BAILIWICK OF GUERNSEY

DATA PROTECTION COMMISSIONER
REPORT FOR 2007

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: Delegates attending the international conference: "Respecting Privacy in Global Networks", held on 11th April, 2007 at St. James Conference and Assembly Hall, St. Peter Port, Guernsey.

CONTENTS

FOREWORD

I am pleased to present my seventh annual report to the States of Guernsey, covering the calendar year 2007.

The major breach of security at HM Revenue and Customs ("HMRC"), resulting in the loss of computer disks containing personal data of 25 million recipients of child benefit, served to highlight the importance of the security of personal data held by public bodies.

Following that breach I wrote to the Chief Minister proposing that government departments should conduct reviews of their processes to reassure the public that such a breach could not occur here.

There was a positive response with many departments deciding to institute improved data security measures and some considering conducting privacy impact assessments of their major IT systems.

The highlight of the year was undoubtedly the 41st meeting of the International Working Group on Data Protection in Telecommunications, which was held at Castle Cornet. This meeting in April was preceded by a highly successful public conference at St. James, in which many of the members of the Working Group participated, and which served to promote Data Protection to a much wider audience from across the Channel Islands.

In July, Les Cotils was the venue for the annual meeting of the Data Protection authorities from the UK, Ireland, Cyprus, Gibraltar, the Isle of Man and Jersey. Active collaboration with our colleagues in other jurisdictions such as these is essential to the effective operation of our Offices.

One particular matter that was discussed at that meeting was the disclosure by UK banks of offshore account information to HMRC, a matter which had been the subject of numerous complaints to many of the participant authorities; subsequently, the Information Commissioner wrote to HMRC, proposing changes to the Special Orders under which the information had been demanded.

My Office continues to receive a steady stream of complaints from individuals that require investigation, but also many requests from organisations for advice, guidance or the delivery of short training courses, which we are happy to provide.

Data Protection Commissioner, March 2008.

DATA PROTECTION ISSUES

Amendments to the Law

In the report for 2006, it was anticipated that the amendments to the Law that had been approved by the States on 27th September 2006 might be enacted during 2007[1]. Unfortunately it appears that there was insufficient legislative drafting time available, but it is hoped that these amendments will come into force during 2008.

HM Revenue & Customs

HMRC obtained warrants requiring the disclosure by UK banks of any information that they held relating to the banking details of the holders of offshore bank accounts. This was ostensibly to discover tax avoidance on interest by UK resident holders of offshore accounts.

The Commissioner received complaints from local residents that their details were disclosed by the banks even though they believed that they were not subject to tax in the UK. Similar complaints were received by the Commissioners in other offshore jurisdictions.

An investigation revealed that the disclosures had not been made by locally based banks, but by their UK partners, which had been processing certain aspects of the information relating to accounts held offshore.

It was evident that the UK banks had appealed the Orders but that the appeals had been rejected on the premise that information was being sought in order to recover substantial amounts of tax from individuals resident in the UK who held accounts offshore.

The complaints were passed to the Information Commissioner, who wrote to HMRC proposing changes to the Special Orders under which the information had been demanded in order to limit disclosure to those persons who were liable to pay UK tax; at the time of writing this report, the matter remained under discussion.

This action by HMRC has led to a re-evaluation by the locally based banks of their policy of undertaking certain processing activities relating to offshore accounts on the UK mainland.

It was evident that many of the customers of these banks were unaware that their financial information was being processed in the UK and accordingly the Commissioner is of the view that compliance with the fair processing principle requires more transparency by the banks as to the location of their processing activities.

[1] Billet d'État XVI, September 2006 p. 1660

Social networking

There has been an explosive rise recently in the use of social networking sites on the Internet, especially by younger people.

These sites provide a powerful opportunity for individuals to share information between friends and acquaintances, but equally can lead to unintended consequences for those who may not appreciate the limited privacy features of the site they are using.

One of the consequences of the availability of ostensibly free storage and dissemination may be a loss of ownership and control. This can mean that information, once uploaded cannot be deleted and furthermore, information intended for sharing just amongst friends may end up being accessible to everyone. Users of the sites may find themselves the targets of unwanted advertising related to the content that they have stored or accessed.

Furthermore, the information uploaded by one individual may in fact relate to others whose permission was not obtained for its disclosure. There is also evidence that social networking can be used by some people for harassment and bullying.

The adverse consequences may be, for example, that employers see embarrassing incidents about their employees or applicants for employment, thereby compromising their employability; or that identity fraudsters are able to obtain sufficient information about individuals to enable them to exploit their identities for unlawful purposes.

In response to these concerns, the Information Commissioner published guidance on his website[2] to highlight the threats and to give advice on how to counter them.

The Commissioner recognises that in the vast majority of cases social networking performs a useful function, which is considered by many people to be of value, but urges all participants to exercise caution and endorses the advice given by the Information Commissioner's Office, as detailed below.

[2] www.ico.gov.uk/youngpeople

The "top tips" from the Information Commissioner are:

- **A blog is for life** – remember you risk leaving a permanent electronic footprint. If you don't think you'll want it to exist somewhere in 10 years time, don't post it
- **Privacy is precious** – choose sites that give you plenty of control over who can find your profile and how much information they can see. Read privacy policies and understand how sites will use your details
- **Personal safety first** – don't allow people to work out your 'real life' location e.g. your place and hours of work. Your personal safety offline could be affected by what you tell people online
- **Password protected** – change your passwords regularly, don't use obvious words like your pet's name and don't use the same passwords on social networking sites as you do for things like internet banking
- **Address aware** – use a separate email address for social networking and one that doesn't give your year of birth or ideally, your full name
- **Reputation is everything** – what seems funny to you and your friends now might be not be to your teachers, university admissions tutor or prospective employer – or to you in years to come

The Surveillance Society

In November, the Information Commissioner's office published the results of a research project that had been undertaken to explore and understand public awareness and perceptions of the various forms of surveillance in society.

Broadly speaking, the majority of the research sample was not unduly worried about 'pure' surveillance or data gathering and some people thought that data collection by the security services could go even further (e.g. compulsory fingerprint/DNA databases) if this would bring about a safer society.

Much of the research was conducted during October, prior to the loss of data by HMRC, and at that time the spontaneous concern was largely

confined to the activities of commercial organisations and to a fear of ID fraud.

Many respondents thought that the risks to their privacy were greater as a result of the trading of personal data within the private sector than from data sharing between government departments, although a minority expressed concern about the drift towards increasing state control of personal information.

The research report concluded that there was little doubt that, *"despite widespread acceptance of the status quo, any future surveillance or data 'disaster' will cause more citizens to wonder why 'nothing was done to prevent it'."*

In November, the Information Commissioner presented evidence to the House of Lords Select Committee on the Constitution, which was examining the subject of Surveillance and Data Collection. The Information Commissioner told the Members of the Select Committee that he was recommending a strengthening of the Law to introduce a criminal offence for those who recklessly flout the data protection principles with a serious consequence.

Notification of Security Breaches

A number of countries have enacted, or are considering the enactment of, legislation requiring organisations to report security breaches involving the loss of personal data either to a regulator or to the individuals affected.

In the United States, 40 of the states have passed security breach notification laws, resulting in 441 security breaches being publicly reported in 2007. 40 states have also passed "credit freeze" laws, whereby individuals can prevent anyone (including themselves) taking out a loan, mortgage or applying for new credit in their name.

The European Commission has proposed that security breaches involving telecommunications data should be notified.

It appears that the UK is considering the enactment of legislation that would require the disclosure of any security breach that had a real and substantial risk of causing damage or distress to individuals.

The Commissioner will continue to monitor the situation and advise the States should he consider it advisable to enact any similar legislation within the Bailiwick.

Privacy Impact Assessment

In December, the Information Commissioner launched an interactive handbook on Privacy Impact Assessment (PIA) in the belief that it would: *"prove to be a dynamic risk-assessment tool for new projects that would minimise customers' privacy concerns or avoid litigation".*

The PIA approach has been widely used in other countries, such as the United States, Canada, Australia and New Zealand, but is a relatively new concept in Europe.

