BAILIWICK OF GUERNSEY

DATA PROTECTION COMMISSIONER REPORT FOR 2005

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: "A private walk" along the Moulin Huet cliff path on the south coast of Guernsey. Downloaded from www.guernseyimages.com

CONTENTS

FOREWORD

I am pleased to present my fifth report on Data Protection within the Bailiwick of Guernsey and, since September 2006 will mark the end of this five year term of office, I have taken the opportunity in this report to reflect on significant historical developments, both within the Bailiwick and elsewhere.

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

The Privacy and Electronic Communications Regulations came into force in 2004 and inter alia ensured that the Bailiwick could not be used as a source of spam email or nuisance phone calls. Work is continuing internationally to target the foreign sources of such unpleasant and harmful material.

A number of weaknesses have been identified that limit the effectiveness of current legislation and it is anticipated that these will be addressed during 2006.

Whilst I have concentrated my efforts over the past five years in raising awareness of Data Protection within the local community and promoting compliance by local organisations, I have also endeavoured to raise the international profile of the Bailiwick by active participation in international conferences and working groups.

The numerous calls for advice and requests for training that we receive are testaments to the success of this domestic policy and the fact that a major international working group has chosen to meet in Guernsey in 2007 may similarly be seen as a positive outcome of that foreign policy.

Further constraints on public expenditure are anticipated in the coming years and, whilst the costs of the office may be ameliorated by a modest increase in Notification fees, future expenditure will also need to be contained. Indeed, effectiveness and benchmarking of supervisory authorities are topics that will be discussed at the British Isles, Irish and Islands' liaison meeting in the coming year.

I am fortunate to have the support of a small but dedicated team in this office, which has built up considerable expertise in this complex area of work and provides invaluable assistance and contributes in no small way to our effectiveness. I must also acknowledge the excellent support received from the staff of the Home Department and the legal advice and assistance that I have received from the Law Officers of the Crown.

Much has been achieved in these last five years and I can confidently predict that Data Protection is well prepared to face the challenges of the future.

Data Protection Commissioner, March, 2006.

DATA PROTECTION LEGISLATION

Historical Perspective

The 12th July 2005 was the twenty first anniversary of the passage of the first Data Protection Act in the United Kingdom. At a commemorative conference held in Manchester, the outgoing Deputy Commissioner, Francis Aldhouse, set out a brief history of the development of Data Protection and its regulation in the UK.

He pointed out that it is a common misconception that Data Protection was somehow foisted on the British Isles by "faceless European bureaucrats". In fact, as early as 1972 the Younger Committee[1] had foreseen the need for legislation for the protection of personal privacy. That Committee had also proposed 10 principles for the protection of personal information. Rather than enact specific legislation at that time, various other measures were adopted, including the licensing of private detectives, the outlawing of covert surveillance and a new tort of disclosing or using information that had been unlawfully obtained.

In 1975, the UK Government published a White Paper "Computers and Privacy"[2] in which the arguments were set out for legislation to ensure that: *"... computer systems in which personal information is held are operated with appropriate safeguards for the privacy of the subject of that information."* The Lindop Committee was established in 1976 to advise on the form of future legislation, to develop the "Younger Principles" and to prepare the way for a statutory authority. The Lindop Committee presented a detailed report to Parliament in December 1978.[3]

Meanwhile, elsewhere in the world, the earliest Data Protection legislation had been made in Hessen in 1970, followed by the first national laws, the Swedish Act of 1973 and the United States Privacy Act of 1974. In addition, the Council of Europe developed Convention 108[4], which was opened for signature in January 1981.

The proposals from the Lindop Committee and the added impetus of ratification of "Convention 108" formed the basis for the UK Data Protection Act, 1984.

The 1984 Act was superseded by the Data Protection Act, 1998, which had been drafted in order to comply with European Directive 95/46/EC[5]. That Directive was intended to impose common standards of Data Protection across the European Union in order to facilitate the operation of the single market and had required all Member States to transpose its standards into domestic legislation within three years of its adoption.

---

[1] Great Britain, Parliament (1972) **Report of the Committee on privacy**. [Chair Rt. Hon. Kenneth Younger] Cmnd. 5012 London, HMSO

[2] Great Britain, Home Office (1975) **White paper: Computers and Privacy.** Cmnd 6353 London, HMSO

[3] Great Britain (1978) **Report of the Committee on Data Protection.** [Chair Sir Norman Lindop] Cmnd 7341 London, HMSO

[4] Council of Europe (1981) **The Convention [108] for the protection of Individuals with regard to Automatic Processing of Personal Data.** Strasbourg, CoE

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 **on the protection of individuals with regard to the processing of personal data and on the free movement of such data**. OJ L281,31

The operation of this Directive was reviewed by the European Commission[6] in May 2003 and again in February, 2004 and, whilst a new Directive is not in prospect, there are indications that Member States will be required to ensure that their domestic legislation accords more closely with its terms. Whether this results in amendments to the UK legislation, or merely involves changes to the enforcement régime, remains to be seen.

