BAILIWICK OF GUERNSEY

DATA PROTECTION COMMISSIONER
REPORT FOR 2009

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 Right to be Left Alone"
Another Time XI by Anthony Gormley, erected at Le Petit Monceau, Herm Island, on 11th March 2010.

CONTENTS

FOREWORD

I am pleased to present my ninth annual report to the States of Guernsey, covering the calendar year 2009.

The approval by the States of the amendments to the Law reinforced the importance of compliance with data protection legislation, since for the first time the option of a custodial sentence will be available for serious breaches of the Law. These amendments, together with the revision of the notification fee, are effective from 1st March 2010.

On the administrative side, it is pleasing to report that the Internet site used for notification was successfully transferred from the UK and is now wholly hosted and maintained locally. Whilst this process did lead to some unanticipated costs, overall expenditure remained within budget and the ongoing costs of maintaining the site in Guernsey should be significantly lower than beforehand.

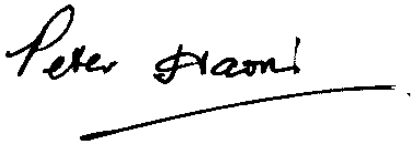
The number of substantive complaints received remained at around three per month which, considering that many of the complaints required some weeks to resolve, resulted in a steady stream of enforcement work, interspersed with the need to respond to more general enquiries.

Approximately 400 people attended talks and presentation that were given during the year, serving to heighten awareness of the Law and refresh knowledge of individual rights. This awareness was reinforced by media releases highlighting important issues of the day.

Following the initiative of the UK Commissioner, there now appears to be a growing body of support within the European Union for the 1995 Data Protection Directive to be amended. I responded to the EU public consultation process and it remains to be seen how many of the suggestions which were made by the respondents find their way into any proposals for the revision of the Directive.

The Assistant Commissioner and I continued the policy of participation in specific international conferences and meetings, thereby both enhancing our knowledge and heightening global awareness of the standards of regulation that apply within the Bailiwick.

My task is made much easier by the positive way in which many local organisations respond to issues raised by my Office. Once again it is pleasing to report that no formal enforcement action was necessary during 2009 and there were no prosecutions for breaches of the Law.



Data Protection Commissioner, May 2010.

DATA PROTECTION ISSUES

Amendments to the Law

On 26th November 2009, the States resolved to strengthen the penalty for unlawful disclosure of personal data by introducing the option of a custodial sentence. This provision was incorporated with other amendments to the Law (that had been previously approved by the States on 27th September 2006) into an amending Ordinance[1], which was laid before the States on 27th January 2010.

This Ordinance, which comes into effect on 1st March 2010, comprises 22 sections, some of which deal merely with cosmetic changes and grammatical issues. There are also updates to some definitions following the reorganisation of the machinery of government when States departments replaced the former committee structure.

The 10 substantive provisions are as follows and are referenced by their section number:

3. Inserts a section into the Law which excludes liability incurred by the Commissioner or by any of his staff for anything that was done in good faith in the discharge of his functions under the Law. This is a valuable amendment since the Commissioner, being an independent self-employed person might otherwise have been successfully sued for damages as a result of an action taken or a decision he may have made.

7. Extends the definition of "public information" in section 34 of the Law to include information held on a public register.

8. Extends the power of the Commissioner to serve an information notice under section 43 of the Law not only on the data controller, but also on another controller or processor if the Commissioner has reasonable grounds for suspecting that the controller or processor holds information that would assist in assessing the compliance of the data controller being assessed.

   This should prove to be an effective mechanism in cases where evidence may be held by a third party that would otherwise not be available to the Commissioner and should minimise the need for the Commissioner to resort to a search warrant in such cases.

10. Adds a "journalistic exemption" to liability under section 55 of the Law for the unlawful obtaining of personal data, analogous to the provision that is proposed in the UK.

[1] The Data Protection (Bailiwick of Guernsey) (Amendment) Ordinance, 2010

11. Allows for the commencement of section 56 (prohibition of enforced subject access) by exempting a disclosure made in accordance with a Code of Practice issued by the Commissioner under section 51 of the Law.

    This exemption includes pre- and post-employment checks using Basic, Standard and Enhanced Disclosures issued by agencies such as the CRB.

12. Introduces custodial sentences for offences under section 55 of the Law. This means that a person guilty of unlawfully disclosing, or procuring the disclosure of, personal data is liable on summary conviction not only to a fine but also to imprisonment for up to 12 months and in a more serious case of conviction on indictment, to a prison term of up to two years plus an unlimited fine.

    This provision is in line with the proposals from the Ministry of Justice in the UK. As well as providing a greater deterrent against the trade in unlawfully obtained data, the prospect of a custodial sentence enables the issue of an arrest warrant where an alleged offence may have been committed across jurisdictional boundaries. This is of particular relevance to the Bailiwick.

13. and

14. Clarify the applicability of the Law to the Crown, to government departments and to the service of notices. The need for these provisions followed difficulties encountered previously by the Commissioner in serving information and enforcement notices on government departments[2].

    Associated with this provision is an Order exempting Crown Appointments from the subject information provisions of the Law.

15. Amends various definitions, in particular that of a health professional, which is of specific relevance to the disclosure of and subject access to, health records.

18. Extends the power of the Commissioner to serve an information notice to support an assessment of compliance with the Privacy Ordinance[3].

    This provision enables a notice to be served not only on the person being assessed, but also on another person if the Commissioner has reasonable grounds for suspecting that the other person holds information that would assist

[2] Data Protection Commissioner's Annual Report for 2005, page 25
http://www.gov.gg/ccm/cms-service/stream/asset?asset_id=2220001&
[3] The European Communities (Implementation of Privacy Directive) (Guernsey) Ordinance, 2004
http://www.gov.gg/ccm/cms-service/download/asset/?asset_id=373006

in assessing the compliance of the person being assessed. This should prove particularly effective in cases where information relating to alleged contraventions such as spamming or phishing may be held by an Internet Service Provider.

Amendments to the Notification Regulations[4], which were also approved by the States in 2006, come into force on 1st March 2010.

The annual notification fee rose from £35 to £50, although there are no plans to levy a higher fee on large companies, as is the case in the UK. At the same time, not for profit organisations are able to notify free of charge.

It is considered that a higher fee for larger companies would not work very well in a small jurisdiction such as Guernsey, where the number of such companies is relatively small. In any case, many financial services companies currently make multiple notifications on behalf of separate entities which are individually registered with the Guernsey Financial Services Commission. As a result, these firms already pay a higher overall fee.

The waiving of a notification fee for non-profit organisations, such as charities, will be of particular assistance to those organisations which for a variety of reasons may not have been exempt from notification and should encourage other charitable organisations, many of which process sensitive personal data, to notify voluntarily as there will no longer be a cost penalty.

European Union Consultation

On 9th July 2009, the Freedom, Security and Justice Directorate of the European Union launched a public consultation[5] on the legal framework for the fundamental right to protection of personal data.

The objective of the consultation was stated as:

"To obtain views on the new challenges for personal data protection in order to maintain an effective and comprehensive legal framework to protect individuals' personal data within the EU."

The main targets of the consultation were private individuals, public authorities and commercial organisations within the EU, but since the Directives have a profound impact on third countries, such as Guernsey, the Commissioner considered that it was important to respond from that perspective. The consultation closed on 31st December 2009 and copies of all responses received are available on the above-referenced website[5]. A copy of the Commissioner's response is reproduced as Appendix A.

[4] The Data Protection (Notification and Notification Fees) (Amendment) Regulations, 2010 http://www.gov.gg/ccm/cms-service/download/asset/?asset_id=11231122

[5] http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm

Development of International Standards

There was significant progress in 2009 in the development of international standards for the protection of personal data and privacy.

The International Standards Organisation (ISO) resolved to establish a Privacy Steering Committee to improve the co-ordination of its work on privacy standards and the International Conference of Data Protection and Privacy Commissioners was able to agree on a joint proposal known as the "Madrid Resolution" which was published at the end of the 31st conference held in Madrid.

A copy of the Press Release by the Spanish Data Protection Authority about this Resolution is reproduced as Appendix B.

Disclosures to HM Revenue and Customs

This matter was originally raised in the annual report for 2007 and was not finally resolved until 2009. The UK Commissioner wrote to the Director at HMRC asking him to ensure that any data relating to offshore account holders resident overseas was processed proportionately and in response HMRC undertook to destroy any data which did not relate to those with a liability to UK Tax.

The Guernsey Commissioner met the Association of Guernsey Banks and emphasised the need to ensure that only relevant information should be disclosed to HMRC.

Immediately prior to the second offshore disclosure campaign in August 2009, HMRC wrote to the Guernsey Commissioner outlining the nature of the campaign and the safeguards that would be put in place.

To date, no further complaints have been received from residents of the Bailiwick about the disclosure of their financial details to HMRC as a result of this second campaign.

Credit Reference Agencies

In the 2006 Report, it was stated that the Home Department had agreed to issue Certificates providing proof that an individual's name and address were included on the Electoral Roll. This scheme was designed to provide assistance to those who were applying for credit as the UK-based credit reference agencies refer to the Electoral Roll to provide proof of an applicant's residential address. Details of the scheme are included in the 'No Credit?' guidance leaflet.

The scheme commenced in July 2007 and Home Department received 11 applications for such certificates in 2007, 13 in 2008 and 24 in 2009. There were no complaints in 2008 or 2009. This level of take-up indicates that the scheme appears to have been beneficial.

E-borders and the Crown Dependencies

"E-borders" has been described as the UK border agencies'[6] "strategic IT solution to the need for acquisition, joint pooling and analysis of electronic passenger, crew, service and freight information".