The aim of a PIA should be to allow the assessment of a project's privacy risks from the outset and should benefit an organisation by identifying privacy risks before they happen.

The Government Business Unit alerted States' departments to the existence of the handbook and encouraged its use for any new information system project involving the processing of a significant amount of personal data.

PIA is of equivalent benefit to both the public and private sectors, and the Data Protection Commissioner's Office would be pleased to assist any organisation that was considering using the technique.

The PIA handbook includes numerous hyperlinks and is best used online in an interactive way; the handbook may be downloaded from the Information Commissioner's website[3] or a copy on CD may be obtained on request from the Commissioner's Office.

[3] http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/1-intro.html

NOTIFICATION

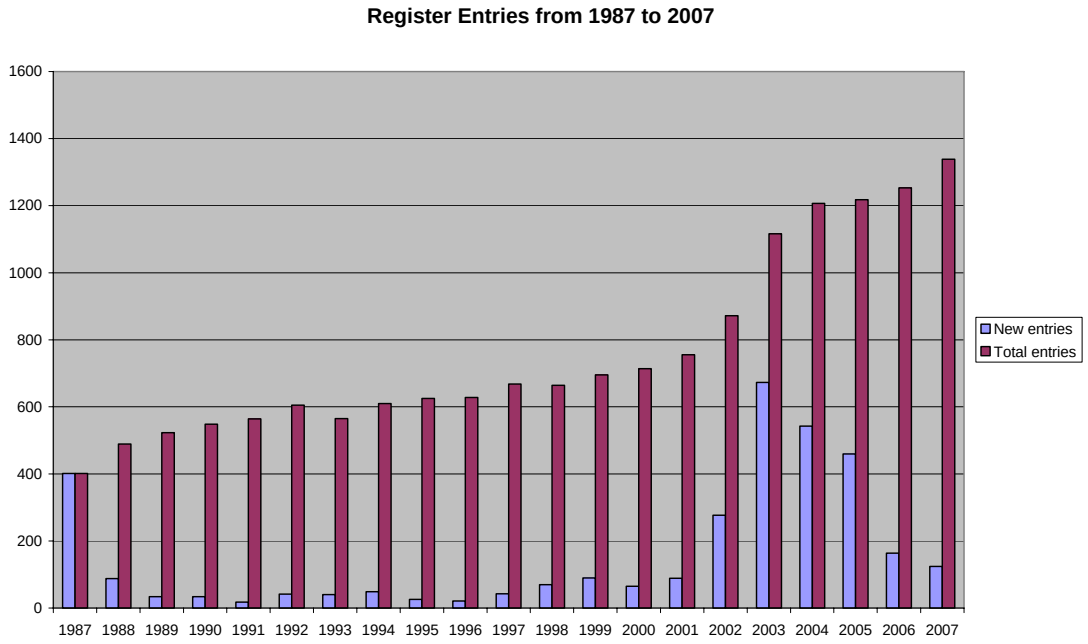
Section 17 of the Law requires Data Controllers to "Notify" the Commissioner of their processing of personal data. This Notification is on an annually renewable basis and covers all processing that is not exempt.

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

The annual fee for Notification remained at £35 throughout the year, as the legislation that had been passed in 2006 increasing the fee to £50 was not enacted during 2007. This meant that the anticipated increase in revenue did not happen.

Register Entries

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



By the end of December 2007, there were 1338 Notifications on the register, compared with 1253 at the end of 2006.

There were 158 new Notifications and 54 closures during 2007 - a net increase of 104, (compared with 164 new and 65 closures in 2006 - a net increase of 99).

Towards the end of the year, a campaign was launched to identify any organisations that had failed to Notify. The last time this had been done was in 2003 and it was felt that significant changes may have occurred in the interim. As a direct result of this campaign, a further 16 Notifications requests were received in December.

A new multi-function document production system was purchased to replace the aging photocopier and it was possible to exploit its scanning capability to capture the historical documentation associated with closed notifications.

By the end of the year almost all of the information associated with the closed Notifications had been scanned, enabling the manual documentation to be destroyed. Trials using computer desktop search tools have established that it is feasible to locate information relating to closed Notifications by searching the scanned image store.

It is planned to build on this experience by commencing a programme of scanning all current Notification data during 2008, possibly using more sophisticated document management software, such that ultimately all manual Notification records may be eliminated.

Internet Statistics

The Notification process may be completed online at the Notification site[4].

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

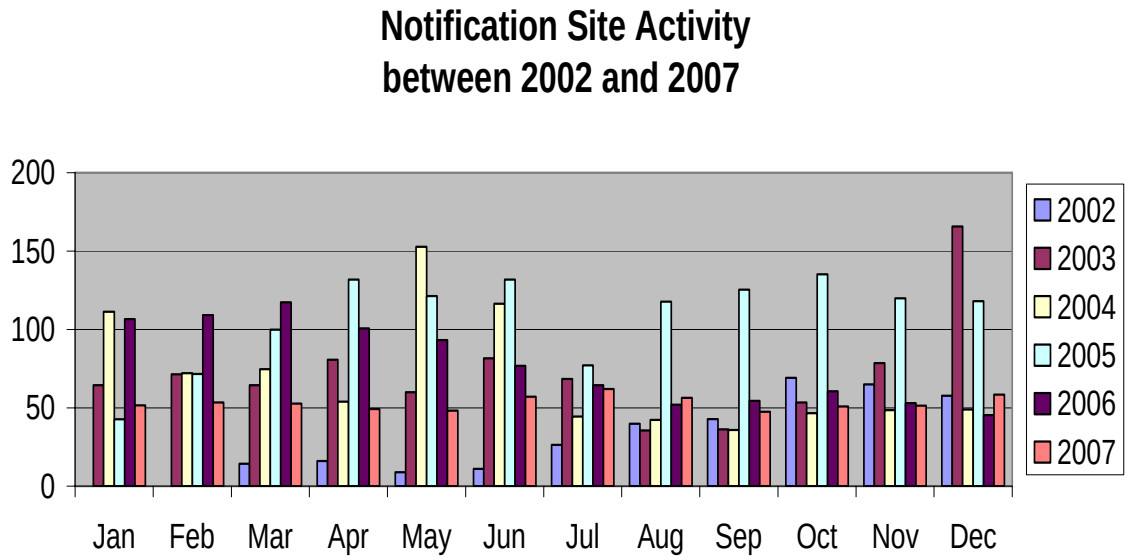
Statistics gathered over the past three years by the hosting service Eduserv show that approximately 38% of the Notification site accesses were for downloads of manuals and information, 20% for administration purposes and the remainder (42%) for online notification activities and enquiries.

The chart below shows the variation in the average daily activity on the online Notification site between the commencement of Notification in 2002 and December 2007; the vertical axis representing the average daily rate of successful requests for pages of data from the site each month.

The variations in activity generally correspond with variations in the volume of new Notifications and renewals that are dealt with each month

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

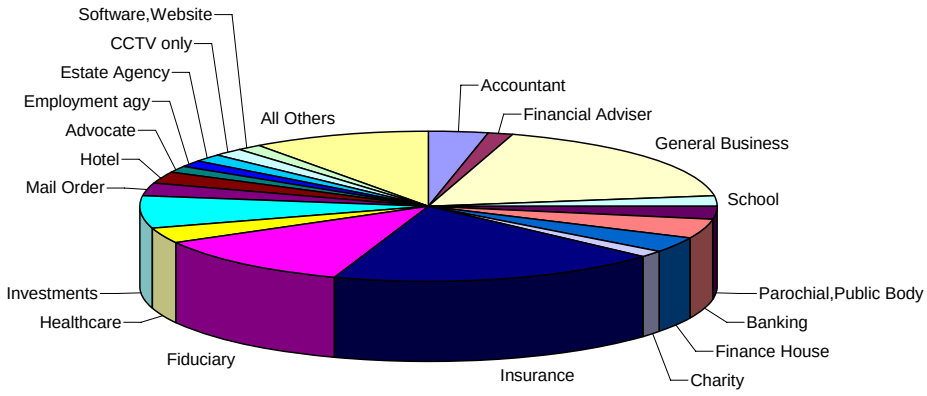
and have stabilised at a level of between 40 and 100 page requests per day over the past two years.