Development of Legislation within the Bailiwick

Guernsey responded to the need for compliance with the standards being adopted by our major trading partners by enacting the Data Protection (Bailiwick of Guernsey) Law, 1986, which was drafted in similar terms to those of the UK Act of 1984.

The passage of this legislation enabled the United Kingdom Government ratification of the Council of Europe Convention 108 to be extended to the Bailiwick.

The European Directive 95/46/EC imposed stricter conditions on the transfer of personal data to those territories in which the protection of personal data was not deemed to be "adequate". It was believed that the absence of a positive determination of "adequate protection" might jeopardise the development of international business in the Bailiwick, as a large amount of such business was conducted with organisations in the UK and in other Member States of the European Union.

It became clear during discussions with the UK Data Protection Registrar and the Home Office officials that it would not be feasible merely to amend the 1986 Law to ensure adequacy within the meaning of the Directive, so the decision was taken by the Advisory and Finance Committee to recommend to the States the drafting of new legislation, again modelled as closely as possible on the legislation in the UK.

As a consequence of the work undertaken by the former Commissioner and his predecessor, Guernsey took the lead amongst the Crown Dependencies in the drafting of Data Protection legislation, and the Data Protection (Bailiwick of Guernsey) Law, 2001 was registered in Guernsey on 29th April, 2002 a year before similar legislation in the Isle of Man and some three years before the passage of similar legislation in Jersey.

The Data Protection Law was commenced on 1st August 2002 and one month later at the opening of 24th International Conference of Data Protection and Privacy Commissioners held in Cardiff, Yvette Cooper, Parliamentary Secretary at the Lord Chancellor's Department, announced during her keynote speech that the European Commission would be pressed for an early decision on the adequacy of the Guernsey régime.

This milestone was achieved over a year later on 21st November 2003[7], when the European Commission published its decision recognising the adequacy of the protection of personal data in the Bailiwick of Guernsey.

[6] http://europa.eu.int/comm/justice_home/fsj/privacy/lawreport/index_en.htm
[7] European Communities**, Commission Decision of 21 November 2003 on the adequate protection of personal data in Guernsey** (2003/821/EC) OJ L 308, pp 27-28

Privacy and Electronic Communications

In 1991, the International Working Group on Data Protection in Telecommunications[8] presented a report to the 13th International Conference of Data Protection and Privacy Commissioners that was held in Strasbourg. That report highlighted the Data Protection issues in telemarketing and led to the adoption six years later within the European Union of Directive 97/66/EC[9] on the protection of personal data within the telecommunications sector. This Directive was implemented within the UK by the passage of the Telecommunications (Data Protection and Privacy) Regulations 1998, which came into effect at the same time as the 1998 Data Protection Act. No such regulations were implemented within the Bailiwick when the 2001 Law was commenced, as it was known at that time that the Telecommunications Directive was about to be superseded.

Associated with the 1998 Regulations were the Telephone and Fax Preference Services, operated by the Direct Marketing Association, whereby individual subscribers in the UK were able to join opt-out lists that signified their objection to the receipt of unsolicited marketing calls. Whilst Bailiwick residents were able to take advantage of registration on the Preference Services, the Regulations themselves did not extend to the Bailiwick, so it was possible for direct marketing operations which did not conform to the Regulations to become established locally.

A significant flaw in the 1997 Directive arose from the rapid growth in marketing by email and SMS. Accordingly that Directive was repealed and replaced by Directive 2002/58/EC[10], which addressed all forms of electronic communications; the associated Regulations were enacted in the UK in 2003.

In 2004, the States of Guernsey approved a policy letter from the Advisory and Finance Committee proposing that similar regulations be enacted in Guernsey in the form of The European Communities (Implementation of Council Directive on Privacy and Electronic Communications) (Guernsey) Ordinance, 2004. Equivalent Regulations were also made in Alderney and Sark.

The passage of these Regulations has ensured that the general standards of personal data protection afforded within the Bailiwick have remained fully in conformance with those in the United Kingdom and the rest of the European Union.

Rehabilitation of Offenders

The Rehabilitation of Offenders (Bailiwick of Guernsey) Law, 2002 was not brought into effect in 2005 as had originally been intended. The need for additional consultation on the Commencement, Exclusions and Exceptions Ordinance had delayed its introduction, but it is expected to be brought into effect during 2006. Associated with this Law will be the commencement of section 56 of the Data Protection Law, which will prohibit the use of enforced subject access to circumvent the provisions of the Rehabilitation of Offenders

[8] http://www.datenschutz-berlin.de/doc/int/iwgdpt/index.htm
[9] Official Journal of the European Communities L 24. 30.01.1998 p.1
[10] Official Journal of the European Communities L 201. 31.07.2002 p. 37.

Law. A number of individuals have complained to this office over the protracted delay in the commencement of this Law.