The aim is to maximise the potential to identify individuals who present a threat to the United Kingdom by capturing and sharing traffic data about goods and people crossing the border.

In this context "the border" extends to the border of the Common Travel Area (CTA) which includes the UK, Crown Dependencies (CD's) and the Republic of Ireland.

The legality of the e-borders programme was endorsed in December 2009 by the European Commission[7] with some provisos that remain subject to further negotiation with the UK Government, but the Commission stated that it was up to each Member State to establish the legal basis in domestic law for the sharing of such data for travel by EU citizens between Member States and the UK.

It is understood that the Data Protection Commissioners of the CD's will be consulted during 2010 about the applicability of e-borders to the CD's.

This matter remains an active topic of discussion within the British, Irish and Islands Data Protection Authorities meeting.

[6] Border and Immigration Agency, UK Visas, HM Revenue and Customs, Police.
[7] Letter from Jonathan Faull, Director General, Freedom Justice and Security to Home Office UK Border Agency, dated 17 December 2009, Ref: JLS/D-5/MDF/et (2009) D19374.

NOTIFICATION

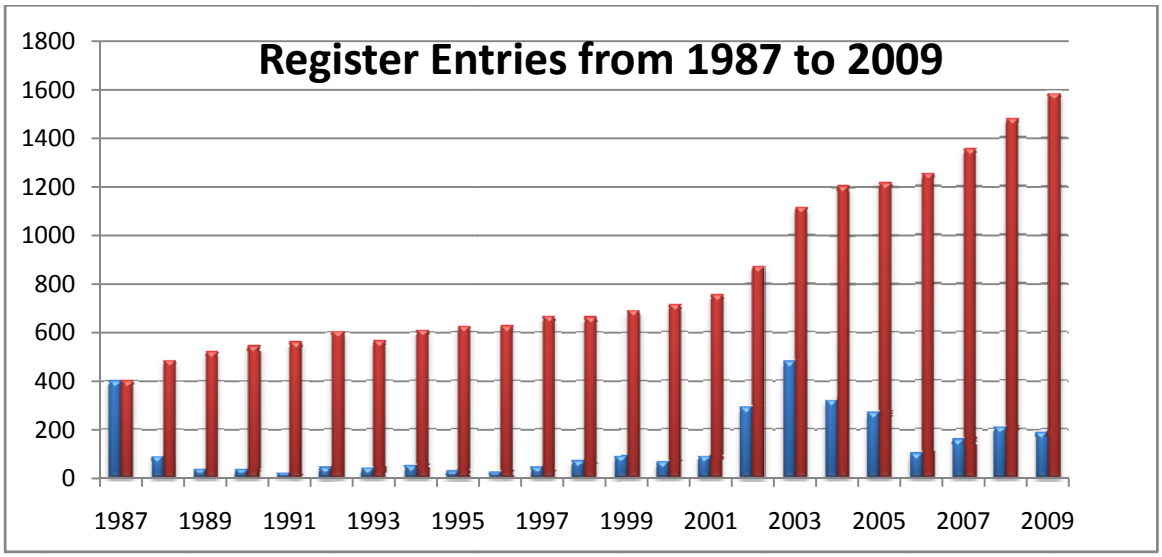
Section 17 of the Law requires Data Controllers to "Notify" the Commissioner of their processing of personal data. This Notification is on an annually renewable basis and covers all processing that is not exempt.

Exemptions from Notification exist 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 remained at £35 throughout 2009, but increased to £50 from 1st March 2010.

Register Entries

The chart shows the sustained increase in the number of Register entries that has occurred since the current Law came into force in 2002.



By the end of December 2009, there were 1586 Notifications on the register, compared with 1479 at the end of 2008.

There were 186 new Notifications and 79 closures during 2009 - a net increase of 107, (compared with 208 new and 85 closures in 2008 - a net increase of 123).

The scanning of the paper records of Notifications continued and by the end of 2009, nearly 90% of the current Notifications and associated correspondence had been scanned into the document management system. It is expected that the wholly electronic storage of historical Notifications will be completed during 2010.

Change of Hosting Service

On 26th March 2009, Eduserv Internet advised the Commissioner that it would be unable to continue to host and maintain the Notification website following the expiry of the annual contract on 31st July 2009.

This news came as a surprise considering that Eduserv had developed and hosted the site over the past eight years. However, under the termination clauses in the contract, Eduserv was required to provide the source code of the notification system and reasonable support to any organisation which took over responsibility for the system after the end of the contract.

The Notification site is used not only for on-line notification by data controllers, but also provides an essential component of the Office administration system.

Eduserv had developed the site (by adapting the pre-existing notification system written for the UK Commissioner) using a scripting language [PERL] and back-end database [Postgres] that were unfamiliar to many local software specialists, so it was quite a challenge to find a service provider able to provide the required level of support and hosting capability in a relatively short time.

The prospect of developing an equivalent notification system from scratch using a different language and database environment in less than four months was not an attractive or cheap option and, following consultation with both the Treasury and Resources IT Unit and the Home Department IT Section, was discounted.

Accordingly, local software company Digimap, (an existing IT partner of the States of Guernsey), was asked to undertake an investigation to determine the feasibility of migrating the site to a local hosting service whilst ensuring the continued maintenance of the existing source code of the online notification system and its associated database environment.

Digimap proposed using a resilient hosting service established on Guernsey and offered to undertake the migration and ongoing software maintenance itself, on a fixed price contract basis.

The migration project proceeded smoothly (with some assistance from Eduserv) and the entire system was transferred and operational before the end of June, one month before the end of the Eduserv contract.

However, routine security testing undertaken following the migration revealed potential weaknesses in the original source code and its environment, which took a further two weeks' work to rectify, but incidentally served to demonstrate Digimap's competence to maintain and update the software system and its environment.

Further maintenance activity, predominantly involving the correction of other latent problems with the original software, proceeded satisfactorily for the remainder of the year and an amendment to the

system was completed in December to prepare for the increase in notification fees that was due from 1st March 2010.

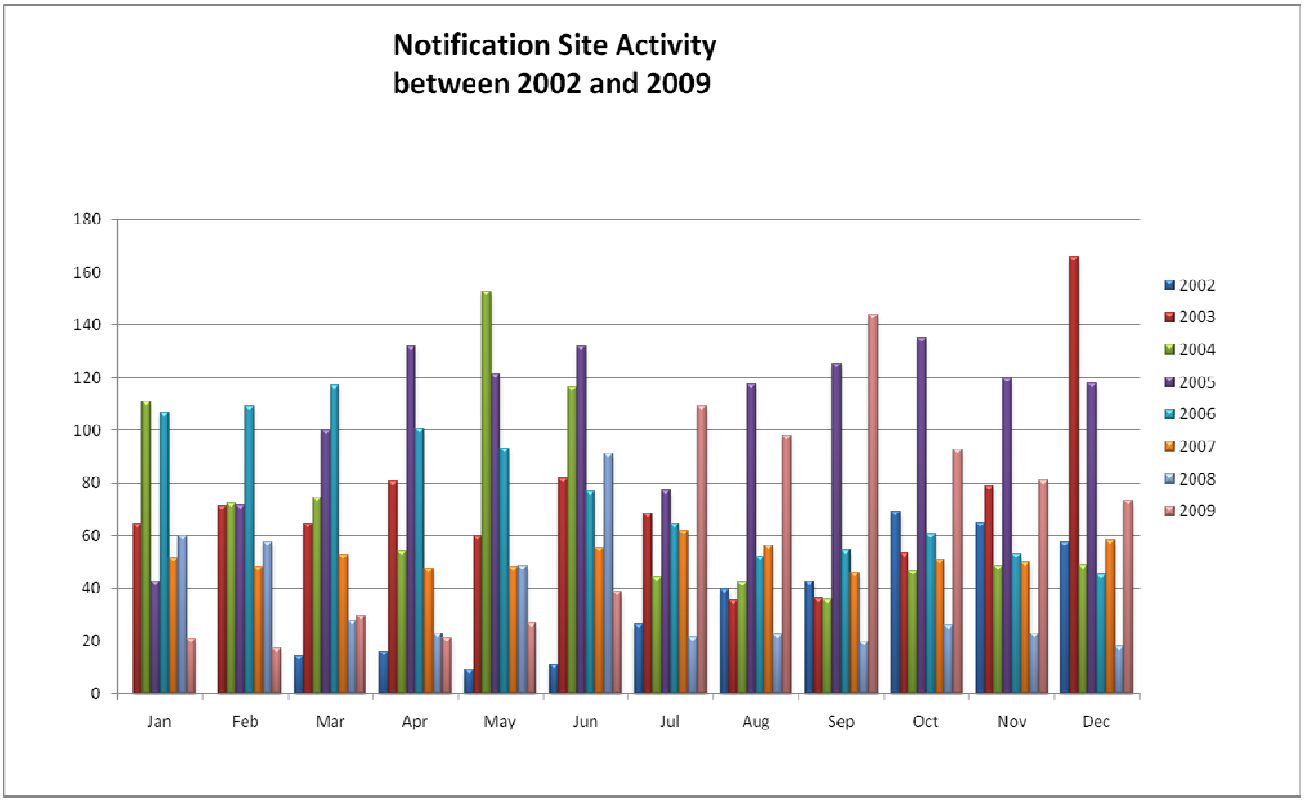
It is planned to upgrade the system during 2010 to incorporate use of the States of Guernsey Corporate Address File.

Internet Statistics

One of the casualties of the migration was the need to change the method of collection of Internet statistics, as the previous method had employed in-house software at Eduserv which it was not practical to migrate.