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.

Notifications by sector in 2007



The chart represents the breakdown of notification templates for 2007 by industry sector.

A General Business template was used by 243 Notifications (19%), with the remaining proportions being: Insurance (20%), Fiduciary (12%), Investments (7%), Banking (5%), Healthcare, Accountant and Finance House (all 4%), Mail Order, Hotel and Parochial/Public body (all 3%), with six classifications [Charity, Advocate, Employment Agency, Estate Agency, CCTV only and Software/website development] being between 1.5% and 2.5% and 'All Others' [27 classifications] collectively amounting to 11%.

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 remained at 39, (3% of the total).

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

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

It is planned to publish the exempt list on the Commissioner's website during 2008.

Payment and communications methods

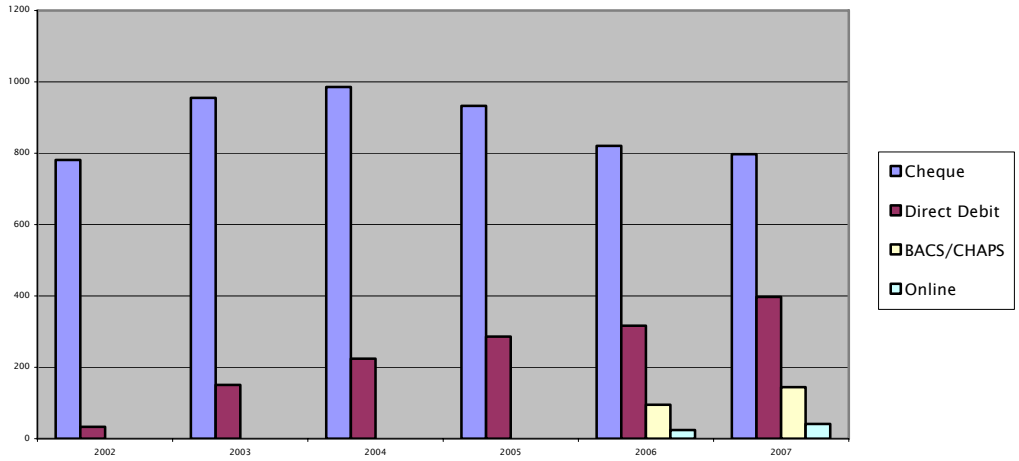
Renewal reminders advised data controllers of the introduction of alternative means for the payment of fees.

The number paying by these various means in 2007 was as follows:

Payment methods for Data Protection fees

Cheque: 786 (57.5%) Online: 41 (3%) BACS/CHAPS: 144 (10%)
Direct Debit: 397 (30%) Cash: 4 (0.3%)

Payment methods 2002 to 2007



In 2005 and 2006, 286 (23%) and 317 (26%) of the fees had been paid by annual Direct Debit, so this method of payment continued to show an increase. BACS had accounted for 95 (8%) and Online payment for 24 (3%) in 2006, so it can be seen that these methods are also increasing in popularity at the expense of cheque payment.

1146 organisations (86%) provided an email address for communication purposes, compared with 1069 (85%) in 2006; this was used for the issue of automatic renewal reminders to those who did not renew by Direct Debit; of those, 229 required a second reminder to be sent by post. Second reminders were also issued to 16 organisations whose first reminder had been sent by post. It was necessary to resort to final reminders in 34 cases and this resulted in some payments being overdue.

It appears that some data controllers do habitually ignore final reminders resulting in the need for follow-up action. In 2007 two police cautions

were administered to data controllers who failed to renew their Notifications without good cause. A significant amount of administrative time is spent on pursuing late payers and it is recommended that a financial penalty should be imposed in the case of those who are late in renewing their notifications.

The most common reason for the issue of second and final reminders was that the data controller's address or the email address of the administrative contact had changed since Notification. Data controllers are reminded that it is an offence for an organisation to fail to keep its registration particulars up to date.

Nevertheless, the use of automated email reminders and Direct Debits continued to reduce substantially the administrative effort involved in the Notification process.

Security Statements

Part 2 of the Notification Form includes a security statement, in which data controllers are required to answer a number of questions related to their information security policy and provisions; the answers given were as follows, with the corresponding figures for 2006 in brackets:

Security Survey Answers

Do your security provisions include:	YES	2007 (2006)
Adopting an information security policy?		87% (86%)
Taking steps to control physical security?		93% (94%)
Putting in place controls on the access to information?		90% (90%)
Establishing a business continuity plan?		90% (89%)
Training staff on security procedures?		85% (83%)
Detecting and investigating breaches of security?		87% (85%)
Adopting British Standard 7799 (ISO 9001)?		13% (12%)

These answers are broadly similar to those in 2006 and show that, in general, security is taken seriously by the overwhelming majority of organisations, and that increasing attention is being given to staff training and to the detection and investigation of breaches.

STAFFING AND STAFF DEVELOPMENT

Since its inception, the Office of the Data Protection Commissioner has comprised just three people: the Commissioner and Assistant Commissioner, both of whom work full time and the Personal Assistant to the Commissioner, who works part-time.

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

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

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

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

In 2007, the use of external consultancy was limited to the provision of expert assistance in the detailed planning and realisation of the Conference and the Working Group meeting and a small amount of legal advice from Pinsent Masons.

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 and relevant conferences and other forms of personal development.

The Commissioner 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.

The Assistant Commissioner has attended GTA seminars, participated in the UK Data Protection Forum and continued her legal studies with the Open University.

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 2007 included the following activities:-

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

Organising a public conference

Over 150 delegates attended the Channel Island conference: "Respecting Privacy in Global Networks", which was organised by the Commissioner to coincide with the 41st meeting of the International Working Group on Data Protection in Telecommunications, and was held at St. James on 11 April 2007.

The Conference was sponsored as a Golden Jubilee event by the Guernsey Section of the British Computer Society, and additional Channel Island sponsorship was received from law firm Carey Olsen and telecommunications company Newtel Solutions Limited. Orchard Events provided a complete organisation and management service to ensure the smooth running of the conference.

The delegate list was enhanced by the presence in the island of over 40 members of the International Working Group on Data Protection in Telecommunications, which was meeting in the British Isles for the first time in its 24-year history.

Some of the speakers were members of the Working Group, whilst others were members of the BCS Information Privacy Expert Panel.

In opening the conference, the Commissioner, who is a member both of the Working Group and the Expert Panel, drew a parallel between the Golden Jubilees of the BCS and the European Union. He postulated that it was primarily the convergence between computers and communications over the past 50 years which had facilitated the development of large multi-lingual and multi-cultural societies, such as the EU.

However, he warned that technology has the potential for harm as well as good. Much of the information circulating on global networks comprises

personal data and without adequate security measures, the confidentiality of such information might be compromised.

Guernsey's Commerce and Employment Minister, Deputy Stuart Falla MBE, welcomed the delegates and spoke of the crucial role of global communication networks in the success of the local economy.

He emphasised that the protection of data online was becoming increasingly important in a community such as Guernsey where the economy relied heavily on financial services and was home to so many international financial transactions each day. However, global networks could be exploited by criminals and it was important to balance the need to disclose information to the law enforcement authorities to fight crime against the need to respect individual privacy.

Dr Alexander Dix, Chairman of the International Working Group and Data Protection and Freedom of Information Commissioner for the State of Berlin, gave the key note address.

He posed the question: *"Has privacy come to an end with the arrival of the Internet?"* and set the tone for the day by flagging up many issues about the threat to privacy from global networks and the rise of the Internet.

Dr Dix recalled that the Working Group had first warned about the threat to privacy on the Internet in 1996 and had been campaigning over the following nine years in an attempt to rectify this. He contrasted the off-line world, where privacy was recognised as a right, with the online world, where it was under threat. *"More and more activities are taking place online, such as communicating, canvassing, expressing political opinions, voting, buying, banking and playing"* he said, *"… but the Internet is an inherently insecure environment and people tend to forget that".*

He warned that there were technical options that allowed for ubiquitous and unprecedented surveillance and he observed that the law

enforcement agencies wanted to exploit these surveillance techniques and were actively doing so.