The Commissioner published revisions of the Draft Code of Practice on the Disclosure of Criminal Convictions in connection with Employment during 2004 and it is intended that a final version of this Code of Practice will be published once the definitive version of the Ordinance has been approved and further clarification has been forthcoming as to the future role of the UK Criminal Records Bureau in the disclosure process locally.

Updating the Law

One of the benefits of a relatively early enactment of the Data Protection legislation within the Bailiwick was the achievement of correspondingly early declaration of adequacy by the European Commission. However, those jurisdictions in which the enactment of the legislation had been delayed were able to address weaknesses that had been identified as a result of the experiences in enforcement elsewhere.

The main potential areas for change involve a clarification of the applicability of the Law to States Departments and the Crown, an extension of the ability to serve an Information Notice and a proposal to increase the fees for Notification, together with some minor "cosmetic and typographical" changes.

The Commissioner has completed a report on these matters for the Home Department and it is anticipated that proposals to update the local legislation will be presented by the Home Department to the States during 2006.

The subject access provisions of the Data Protection law are limited to requiring the disclosure to an individual [data subject] of personal data relating to that individual. This is normally interpreted as information held on electronic media indexed by personal attributes of that individual (such as name, address, account or ID number, etc.) Such a definition is adequate for most private sector organisations, but is not always appropriate for information held by public bodies.

Much of the information relating to decisions made by government departments is not always structured by reference to individuals or may still be held in manual files and accordingly may not necessarily be accessible to an individual member of the public under Data Protection Law.

This limitation of access to government information is remedied in most democratic societies by the enactment of freedom of information legislation. There has been little political pressure to date for such legislation to be enacted within the Bailiwick. Indeed, provided that the government departments adopt an enlightened attitude to the publication and disclosure of the information that they hold, the need for such legislation could well be lessened.

DATA PROTECTION ISSUES

Public Security

The fight against serious organised crime and international terrorism has prompted many countries to adopt special measures in an endeavour to combat these threats.

This situation has highlighted the need to strike the right balance between the improvement of security on the one hand and the limitation of individual privacy on the other.

The terrorist attacks that have been witnessed in the last few years have shown that the threat of terrorism remains very real, but at the same time it should be remembered that even in such circumstances the fundamental rights of citizens should, wherever possible, be respected and observed.

Accordingly, there has been some tension between the European Data Protection Commissioners and the Member States and the European Commission over the proportionality and effectiveness of the counter terrorism measures that are being put in place.

A specific example is provided by the European Directive concerning the mandatory retention of communications records by the telecommunications companies. This information, which is primarily collected for billing purposes, is required by the law enforcement authorities in order to gain evidence of the activity and location of terrorist suspects. In their Opinion, adopted on 21st October 2005[11] the European Commissioners considered that the mandatory retention period for such data should be minimised and that such private and confidential data should be disclosed only on a case by case basis on judicial authority.

Within the Bailiwick, any interception of communications by the law enforcement authorities has historically been subject to judicial oversight and it is the Commissioner's view that any proposals that would seek to gain access to communications data should include similar safeguards.

The Protection of Children and Vulnerable Adults

There are few more emotive topics than the protection children and vulnerable adults from abuse and the revelations from some disturbing cases in the UK led to calls for better data sharing between the various support agencies to identify such cases at the earliest possible stage. The Commissioner recognises the importance of preventing and dealing with such abuse cases and the need for adequate information sharing to take place, especially between the authorities in the Bailiwick and their counterparts in the UK.

[11] Opinion 113/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communications Services and Amending Directive 2002/587/EC (COM(2005)438 final of 21.09.2005)

However, he shares the concern of the UK Commissioner over proposals to establish a national database of all children as outlined in the Children Act of 2004. This could well be viewed as a disproportionate response and give real concerns as to how the information in such a database would be kept secure and up to date as would be required by Data Protection legislation.

Furthermore, there is considerable uncertainty and potential for detriment with the use of 'cause for concern' indicators and a real risk that the privacy of children and parents in general will be compromised.

Identity Cards

The UK Government has pressed ahead with plans to implement a comprehensive Identity Card system and supporting National Identity Register, despite a number of calls for a re-evaluation of the technical basis upon which the project has been founded.

The London School of Economics undertook a major project on the ID Card system and published a controversial report that was severely critical of the government proposals[12].

Many of the objections have been on economic, technical or political grounds and, whilst the possession of an ID card remains voluntary, there can be only limited objections from a Data Protection standpoint. However, should it ever be proposed that possession of the card become mandatory to enable access to government services or entitlement to benefits, those concerns would become more significant. The UK Information Commissioner has endeavoured to inform the debate on this issue stressing the problems with the extent and relevance of the information that it is proposed to hold, the access controls on the data and the need for Data Protection safeguards to be given greater prominence.

In particular, the UK Information Commissioner has specifically criticised the plan to store an excessive amount of personal and biometric data in the National Identity Register (NIR), which is the central database that has been proposed to support the ID Card scheme. The data trail that would be generated by each check of an Identity Card against the NIR could enable a detailed picture of the private life of an individual to be built up, particularly if such data were combined with information from CCTV surveillance, automatic vehicle number plate recognition systems or satellite-based congestion charging schemes.