It was decided to use Google analytics for the new system, but this meant that the new statistics were not entirely comparable to those taken from the original system.

The Google statistics for the six months between 1st July and 31st December 2009 showed that the site usage varied between a minimum of 72 and maximum of 201 visits per week and averaged around 150 visits per week. The figures for the first six months of the year, complied using the Eduserv statistics software, had been significantly lower than that.

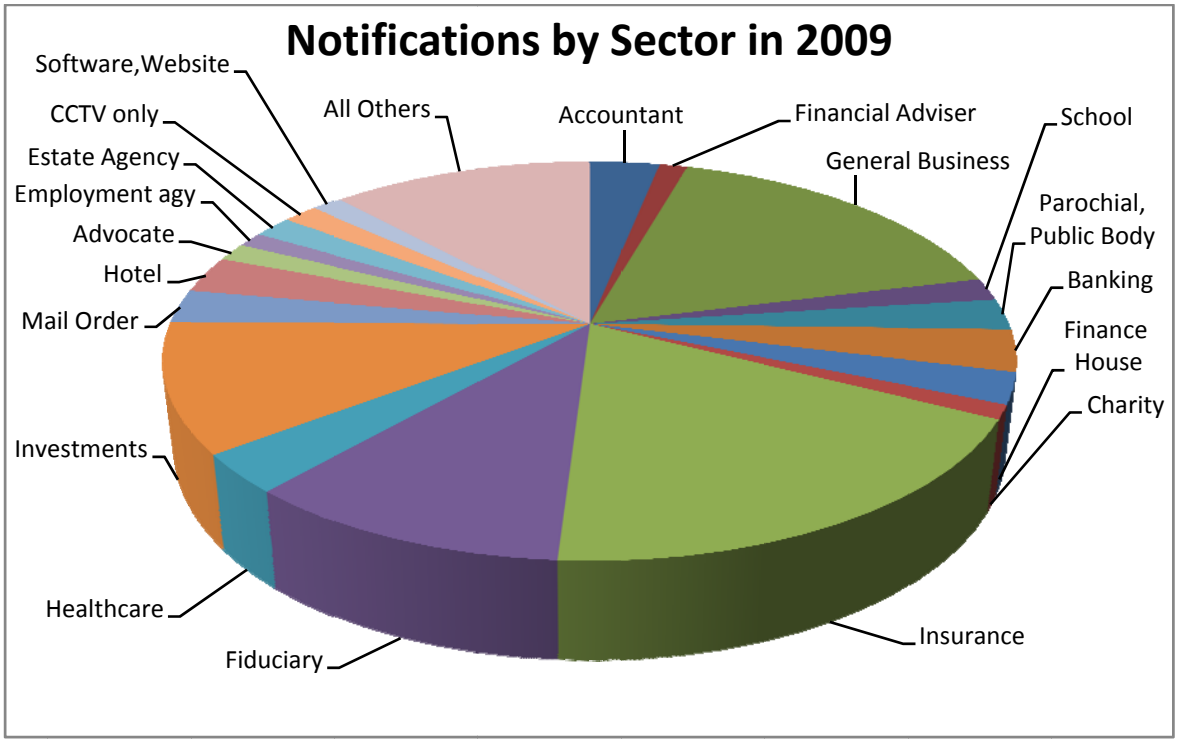


The chart above shows the Google statistics overlaid on the Eduserv statistics to give an indication of the trends in utilisation of the notification website between 2002 and 2009.

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 pie chart below represents the breakdown of notification templates for 2009 by industry sector; changes in percentages since 2008 are relatively small, with the sectors showing the most increase being Insurance (up from 20% to 23%), Fiduciary (from 12% to 13%) and Investments (from 11% to 13%).



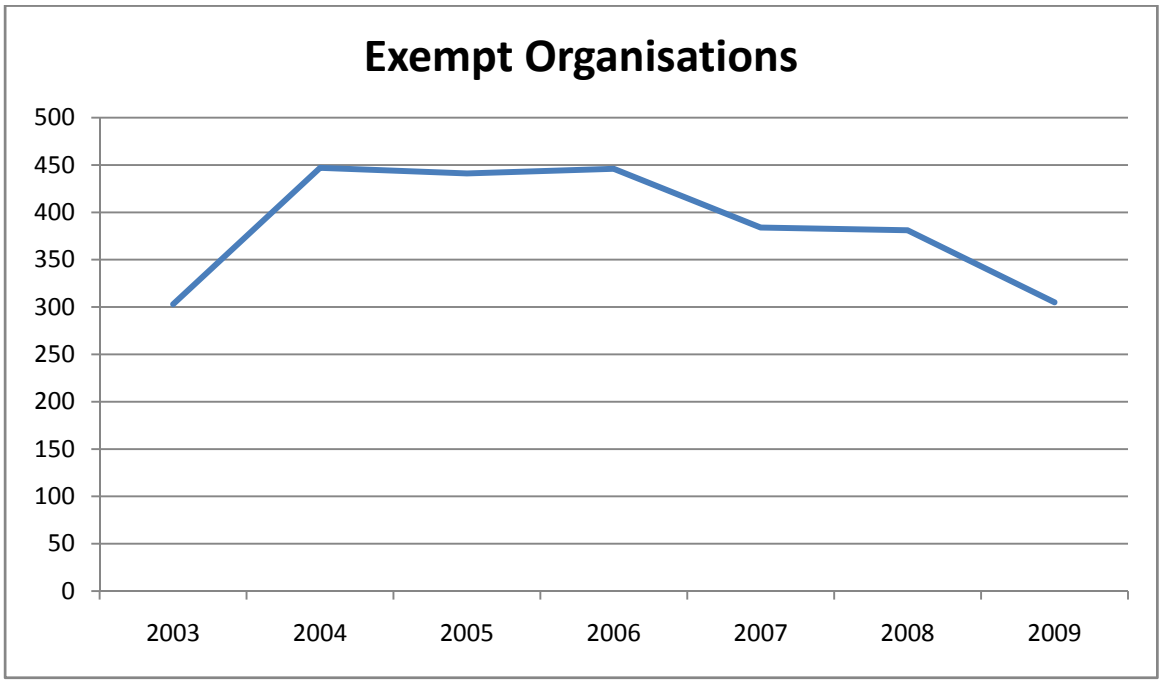
Exemptions

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). This figure is expected to increase in 2010 once non-profit organisations become exempt from the payment of a notification fee.

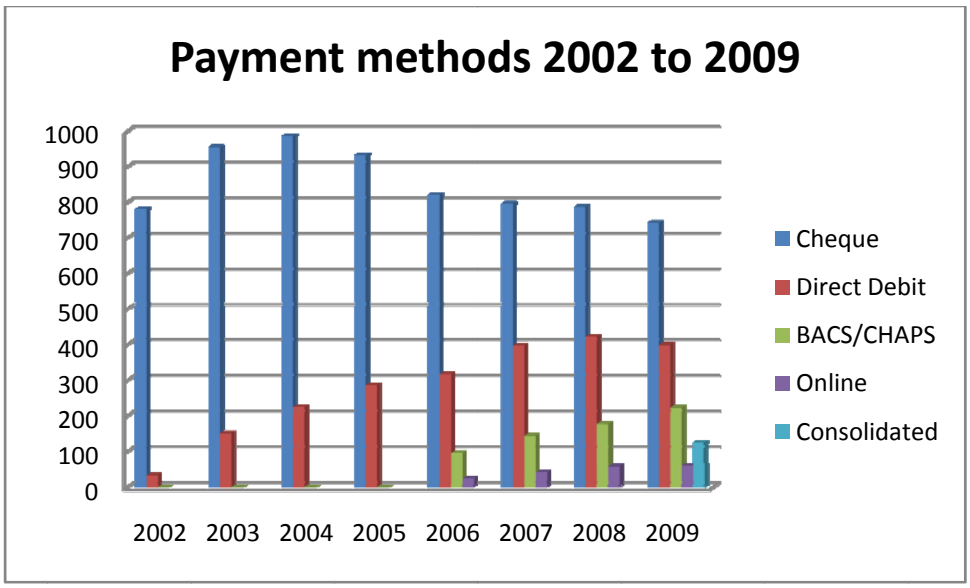
The trend in the number of organisations that have claimed exemption from Notification is shown below. Of the 305 organisations who claimed an exemption in 2009, 158 (52%) were for the core business purposes, 72 (24%) processed manual data only, 29 (9%) were not for profit organisations, 14 (4.5%) held corporate data only, 7 (2%) were trading subsidiaries and the remaining 25 (8%) claimed an exemption for various reasons (including not being a local data controller).



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 were offered the facility to renew them by means of a single consolidated payment.

The trend in payment methods between 2002 and 2009 is shown below.



Although more than half of the renewals were paid by cheque, the number of BACS and online payments continued to rise. The number of individual Direct Debit payments saw a slight reduction because of the effect of consolidated payments, which are shown separately.

1,234 notifications (78%) included an email address for communication purposes, compared with 1,256 (85%) in 2008; the reason for the fall is predominantly due to the fact that 125 email addresses were removed from those notifications which were renewed using consolidated payments. When those were taken into account, the email percentage rose back to 84%.

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

Second reminders were issued to 175 (292) controllers. It was necessary to resort to final reminders in 60 (39) cases; this resulted in some payments being overdue.

There were 2 referrals to the Law Officers (3 in 2008) which resulted in the overdue fees being paid, but 0 (2) police cautions were 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 2009, which in the Commissioner's opinion represents the minimum level necessary for the effective performance of his functions.

