BAILIWICK OF GUERNSEY

DATA PROTECTION COMMISSIONER
REPORT FOR 2010

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: The Israel Museum, home of the dead sea scrolls, in Jerusalem, which hosted the 32nd International Conference of Data Protection and Privacy Commissioners in October, 2010.

CONTENTS

FOREWORD

I am pleased to present my tenth and final report to the States of Guernsey, covering the calendar year 2010. I should like to preface my remarks by recalling some significant events of the past 10 years.

The Data Protection (Bailiwick of Guernsey) Law, 2001 was commenced in August 2002, following which the European Commission published a declaration of the adequacy of the data protection régime within the Bailiwick in 2003. By facilitating the transfer of personal data from within the European Union to the Bailiwick, this provided a competitive trading opportunity over other similar territories.

The Privacy and Electronic Communications Regulations came into force in Guernsey in 2004 (somewhat later in Sark and Alderney) and inter alia ensured that the Bailiwick could not be used as a source of spam email or nuisance phone calls.

In 2006, the States approved a number of amendments to the 2001 Law, which, together with other changes approved in 2009, were implemented by an amending Ordinance, Statutory Instruments and Orders in 2010.

The scope of the work of this office has changed dramatically over the years. Initially, regulatory activities were primarily concerned with the compliance of relatively large organisations (including government departments), where personal data was processed in monolithic databases for discrete and identifiable purposes. The emphasis was on lawfulness of processing and the rights of individuals to be informed about, and if necessary complain about, the processing of their data.

Whilst ensuring the compliance of large organisations remains a priority, technology has advanced to the point where large and small organisations employ information and communications technology on a routine basis for a much broader range of applications, raising the possibility that personal information might be widely disclosed and used for a multitude of purposes.

The advent of sophisticated search engines revolutionised the usefulness of the Internet, but the downside of using freely available search engines can be the resulting proliferation of behavioural advertising targeted at individual users.

Technology has become commonplace not just in the workplace but also in the home and the use of email has given way to social networking as a prime means of communication; however, the users of social networks, especially younger people, may not be aware of the need to adjust their privacy settings to minimise the potentially invasive processing of personal information that they intend to share only with close friends.

The more recent development of "smart phones" and other mobile devices with location intelligence pose further problems as the wide availability of free "apps" can mean that individuals run the risk of being tracked and divulging their location without even realising it.

Technological developments have dominated much of the debate and discussion at data protection conferences in recent years; I have been honoured to have been invited to present papers and chair sessions at many of these international conferences.

In 2010 I was invited to participate in the inaugural meetings of the Global Privacy Enforcement Network (GPEN), which has been formed on the initiative of the US Federal Trade Commission to improve communication and cooperation between privacy and data protection authorities worldwide. This liaison is vitally important because of the growing trend of globalisation and the difficulty of identifying the location where unlawful processing may be occurring.

It is clear that the challenges for data protection regulators will continue to increase as technology becomes more sophisticated and ubiquitous. Close co-operation will become essential in order to meet the threats posed by unlawful processing on a global scale. Harmonisation of legislation and the development of international standards are important steps towards countering such threats.

The States have shown in the past an appreciation of the need for effective legislation in this arena. Inevitably there will be a need to keep the legislation in step with international standards of regulation and the support of the States in giving this legislation due priority in future will be most beneficial.

I have been extremely fortunate to have had the support of my two colleagues who have ensured the smooth running of the Data Protection Office throughout my two five-year terms of office and I have enjoyed an excellent working relationship with the Law Officers, in respect of legal advice, legislative drafting and dealing with offenders. Administrative assistance has always been promptly forthcoming from the staff of the Home Department and technical assistance from the Information Technology Unit.

My second five-year term of office terminates in September, 2011 and I am confident that my successor will benefit from this high level of support and assistance.

I wish my successor and colleagues bonne chance!

Data Protection Commissioner, April 2011.

DATA PROTECTION ISSUES

Amendments to the Law

The Data Protection (Bailiwick of Guernsey) (Amendment) Ordinance, 2010[1], together with associated Statutory Instruments[2] and Orders, commenced on March 1st, 2010.

Amongst its provisions, this Ordinance increased the penalties for unlawful disclosure of personal data to provide for custodial sentences of up to 2 years in the most serious cases and gave the Commissioner statutory power to obtain information from any person in relation to alleged breaches of the Privacy and Electronic Communications Regulations (previously it had only been possible to obtain information from an offending controller).

This power should be of particular value during the investigation of alleged email breaches, such as spam, phishing, etc., where it should now be possible to obtain details of the alleged offender from the Internet Service Provider and should provide the means of obtaining relevant information without the need to resort to a warrant.

In addition, Notification fees were increased to £50, except for bona fide registered charities, who are now able to notify free of charge.

In May, the Home Department made an Order under Schedule 2 to the Law[3] legitimising the disclosure by the Environment Department of the name and address of the registered keeper of an apparently abandoned vehicle on private land. This Order was designed to facilitate the provision of personal information to expedite the disposal of the vehicle.

In June, an Order was made by the Home Department[4] increasing the maximum fee which may be levied for subject access to medical information. This Order was designed to maintain the ability of an individual to have access to their own limited medical information for a nominal fee of £10, whilst permitting a higher fee to be charged for access to the more extensive medical records that are often requested for the purpose of litigation.

---

[1] http://www.guernseylegalresources.gg/ccm/legal-resources/ordinances/data-protection/data-protection-bailiwick-of-guernsey-amendment-ordinance-2010.en

[2] See the Annual Report for 2009 for full details of these amendments to the Law, which are also available as SI's 7,8,9 & 10 of 2010 from the Guernsey legal resources website at: http://www.guernseylegalresources.gg/ccm/navigation/statutory-instruments/guernsey---bailiwick/2010/1---50/ .

[3] SI 51 of 2010 ; available from the Guernsey legal resources website as above: …/51-100/

[4] SI 59 of 2010 ; available from the Guernsey legal resources website as above : …/51-100/

European Union Developments

In January 2010, the European Commission published preliminary proposals for a future EU-US international agreement on personal data protection and information sharing for law enforcement purposes.[5]

These proposals were the subject of much discussion and comment, but on 9 December, European Union and United States officials were able to commence detailed talks in Washington on a personal data protection agreement when cooperating to fight terrorism or crime.[6]

"The aim was to ensure a high level of protection of personal data such as passenger data or financial information that is transferred as part of transatlantic cooperation in criminal matters. Once in place, the agreement would enhance EU and US citizens' right to access, rectify or delete data when it is processed with the aim to prevent, investigate, detect or prosecute criminal offences, including terrorism. For the EU, effective judicial review and a more proportionate use of data by public authorities are key objectives of the agreement."

In June, the European Commission formally requested to the UK to strengthen the powers of its data protection authority to ensure better compliance with the EU Data Protection Directive (95/46/EC).

Some of these criticisms had already been addressed following the commencement an amendment to the UK legislation in April which gave the Information Commissioner power to conduct audits of data controllers and issue monetary penalties of up to £500,000 for serious breaches of the data protection principles. Other criticisms, if accepted by the UK, might result in the need for amendments to legislation.

Imposition of the first monetary penalties (of £100,000 and £60,000) on a private company and a county council respectively, for serious security breaches was announced by the ICO in November.[7]

In July 2010, as a follow up to the public consultation launched in 2009 on the review of the data protection regulatory framework, the European Commission organized a consultation meeting with key stakeholders. The purpose of this meeting was to consult non-public sector stakeholders on a range of issues pertaining to existing data protection rules, identify problems and discuss possible solutions.

---

[5] http://ec.europa.eu/justice/news/consulting_public/news_consulting_0005_en.htm

[6] http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/661&format=HTML&aged=0&language=EN

[7] http://www.ico.gov.uk/~/media/documents/pressreleases/2010/first_monetary_penalties_press_release_24112010.ashx

In November, the Commission published: "A comprehensive approach on personal data protection in the European Union"[8]. Building on the responses to the earlier consultations, a number of specific challenges were identified:

- *Addressing the impact of new technologies*
- *Enhancing the internal market dimension of data protection*
- *Addressing globalisation and improving international data transfers*
- *Providing a stronger institutional arrangement for the effective enforcement of data protection rules*
- *Improving the coherence of the data protection legal framework*

It is anticipated that the development of this new regulatory framework will take at least a further two years to complete.