Without inbuilt privacy protection, the long term success of global networks would be undermined, he told the audience.

Dr Dix closed by recalling comments made by Bill Gates in March 2007: *"… historically we've essentially relied on incompetence to protect our privacy, but this will no longer suffice. It would be a strong milestone to have an all-inclusive uniform privacy law that would give consumers control over their personal information. This would increase their confidence in providing information to legitimate organisations."*

Advocate Mark Dunster, Partner at Carey Olsen, one of the joint sponsors of the conference, offered some practical examples of how the data protection laws could be perceived to come into conflict with the requirements of business and Ben Bunn, Senior Systems Engineer with Broadsoft, a firm which works closely with the other local sponsor, Newtel Solutions, examined privacy threats to the development of internet telephony.

Susan McDonald Cooper, Counsel for International Consumer Protection at the US Federal Trade Commission, discussed the measures being undertaken by the FTC to combat the threats from spam and spyware, and described the US-SAFE WEB act, which for the first time allows for the exchange of information between the FTC and foreign law enforcement agencies to combat Internet-based crime.

Peter Fleischer, European Legal Counsel for Google announced that Google had recently taken the step to protect the anonymity of its customers by removing all personal data from its archived search history database. Whilst this action may not have gone far enough in the view of some European Data Protection authorities it was nevertheless a major step forward and one which he expected would be followed by Google's major competitors.

Toby Stevens, Director of the Enterprise Privacy Group and Chair of the BCS Information Privacy Expert Panel outlined some of the privacy concerns with the UK Government's proposals on introducing satellite-based road pricing. He raised the spectre of itemised road pricing bills being used as evidence in divorce proceedings.

Prof. Dr. Hans-Jürgen Garstka, the Director of the European Academy for Freedom of Information and Data Protection, covered the related issue of the 'black boxes' now being fitted into modern vehicles for onboard monitoring purposes. The data collected by such devices was of great interest not only to the manufacturers but also to traffic police, emergency services, insurance companies, hire car operators and employers. There was even the prospect that a driver might need to

insert a chip-encoded driving licence into the 'black box' before being allowed to drive the car.

Paula Ortiz Lopez, legal adviser for international affairs in the Spanish Data Protection Agency described the Spanish electronic ID card, which was being developed in a privacy-friendly way and Dr Fleur Fisher, a member of the BCS Information Privacy Expert Panel and Director of a Healthcare-ethics consultancy, described the apparent flaws in the NHS patient records database, which limited the ability of NHS patients to control the use of their sensitive medical data and urged the Channel Islands' government Health Departments not to follow blindly down the same route as the NHS.

In summarising the day and thanking Fiona Murray of organisers, Orchard Events, Dr. Harris added that it had been clear that the delegates had been impressed with the breadth of expertise on show and the wide ranging nature of the presentations; it was evident that global networks impact on all of our lives and the privacy risks are real and on the increase.

Further details of the conference and the speakers, including some of the presentations, may be found on the conference website managed by Newtel Solutions[5]:

The conference resulted in a number of Press articles, television and radio interviews and was also a financial success, with the surplus from the conference being used to offset some of the costs of hosting the International Working Group meeting on the following days. The delegates were particularly complimentary about the organisational arrangements which had been masterminded by Orchard Events.

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: schools, nursing homes, finance institutions, law firms, retail businesses and voluntary organisations.

The total audience reached in this way was around 579, compared to 358 in 2006.

In addition, copies of the training DVD entitled: "The Lights are On", produced by the Information Commissioner's Office, are available free of charge from the Commissioner's Office.

[5] www.networkprivacy.gg

Involvement in Working Groups

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

Making use of the media

25 articles or letters relating to Data Protection were published in the local media during 2007, (compared with 28 in 2006) covering topics such as:

- Identity theft;
- ID cards;
- Conference and Working Group meeting;
- Freedom of Information legislation;
- Enforcement action against unsolicited marketing;
- HMRC data breach;
- Prosecution for alleged offences under section 55 of the Law;
- Disclosure and retention of credit card numbers by merchants;
- Breach of privacy in Mobile phone top-ups;
- Data on insurance disks
- European Data Protection day.

Guidance Notes

The number of Guidance Notes published by the Commissioner during the year remained at 29, but new editions of all the Guidance Notes were created, published in booklet form and made available on the web site.

A full list of available publications is given overleaf.

An estimated 1,096 hard copies of the literature were distributed to individuals and organisations during 2007, compared with 905 copies in 2006.

This is in addition to the unknown number of electronic copies of these guidance notes that were viewed or downloaded from the website[6].

[6] www.gov.gg/dataprotection

Guidance Notes published by the Data Protection Office

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

Developing the Internet Web Site

Work continued throughout the year to keep the information on the official website[7] up to date.

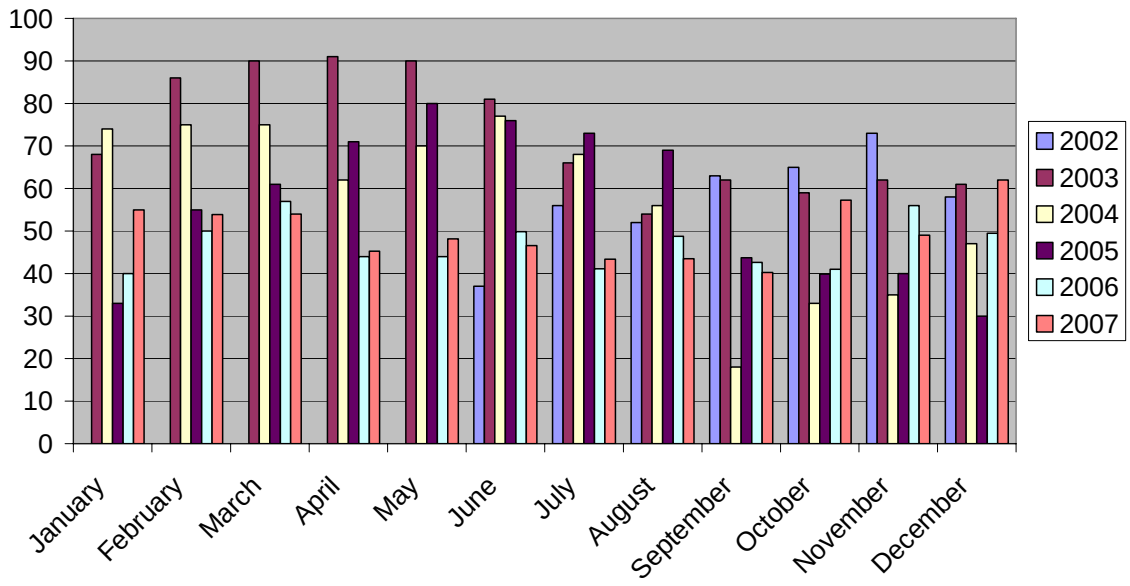
A chart of the average number of pages viewed per day between October 2004 and December 2007 is shown below.

The data for this chart are provided by the Information Technology Unit.

Currently, it would appear that about 50 pages per day are being accessed, compared with a peak of 90 pages per day in 2003; the most popular pages continuing to be those containing Guidance Notes.

This is reinforced by the number of calls received at the office which refer to the guidance that has been published on the Internet.