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.

The Assistant Commissioner broadened her experience by attending a case handling workshop, organised by the European Data Protection Commissioners. This was a practical session at which different approaches to the handling of real cases were discussed. It is planned for her to participate in another case management workshop in 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 2009 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 in 2009 was around 390 compared with 380 in 2008.

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. Approximately 30 copies of this DVD, which are obtainable free of charge from the Commissioner's Office, were distributed in 2009.

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 2009, (the same number as in 2008). Topics covered included:

- Identity theft;
- Disclosure of the identity of public servants;
- Credit card security;
- Privacy issues with social networking;
- Mobile telephone directory service (118 800);
- Case studies from the annual report;
- Amendments to legislation
- A who's who publication that appeared to be a scam.

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

Guidance Notes

One additional guidance note on subject access to health records was issued in 2009.

A full list of the 32 available publications is given overleaf. These are available in hardcopy as leaflets or booklets and are published on the Commissioners website[8].

Approximately 630 hard copies of the literature were distributed to individuals and organisations during 2009, compared with 566 copies in 2008.

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

[8] 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 – a Simple Guide
Notification – a Full Guide
Notification 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 : ***Guidance on Applying for Police Disclosures*** ***Code of Practice & Explanatory Guide*** ***Disclosure Policy for Police***
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

Developing the Internet Web Site

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

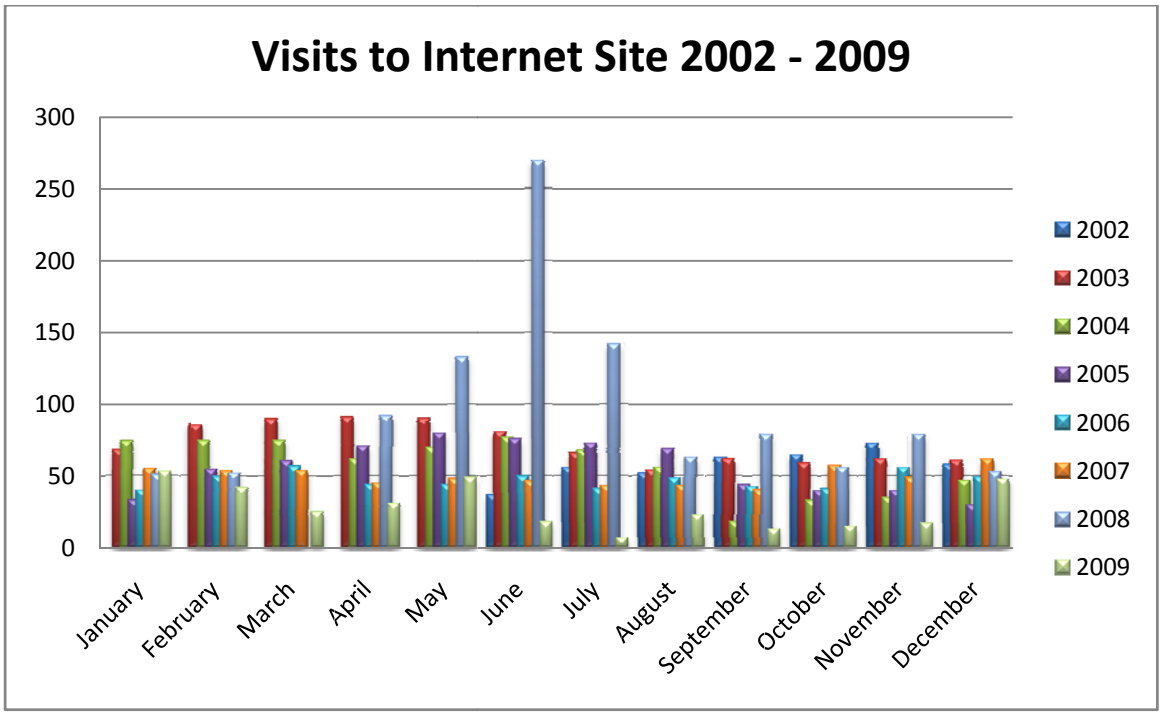
Google Analytics reported a 70% fall in the page views from 1,031 in 2008 to 309 in 2009.

The chart below includes statistics collected for the years 2002 to 2009 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 about 25 to 30 unique pages are being accessed each month. 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)[9] 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)[10] allows any individual or business with a fax machine to opt out of the receipt of unsolicited marketing faxes.

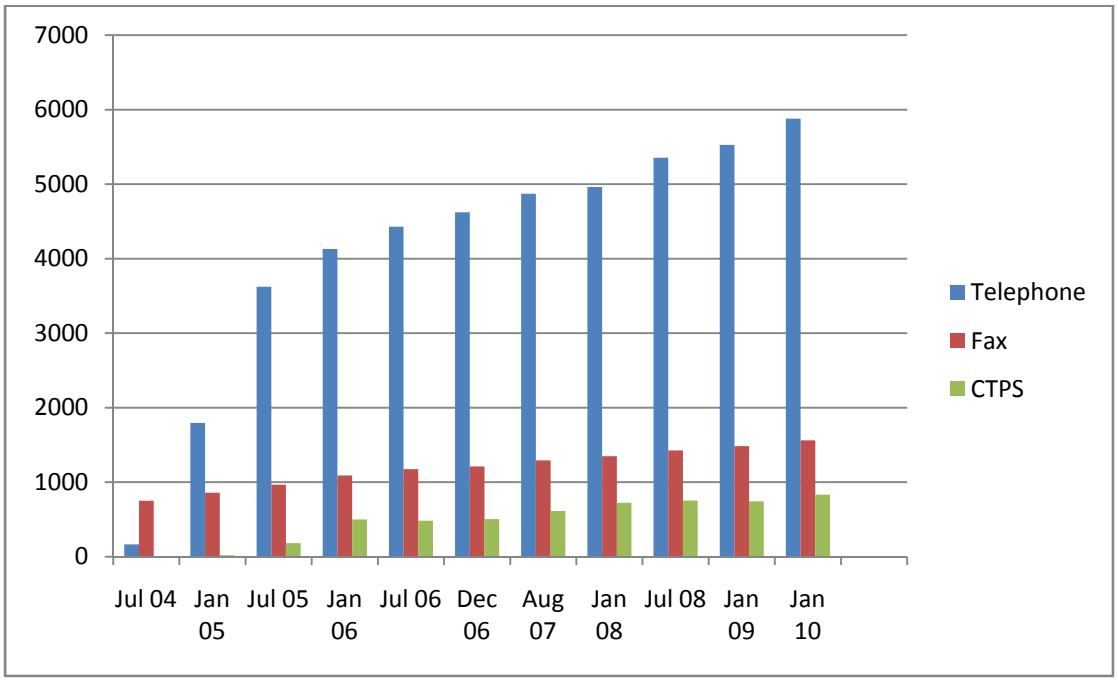
Since 2004, the Office has assisted 476 individuals to register with the TPS and FPS services, but nowadays most people register for themselves by telephone or online. In 2009 just 6 such registrations were made by the Office, compared with 14 in 2008 and 152 in 2005.

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 5,878 numbers having been registered at the end of 2009, compared with 5,527 at the end of 2008.

Registrations for FPS have increased by from 1,484 to 1,561 and those for CTPS have risen from 743 to 833.

Registrations for TPS represent about 11% of all the residential and business subscribers on fixed lines in the Bailiwick.

Registrations with the Preference Services



[9] www.tpsonline.org.uk
[10] 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 was expanded to cover non-compliance with those Regulations.

Notices

No Information or Enforcement Notices were served during 2009.

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. There were no Police Cautions administered during 2009, although there were two referrals to the Law Officers, 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 and personal callers into the office.

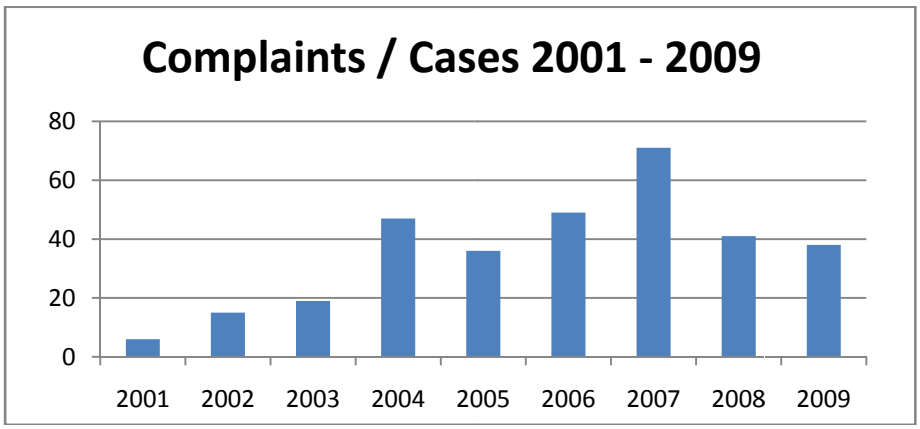
Substantive enquiries that involve some effort to resolve are recorded by the Office. During 2009 the Office recorded 23 substantive enquiries by email, 35 by letter and 4 from individual callers. Detailed records were not kept of general telephone enquiries, though it is planned to commence a record of these in 2010.

A sample was taken of the general telephone enquiries received in December, which revealed that the main queries related to: subject access to information, notification, marketing and specific questions about data transfer, retention and sharing.