Undoubtedly, once the legislation on Identity Cards has received parliamentary approval in the UK, there will be pressure on the Bailiwick authorities to introduce a similar scheme. The Commissioner would not necessarily be opposed to the principle of an Identity Card system but would strongly recommend that any such scheme were designed from the outset such that the privacy rights and freedoms of individuals were adequately safeguarded. In particular, he would be opposed to the excessive sharing of personal data relating to Bailiwick residents onto the NIR.

[12] The Identity Project – an assessment of the UK Identity Cards Bill and its implications; LSE June 2005.

Exporting Personal Data

The eighth Data Protection principle states that: *"personal data shall not be transferred to a country or territory outside the Bailiwick unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of their personal data."*

Any transfer to a country within the European Economic Area is deemed to be compliant with the eighth principle as is a transfer to anywhere that has been designated as providing adequate protection by a decision of the European Commission. To date adequacy decisions have been made for: Argentina, Switzerland, Guernsey, the Isle of Man, Canada and those US entities that have self-certified compliance under the "Safe Harbour" scheme.[13]

Transfers elsewhere need to be assured of protection in other ways: for a transfer to another organisation that will be acting as a data controller or data processor than it will normally be necessary to incorporate standard clauses into the contractual agreement between the parties. These can be onerous and time consuming to implement; alternatively, multi-national corporations may choose to implement specific arrangements, such as internal rules, codes of practice, etc, collectively known as "Binding Corporate Rules" [BCR] to cover transfers to subsidiaries that may be located anywhere in the world.[14]

Once these BCR have met the approval of one European Data Protection authority, then they may be used to legitimise transfers throughout branches of the corporation located in different Members States and Third Countries. The earliest successful examples of the implementation of BCR have been achieved by Daimler-Chrysler (Germany) and General Electric (the UK).

In 2005, the Commissioner published a specific Guidance Note on Exporting Personal Data in response to the numerous questions and enquiries that had been received on this particular subject.

Unsolicited Telemarketing

The Commissioner continues to receive complaints from residents about the receipt of nuisance telephone calls and junk faxes and generally advises the recipients of such calls to register with the Corporate Telephone Preference Service (CTPS), Telephone Preference (TPS) or Fax Preference Service (FPS)[15], or in some cases will undertake the registration process on behalf of the complainant.

By the end of 2005, the number of Bailiwick telephone numbers registered on the TPS exceeded 4,000 and the number of registration on the FPS was a little over 1,000. About 10% of these registrations had been undertaken by the Office in response to requests from members of the public.

[13] http://www.export.gov/safeharbor/
[14] http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp108_en.pdf
[15] www.tpsonline.org.uk and www.fpsonline.org.uk

The UK telecommunications regulator OFCOM has proposed further regulations in the UK in respect of marketing calls, especially "silent calls" that result from automatically dialled calls which are subsequently not completed.[16] These regulations would require marketing companies to provide a call return facility and/or a recorded announcement identifying the originator of such calls.

Whilst the Preference Services and the proposed OFCOM regulations appear to be reasonably effective in regulating unwanted marketing calls originating from within the British Isles, they would appear to be of limited effectiveness in dealing with calls that originate from abroad – especially those from the USA. The main problem with such calls is that their origin cannot easily be identified as they normally do not contain any calling line identification (CLI) that is visible to the recipient; hence it is not practical to deal effectively with any complaints. It would appear unlikely that there could be international agreement over any requirements that all direct marketers should include CLI information within their unsolicited calls.

The International Working Group on Data Protection in Telecommunications is considering this issue and in particular whether it would be practical to propose that a Telephone Service Provider (TSP) should offer a means whereby subscribers who receive an unwanted marketing call were able to dial a short code; this would not only cancel the call, but also automatically log the internal CLI which, although hidden from the subscriber, should normally be available to the TSP.

Such a scheme would enable a record of persistent offenders to be rapidly built up by the TSP as the date, time and identity of the caller and the called number could be readily recorded and used to support the complaint handling process, especially on an international basis**.**

RFID

Radio Frequency Identification Devices[17] have been hailed by many retailers as the "holy grail of supply chain management", as they enable the identification and tracking of individual items from initial manufacture all the way to sale and eventual deployment.

RFID technology has a wide range of potential applications and has already been used in razor blades, world cup tickets and passports and in high value goods that may need tracing for theft detection or preventative maintenance purposes.

The elements of this technology that give particular cause for privacy concerns include:

- unobtrusiveness – unlike bar codes, RFID chips may be placed unobtrusively within items and may be read remotely, customers have no easy way of knowing whether an object contains an active RFID chip or not;
- item level tagging – because each item is individually tagged and identified, its purchase may be associated with an individual and unless the chip is deactivated,

[16] **Statement of policy on the persistent misuse of an electronic communications network or electronic communications service** http://www.ofcom.org.uk/consult/condocs/misuse/
[17] http://www.epic.org/privacy/rfid/

it may be read after purchase, essentially enabling the movements of that individual to be tagged.