Average Daily Visits to Internet Site



[7] http://www.gov.gg/dataprotection

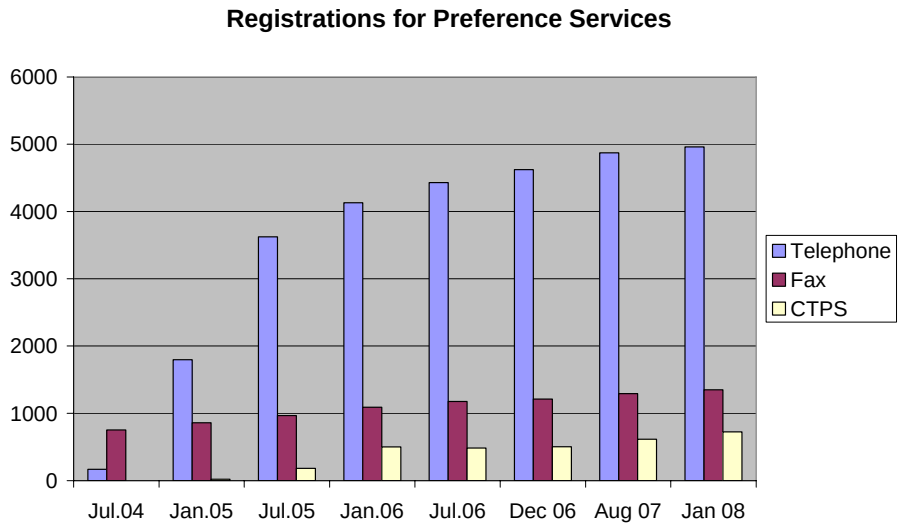
Registrations with the Preference Services

The Telephone Preference Service (TPS)[8] allows individuals to opt-out of the receipt of unsolicited marketing calls. Although the regulations covering the TPS apply only to marketing organisations based in the British Isles, in practice TPS registration appears to reduce, but not eliminate, the receipt of calls originating from overseas, since many reputable overseas telemarketers appear to screen their calls against the TPS database.

The Fax Preference Service (FPS)[9] allows any individual or business with a fax machine to opt out of the receipt of unsolicited marketing faxes whereas the Corporate Telephone Preference Service (CTPS) is for use by organisations wishing to opt out of the receipt of marketing calls.

The Preference Services were initially promoted in Guernsey by the Office in 2004, following a number of complaints about marketing calls and a service was offered whereby the Office undertook the registration on behalf of local residents. The services are now advertised within the information pages at the front of the Cable & Wireless and Wave Telecom directories and it appears that the majority of people now feel confident to register for themselves as requests to this office for registration have declined.

The chart below, derived from data provided by the Direct Marketing Association, shows that registrations for TPS continue to show a small increase, with 4,961 numbers being registered, compared with 4,622 at the end of 2006 and 4,130 in 2005. Registrations for FPS have increased by 55 to 1348 and those for CTPS have risen by 109 to 724.



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

ENFORCEMENT

The Law provides for a number of offences:-

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

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

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

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

Notices

One data controller was served with a Preliminary Enforcement Notice in 2007, whereas in 2006 no Enforcement Notices had been served. Two Enforcement Notices had been served in 2005. All these Notices concerned non-compliance with the Regulations in relation to email marketing.

No Information Notices were issued in 2007 or 2006. Two Information Notices had been issued in 2005. This demonstrates that data controllers are increasingly co-operative in providing information to the Commissioner when he is assessing complaints.

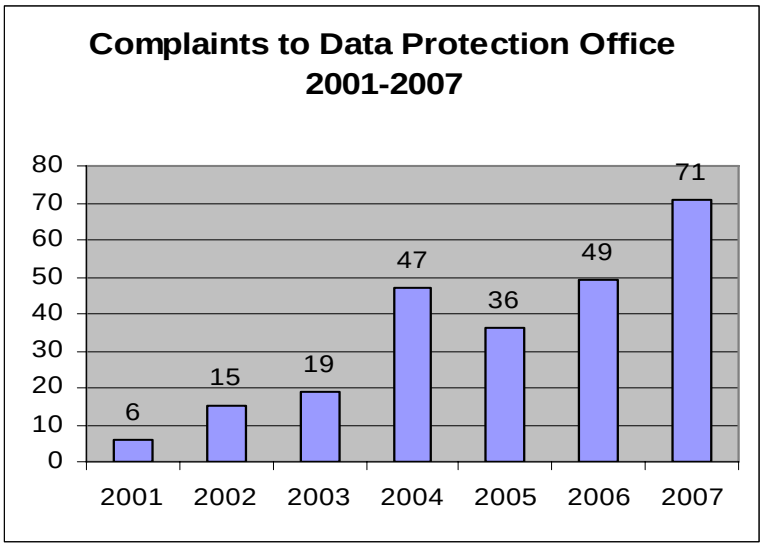
Police Cautions

Some data controllers do habitually ignore final reminders to renew their Notifications, resulting in the need for follow-up action. In 2007 two Police Cautions were administered to data controllers who had failed to renew their Notifications without good cause. A significant amount of administrative time is spent on pursuing late payers and it is recommended that a financial penalty should be imposed in the case of those who are late in renewing their notifications.

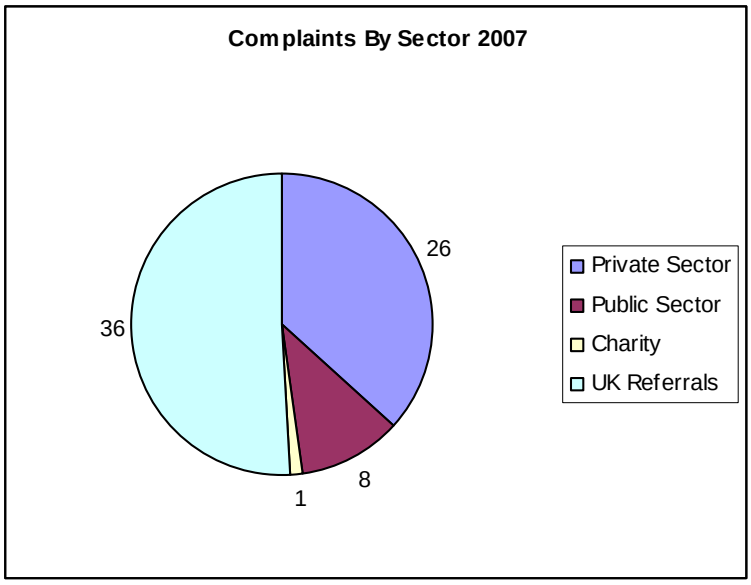
This action would be likely to prevent the need to refer such matters to the Law Officers, thus saving their time as well as the time of the Police.

Complaints

There were a total of 71 complaints received by the Commissioner during 2007, compared with 49 in 2006, 36 in 2005 and 47 in 2004. A relatively smaller number of complaints were processed in prior years, as is shown opposite.

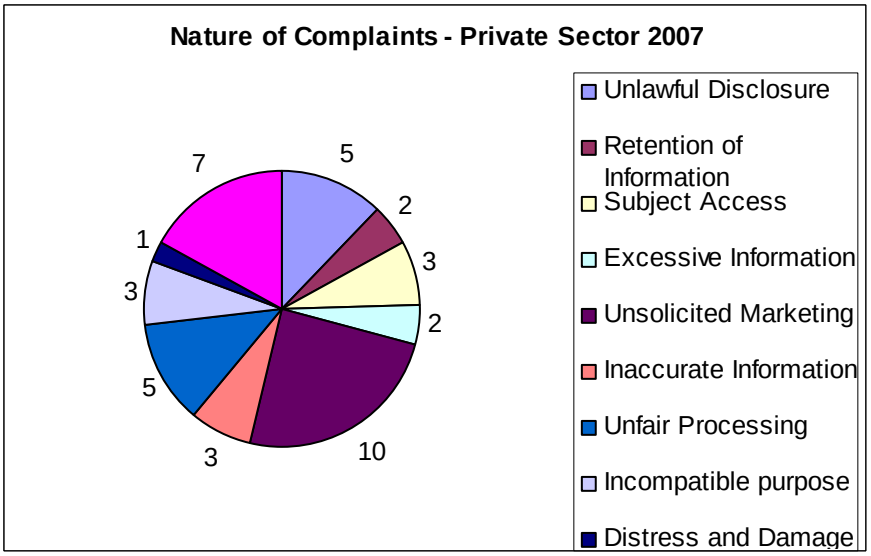


The breakdown of complaints received in 2007 and depicted opposite, shows that 26 related to the private sector, 8 to the public sector and one concerned a local charity. There were 36 complaints referred to the UK.