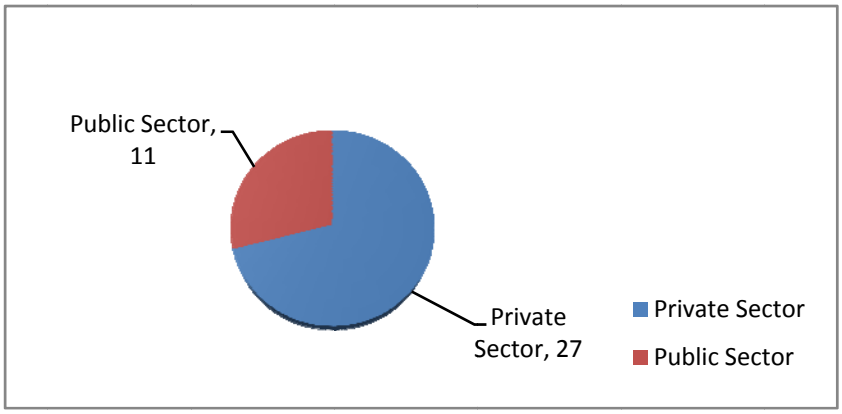
Those cases which resulted in formal complaints, requests for assessment or other actions are dealt with below.

Complaints / Cases

There were 38 complaints received by the Commissioner during 2009, 2 of which were brought forward from 2008 and another two carried forward to 2010. One of these complaints was against 8 separate data controllers; it is recorded as one *case* as it was determined that the complaint had no substance. The investigation did, however, incur a significant amount of time and effort. Another case necessitated the investigation of a complaint which involved 2 States Departments.



The chart above shows the number of complaints / cases received over the last 8 years. The significant increase in 2007 was due to the disclosure of Guernsey residents' personal details by UK banks to the HMRC; these 29 complaints were referred to the UK Commissioner.



This chart shows that, of the 38 cases, dealt with in 2009, 27 related to the private sector and 11 to the public sector.

Of those 27 private sector complaints, 2 were referred to the UK, 3 to Jersey and 1 to Iceland. The referrals to the UK and Jersey concerned unsolicited marketing while the referral to Iceland concerned the alleged publication of Landsbanki depositors' details on a website.

26 complaints were upheld, 8 were not upheld and 4 were not progressed. Some individuals do not progress their complaints when, after liaison with the Data Protection Office and after consideration of other factors, they realise that pursuing the complaint would result in little or no particular benefit to them.

Case Studies

Case Study 1 – Guernsey Pub Watch and the Police

A complaint against Guernsey PubWatch and Guernsey Police was received in 2008 and, due to its complexity, was not finally resolved until 2009.

The substance of the complaint was that a PubWatch ban imposed on an individual and the subsequent circulation of his police photograph to PubWatch Scheme licensees constituted a breach of the Data Protection Law.

Guernsey PubWatch was based on the Pub Watch schemes in the UK, which exist for the prevention and detection of crime on licensed premises. A scheme comprises the voluntary membership of licensees, who elect a Committee to sanction the banning from their premises of any individual who has either committed an offence, or who has caused trouble, on their premises. The decision making process at these meetings must be carefully documented to show that any action taken is compatible with the prevention and detection of crime.

The Police should normally have a restricted role at PubWatch meetings. The Crime Prevention Officer should be the nominated representative of the Police whose function would be to inform the Committee of the nature of any offence and the sentence imposed by the Courts on an individual who has been found guilty of committing an offence on or near licensed premises. In the event that a ban is imposed then after due consideration of all the facts the Police might provide the Committee with copies of the individual's photograph for circulation to licensees on the scheme.

On investigating the complaint it was apparent that the Police had been too closely involved in the administration and operation of the scheme, rather than merely providing advice and guidance.

The Chairman's role had been limited to participating in discussions as to whether or not to enforce a ban. Other Committee members were not officially elected and the composition of the Committee would vary from meeting to meeting thus providing little or no continuity.

Guernsey PubWatch did not satisfy the criteria of being a data controller and were not notified as such.

Accordingly, the data protection complaint was assessed in relation to the Police. The assessment concluded that the Police involvement had resulted in breaches of five data protection principles. The Police accepted the assessment and undertook to address all of the matters that had been identified.

The Commissioner decided that the photographs of the individual should be returned by the licensees to the Police and recommended that the constitution of Guernsey Pub Watch should be revised to strengthen the role of the Committee and reduce the role of the Police to be an advisory one.

As a result, Guernsey Pub Watch is now in the process of being reconstituted and has notified as a data controller. The role of the Police has been reduced to that of an advisory capacity.

Case Study 2 – Mobile Number Portability (MNP)

MNP was introduced to Guernsey on 1st December 2008. From that date mobile customers were able to change their mobile telephone operator and keep their full number, including the dialling prefix.

Under the provisions of the voluntary MNP Code of Practice agreed by all 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 Commissioner was asked to rule on whether the practice of unsolicited direct marketing by email or SMS to a former customer of a mobile telephone operator after the end of the Prohibition Period would be lawful.

Following the end of the Prohibition Period, the provisions of the Electronic Communications Regulations[11] become particularly relevant. Note that in the Regulations "electronic mail" is taken to include SMS. Regulation 20 states that:

[11] The European Communities (Implementation of Privacy Directive) (Guernsey) Ordinance, 2004; The European Communities (Implementation of Council Directive on Privacy and Electronic Communications) (Sark) Ordinance, 2004; The European Communities (Implementation of Council Directive on Privacy and Electronic Communications) (Alderney) Ordinance, 2009.

"20. (1) This section applies to the transmission of unsolicited communications by means of electronic mail to individual subscribers.

(2) Except in the circumstances referred to in subsection (3), a person shall neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified the sender that he consents for the time being to such communications being sent by, or at the instigation of, the sender.

(3) A person may send or instigate the sending of electronic mail for the purposes of direct marketing where -

(a) that person has obtained the contact details of the recipient of that electronic mail in the course of the sale or negotiations for the sale of a product or service to that recipient;

(b) the direct marketing is in respect of that person's similar products and services only; and

(c) the recipient has been given a simple means of refusing (free of charge except for the costs of the transmission of the refusal) the use of his contact details for the purposes of such direct marketing at the time that the details were initially collected and where he did not initially refuse the use of the details, at the time of each subsequent communication.

(4) A subscriber shall not permit his line to be used in contravention of subsection (2)."

The Commissioner interpreted that section to mean that a mobile telephone operator may send marketing messages to an existing customer who has consented to, and not subsequently opted out of, the receipt of such messages.

In the case of a former customer, the Commissioner interpreted the Regulations to mean that any consent, which may have been obtained for direct marketing purposes whilst the individual was a customer, should be considered to have lapsed at the end of the Prohibition Period.

Accordingly, he 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.

Case Study 3 – Inappropriate subject access requests

(a) Medical Records

A family had moved from Guernsey to the United Kingdom (UK) and the National Health Service asked the parents for the vaccination record of their child. The parents, under the Data Protection Law (the Law), requested a copy of their child's medical records from a local medical practice. It was their intention to give this copy to the new GP in the UK.

In response to the request they were provided with a printout summary of the child's medical history which included an account of all immunisations which the child had received.

The parents complained to the Commissioner that the local medical practice had not provided the complete medical record and so had not abided by section 7 of the Law which gives individuals or their representatives the right of access to their personal information.

Under section 7(1)(c) of the Law an individual is entitled to have communicated to him in an intelligible form "the information constituting any personal data of which that individual is the data subject". This means access to information but not necessarily the right to obtain copies of all documents which may contain that information.

The parents had received a printout which summarised the medical history and they admitted that this summary was comprehensive and adequate enough for their child's present needs. They accepted that the medical practice had responded adequately to the subject access request. However it is preferable that the new GP should have the complete medical record and this is best achieved by GPs transferring records between themselves provided they do so with the necessary consent.

This is a case which illustrates that using the subject access route is not always the most appropriate way for individuals to obtain the information which is most relevant to their needs.

(b) Criminal Records

An individual was asked by a prospective employer to provide a copy of his criminal record. This individual made a subject access request to the police and subsequently received a report on offences which were committed a long time ago and which were now considered as spent. He complained to the Data Protection Office that the police had provided irrelevant and excessive information.

He was advised that the police had responded correctly to his request in that they had provided the information which constituted his personal data and they had provided that information in an intelligible form. He was further advised that if the new employer only needed information about unspent convictions then a request for a Basic Police Disclosure should have been made instead of a subject access request. He subsequently requested a Basic Police Disclosure and obtained the information which the employer actually required.

The Commissioner would advise that individuals give careful consideration to the information they actually need for which specific purposes before making subject access requests.

Case Study 4 – Subject access requests for the purpose of litigation

The right of subject access is enshrined within the European Directive 95/46/EC, "...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..."

The Directive further provides that subject access "shall be without constraint and at reasonable intervals and without excessive delay or expense"

Therefore the rationale behind subject access is that individuals must be able to verify if the data processed about them are accurate and that the processing of the data is lawful. This is particularly relevant to the consideration of the processing of health data.

Typically, when individuals request access to their health data and / or ask to have particular treatments explained to them this is done within the health professional / patient relationship.

However, it was brought to the Commissioner's attention that the medical practices on the island and the Health and Social Services Department frequently receive subject access requests from members of the legal profession on behalf of their clients. These requests are typically in pursuit of litigation.

The practices reported that these requests can prove to be quite onerous in that all the information recorded on a patient is requested rather than just specific limited information. Therefore a lot of time and effort is expended to meet the request and only £10, the statutory maximum subject access fee, can be charged for all the effort taken.

