMMUNICATIONS REGULATIONS

1. Telecommunications services must be secure and information processed within such services must be kept confidential.

2. Traffic data should not be retained for longer than necessary and the detail of itemised billing should be under subscriber control.

3. Facilities should be provided for the suppression of calling line and connected line information.

4. Information on the subscriber's location should not generally be processed without consent.

5. Subscribers may choose not to appear in directories.

6. Automated calling systems may not be used for direct marketing to subscribers who have opted out.

7. Unsolicited faxes may not be sent to private subscribers unless they have opted in or to business subscribers who have opted out.

8. Unsolicited marketing calls may not be made to subscribers who have opted out.

9. Unsolicited email marketing may not be sent to private subscribers and must never be sent where the identity of the sender has been disguised or concealed.

10. The Data Protection Commissioner may use enforcement powers to deal with any alleged contraventions of the Regulations.

Further information about compliance with the Data Protection (Bailiwick of Guernsey) Law 2001 can be obtained from:

Data Protection Commissioner's Office
P.O. Box 642
Frances House
Sir William Place
St. Peter Port
Guernsey
GY1 3JE

E-mail address: dataprotection@gov.gg
Internet: www.gov.gg/dataprotection
Telephone: +44 (0) 1481 742074
Fax: +44 (0) 1481 742077