European Directive 2009/136/EC[9], which amends the Privacy and Electronic Communications Directive, comes into force in 2011. The provisions of relevance concern the notification of security breaches and the tightening of the rules on unsolicited communications.

It is expected that there will be amendments to the UK legislation flowing from this Directive, which may result in recommendations to make corresponding amendments to the local Privacy and Electronic Communications Regulations in due course.

Rolling Census

In July, 2010, the States resolved not to undertake a traditional census of the population on 27th March 2011, which is when the census was conducted throughout the remainder of the British Isles.

Instead, the States agreed to the establishment of a corporate database containing basic personal data relating to citizens. This database should provide the means for personal data, held by separate government departments, to be linked for statistical purposes using confidentially maintained keys.

It is understood that basic personal data assembled in this way will be supplemented by sample surveys on a continuous basis to complete the data that would normally be gathered by a census. The system is being designed to ensure that confidential personal data held by government departments will be accessible only by the census unit via these confidential keys, will be used purely for statistical purposes and will not be accessible by other departments.

[8] http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf
[9] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF

The Commissioner will continue to liaise with the census office over the means being used to ensure the confidentiality and security of the information in the corporate database.

Mobile Number Portability (MNP)

MNP was introduced to Guernsey in 2008; from that date any subscriber to one of the three competing mobile service providers was able to 'port' their whole number (including the dialling prefix) to either of the other providers.

Under the provisions of the voluntary MNP Code of Practice agreed by the three mobile telephone operators, the transmission of any marketing information to a former customer in an attempt to 'win back' custom is prohibited for a period of 60 days following the porting of that customer's number [referred to below as the "Prohibition Period"].

The mobile operators asked for a ruling on what should happen at the end of the Prohibition Period. The Commissioner interpreted the Privacy and Electronic Communications Regulations to mean that any consent for direct marketing which may have been obtained from a former customer who had subsequently ported their number should be considered to have lapsed at the end of the Prohibition Period.

Accordingly, the Commissioner ruled that mobile telephone operators should not send marketing communications [by email or SMS] to former customers who had not subsequently provided their express consent to the receipt of such marketing communications.

Google Street View

Google commenced collecting "Street View" imagery in Jersey and the Isle of Man in May 2010, but following the concern throughout Europe over allegations of unauthorised collection of personal data from domestic wi-fi routers, suspended their operations in the Islands.

Subsequently, following joint action by the authorities of all three jurisdictions, Google agreed to:

- notify its processing of personal data in each jurisdiction,
- not to collect data from private roads,
- not to collect any wi-fi data in the Islands and
- to provide advance publicity of future collection activities.

Collection of Street View imagery in Guernsey and Alderney commenced in August, 2010 but it transpired that Google did not have accurate information to identify private roads and, following preliminary enforcement action by the Commissioner, suspended their collection operations and agreed to destroy any images that had been collected from those private roads.

Google did not return to complete its photographic survey in 2010 and there is no information available as to when this work might be completed.

The company agreed to mount further publicity should it plan to return to collect more imagery and whenever any processed images are about to be published on Street View, to give residents an opportunity to report any images which they believe might invade their privacy.

E-borders and the Crown Dependencies

Data Protection Commissioners and immigration officials from the Crown Dependencies, together with the Information Commissioner and his staff were invited to the National Border Targeting Centre in July to witness the progress that had been made by the UK Borders Agency and its partners in implementing measures to increase the security of the "UK Border".

It was evident that the final objective was to be able to record all inward and outward passenger movements across the border in order to identify any suspicious activity that might pose a threat. It was demonstrated that the analysis of passenger movements was highly automated such that only those events which were assessed as suspicious were highlighted and brought to the attention of the staff.

It was made clear that the requirement to collect passenger data would ultimately extend to all passenger movements to and from outside the Common Travel Area and so would involve data collection at the ports in the Crown Dependencies.

It was emphasised by the Borders Agency that the system was being developed with due regard for data protection requirements and a single point of contact had been established to deal with subject access requests and enquiries from individuals in relation to the E-Borders system.

NOTIFICATION

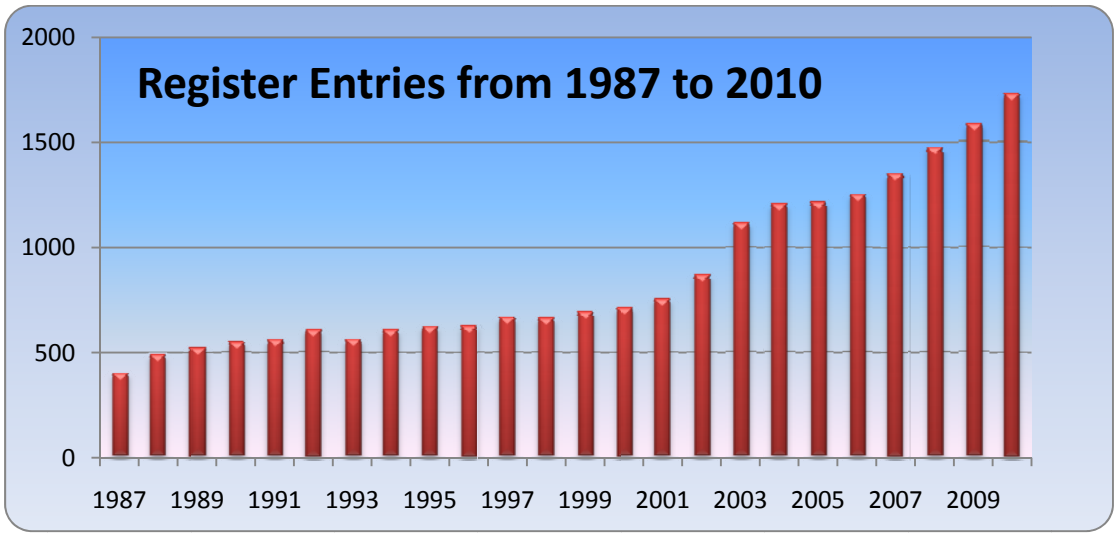
Section 17 of the Law requires most Data Controllers to "Notify" the Commissioner of their processing of personal data. This Notification is on an annually renewable basis and covers all processing that is not exempt.

Exemptions from Notification exist where processing is restricted to manual data, for processing by 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 any organisation from the requirement to conform to the data protection principles and the remainder of the Law.

The annual fee for Notification increased from £35 to £50 on 1st March 2010, but at the same time the notification fee for registered charities was reduced to zero.

Register Entries

The chart shows the sustained increase in the number of Register entries that has been maintained since the commencement of the previous Law in 1987. This number is now more than four times the initial figure of 400 registrations in 1987 and more than twice the number at the commencement of the current Law in 2002.



By the end of December 2010, there were 1732 Notifications on the register, compared with 1586 at the end of 2009. This number included 34 free of charge notifications by elected members and 40 by registered non-profit and charitable organisations.

There were 241 new Notifications and 95 closures during 2010 - a net increase of 146, (compared with 186 new and 79 closures in 2009 - a net increase of 107).

Hosting Service

The hosting service provided by Digimap operated without significant problems during the year.

The web pages were updated in March to reflect the change of notification fee and some problems with the sending of automatic email reminders were corrected.