As previously stated, the primary reason for giving an individual the right to access his personal data should be so he can verify its accuracy and whether or not the data are processed lawfully. The pursuit of litigation would not be in keeping with the purposes stated in the Directive. This was reinforced in the Appeal Court judgement of Durant v. Financial Services Authority[12] when Auld LJ ruled that the subject access route should not be used for the purpose of pursuing litigation, especially litigation against third parties. The Judge ruled that discovery of documents should be the preferred method to be used.

Under subject access a person may only access his own personal information but when discovery is used non-personal information may also be accessed and a response can be requested in a shorter period of time. There may therefore be an advantage in taking the discovery route.

During 2009 the Commissioner issued a new guidance note entitled "Subject Access to Health Records" in which he explained the circumstances where the use of data protection legislation to obtain information for the purpose of litigation might be considered to be inappropriate.

[12] Durant v Financial Services Authority [2003] EWCA Civ 1746

Case Study 5 – Abandoned vehicles

A member of the public complained to the Commissioner that the Environment Department had unlawfully disclosed his name and address to the Housing Department. He further alleged that when he complained to Environment he was informed that Housing had accessed the information directly.

The individual had received a letter from Housing advising him that if he did not remove his motor vehicle from States owned land action would be taken to dispose of the vehicle and that he would be liable for the costs incurred. He went on to explain that he had sold the vehicle and so Environment should not have disclosed his personal details as he was no longer the registered owner of the vehicle. He claimed the new owner had taken possession of the vehicle three weeks before and he had sent notification of the change of ownership to Environment using the correct documentation.

If this complaint had substance it would mean that Environment had breached at least two data protection principles, i.e. the fourth principle by not keeping accurate and up to date records and the seventh principle by making an unauthorised disclosure and permitting another States department to directly access information.

The investigation revealed that Housing had not directly accessed the information but had requested it in writing on the grounds that the vehicle was "illegally parked". As an offence was alleged to have been committed Environment had not breached the seventh principle. Section 29 of the Law permits the disclosure of personal information for the prevention and detection of crime.

Environment also provided a copy of the "Notification of Change of Keeper of a Registered Motor Vehicle" which had been completed by the complainant. The form had been stamped as being received on the same day that the complainant had been contacted by Housing. However the log book had not been received by the Department. The complainant was therefore still regarded as the registered vehicle keeper and so the record was accurate. It was concluded that Environment had not breached the data protection principles.

Housing was then asked to clarify where the car was actually parked. The information had been obtained on the grounds that the car was "illegally parked". Illegal parking can only occur on public land yet the letter which the complainant received referred to States owned land. Housing confirmed that the vehicle was parked in a Housing Department car park on one of its Housing Estates; it was private land which had not been designated 'Terre L'Amende'.

As the vehicle had not been "illegally parked" Housing appeared to have obtained the information on a false ground. The Commissioner met with representatives from Housing, Environment and the Law Officers. Housing claimed that in obtaining information to deal with abandoned vehicles it was acting within its mandate of carrying out its public functions and therefore the obtaining and subsequent processing of the information was justified under paragraphs 5(c) and 5(d) of the Data Protection Law; abandoned vehicles could pose health and safety risks and the Department had a responsibility for health and safety on its estates.

Whilst the Commissioner understood this view he expressed concern that reliance on paragraphs 5(c) and 5(d) might become the norm for the disclosure of personal data between States Departments. He therefore recommended the Home Department to draft an Order under section 6(2) of the Data Protection Law that would legitimise the disclosure of personal data relating to a registered keeper of a vehicle which appears to have been abandoned. Such a provision would be of assistance not only to the Housing Department but to other States Departments as well as private landowners. The Home Department agreed to draft this Order.

The Commissioner stated that, until the Order comes into force, the Housing Department may continue to obtain information of vehicle keepers but must not do so on the ground of "illegal parking". It must also erect a limited number of appropriate worded signs at strategic points on its Housing Estates to inform drivers that it will take action against owners of abandoned vehicles. This is an obligation imposed by the first data protection principle that all processing must be fair and transparent. Even when the Order comes into force this obligation under the first principle must still be met.

Case Study 6 – Employment questionnaire

The following complaint was not upheld by the Commissioner, but on his recommendation, company procedures were revised.

An individual considered that his privacy was being invaded by his employer's requirement for him to complete a questionnaire. He complained that a lot of very sensitive personal information had to be provided on the form which he considered not to be necessary. The third data protection principle states that personal data must be relevant, adequate and not excessive for the purpose(s) for which it is processed.

The company informed the Commissioner that it is subject to the Food Safety Laws and so is required by the Environmental Health Department to implement Hazard & Critical Point (HACCP) Manuals in all divisions of its business. The questionnaire forms part of the employee health checks which are crucial to any HACCP / food safety manual. The complainant does handle food and so was asked to complete the questionnaire.

The form was intended to be used as a pre-employment questionnaire but as the HACCP manuals had just been implemented the company was advised that current employees should fill in the questionnaire to establish a commencement bench mark. This was explained to all employees and they were informed that they could speak to any of the Directors or the HACCP manager if they were uncomfortable about filling in any part of the form as no part of the form is compulsory for current employees.

On the recommendation of the Commissioner the company stated it would add a "non- applicable" column to the questionnaire which would improve the process of completion.

In addition, the employees would be assured that all information on the form would be accessed only by a nominated person within the company and that it would be subject to doctor / patient confidentiality. The company would act only on advice and directions from the medical examiner in consultation with the employee concerned.

INTERNATIONAL LIAISON

International Conference of Data Protection Authorities

The Commissioner and Assistant Commissioner joined over 1,000 delegates from over 50 countries who attended the 31st International Conference of Data Protection and Privacy Commissioners, which was hosted by the Spanish Data Protection authority and held in Madrid from 4th – 6th November 2009.

Data Protection Commissioners attending the conference during their official visit to the Lower Chamber of Parliament.

The conference comprised public sessions, parallel stream workshops and a closed meeting, which was restricted to Commissioners.

Full details of the conference are available on its website[13].

A major product of the conference was the "Madrid Resolution", which aims to define a common set of principles and rights that would guarantee the effective protection of privacy at an international level.

A copy of the press release about the Madrid Resolution is contained in Appendix B.

The 32nd Conference will be held in Jerusalem in October 2010.

[13] http://www.privacyconference2009.org

European Spring Conference

The Commissioner and Assistant Commissioner attended the annual spring conference of European commissioners, which was held from 23rd – 24th April 2009 in Edinburgh[14]. They also participated in a 'fringe' workshop organised by Privacy Law and Business, in their role as contributors to a survey about data breach legislation in Europe.

The conference centred around a discussion on the findings of the assessment of the effectiveness of the European Directive on Data Protection[15]. This had been undertaken by the Rand Corporation and had been commissioned by the UK Information Commissioner.

Detailed topics included:

- Do we need reforms at all?
- What outcomes should regulation achieve?
- The international context of regulation.

The conference issued a communiqué calling on all European States to ensure that the applicable standard of data protection is respected when concluding international agreements. In this respect the conference advocated including standard data protection clauses in those agreements.

The next European conference will be held in Prague in April, 2010.

International Working Group on Data Protection in Telecommunications

The Commissioner attended the two meetings of this International Working Group that were held in 2009.

The 45th meeting was held in Sofia on 12th and 13th March.

The 46th meeting was held in Berlin on 7th and 8th September.

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

- Vehicle Event Recorders;
- Processing of personal data for investigation of copyright offences;
- Deep Packet inspection;
- Proposed Charter of Digital Data Protection and Freedom of information;
- Privacy and email heritage;
- Privacy and Road pricing;
- Storage of SMS messages for Law enforcement;

[14] http://www.ico.gov.uk/springconference2009.aspx
[15] http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive_summary.pdf

- Social networking;
- Use of location information;
- Geospatial data;
- International standardisation.

The papers adopted by the Working Group are published on its website[16]. Many of the adopted papers are subsequently submitted to the annual International Conference as draft resolutions for debate during the closed session.

The 47th meeting of the Working Group will be held in Granada in the spring and the 48th meeting will be held in Berlin in the autumn.

British, Irish and Islands' Data Protection Authorities

The Commissioner and Assistant Commissioner joined 13 other representatives of the authorities from the UK, Ireland, Cyprus, Jersey, Isle of Man, Malta, Gibraltar and Bermuda at the "BIIDPA" meeting held on 23rd - 24th July 2008 in Dublin.

This meeting provided an opportunity to meet the newly appointed UK Information Commissioner, Christopher Graham.

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. The topics included:

- The Personal Information Protection Act being drafted in Bermuda, which is based largely on the Alberta legislation;
- the introduction of custodial sentences for criminal breaches of the legislation and the advent of civil penalties in the UK;
- notification of security breaches;
- naming of suspects in historic child abuse cases;
- whether blogs published by private individuals were covered by the special purposes and journalistic exemptions;
- legitimacy of use by employers of personal information disclosed on social networking sites;
- jurisdictional issues relating to disclosures of taxation data and passenger name records of travellers, specifically e-borders and its impact on the Common Travel Area;
- different approaches to Freedom of Information.

The delegates were updated on developments within the EU and discussed forthcoming issues to be raised at the international conference.

[16] www.berlin-privacy-group.org

Liaison with the UK Government

Two liaison meetings were held between the Crown Dependencies and Ministry of Justice officials, the first being in London on 21st January and the second in the Isle of Man on 14th October, 2009.

Topics included:

- custodial sentences and civil penalties;
- the EU Information Management strategy;
- the EU Data Protection Framework Decision (2008/977/JHA);
- the Article 31 inter-governmental committee;
- Council of Europe Convention on Access to Official documents;
- Council of Europe Convention 108 and its additional protocol, which has yet to be ratified by the UK.