These issues were originally raised by the International Working Group on Data Protection in Telecommunications in a report to the 2003 International Conference of Data Protection Commissioners[18], which resolved that whenever RFID tags are in the possession of individuals, they should have the opportunity to disable the tags and destroy the data they contain.

Systems based on these devices are now beginning to be widely implemented and it is evident that the publicity associated with the privacy risks of RFID has had a beneficial impact on deployment strategy that has been employed for this technology.

Near Field Communications (NFC)[19] links the technologies of RFID and Bluetooth used in mobile phones. Potential applications for NFC, whilst offering a "number of exciting technological possibilities", threaten to be even more privacy invasive than RFID.

The applications of technologies are still in their infancy and it will be necessary for the privacy aspects of both RFID and NFC to be kept under review.

Spam

In 2001, junk e-mail accounted for approximately 10% of all e-mail traffic; by 2005 this had risen to nearly 60% with over 40% of this emanating from the USA.

Spam is not merely privacy invasive, but can pose a real threat as frequently the junk e-mails carry with them a virus that can infect an individual's computer or a 'phishing' request that is designed to steal personal details such as account numbers, passwords or credit card details.

Concerted action through Directive 2002/58/EC appears to have reduced the activities of spammers located within Europe and the CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing Act), introduced in the USA in 2004, is beginning to have a positive effect, according to the report published by the Federal Trades Commission in December 2005.[20]

The report notes the success of the London Action Plan on International Spam Enforcement Cooperation, which now spans five continents with 33 government agencies from 23 participating countries as well as 24 private sector entities being involved.

The report also reveals that 50 successful prosecutions were made in the USA in 2004 and 2005 and that the there are firm indications that the amount of spam is at last beginning to decrease.

More effective international action is anticipated by the passage of the US SAFE WEB Act **(**Undertaking Spam, Spyware And Fraud Enforcement with Enforcers beyond Borders) which would facilitate worldwide cooperation by the FTC.

---

[18] www.privacyconference2003.org
[19] http://www.nfc-forum.org/home
[20] **Effectiveness and Enforcement of the CAN-SPAM Act A report to Congress, FTC, December 2005** http://www.ftc.gov/reports/canspam05/05122canspamrpt.pdf

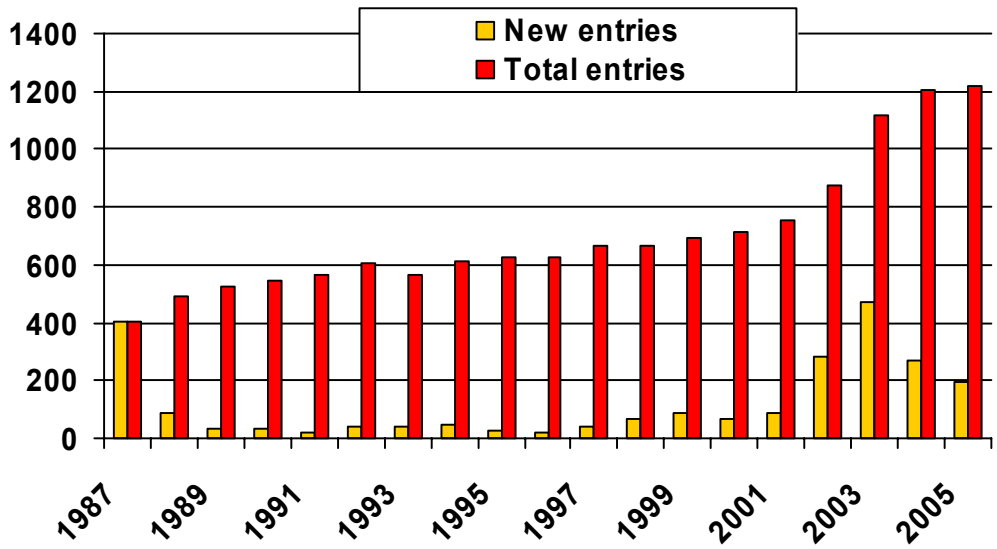
NOTIFICATION

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.