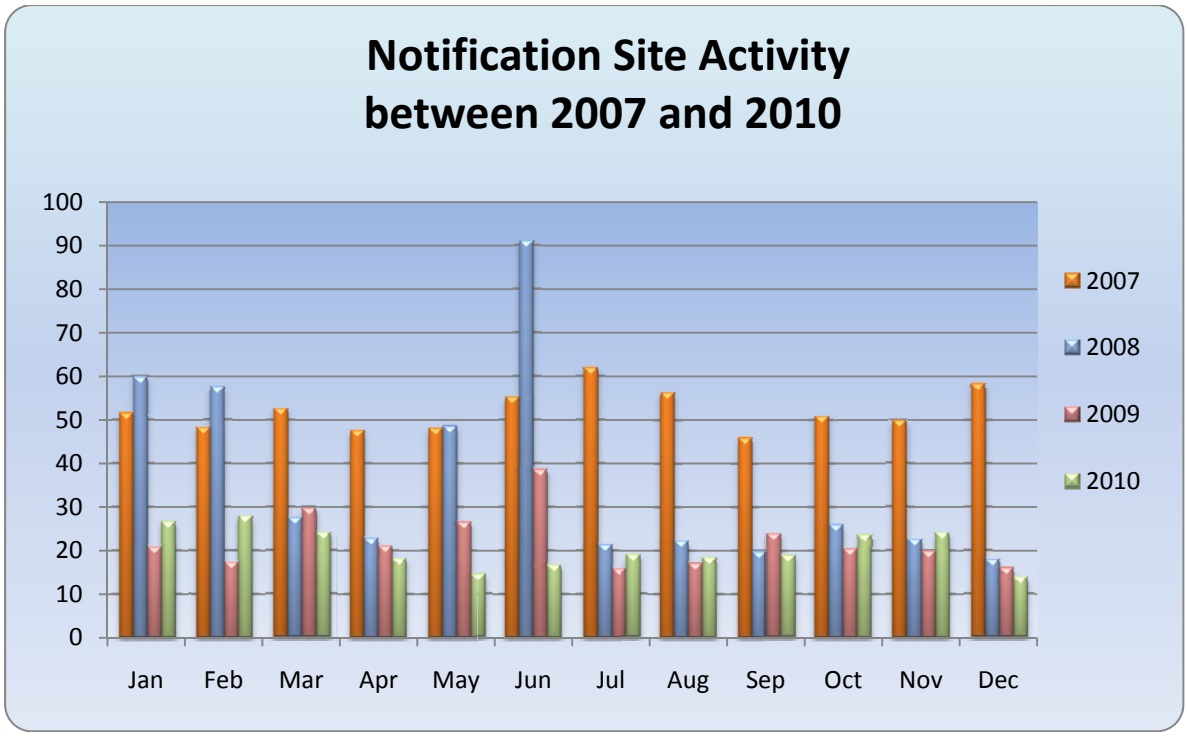
The system was upgraded in the autumn to incorporate use of the States of Guernsey Corporate Address File (CAF) for local addresses and the UK Postal Address File for any UK addresses. This welcome enhancement was designed to improve the accuracy of address information and also to simplify the entry of addresses during the online notification process.

Subsequently, the CAF address search algorithm needed to be amended to cater for the new "GY10" postcodes introduced for Sark.

Internet Statistics

The Google Analytics statistics revealed that the site usage varied between a minimum of 14 and maximum of 27 visits per day, broadly similar to the figures for the second half of 2009, when monitoring using Google Analytics had commenced.

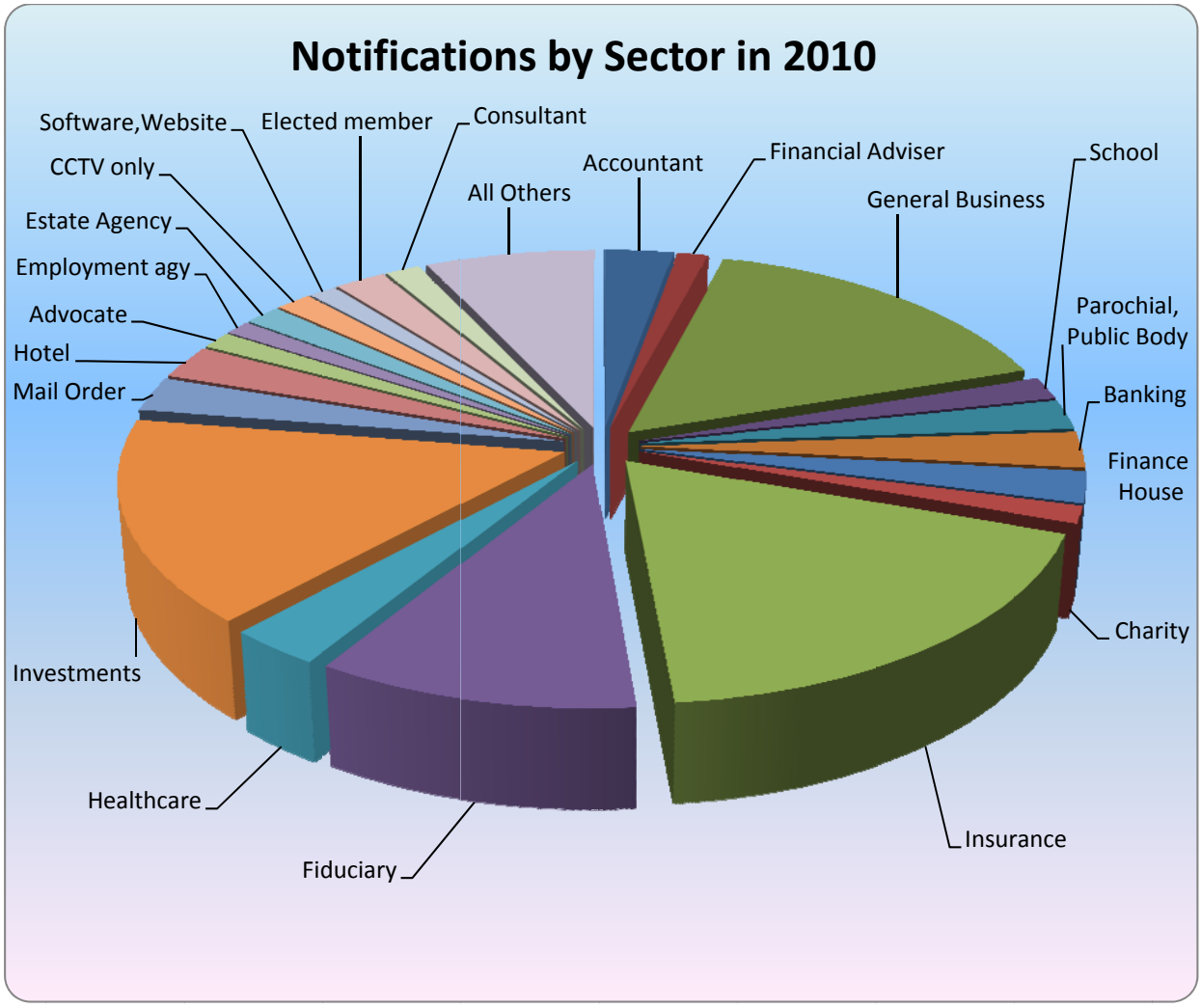
Figures from earlier years were collected on a different basis and so are not strictly comparable to the Google-based statistics.



Notifications by Sector

The Notification process encourages data controllers to indicate the nature of their business activity. This 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 pie chart below represents the breakdown of notification templates for 2010 by industry sector; there has been little change in individual percentages since 2009.



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, but a non-profit organisation remains exempt from the payment of a fee.

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 by 17 to 60 (3.5% of the total).