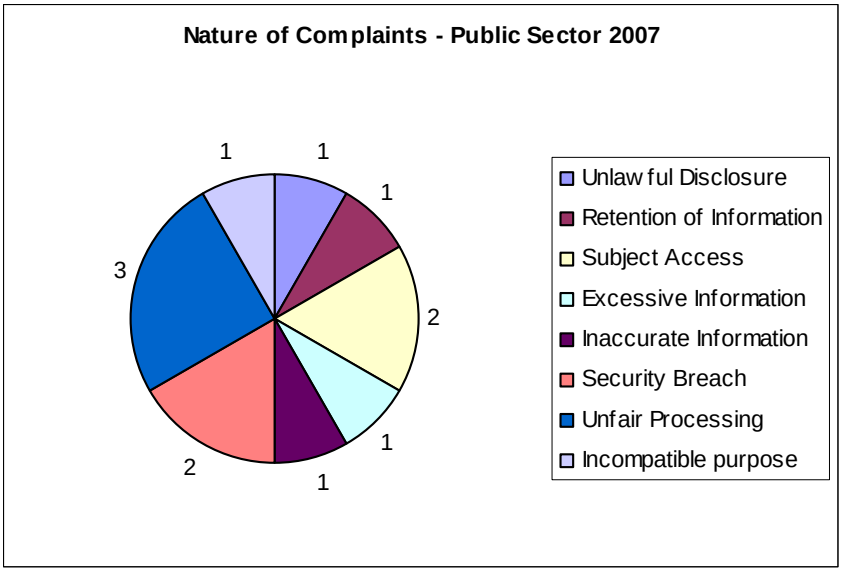
Of the 36 complaints against locally based controllers, 20 were upheld, one was partially upheld and 14 were not upheld, by the Commissioner.

A breakdown of the subject matter of the 26 complaints against the private sector can be seen opposite. Any one complaint may involve an alleged breach of one or more of the data protection principles.



For instance an inappropriate disclosure of information may not only be a breach of security but could also be construed as unfair processing, i.e. using the personal information of someone without informing them that this is being done. This may also have the effect of causing damage and distress. Likewise, damage and distress may also be caused if information is recorded inaccurately or used for a purpose which was not communicated to the individual at the time of collecting the information.

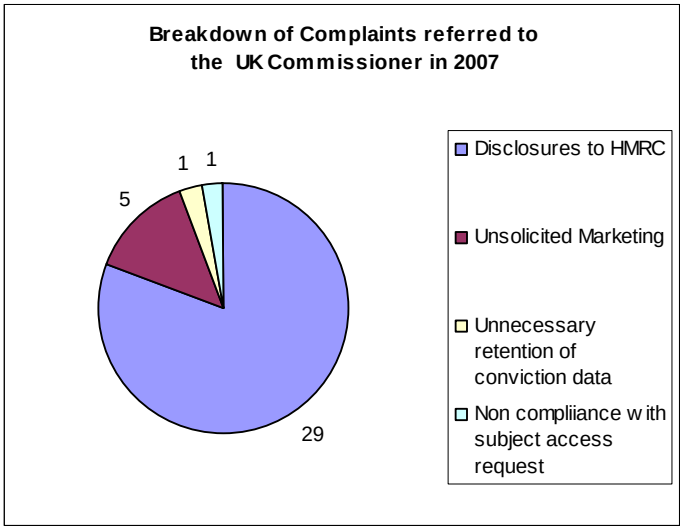
The diagram opposite provides a breakdown of the subject matter of the 8 complaints made against the public sector, involving alleged breaches of 12 principles.



The one complaint received against a local charity concerned the alleged unlawful disclosure of personal information to a third party.

Such a disclosure would be an offence under section 55 of the Law. In this particular case the complaint was not upheld by the Commissioner.

Of the 36 complaints referred to the UK Commissioner in 2007, 5 involved unsolicited marketing, 1 involved the unnecessary retention of spent convictions, and another was to do with non-compliance with a subject access request.
The remaining 29 complaints concerned the disclosure by UK banks of Bailiwick residents' bank account details to Her Majesty's Revenue and Customs (HMRC). Consideration of this disclosure remained ongoing at the end of 2007.



The Commissioner acknowledges with thanks the assistance that has been provided in the resolution of these complaints by the staff from the Office of the Information Commissioner.

In addition, the Commissioner appreciates the provision of legal advice from the Law Officers of the Crown which has assisted his determination of these cases.

Case Studies

A selection of the complaints dealt with during the year have been grouped into topics and detailed below in the form of case studies.

Topic 1 –Processing of Electoral Rolls throughout the Bailiwick

The purpose of the Electoral Rolls as stated in legislation is to list those individuals who are entitled to vote at elections. Individuals who are eligible to vote make a written application to be inscribed on the Roll, but in none of the Islands is registration compulsory.

The Electoral Rolls should not be used for other purposes such as marketing. In addition copies of the Rolls are not to be provided to any organisation or individual other than for electoral purposes. However, Government must allow members of the public to view the Rolls.

1) Alderney

The Commissioner investigated a complaint that the Alderney Electoral Roll had been used for the purpose of sending out survey forms. The complainant claimed that this was not the purpose for which the Roll was legally constituted and therefore was unlawful. The Commissioner drew the complainant's attention to an exemption allowed for in the Law for purposes of research. The use of the Roll for sending out survey forms might be permissible as long as the information obtained was not used to make a decision about any individual. The Commissioner further advised that persons should be informed that the Roll may be used for this secondary purpose, possibly by a short statement on the Electoral Roll application form. This would give an individual the opportunity to opt out of the receipt of survey forms. When people apply to go on the Electoral Roll they do so for the express purpose of being able to vote. If their information is to be used for research, which is not the primary purpose stated in statute, it is the Commissioner's view that they should have the opportunity to consent or object to this.

2) Sark

Candidates for election are permitted to obtain a copy of the Electoral Roll for the purpose of electioneering. If elected, the candidate may retain the information for constituency purposes, but otherwise should return or destroy the information. During an investigation of a complaint, a person informed the Commissioner that he had a personal copy of the Electoral Roll which he had been given as he sat on a Sark committee. Information from the Roll had been used for the circulation of political material. The Commissioner hopes that this was an isolated incident and recommends that this should not be the usual practice.

3) Guernsey

A Guernsey resident kept receiving the postal mail of a former occupant of his house. This former occupant had left the island and could not be traced. Cards to update the Electoral Roll details were delivered to the house both for the present and former occupants. The present householder updated his card requesting that the former occupant be disassociated from his address. He was informed that this was not possible as the Law does not allow someone to remove another person from the roll. This highlights a potential need for this legal provision to be amended as, not only could it lead to a non-eligible person being able to vote, but also to the fraudulent use of their name and address. It is understood that the House Committee is considering this matter.

Topic 2 - Credit Reference Agencies

Credit reference agencies keep records of debtors to enable providers of products and services to make informed decisions on whether or not to accept people as customers. One method of getting information about debtors is to obtain copies of court judgements and keep them on file. Information is retained by the agencies for six years and so it is important that this information is accurate and up to date.

1) A husband and wife were refused credit and on enquiry learnt that there was a court judgement against them for a significant sum of money. They were confused about this and obtained a copy of their credit reference record. The record gave details of a court judgement, which had never been made against the couple and so it was necessary for an advocate to provided evidence to the agency that this was the case. The agency had misinterpreted the report of the court judgement. The agency offered to put a notice of correction on the record but it took the input of the Commissioner to have the record fully deleted.

2) *An individual was advised to contact a credit reference agency to find out why his custom had been refused. He was shocked to discover that details of a court judgement which had been settled by his insurance company four years before was on record. He was informed by the agency that it was his responsibility to contact the agency once the judgement had been settled. However he did not know that a credit reference agency would be holding information on him because as far as he was aware he had not been in debt. The record was subsequently amended to show that the judgement had been satisfied.*

The Commissioner stresses that it is important for individuals to inform credit reference agencies that a court judgement against them has been settled. Whereas information about court judgements is in the public domain, the satisfaction of the court order is often a private matter between plaintiff and defendant.