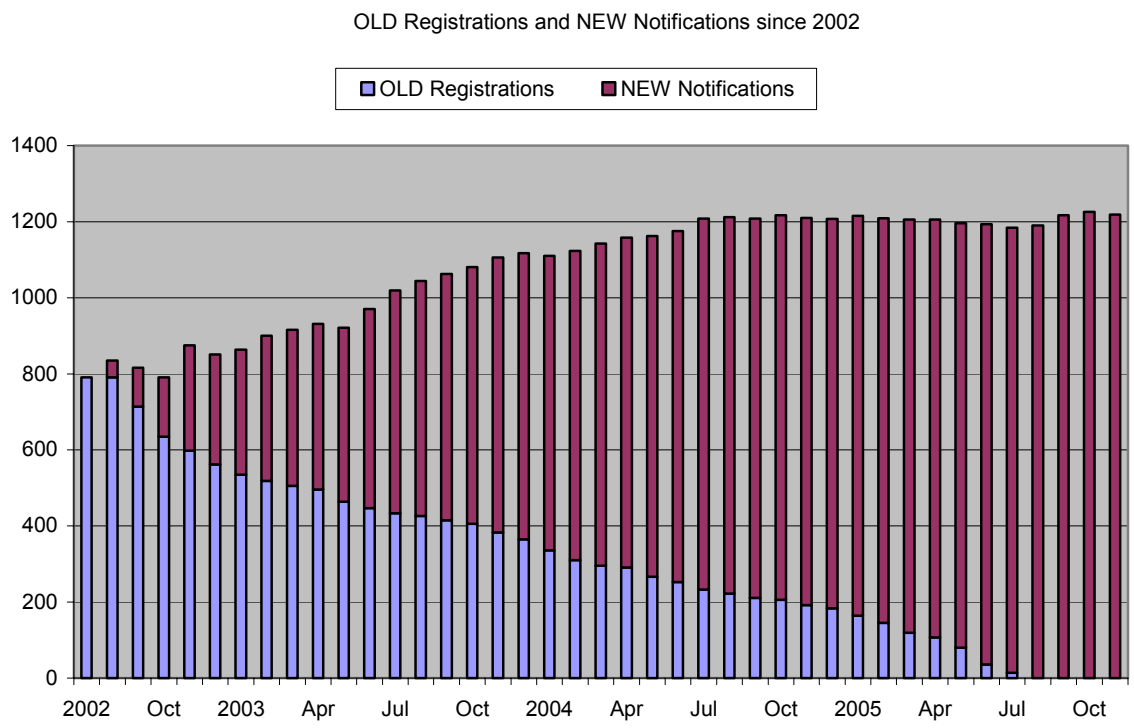
The chart below illustrates the rise in register entries since Registration under the 1986 Law commenced in October, 1987. As expected, the number of Notification entries appears to have stabilised at around 1200, which is 50% more than the number of Registrations that had been made by the end of the previous legislation in 2002 and three times the number of Registrations that had been made at its commencement in 1987.

GROWTH IN DATA PROTECTION REGISTER ENTRIES



The chart overleaf depicts the monthly decrease in triennial Registrations under the old (1986) Law and the corresponding growth in annual Notifications under the new (2001) Law, since its commencement in August 2002; this chart demonstrates that all the Registrations had either been closed or replaced by Notifications, as expected, by the end of July 2005.

At the end of December, 2005 there were 1219 Notifications on the register whilst 791 Registrations and 146 Notifications had been closed since 2002.



The entire Notification process may be completed online at http://www.dpr.gov.gg. 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 two years show that approximately 40% of the site accesses were for downloads of manuals and information, 18% for administration purposes and the remainder (42%) for online notification activities.

The Notification system and web site were developed by Eduserv Technologies Limited and were based on a similar system developed by Eduserv for the Information Commissioner's Office.

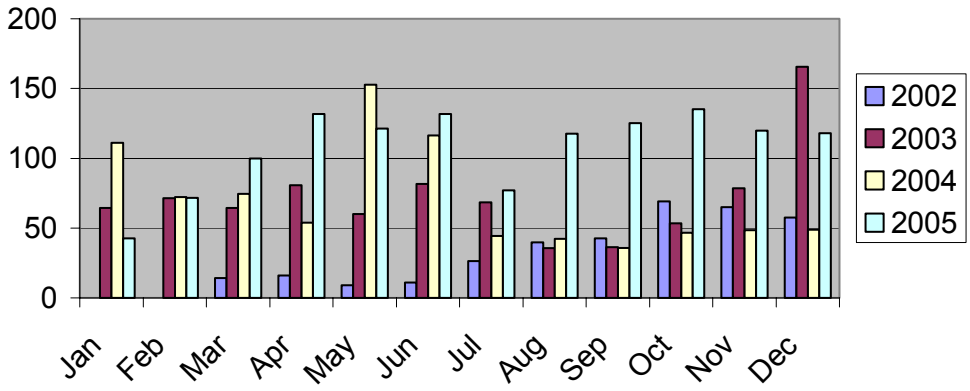
The system went into live operation in July 2002, one month before the commencement of the Law. Once the initial teething troubles had been resolved, the system proved to be extremely reliable with almost no significant down time having been recorded during normal working hours throughout the whole of this three and a half year operational period. Statistics collated by Eduserv show that during 2005 there was one unplanned outage lasting 50 minutes when there was a major failure of communications links in the Bath area – otherwise the site has shown 100% availability.

A total of 44 software issues were logged during the first 6 months of operation from August to December 2002; 46 issues were logged during 2003, 29 during 2004 and just 19 for the whole of 2005, all bar three of which had been resolved by the end of the year.