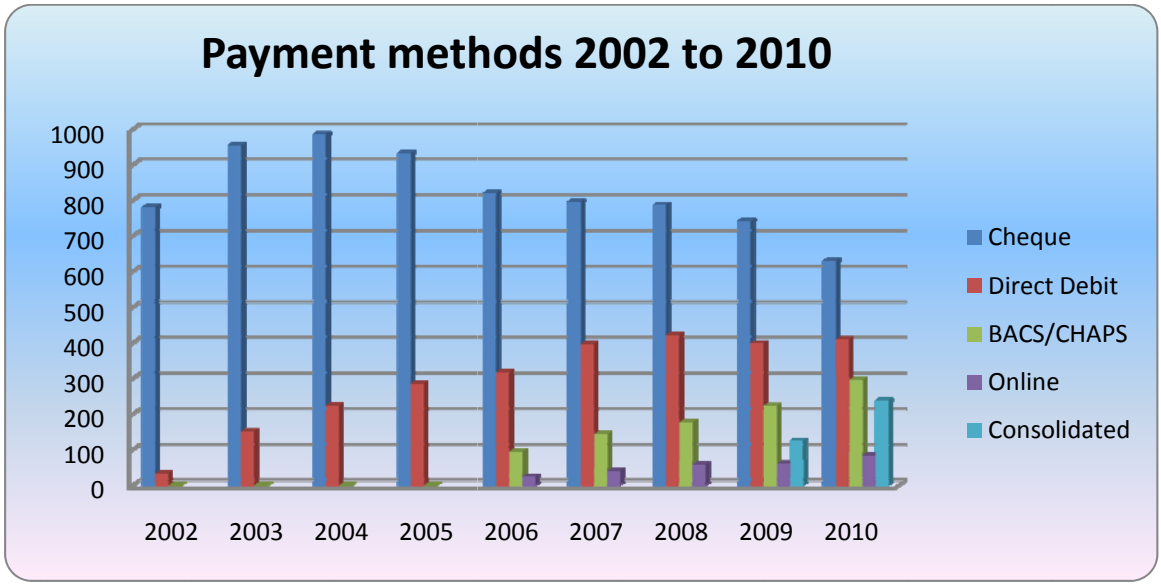
The trend in the number of organisations that have claimed exemption from Notification is shown below. Of the 236 organisations who claimed an exemption in 2010, 111 (47%) were for the core business purposes, 53 (23%) were for both core business purposes and processing manual data. 37 (16%) processed manual data only, 27 (11%) were not for profit organisations, the remaining 8 (3%) claimed an exemption for various reasons including only having corporate clients.

The fall in exemptions has been partially due to an increase in notification by charities, following the cessation of the notification fee.

Payment and communications methods

The Notification fee may be paid by cash, cheque, direct debit, bank transfer (BACS/CHAPS) or Online using the States payment portal. Some organisations which are responsible for the administration of a large number of notifications have taken the opportunity, (which was originally offered in 2009) to renew them by means of a single consolidated payment.

The trend in payment methods between 2002 and 2010 is shown below.



For the first time, fewer than half of the renewals were paid by cheque, with the number of BACS and online payments continuing to rise. The number of individual Direct Debit payments saw little change. The number of consolidated payments nearly doubled.

506 renewals were made before 1st March at the lower fee of £35, whilst 1,159 were made thereafter at £50; 36 notifications (from non-profit organisations or elected members) were at a zero fee; 238 notifications were paid for using consolidated payments (216 by cheque and 22 by BACS).

1,367 notifications (78%) included an email address for communication purposes, compared with 1,234 (also 78%) in 2009.

Where possible, receipts were sent electronically to those who had provided a valid email address.

Second reminders were issued to 166 controllers (175 in 2009). It was necessary to resort to final reminders in 45 (60) cases; this resulted in some payments being overdue.

There were 2 referrals to the Law Officers (2 in 2009) for cases of non-renewal which resulted in the overdue fees being paid and 2 (0) Police Cautions being issued.

STAFFING AND STAFF DEVELOPMENT

Schedule 5 to the Law provides that:

"2. (1) The Committee [the Home Department] must make available to the Commissioner such number and descriptions of staff as he may reasonably require for the proper and effectual discharge of his functions."

There was no change to the staff complement during 2010. 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, who works part time, 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 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 continues to work as a member of the International Standards Organisation Working Group and the BCS Information Privacy Expert Panel.

During 2010 the Assistant Commissioner actively participated in case handling workshops in Brussels and London where she chaired sessions and gave presentations. These workshops discuss and explore different approaches to the assessment and handling of complaints. As real cases are used as the basis for analysis these workshops prove to be of great value in influencing and enhancing the management of complaints.

Discussions with the Home Department over planning the successor to the Commissioner commenced in the autumn of 2010.

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 2010 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 a total of 28 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 in 2010 was 360 compared with 390 in 2009.

In addition to partaking of formal training, any organisation may obtain a copy of a training DVD entitled: "The Lights are On", produced by the UK Information Commissioner. 34 copies of this DVD, which are obtainable free of charge from the Commissioner's Office, were distributed in 2010.

Involvement in Working Groups

The Commissioner and Assistant Commissioner continued to liaise with 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.

In addition, the Commissioner provided specific data protection advice in his capacity as a co-opted member of the Land Registry Steering Group and the Criminal Justice IT Working Group and through his attendance at meetings of the Digimap Management Board.

Making use of the media

10 articles or letters relating to Data Protection were published in the local media during 2010, (the same number as in 2009). Topics covered included:

- Amendments to the law and the increase in fees;
- Personal privacy on Social networking sites;
- Google street view;
- Electronic census;
- Access to medical records;
- "Pubwatch" compliance issues;
- Publication of local paedophiles' details by an individual in the UK;
- Taking pictures at nativity plays.

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

Guidance Notes

The Code of Practice on Criminal Records checks was revised to take account of the establishment of the Guernsey Vetting Bureau. This meant that 3 guidance booklets were replaced with one.

A full list of the 30 available publications is given overleaf. These are available in hardcopy as leaflets or booklets and are published on the Commissioners website[10].

Approximately 1,051 hard copies of the literature were distributed to individuals and organisations during 2010, compared with 630 copies in 2009.

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

[10] www.gov.gg/dataprotection then navigate to: Guidance Notes, selecting General Guidance, Guidance for Organisations, Guidance for States Members and Departments, or Guidance for Individuals.

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
Direct Marketing – A Guidance for Businesses
Disclosure of Medical Data to the GMC
Disclosures of vehicle keeper details *Explains when vehicle keeper details can be disclosed*
Exporting Personal Data
Facebook – How to protect your Privacy
Financial Institutions
Health Records – Subject Access
Individuals - Your rights under the Law
Mail, telephone, fax and e-mail preference service *How to stop the receipt of unsolicited messages.*
No Credit: *How to find out what credit references agencies hold about you and how you can correct mistakes*
Notification – *Simple Guide* – *Complete Guide* - *Exemptions*
Personal Data & Filing Systems *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 : ***Code of Practice - Criminal Records Check***
The Data Protection Law and You: *A Guide for Small Businesses*
Spam – *How to deal with spam*
States Departments – Guidance
Transparency Policy
Trusts and Wills – 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

Developing the Internet Web Site

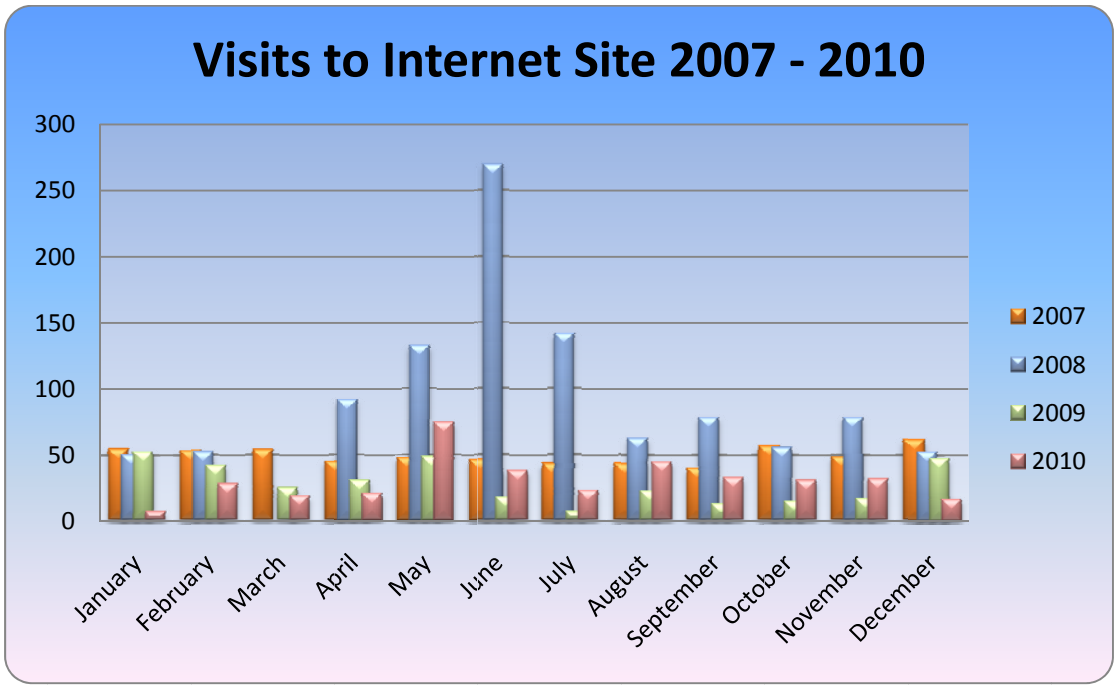
Work continued throughout the year to keep the information on the official website www.dataprotection.gov.gg up to date.