Topic 3 – Processing without Consent

When personal information is either procured or disclosed without the consent of the data controller (i.e. the organisation that holds the information) it is an offence under section 55 of the Law. Some individuals complained to the Commissioner that their information had been disclosed in contravention of section 55.

1) *An employee of a local charity was asked by another organisation to accompany them on an investigation so that use could be made of her expertise and specialist knowledge. The employee took photographs during the visit and sent copies of these to a third party. The subject of the investigation claimed that this was an unlawful disclosure with detrimental affect. The Commissioner concluded that, as the charity employee had not been requested by the investigating organisation to take the photographs or to hand them over after the visit, the photographs were her property to do with as she liked. As she did not need the consent of the other organisation to process these photographs a section 55 offence could not have been committed.*

2) *An individual complained that a public body had procured personal information from him when it had no authority to do so. The Commissioner found that the information was procured to enable the organisation to carry out its regulatory function and so the procurement was covered by the exemption in section 31 of the Law.*

3) *An advocate claimed that an individual had taken a business database without the consent of his ex-employer and was utilising it for commercial advantage in a new place of work. This case could not be proceeded with as no evidence could be produced to substantiate the claim.*

Topic 4 – Disclosure of Medical Data

A patient complained that her medical details had been disclosed to the General Medical Council (GMC) without her consent.

The disclosure had been made because there were concerns about the treatment that this patient had received from a local medical professional.

The GMC is a UK authority that regulates the medical profession and has statutory authority to investigate complaints made against its members. If a patient does not consent to the release of records to enable the GMC to investigate a complaint, then section 35(A) of the Medical Act 1983 may be used to obtain them.

The Medical Act is a piece of UK legislation which does not extend to the Bailiwick of Guernsey and so the complainant considered that the disclosure was unlawful as she did not give her consent.

However, local legislation makes it a criminal offence for any doctor, dentist or pharmacist to practise locally unless they are registered as practitioners in the UK and are on the register maintained by the Health and Social Services Department (HSSD). Before the HSSD accepts a practitioner on its register it must be satisfied that the person is registered in the UK. Therefore all local medical practitioners are accountable to the GMC and will be subject to its disciplinary investigation procedures.

Secondary legislation under the Data Protection Law provides for the disclosure of sensitive personal data such as health information without consent if this is considered to be in the substantial public interest. An example of a disclosure in the substantial public interest would be an investigation of a practitioner where there were concerns about his or her fitness or competence to practise.

Having considered the facts of the case and relevant local legislative provisions, the Commissioner concluded that the disclosure in question was lawful. He intends to issue detailed guidance to the local medical profession as a result of this case.

Topic 5 – Marketing by Email

Marketing by email is regulated by the Privacy and Electronic Communications Regulations[10] (see also the Appendix).
The basic rules are:

- *individuals must in general give explicit consent to be marketed by email;*
- *businesses may be sent an initial email without prior consent provided there is an unsubscribe facility provided within the email;*
- *emails must not be sent to an address which has been unsubscribed.*

1) *An individual complained that he had been receiving emails from a company despite having unsubscribed several times. On investigation, it was discovered that the unsubscribe messages were getting caught in the company's spam filter. Due to the size, commercial commitments and available resources of the company, the Commissioner issued a Preliminary Enforcement Notice even though there had been no prior complaints against that company.*

2) *Another individual complained that he had received an email from a company after having unsubscribed. In sending this email the company did acknowledge that the person had unsubscribed and informed him that he would not be sent further emails if he did not positively request them. However, the company also included details of new products and services that were available. The Commissioner considered that this constitutes a promotional and marketing email and accordingly was in breach of the Regulations. The company apologised to the ex-customer and stated that it would use different methods of promotion in future.*

[10] The European Communities (Implementation of council directive on privacy and Electronic Communications (Guernsey) Ordinance, 2004.

Topic 6 – Ensuring Adequate Security

Organisations will be in breach of data protection principles if they do not employ appropriate technical and organisational measures to ensure the security of personal information. While there have been no major security breaches reported locally [by comparison with the HMRC breach in the UK], the Commissioner continues to receive some complaints from individuals about their information not having been processed securely.

1) *When a person used an automatic cash dispenser, a bank card of another person was returned to him in addition to his own. This had occurred because of a technical fault and was quickly remedied when it was brought to the bank's attention after the weekend. However, if the recipient of the card had not been honest, the other cardholder could have been exposed to the likelihood of fraud or identity theft.*

2) *A tenant in a block of flats complained that an organisation had disclosed his personal details to other tenants and that this information could have conveyed the wrong impression that he was in debt to the organisation. An employee of the organisation had left an open card in a communal area of the flats. The organisation agreed to put cards in an envelope marked to the addressee in similar circumstances in future.*

3) *A patient complained that details, of a diagnostic test were visible through a window on an envelope and this had resulted in disclosure of the fact that the test had occurred. The organisation undertook to instruct its staff to take more care when inserting material into window envelopes in future.*

Organisations must be aware that there must be satisfactory staff training and supervision, appropriate procedures and resources in place to ensure the security of processing of personal information. The Commissioner accepts that there may be "once off" incidents but details of breaches are kept on record and will be considered in the event of similar complaints in future.

International Conference of Data Protection Authorities

The Commissioner attended the 29th International Conference of Data Protection and Privacy Commissioners, which was held in Montréal from 25th – 28th September 2007.

The conference program was focused on the challenging issues confronting data protection and privacy commissioners now and in coming years.

The main themes covered in the plenary sessions were identified as "dragons" in keeping with the conference theme of *Terra Incognita*.

The 6 dragons that were identified for the conference were:

1. Public Safety	4. Ubiquitous Computing
2. Globalization	5. The Next Generation
3. Law Meets Technology	6. The Body as Data

The conference passed three resolutions on:

- the urgent need for global standards for safeguarding passenger data;
- the Development of International Standards;
- International Co-operation between data protection authorities.

Full details of the conference are available on its website[11]:

The 30th International Conference will be co-hosted by the Commissioners of France and Germany, both of whom are celebrating their 30th anniversary, and will be held in the border city of Strasbourg from 15th - 17th October 2008.

European Spring Conference

The Assistant Commissioner attended the European Spring conference, which was held in Lanarka, Cyprus on 10th -11th May 2007. She was one of 109 delegates representing 47 data protection authorities throughout Europe.

The conference focused on the challenges faced by data protection authorities in protecting the rights of individuals in regard to the processing of their information in the world of today.

The 2008 meeting will be held in Rome on 17th – 18th April.

[11] http://www.privacyconference2007.gc.ca

International Working Group on Data Protection in Telecommunications (IWGDPT)

The Commissioner attended the two meetings of the International Working Group that were held in 2007.

The 41st meeting was held at Castle Cornet on 12th and 13th April and was preceded by the public conference entitled: "Respecting Privacy in Global Networks", that was held at St. James.

Dr. Alexander Dix, chairman of the IWGDPT firing the "noon-day gun" at Castle Cornet, to commemorate the Group's 41st meeting.

The 42nd meeting of the Working Group was held in Berlin on 5th and 6th September.

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

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

At the meeting in Guernsey, the Working Group approved a paper, originated by the Commissioner, recommending further action by governments and the telecommunications industry to establish better procedures to combat cross-border telemarketing.

A full list of papers published by the International working group since its inception may be found on its website[12].

The 43rd meeting of the Working Group will be held in Rome on 12th and 13th April 2008 and the 44th meeting will be held in Berlin at the beginning of September 2008.

Liaison between the British, Irish and Islands' Data Protection Authorities

The Commissioner and Assistant Commissioner welcomed representatives from the authorities of Cyprus, Gibraltar, Ireland, the Isle of Man, Jersey, Scotland and the UK at the annual Data Protection Authorities' meeting, which was held at Les Cotils on 12th July.

International Delegates to the Authorities' meeting at les Cotils

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

The Commissioner summarised the main issues being discussed at the International Working Group on Data Protection in Telecommunications and the Isle of Man Supervisor introduced the topic of mandatory notification of security breaches, a practice that originated in the United States, and which was under consideration by the European Union.

The Assistant Commissioner for Scotland outlined his role, which is limited to Data Protection matters, as there is a separate Freedom of Information Commissioner for Scotland.