Data Protection Roundtable

On 26th June 2009, the Commissioner joined a distinguished panel hosted in London by Field Fisher Waterhouse and Data Protection Law & Policy.

The discussion panel included the Chief Privacy Officer for the US Department of Homeland Security, The Data Protection consultant for the government of Bermuda and the Head of the Information Policy Division, Ministry of Justice.

The topic of the roundtable was: Privacy Practices in Government - UK and USA approaches compared.

Data Protection Forum

The Assistant Commissioner attended three meetings of the Data Protection Forum that were held in London during 2009; the topics covered in the meetings included:

- Updates from the Information Commissioner's Office;
- The Surveillance society - implications for human rights;
- 2008 Benchmarking survey;
- Managing information security around third party relationships;
- Cyber Crime and Cyber security;
- The role of standards – BS 10012;
- Fraud.

The Commissioner was invited to join a panel at the annual "Commissioners' Question Time" that was held on 1st September.

Other members of the panel were the Irish Data Protection Commissioner, the UK Deputy Commissioner and the Isle of Man Supervisor.

The Commissioner outlined the changes to the Law, in particular the provisions dealing with cross-border offences.

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 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[17]

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 one meeting 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. Progress in this area remains slow, since it normally requires international consensus, which is challenging to achieve.

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

OBJECTIVES FOR 2010

The primary objectives for 2010 encompass the following areas:-

- ***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 and complaints will be archived to electronic media.

  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 in September 2011.

  Discussions with the Home Department will commence in 2010 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	2009 £	2008 £
Data Protection Fees [1]	52,760	49,125
EXPENDITURE		
Rent[2]	13,030	15,526
Salaries and Allowances[3]	166,996	176,345
Travel and Subsistence	11,171	10,294
Furniture and Equipment[4]	17,940	12,761
Publications	2,623	3,075
Post, Stationery, Telephone	4,177	4,332
Heat Light, Cleaning	6,918	6,247
TOTAL EXPENDITURE	**£222,855**	**£228,580**
EXCESS OF EXPENDITURE OVER INCOME	**£170,095**	**£179,455**

NOTES

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

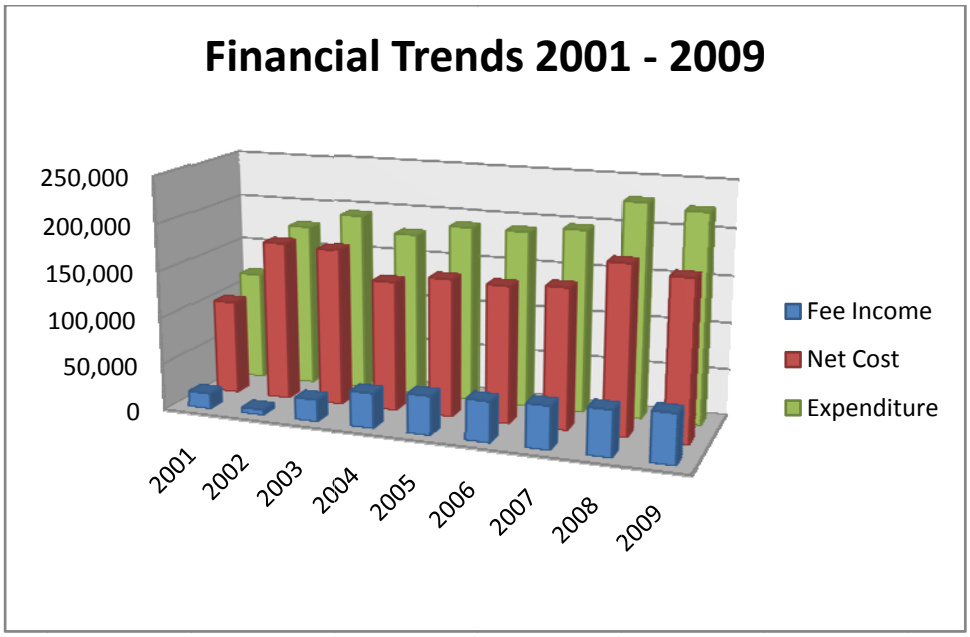
The cash received for notifications in 2009 was £54,460 (£50,750 in 2008) representing the 1,556 (1460) annual notifications and renewals that were processed during the year.

[2] The rent was reviewed upwards in 2009, but the December rent payment, being an advance payment, will be included in the accounts for 2010.

[3] This includes an amount of £7,210 (£25,520 in 2008) for consultancy fees.

[4] This includes the one-off migration costs for maintenance and hosting of the Notification website, which was transferred from Eduserv to Digimap during 2009.

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



Expenditure for 2009 fell by £5,625 (2.5%), primarily due to the fall in consultancy costs; these were exceptional in 2008 due to the investigation of the website security breach. However, increased costs of around £14,000 in consultancy and computer charges were incurred due to the unplanned need to migrate the Notification website.

Income from notification fees rose by £3,635 (6.9%) based on an unchanged notification fee of £35.

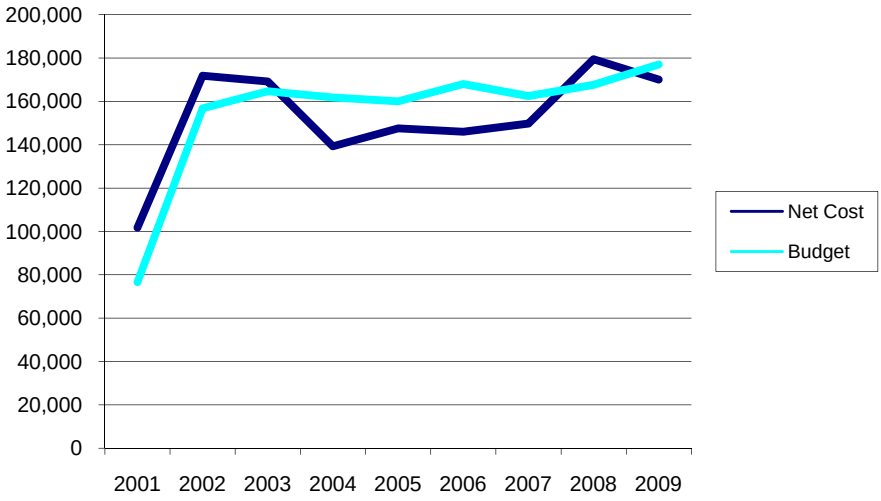
Hence, the net cost of the Office to the taxpayer fell by £9,360 (5.2%) from 2008 but was 13% above the figure for 2007.

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.

Particular effort will be made in 2010 to minimise expenditure and keep well within budget. Income is expected to rise, following the increase in Notification Fees from 1st March 2010, further reducing the net cost.

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, but returned to be within budget in 2009.

Net cost vs budget 2001 - 2009



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 2009.

Appendix A - *EU Consultation on the legal framework for the fundamental right to the protection of personal data.*

Response by the Data Protection Commissioner for the Bailiwick of Guernsey.

1. New **Challenges for personal data protection.**

1.1. The 1995 Directive (95/46/EC) was drafted within an environment where much processing of personal data was visibly concentrated in databanks of manual files or in stand-alone mainframe computers with integral electronic storage devices. Accordingly it was easy to identify a 'data controller', the location where personal data were processed and the relatively limited purposes for which those data were processed, whether manually, automatically or in some combination.

1.2. The 1995 Directive appeared primarily to be aimed at the protection of data to a uniform standard to facilitate the exchange of data between Member States in order to promote the operation of the internal market. It did not appear to be particularly concerned with data privacy *per se*.

1.3. The inadequacy of the 1995 Directive to deal with personal data within telecommunications networks was recognised within the 2002 Directive 2002/58/EC, which aimed to extend the protection, afforded by the 1995 Directive, to data in such networks and explicitly included data privacy in its objectives.

1.4. The commencement of the Lisbon treaty has enabled the extension of the data protection régime to third pillar activities and accordingly calls into question whether, for example, adequacy determinations may be applied to third pillar activities related to third countries in future.

1.5. In the interim, the relationship between the Data Protection Framework Decision and the 1995 Directive may need to be refined and clarified.

1.6. Any new legislative environment needs to viewed as having a long term effect such that it is able to cope not only with current challenges, but anticipated challenges over the next ten to twenty years in areas such as:

- The increasing capability of technology to process vast amounts of personal data;
- The increasingly distributed nature of both processing and data storage rendering the concept of the location of a controller or the location of processing at best indeterminate;
- The ubiquitous nature and extent of processing operations and the growth of mobile computing devices;
- The benefits to be derived from the exploitation of privacy enhancing technologies;
- The need to protect personal data from increasingly sophisticated attack and exploitation by organised criminals;

- The need to respect and enhance the privacy of individual law abiding members of society (i.e. the over-riding need to comply with the European Convention on Human Rights);
- The increasing pressure by governments and public sector agencies to collect, aggregate and share disparate personal information ostensibly to provide enhanced public services and fight serious organised crime;
- The need to integrate third pillar activities within a consistent legislative framework;
- The need to balance individual rights against societal benefit and the protection of society;
- The increasing tendency for large transnational corporations to collect, share, aggregate and exploit personal data obtained during the course of business transactions in diverse sectors;
- The need for more uniform standards of personal data processing to apply across the EEA;
- The need to recognise the extent to which alternative data protection and privacy standards in force in other countries and territories may offer adequate protection for the data of EU citizens;
- The need for effective enforcement regimes both within the EEA and throughout the world;
- The need for individual users of web-based services, such as social networking to be aware of the privacy implications of publishing personal data of themselves and others on the internet;
- The need for commercial and governmental organisations to be aware of and counter the risks of using web services such as cloud computing and similar developments in future;
- The fundamentally insecure nature of current computer operating systems and networking environments;
- The need for legislation to be as far as possible technology independent and future proof;
- The perceived need for higher standards of protection to be applied to higher risk areas such as:
    - existing categories of sensitive personal data;
    - financial data such as bank accounts and credit card information;
    - data processed by the public sector;
    - behavioural and profiling data such as those collected from users of web services.