The chart below includes statistics collected for the years 2007 to 2010 and shows that 2008 was a particularly active year for the website, possibly on account of the interest that was generated in the website breach.

These figures exclude accesses to the Notification site www.dpr.gov.gg, which are counted separately.

Currently, it would appear that between 7 and 75 unique pages were accessed each month in 2010. This compares with a long term average of about 50 pages. The most accessed pages are those relating to the Law and the Guidance Notes.

Whilst the number of accesses is at a lower level than in the past, it is clear that the provision of information on the website reduces the number of routine enquiries that would otherwise be dealt with over the telephone or by letter. The website also provides the facility for specific enquiries to be submitted via email.



Registrations with the Preference Services

The Telephone Preference Service (TPS)[11] allows individuals to opt-out of the receipt of unsolicited telephone marketing calls, whereas the Corporate Telephone Preference Service (CTPS) offers a similar service for use by commercial organisations.

The Fax Preference Service (FPS)[12] allows any individual or business with a fax machine to opt out of the receipt of unsolicited marketing faxes.

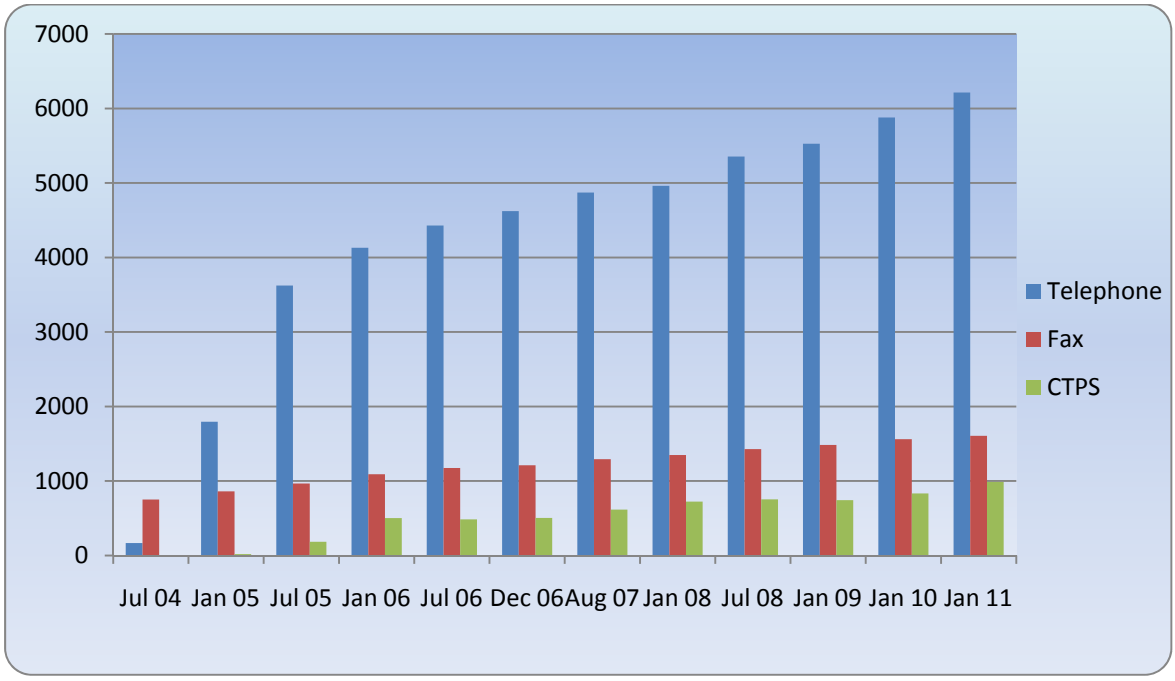
Since 2004, the Office has assisted 488 individuals to register with the TPS and FPS services, but nowadays most people register for themselves by telephone or online.

Registration does not entirely prevent calls which originate from abroad and the office continues to receive complaint from subscribers who receive such calls. Where possible, these complaints are forwarded to the authorities in the originating country.

The chart below, derived from data kindly provided by the Direct Marketing Association, shows that overall registrations for TPS continue to show a small increase, with 6,213 numbers having been registered at the end of 2010, compared with 5,878 at the end of 2009.

Registrations for FPS have increased from 1,561 to 1,607 and those for CTPS have risen from 833 to 987.

Registrations with the Preference Services



[11] www.tpsonline.org.uk
[12] 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.

Notices

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 was expanded to cover non-compliance with those Regulations.

No Information or Enforcement Notices were served during 2010.

Police Cautions

A small number of data controllers 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. There were no Cautions administered during 2009, but in 2010 two Cautions were issued in relation to late renewals, which resulted in the late renewals finally being completed.

Dealing with Requests for Assistance

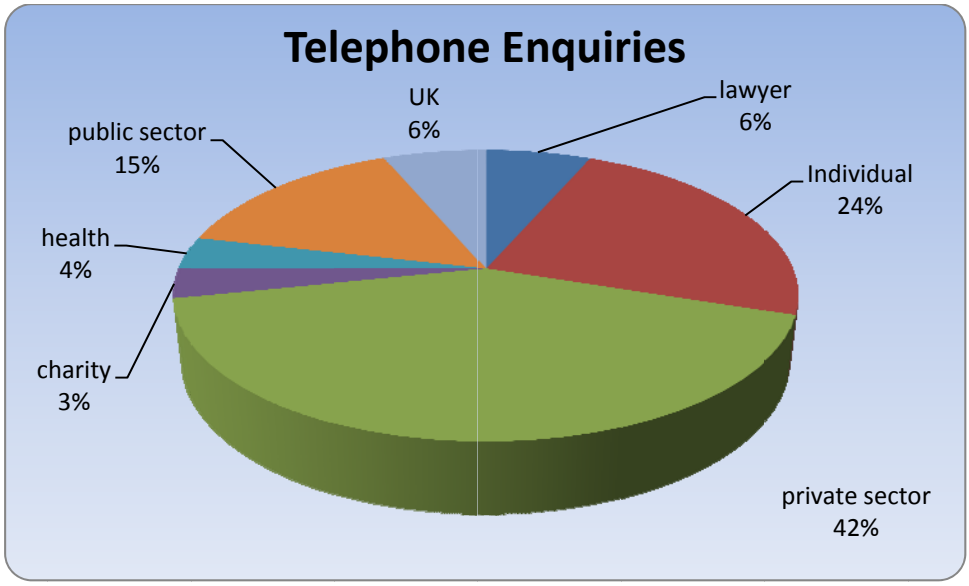
The Office deals with numerous general enquiries and requests for assistance each year.

The source of these requests can be letters, telephone enquiries, emails (directly and via the websites) and personal callers to the office.

A record was kept of substantive telephone enquiries and it can be seen from the chart that 42% of the telephone enquiries were received from private sector organisations, with 24% coming from individuals, 15% from the public sector and 6% from the UK.

The majority of enquiries and requests were resolved on the same day, with just a small number resulting in more detailed investigations.