The chart below shows the variation in the average daily activity on the online Notification site between 2002, when Notification commenced and the end of 2005; the vertical axis represents the average daily rate of successful requests for pages of data from the site each month.

The variations in activity generally correspond with the number of new Notifications and renewals that are dealt with in each month. Activity appears to be much more evenly spread throughout the year than previously, now that all notifications are renewed on an annual basis.

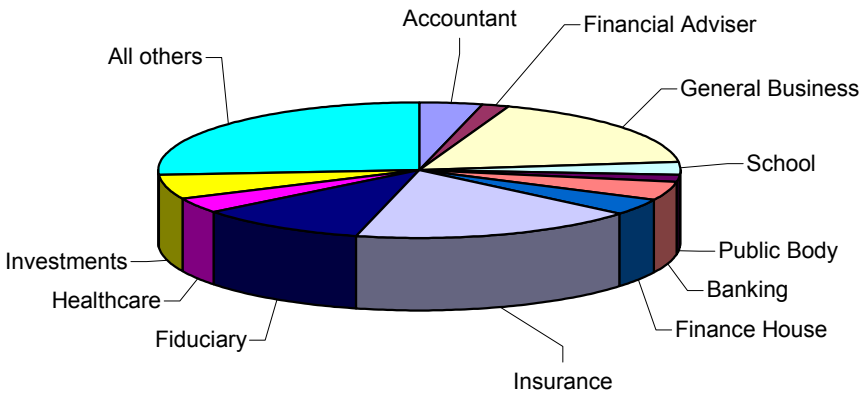
Comparison of Notification Site Activity between 2002 and 2005



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

The chart depicted below shows the cumulated distribution of notifications at the end of 2004 by industry sector, continuing a similar pattern to that of previous years.

Notifications by Sector in 2005



The largest proportion of Notifications used the General Business template (23%), followed by Insurance (19%), Fiduciary (13%), Investments (7%), Banking (6%), Healthcare (5%), Accountant and Finance House (both 4%), schools and public bodies (both 3%), financial advisers (2%), whilst 'All Others' comprised 12%.

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, the exemption from notification is 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 by 4 to 47, (4% 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 advised us that they were exempt.

During 2004 a further 144 organisations informed the Office of their exempt status making a total of 447 exempt controllers.

Some previously exempt organisations notified during 2005 as their circumstances had changed and a few others were added to the list, such that the total number of exempt organisations fell by 6 to 441. This represents 26% of the overall total [of 1660 exempt and notified organisations].

The online notification system was enhanced, with the assistance of the Treasury and Resources Department, in December 2005 to provide a link to the States of Guernsey Online Payment portal that allows for the online payment of the notification fee using a debit or credit card.

Online access to the Commissioner's bank account will facilitate acceptance of payments made via BACS as well as those by direct debit and by cheque.

It is intended that renewal reminders issued in future will advise data controllers of these new alternative payment options.

During 2005, 286 organisations paid by annual Direct Debit (approximately 23%).

1061 organisations (87%) provided an email address for communication purposes; this was used for the issue of automatic renewal reminders to the 702 organisations with an email address who did not renew by Direct Debit; of those, 183 (26%) required a second reminder to be sent by conventional post.

The most common reason for this was that the email address originally provided for the administrative contact had changed since notification.

Nevertheless, the use of automated email reminders and Direct Debits continues to reduce substantially the administrative effort involved in the notification process. It is to be hoped that this effort should reduce still further once online payments and payments by BACS as well as by Direct Debit become more widely adopted.

STAFFING AND STAFF DEVELOPMENT

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

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

The Assistant Commissioner devotes the majority of her time to compliance activities, responding to enquiries from individuals and organisations and running training courses for the public and private sector.

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 remains of the view 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 level of staffing resource, which enables him to discharge his responsibilities under the Law.

The use of external consultancy has again been limited to the provision of expert legal advice in those cases where it was not possible for such advice to be sought from the Law Officers.

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 Training Agency and the Guernsey Digimap Management Board and attends the seminars and workshops organised by the Agency and the local section of the British Computer Society. He was invited to speak at a conference organised by the Jersey Commissioner to publicise the Jersey Data Protection legislation in January, 2005.

The Assistant Commissioner has also attended some Training Agency seminars, in addition to participating in the DP Forum and continuing her legal studies with the Open University. She also furthered her knowledge by attending conferences in the UK organised by the Direct Marketing Association and by 'Data Protection Law and Policy'.

During 2005, the Personal Assistant enhanced her training by attending a specialised course dealing with the administration and content management of the Data Protection pages within the www.gov.gg government web site.

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 2005 has 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

In addition, the Office has assisted in sourcing the provision of external training specialists for a number of organisations.

Delivering presentations and training

The Commissioner and Assistant Commissioner delivered a number of talks and presentations throughout the year to many professional associations and organisations in the public and private sectors. These included: schools, finance institutions, law firms and retail businesses.