2. Does the current legal framework meet these challenges?

2.1 There could be a greater emphasis on data privacy rather than merely data protection;

2.2 there appears to be divergence between Member States over some of the basic definitions, such as the interpretation of what constitutes personal data;

2.3 notification and registration requirements in Member States appear to differ;

2.4 sanctions and penalties vary widely within the EU;

2.5 the current legal framework does not appear to facilitate or mandate the use of technological means for privacy protection (e.g. encryption, PET);

2.6 the process of obtaining adequacy status appears to be bureaucratic, time consuming and ineffective;

2.7 the current legal framework does not distinguish between large scale processing of personal data in a third country and processing on an end-users PC, where that PC may be in a third country, hence:

- Session cookies, which can be essential to the correct operation of web services; and
- Persistent cookies which in many cases are set to facilitate use by a returning customer;

appear to be governed by the same rules as those applied to wholesale data export and processing in a third country by a data processor or "co-controller";

2.8 the provisions on applicable law appear unenforceable; it is often impractical to determine where processing takes place, and the identity of 'the controller' may be indeterminate;

2.9 even though a third country may be deemed adequate, the Directive does not recognise the applicability of its national law;

2.10 the technical difference between transferring data to a third country and using equipment in a third country for processing is often unclear, but different rules apply;

2.11 it could be made clearer that the third country provisions are primarily meant to protect the personal data of EU citizens, rather than all data, processed in those countries;

2.12 it appears that the protection afforded by legislation flowing from Directive 2002/58/EC may not adequately protect online purchasers of goods and services who may unknowingly agree to unfavourable terms and conditions buried in privacy statements;

2.13 The distinction between personal and family processing and public processing is blurred with the advent of blogs and social networks, where personal data may be disclosed without consent within a 'family' context.

3. What future action would be needed to address the identified challenges?

Potential areas of action are to:

3.1. Ensure a closer approximation between member states in their transposition of the Directive into national law;

3.2. Provide uniform rules covering personal data protection, privacy in communications and third pillar processing activities;

3.3. Provide a clear set of minimum standards to be applied to the processing of EU citizens' personal data in third countries;

3.4. Simplify the bureaucratic process for the determination of the adequacy of a third country;

3.5. Build in a requirement for mandatory privacy impact assessment into all public sector project planning;

3.6. Reinforce the role of the individual as the owner of his personal data;

3.7. Enhance the protection afforded to "online consumers";

3.8. Consider whether the reporting of significant breaches of the security of personal data should be mandatory;

3.9. Adopt a more risk-based approach, by for example drawing a clear distinction between rules which should apply to processing by:

- large multi-national corporations;
- government and law enforcement agencies;
- smaller national enterprises;
- Individuals (including processing on personal mobile devices)

3.10. Enhance the role of the Article 29 Working Party in setting and enforcing common standards across the EU;

3.11. Enhance the role of the EDPS for example in the approval of public sector processing.

Efforts should be made to reach agreement with other countries and groupings such as APEC and standardisation bodies such as ISO with the aim of agreeing the minimum standards that should apply to the processing of personal data in international trade and commerce.

International agreement should aim to reduce the omnibus processing of personal data by law enforcement and governmental bodies without consent. A prime example appears to be airline PNR processing, where the benefits of such processing are by no means apparent.

The scope and range of personal data and the devices on which data are processed nowadays differ dramatically from those which were in place when the Directive was drafted.

A major challenge will be to craft a legislative environment which can cope with the current and anticipated range of software and hardware technologies and the ever increasing scope of personal data processing that will be employed over the next generation.

Appendix B - *The Madrid Resolution*

Data protection authorities from over 50 countries approve the "Madrid Resolution" on international privacy standards

• The Madrid Resolution brings together all the multiple approaches possible in the protection of this right, integrating legislation from all five continents.• It constitutes the basis for the drawing up of a future universally binding Agreement.
• The approved resolution includes a series of principles, rights and obligations that any privacy protection legal system must strive to achieve.
• One of the most relevant chapters of the document is the one that refers to proactive measures, whereby States are encouraged to promote a better compliance with the laws applicable on data protection matters, and the need to establish authorities to guarantee and supervise the rights of citizens.
• A group comprised of top executives from 10 large multinational companies has signed a declaration of support for the adopted proposal.

The Joint Proposal on International Standards for the Protection of Privacy has been positively welcomed by Protection Authorities of 50 countries gathered within the framework of the 31st International Conference of Data Protection and Privacy, through the adoption of the "Madrid Resolution".
This document, approved at the closed session attended by the data protection authorities, constitutes the base for the development of an internationally binding tool that will contribute to a greater protection of the individual rights and freedoms at a global level.
The proposal, which has been elaborated during the past year **under the coordination of the Spanish Data Protection Agency** (AEPD), has resulted in a document that tries to include the **multiple approaches possible in the protection of this right, integrating legislation from all five continents**.
According to Artemi Rallo, these standards are a proposal of international minimums, which include a set of principles and rights that will allow the achievement of a greater degree of international consensus and that will serve as reference for those countries that do not have a legal and institutional structure for data protection. Even though the approved resolution is not directly binding at an international level, Artemi Rallo has pointed out that this document **will have "immediate value" as a reference tool and, moreover, as a starting point** for those countries that still lack legislation on the matter, and for the corporate world and international companies.
According to the director of the AEPD, the Madrid Resolution will, thus, become a **"soft law" tool, widely demanded** mainly by international companies, in order to respect the minimum privacy needs of citizens worldwide.
In this sense, the approved resolution entrusts upon the AEPD and the Authority in charge of hosting the 32nd International Privacy Conference the coordination of a contact group for the promotion and broadcasting of the joint proposal, as the basis for future work on the elaboration of a universally binding Agreement.

Content of the resolution: articulation and basic principles

The proposal on international standards includes a series of principles, rights and obligations that any privacy protection legal system must strive to achieve.

The text's purpose is to **define a series of principles and rights** that guarantee the effective protection of privacy at an international level, as well as to ease the **international flow of personal data**, essential in a globalized world. Among the basic principles that must govern the use of personal data, and which have inspired the document, we find those of **loyalty, legality, proportionality, quality, transparency and responsibility**; all of them are common to the different existing legal texts in the various regulations on the matter and enjoy wide consensus in their corresponding geographical, economic or legal application environments.
The Joint Proposal of International Privacy Standards includes, in addition, in its articulation, the need for the existence of supervisory authorities, and for the different states to cooperate and coordinate their activities. Furthermore, the set of rights such as **access, rectification, cancellation and objection** and the way in which they can be exercised. It also includes obligations such as **security of personal data**, through those measures that are considered appropriate in each case, or **confidentiality**, which affects the controller as well as anyone who participates in any of the stages in which personal data is managed.
In addition, in includes the requirements that must be met for the legal collection, preservation, use, revelation or erasure of personal data, such as, for example, the prior obtaining of the free, unequivocal and informed consent from the person providing the data.
The document also defines sensitive data as that data that affects the most intimate side of a person or whose misuse can originate an illegal or arbitrary discrimination, or may imply a severe risk for the said person.
On the other hand, the text recalls that, as a general rule, **international personal data transfers** may be performed when the State to which the data is transferred offers, at least, the level of protection foreseen in the document; or when whoever wants to transfer the data can guarantee that the addressee will offer the required level of protection, for example, through appropriate contractual clauses.
One of the most relevant chapters of the document is the one that refers to **pro-active measures**, which encourages States to **promote a better compliance with the applicable laws regarding data protection matters**, through instruments such as the establishment of procedures aimed at the prevention and detection of offences, or the periodic offering of awareness, education and training programs.

Declaration of corporate support and the Council of Europe
A group of 10 large companies (Oracle, Walt Disney, Accenture, Microsoft, Google, Intel, Procter & Gamble, General Electric, IBM and Hewlett-Packard) has signed a declaration in which they proudly welcome the initiative from the 31st International Conference for exploring frameworks to achieve an improved global coordination of the different privacy policies.
In this declaration, the signing companies encourage Data Protection and Privacy Authorities to continue insisting and collaborating in the development of transparent systems that will allow the taking on of responsibilities and that will provide accurate information to the citizen, granting him/her the power to decide.
Also, recently, the group on data protection from the Council of Europe, in a meeting celebrated just a few months ago, decided to support the initiative approved by the data protection authorities to adopt these international privacy standards and, with this, contribute to expand and promote a worldwide framework for the protection of privacy.

Necessary and urgent standards

The mission of approving this Joint Proposal was the **main priority of this 31st International Conference,** a result of the task entrusted and included within the unanimous resolution adopted by the prior Conference celebrated in Strasbourg. This resolution stated the urgent need to protect our privacy in a world without borders and to attain a joint proposal for the establishment of international standards on privacy and data protection.

In consonance with this mandate, the AEPD established a Working Group which has been working since then to elaborate this Joint Proposal, assuming that all these common principles and approaches contribute valuable elements to the defence and promotion of privacy and personal information, with the aim of extending those criteria and incorporating applicable solutions.

Appendix C

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 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.gov.gg/dataprotection
Telephone: +44 (0) 1481 742074
Fax: +44 (0) 1481 742077