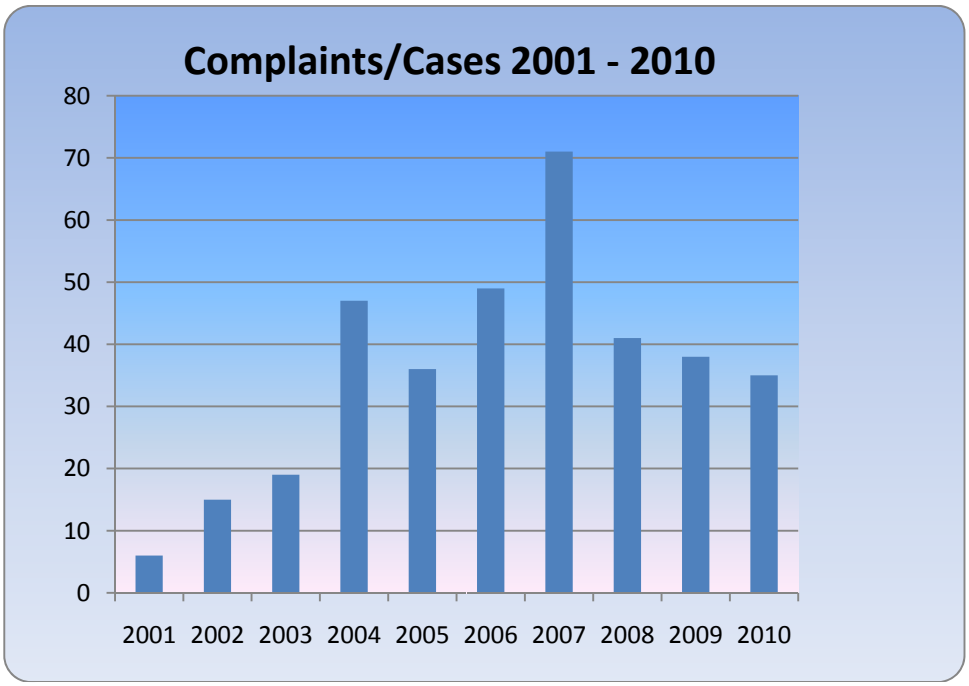
Those cases which resulted in formal complaints, requests for assessment or other actions are dealt with in the following section.



Complaints / Cases

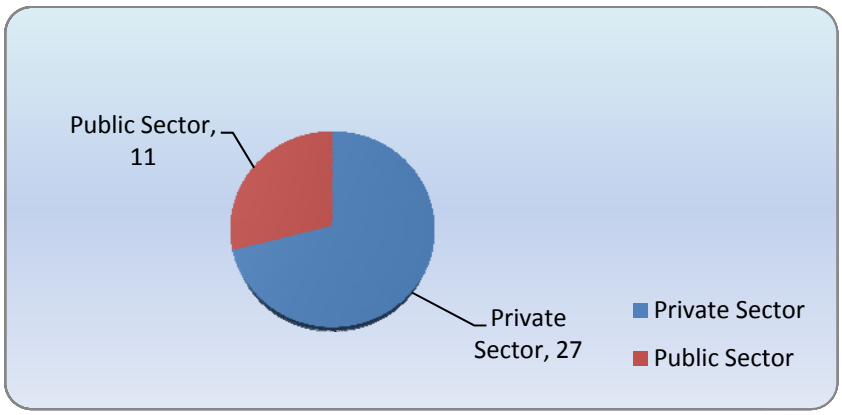
Section 42 of the Law provides that a request may be made to the Commissioner for an assessment as to whether the processing of personal data is compliant with the Law.

There were 35 complaints dealt with by the Commissioner during 2010, 2 of which were brought forward from 2009 and another 2 carried forward to 2011.



The chart above shows the variation in the number of complaints / cases received over the last 9 years.

This chart below shows that, of the 35 cases, dealt with in 2010, 24 related to the private sector and 11 to the public sector.



Of those 24 private sector complaints, 3 were referred to the UK.

21 complaints were upheld, 11 were not upheld, 1 was not progressed by the complainant and 2 have been carried forward into 2011.

Case Studies

Case Study 1 – Disclosure of Personal Data

An insurance company disclosed a copy of an insurance policy to an advocate without informing the policy holder. There was no court order. The policy was presented in court to prove that the defendant was permitted to drive under cover of the policy.

The policy stated it covered any person who drove with the consent of the policy holder. The company informed the advocate that it did not know if consent had been given to her client.

The policy holder stated in court that he had not given the necessary consent, but the court ruled in the defendant's favour.

This resulted in the policy holder suffering distress and illness and time off work.

Section 35 of the Data Protection Law permits the disclosure of personal information for the purpose of legal proceedings. However it must be emphasised that such disclosure is permissible but not obligatory. Organisations have certain obligations to their clients and any processing of personal information must be compliant with data protection principles.

The first data protection principle states that the processing of personal information must not only be lawful but also fair.

Whilst the disclosure in this case was lawful it was unfair to the policy holder. He had an expectation that the insurance company would maintain and respect his confidentiality. He should have been informed that the advocate had asked for a copy of his policy and his consent should have been sought.

Disclosure of personal information may occur without consent if it would be in the interest of the organisation or any third party as long as it is not unduly prejudicial to the data subject. In this case the policy holder suffered distress and illness as a result of the disclosure. Not being believed in court had a negative impact on him.

Where the information is necessary for the prosecution of offenders then, under section 29 of the Law, information relating to the data subject may be disclosed without informing him. In this case as the data subject (the policy holder) was not being prosecuted the section 29 exemption did not apply.

The Commissioner advises organisations to give careful consideration to the use of the section 35 exemption. In disclosing personal information about clients or staff without informing them and obtaining their consent trust and confidence is very likely to be lost. If the requested information is absolutely necessary for the purpose of court proceedings then it is preferable for a court order to be issued particularly in cases such as this.

The company in this case gave an undertaking to the Commissioner that no disclosures would in future be made under section 35 unless the policy holder consented or where a court order was issued.

Case Study 2 –Payment Card Security

When paying by cheque, a person was asked by the merchant to produce her debit card. The merchant then entered the card details including the CVV number (from the back of the card) on to a form which the person was asked to sign. The person protested about the storage of the CVV number, but as she needed the product immediately ,she reluctantly signed the form. She contacted the Commissioner about her concerns.

The merchant when contacted explained that cheques of any value were accepted provided that a customer signed a form and provided their debit card details as back up in the event of a problem with the cheque. The form was retained by the merchant for a period of 30 days so, for instance, payment could be obtained when a cheque bounced.

According to the Payment Card Industry (PCI) Regulations, the CVV number must only be used to authenticate the card in non-face to face transactions. Its purpose is not as an alternative form of payment. The retention of CVV numbers by merchants creates a significant risk to the security of personal data as card details may be used to fraudulently purchase goods on-line or by telephone.

The merchant was informed of the PCI Regulations and was referred to advice which the Commissioner has issued in media releases on this issue. The merchant ceased the practice and stated that other methods of payment guarantee would be considered.

Case Study 3 – Itemisation of Combined Telephone Billing

An individual complained to the Commissioner that a local telecommunications company had breached her data protection rights, had unlawfully shared her personal data with another party and had caused her considerable distress in the process.

On wishing to swap over to a new blackberry contract, she was informed by a staff member that for the transfer to be compliant with data protection the consent of her husband was necessary. She had held a contract in her own name for some years.

Apparently, the company had decided some weeks before this incident to amalgamate mobile phone billing with landline billing of customers living in the same household.

The company explained that it had notified its customers by text that it would change its billing process. There was an assumption that subscribers who did not wish this to happen would inform the company if they did not want their bill merged with the bill of any member of their household.

This complaint was investigated in conjunction with the Director of the Office of Utility Regulation (OUR).

Subsequently the company sent letters to all customers affected by the merging project to inform them they could revert to individual billing if they wanted to. They were given a choice to have either an individual or joint account.

In addition, the Commissioner and the Director of OUR invited all the local telecommunications companies to help in developing guidelines on the processes that should be followed when customer bills are merged.

These guidelines are now in operation and followed by all local companies. Every customer has the right to request a personally addressed bill from a telecommunications service provider.

In addition to the Data Protection Law, the Commissioner is also responsible for the enforcement of the Privacy and Electronic Regulations. These regulations prohibit unsolicited e-mail /SMS marketing to individuals unless they have given prior consent.