There was a specific discussion centred on the disclosure by UK Banks to HMRC of non-UK resident offshore account details; the UK Information Commissioner agreed to investigate this matter.

The Authorities also discussed the different legislative and supervisory approaches that were being adopted by the participating territories to the facilitation of Public Access to Official Information, otherwise known as Freedom of Information.

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

The next meeting of the Authorities will be held in Gibraltar on 25th June 2008.

Liaison with the UK Government

No formal meetings were held with staff from the Ministry of Justice during 2007. However, email contact with officials was maintained and informal meetings held during the various conferences that were attended during the year.

Data Protection Forum

The Assistant Commissioner attended three meetings of the Data Protection Forum that were held in London during 2007; the topics covered in the meetings were:

- *The development of international standards for data retention*
- *Data sharing across the public and private sectors*
- *The re-use of public sector information*
- *The work of the UK Information Tribunal*
- *The role and responsibilities of the UK Passport Agency*

- *Perspectives from data protection authorities in the UK, Ireland and Crown Dependencies*
- *Developments in European data protection*
- *Review of data protection issues during 2007*

The Commissioner was invited to join a panel at a "Commissioners' Question Time" that was held on 6th September, 2007. Other members of the panel were the UK Commissioner, the European Data Protection Supervisor, the Cyprus Commissioner and the Isle of Man Supervisor.

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.

The IPEP includes members from academia, the public and private sectors and has considered various topics, including the UK Government proposals on Identity Cards and data sharing initiatives within the public sector.

The cost of attendance at these meetings of the IPEP and at any related meetings is borne by the BCS. Another positive outcome of the Commissioner's involvement was the participation by members of the IPEP in the 2007 conference at St. James and its sponsorship by the Guernsey International Section of the BCS.

OBJECTIVES FOR 2008

The primary objectives for 2008 will encompass the following areas:-

- ***Legislation***

  Detailed work on the 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.

  Promotion activities will concentrate on privacy-friendly data sharing, the importance of information security and the benefits of undertaking privacy impact assessments.

- ***Compliance***

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

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

- ***Government***

  Close liaison with the States of Guernsey Government departments will continue with the aim of promoting data sharing protocols and the further development of subject access procedures. Opportunities will be taken to promote the use of Privacy Impact Assessments where appropriate.

- ***Administration***

  The process of moving all notification data onto electronic media will continue, with the aim of dispensing with all manual records of notification by the end of 2009.

  The periodic review of the business recovery plan will be undertaken.

FINANCIAL REPORT

The Data Protection Office is funded by a grant from the States of Guernsey that is administered by the Home Department. This grant is based on a budgetary estimate of expenditure prepared annually 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 Data Protection Office's Income and Expenditure, which are included within the published accounts for the Home Department, have been as follows:

INCOME	**2007**	**2006**	**2005**
	£	**£**	**£**
Data Protection Fees [1]	46,010	43,382	41,686
EXPENDITURE			
Rent	15,526	15,526	16,276
Salaries and Allowances[2]	147,971	138,328	137,251
Travel and Subsistence	8,926	10,588	9,751
Furniture and Equipment	11,790	13,806	14,237
Publications	2,910	2,886	2,609
Post, Stationery, Telephone	3,977	3,542	4,253
Heat Light, Cleaning	4,681	4,743	4,874
TOTAL EXPENDITURE	**£195,782**	**£189,419**	**£189,251**
EXCESS OF EXPENDITURE OVER INCOME	**£149,771**	**£146,037**	**£147,565**

NOTES

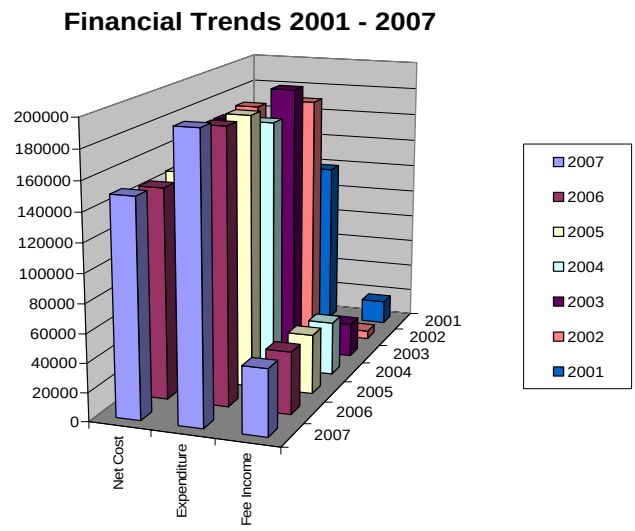
[1] Fees were £35 per notification or renewal of a notification.

Income from fees is accrued on a monthly basis.

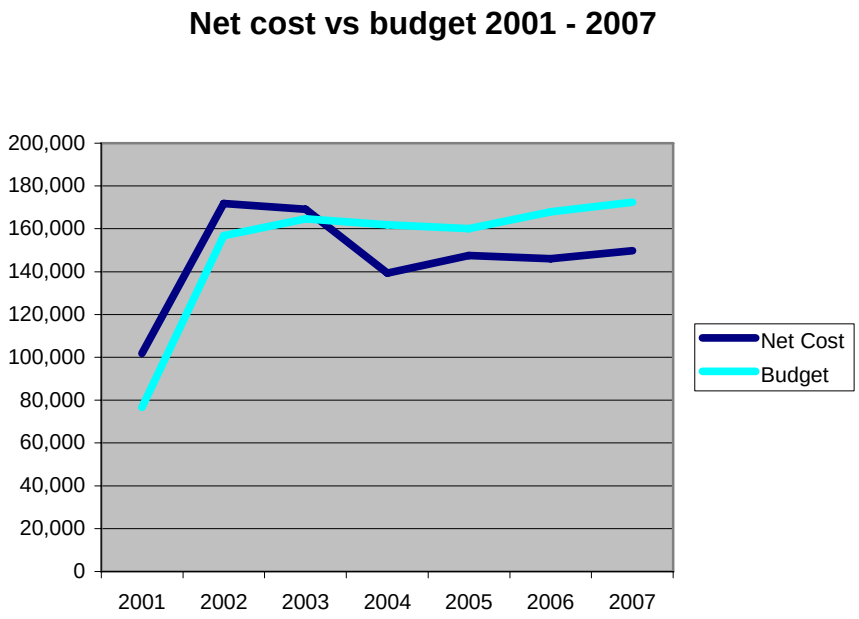
The cash received for notifications in 2007 was £47,810 (£43,505 in 2006 and £42,665 in 2005) representing the 1,366 annual notifications and renewals that were processed during 2007.

[2] This includes an amount of £5,510 (£1,662 in 2006 and £6,270 in 2005) for consultancy fees.

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



Expenditure for 2007 rose by £6,362 (3.3%), whereas the income from fees rose by £2,628 (5.7%); hence, the net cost of the Office to the taxpayer increased by £3,734 (2.5%) and remained below the authorised budget. It is anticipated that the increase in Notification Fees, which has been approved by the States but not yet implemented, would bring in an additional £17,000 of income in a full year, enabling the net cost of the Office to be reduced.



During the year, the aging photocopier began to fail and it was replaced from the capital budget of the Home Department with a multi-function device which combined the functions of network printer, photocopier and scanner.

The cost of this equipment at £5,606 has not been included in the above statement as it was funded directly by the Home Department.

In addition, thanks to technical and operational support from the Information Technology Unit (ITU) of Treasury & Resources, it was possible to replace the three Personal Computers and a faulty Ethernet router.

The Commissioner appreciates the financial support that has been forthcoming from the Home Department and is grateful for the continuing technical support from the ITU.

It is hereby confirmed that no gifts or hospitality were received by the Commissioner or his staff during 2007.

APPENDIX

THE DATA PROTECTION PRINCIPLES

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

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

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

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

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

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

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

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

THE PRIVACY AND ELECTRONIC COMMUNICATIONS REGULATIONS

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

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

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

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

5. Subscribers may choose not to appear in directories.

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

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

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

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

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

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

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

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