Case Study 4 – Disclosure of Email Addresses

A company sent a newsletter by e-mail to a customer but included his e-mail address in a list of 1,170 other recipients. He had not wanted his personal e-mail address disclosed to such a vast number of other people. Moreover he stated that he had not given his e-mail address to the company. He complained to the Commissioner that there had been an invasion of his privacy and confidentiality.

The Commissioner wrote to the company and informed them that this practice appeared to contravene the European Communities (Implementation of Council Directive on Privacy and Electronic Communications) (Guernsey) Ordinance, 2004, in particular paragraphs 4 (confidentiality of communications) and 20 (use of e-mail for marketing purposes).

He advised the company that the correct way to send out mass mailings by email was to use the "bcc" facility which ensures that the address of each recipient is revealed only to that recipient.

Subsequently, the company:

- *Issued an apology to all the recipients;*
- *Offered assistance to anyone who needed to change their e-mail address as a result of this breach;*
- *Deleted information from its marketing database and included only those people who explicitly had consented to be communicated with by email; and*
- *Adjusted its E-mailing procedures to ensure the "BCC" option was used at all times.*

Case Study 5 – Insurance Policy Requirements

A person ,when taking out a policy for a second vehicle, was asked to produce a copy of his driving licence. He queried the need for this and was informed that it was the company's policy to do so. Upon further enquiry he was informed that it was to ensure he was covered to drive the particular vehicle.

He raised certain data protection concerns such as the licence containing other information not relevant to a motor insurance policy and that once scanned onto a computer system the information would stay there and not be updated. If this was correct there would be a likelihood of a breach of the 3rd and 4th data protection principles.

Upon enquiry the insurance company explained that it acts as an intermediary to arrange policies for its customers. The purpose of the scanning procedure was to ensure that the individual holds a valid driving licence for the vehicle for which they require insurance cover and also to check for details of any relevant convictions. Asking to see a driving licence when customers take out new policies or when adding new drivers to existing policies is essential in ensuring that the policies which are arranged are valid. This is the main reason why driving licences are inspected and scanned on to the computer. As the original licence is scanned the accuracy of the information is assured.

It was therefore concluded that the practice of scanning driving licences on to computer was in the customers' best interests in that it ensures that the terms quoted for insurance are correct and that the policies which are arranged are not likely to be invalidated.

Case Study 6 – Conduct of Telephone Surveys

Two complaints were received from elderly people who thought that a telephone survey was a hoax, as they were asked about their income and any benefits which they received. This caused them a certain amount of worry. The situation was compounded as questions were asked about child care, a subject which was of no relevance to them. Both complainants reported that the interviewer persisted in asking them questions even when they said that they had no interest in child care.

On investigation it was found that this was a genuine research survey. Unlike telephone calls made for direct marketing purposes and which are governed by data protection rules telephone calls made or the purpose of research are covered by an exemption in the law. This basically means that researchers may legitimately make "cold" calls.

However, due to concerns about the conduct of the survey, the organisation responsible was approached. It was explained that the provision of child care was being reviewed in Guernsey and a telephone research campaign was conducted to obtain the views and perceptions of Guernsey residents on child care needs. It was aimed at all sections of the community, those with young children and those who have either grown up or no children.

A UK company was contracted to carry out the research. Press releases were issued to inform the public of the campaign as well as an information statement on the States of Guernsey website.

As a result of the complaints, another press release was issued and the conductors of the research were asked to give clearer explanations when doing interviews. They also agreed to give out their own direct telephone numbers rather than the generic number of the research society which employed them.

INTERNATIONAL LIAISON

International Conference of Data Protection Authorities

The Commissioner attended the 32nd International Conference of Data Protection and Privacy Commissioners, which was held in the historic city of Jerusalem from 27-29th October, 2010.

The theme of the conference was "Privacy: generations" and the full programme is available on the conference website[13]

The Commissioner attended the closed session for accredited authorities, at which the Federal Trade Commission of the United States was officially admitted, together with authorities from Albania, Bulgaria, Nova Scotia, Mexico and Moldavia.

The conference unanimously resolved to encourage the adoption of the foundation principles of "Privacy by Design":

- Proactive not Reactive
- Preventative not Remedial
- Privacy as the Default
- Privacy Embedded into Design
- Full Functionality: Positive-Sum, not Zero-Sum
- End-to-End Lifecycle Protection
- Visibility and Transparency
- Respect for User Privacy

The 33rd Conference will be held in Mexico in November, 2011.

European Spring Conference

The European Conference was held in Prague on the 29th and 30th April, 2010. The Assistant Commissioner was one of the 200 delegates who attended.

The conference discussed the challenges which data protection authorities face from the use of new information technologies and the increasing demand for the secondary use of personal data, namely in relation to combating serious crime and terrorism. To this end the need for data protection arrangements guaranteeing a high and equivalent standard of data protection were identified and a resolution was formulated.

Presentations and discussions centred on striking a fair balance between the effectiveness and necessity of new technological devices and their impact on the privacy of individuals.

Topics of interest included cloud computing, privacy by design, use of body scanners at airports, ethnic profiling and children's social networking. The next conference will be in Brussels in April, 2011.

[13] http://www.justice.gov.il/PrivacyGenerations

International Working Group on Data Protection in Telecommunications

The Commissioner attended the two meetings of this International Working Group that were held in 2010.

The 47th meeting was held in Granada on 12th and 13th March.

The major outcome of the Granada meeting was:

"The Granada Charter of Privacy in a Digital World" [14]

The 48th meeting was held in Berlin on 7th and 8th September.

Both Working Group meetings discussed the production of working papers and draft recommendations addressing the following issues:

- Vehicle Event Recorders;
- Deep Packet inspection;
- Privacy and email heritage;
- Privacy and Road pricing;
- Storage of SMS messages for Law enforcement;
- Social networking;
- Use of location information;
- Geospatial data;
- International standardisation.

The papers adopted by the Working Group are published on its website[15].

Many of the adopted papers are subsequently submitted to the annual International Conference as draft resolutions for debate during the closed session.

The 49th meeting of the Working Group will be held in Montréal, Canada in the spring and the 50th meeting will be held in Berlin in the autumn.

British, Irish and Islands' Data Protection Authorities

The Commissioner and Assistant Commissioner joined 12 other representatives of the authorities from the UK, Ireland, Cyprus, Jersey, Isle of Man, Gibraltar and Bermuda at the "BIIDPA" meeting held on 25th June 2010 in Jersey.

The discussions at these meetings are informal in nature, but help to ensure a consistent approach to the treatment of issues which are of common interest.

[14] Granada Charter of Digital Data Protection and Freedom of information.
[15] www.berlin-privacy-group.org

The delegates learnt how the Information Commissioner was using his new powers to impose monetary penalties, discussed the issues raised by some active cases in each jurisdiction, were updated on developments within the EU and on forthcoming issues to be raised at the international conference.

Liaison with the UK Government

The annual liaison meeting was held between the Commissioners from the Crown Dependencies and senior staff from the Ministry of Justice in London on 4th May 2010.

The meeting included discussion of the following topics:

- recent legislative changes in the UK;
- the forthcoming review of the EU Directive on Data Protection;
- other international data protection issues; and
- Freedom of Information policy.

Data Protection Forum

The Assistant Commissioner attended three meetings of the Data Protection Forum that were held in London during 2010; the topics covered in the meetings included:

- Updates from the Information Commissioner's Office (ICO) which included the Commissioner's new powers to impose civil penalties, to carry out audit and inspection visits and his right to do government spot checks;
- The Code of Practice on Assessment Notices *(these Notices apply when the ICO identifies a risk and the organisation is unwilling to participate in a data protection audit)* ;
- How the Freedom of Information Act has impacted on the definition of personal data;
- Data Security;
- Challenges and legal obligations of organisations in safeguarding personal data when using the services of contractors;
- Data Protection in the HR context;
- Measuring the success of data protection training.

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 drafting responses to UK Government proposals for increased enforcement powers for the Information Commissioner.

The IPEP contributed to the BCS response to the EU Consultation on the future of the Data Protection Directive.

Copies of the BCS responses to consultations may be viewed on its website[16]

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 attended two meetings of Panel 5 of the SC27 Working Group of the International Standards Organisation, in London. Remaining work was conducted by email.

This Panel is concerned with the development of International Standards in the ISO 29100 series on information management and privacy. The majority of the work was conducted by email and comprised comments on committee drafts of individual proposed standards. It is expected that the first of this series of standards will be published in 2011.

[16] http://www.bcs.org/server.php?show=nav.5853

OBJECTIVES FOR 2011

The objectives for 2011 remain as follows:-

- ***Legislation***

  Detailed work on any 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***

  The programme of targeted compliance activities will continue with the aim of increasing the number of Notifications. 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, incorporating Privacy Impact Assessments into project planning and the further development of subject access procedures.

- ***Administration***

  Further paper files relating to past assessments, complaints and financial transaction will be archived to electronic media. The filing space released will be exploited for the better storage of other documents (such as contracts and administration records) that need to be kept on paper.

  A review of the communications infrastructure will be carried out with the aim of improving both voice and data communications and enhancing their security.

- ***Succession Planning***

  The contract of the present Commissioner terminates at the end of September 2011.

  Discussions with the Home Department will continue in order to plan the appointment of a successor and ensure an orderly transfer of functions in 2011.

FINANCIAL REPORT

The Data Protection Office is funded by a grant from the States of Guernsey administered by the Home Department in accordance with Schedule 5 to the Law 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	2010 £	2009 £
Data Protection Fees [1]	63,611	52,760
EXPENDITURE		
Rent[2]	16,460	13,030
Salaries and Allowances[3]	166,355	166,996
Travel and Subsistence	9,119	11,171
Furniture and Equipment	12,278	17,940
Publications	3,035	2,623
Post, Stationery, Telephone	3,592	4,177
Heat Light, Cleaning	7,232	6,918
TOTAL EXPENDITURE	**£218,071**	**£222,855**
EXCESS OF EXPENDITURE OVER INCOME	**£154,460**	**£170,095**

NOTES

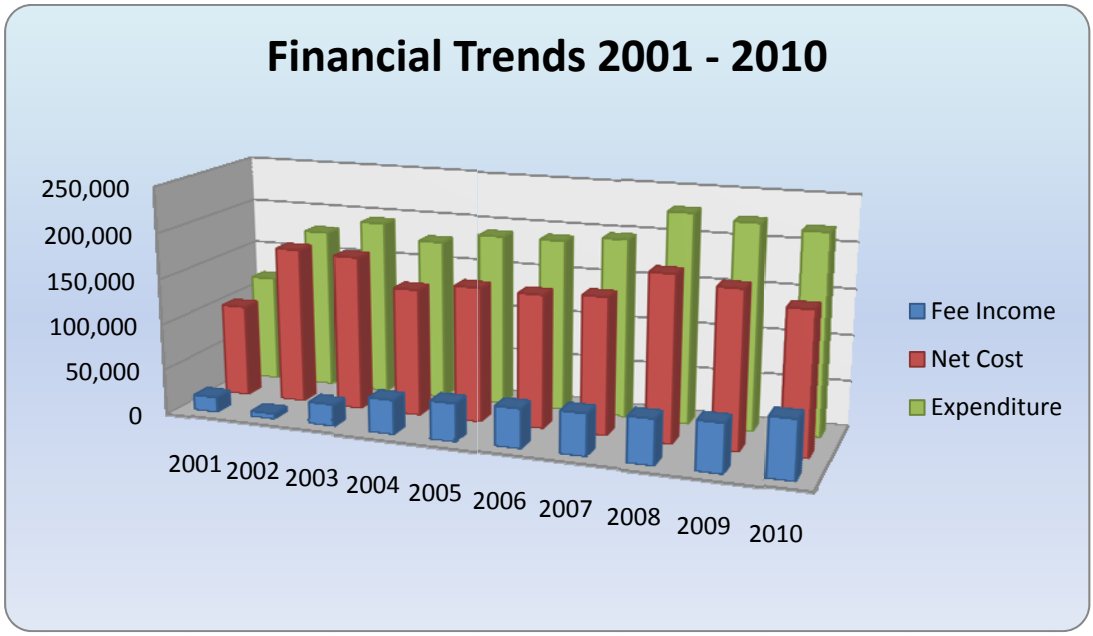
[1] Fees increased from £35 to £50 per notification or renewal of a notification on 1st March 2010.

The cash received for notifications in 2010 was £75,658 (£54,460 in 2009) representing the 1,701 (1,556) annual notifications and renewals that were processed during the year.

[2] The rent was reviewed upwards in the autumn of 2009, with effect from 2010, but because of accruals, the rental accounted for in 2009 was artificially low.

[3] This includes an amount of £500 (£7,210 in 2009) for consultancy fees.

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

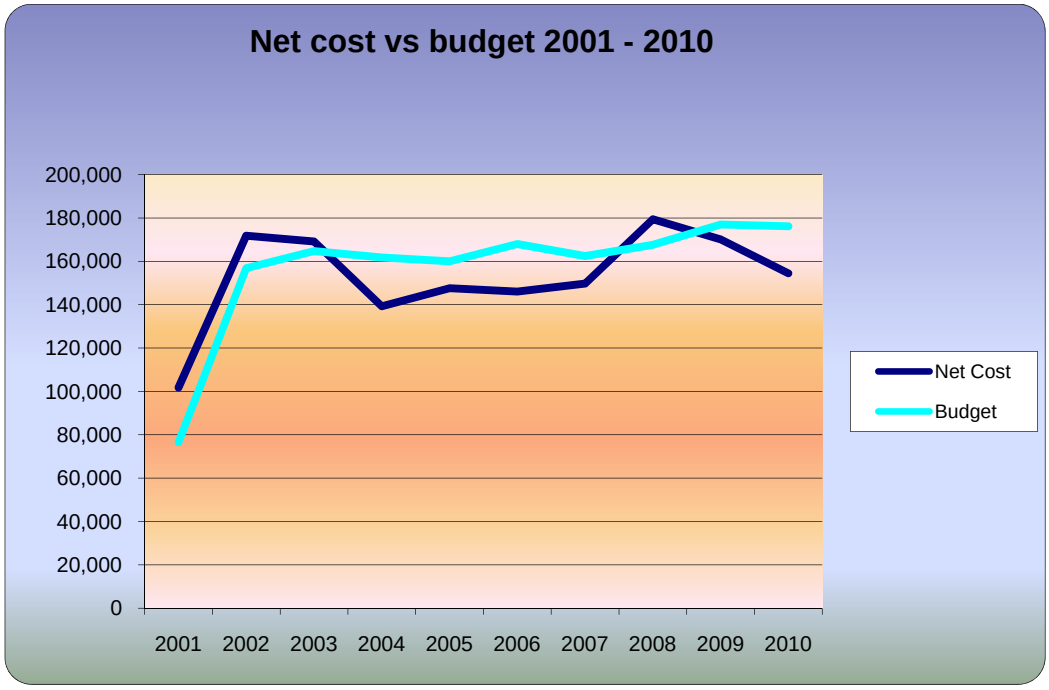


Expenditure for 2010 fell by £4,784 (2.1%), primarily due to reduced consultancy costs and travelling expenses. Income from notification fees rose by £10,851 (20%) as a result of the increased notification fee of £50 and a small increase in the number of notifications.

Hence, as a result of these measures, the net cost of the Office to the taxpayer fell by £15,635 (9.2%).

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 2010. The combined effect of a reduction in expenditure and an increase in income has enabled the cost to fall to a similar level as in 2007.



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 reporting standards contained within the Internal Audit report, the Commissioner hereby confirms that no gifts or hospitality were received by him or his staff during 2010.

Appendix A -

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 unless they have opted in.

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 and the Privacy and Electronic Communications Regulations in Guernsey, Alderney and Sark, 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.dataprotection.gov.gg
Telephone: +44 (0) 1481 742074
Fax: +44 (0) 1481 742077