The total audience reached in this way was around **916**, compared with 564 in 2004 and 770 in 2003.

The Training Agency ran the first local course leading to the award of the ISEB Certificate in Data Protection and a further course is planned for 2006.

Involvement in Working Groups

The Commissioner and Assistant Commissioner have been invited to participate in the newly-formed States Data Guardians Group, which should meet early in 2006.

Making use of the media

15 articles or letters relating to Data Protection were published in the local press in 2005, (compared with 28 in 2004, 22 in 2003 and 19 in 2002) covering topics such as:

- Nuisance telephone calls;
- Inaccurate information, including ex-directory numbers, appearing in the Wave telephone book;
- Alleged denial of access to personal data by a States Department;
- ID Cards;
- The "Montreux Declaration" of the 2005 International Conference;
- The impact of the Jersey Data Protection legislation.

Guidance Notes Published by the Commissioner

The number of Guidance Notes published by the Commissioner during the year rose to **23**, compared with 20 in 2004, 18 in 2003 and 17 in 2002.

All of the existing publications were revised and the new A5 publications published in 2005 were:-

- Dealing with Subject Access Requests
- Exporting Personal Data
- Guidance for States Departments.

A full list of available publications is given below.

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.*
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 which manual records are covered by the Law*
Privacy Statements on Websites – a Guidance
Respecting the Privacy of Telephone Subscribers
The Data Protection Law and You: *A Guide for Small Businesses*
Spam – *How to deal with spam*
States Departments – a Guidance
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*
Your rights under the Law: *A Guidance for Individuals*

The Assistant Commissioner circulated this literature to a number of public, private and voluntary organisations throughout the Bailiwick and they are all available in PDF format for viewing or download from the Commissioner's web site.

Approximately **1,664** hard copies of the literature were distributed during 2005, compared with 1,500 copies in 2004, 4,000 in 2003 and 500 in 2002. Notification Guidance Handbooks were sent out to those data controllers whose registrations under the 1986 law were about to expire.

In addition, copies of the more detailed guidance on the Privacy and Electronic Communications Regulations and the monitoring of staff at work that had been produced by the UK Information Commissioners Office were made available.

Developing the Internet Web Site

During 2005, all of the information that had previously been published on: www.dataprotection.gov.gg was restructured and published on the Guernsey Government portal: www.gov.gg/dataprotection .

The Commissioner acknowledges the support received from the Information Technology Unit of the Treasury & Resources Department in enabling this transformation to be achieved in an efficient and effective manner.

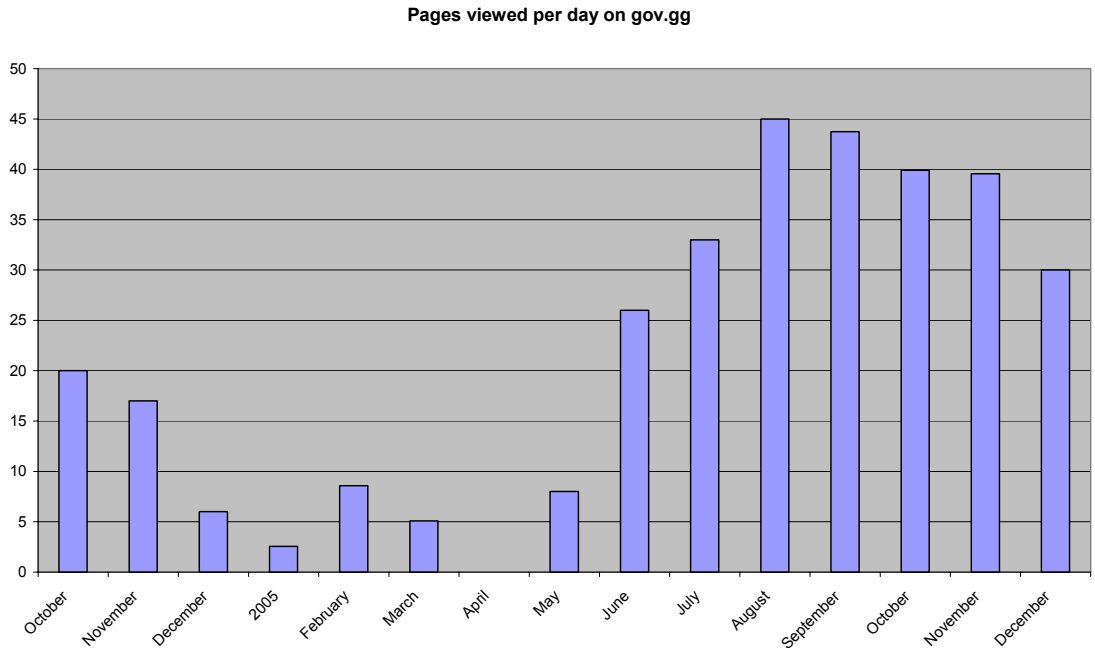
This new site uses content management technology which supports improved techniques for the location of information by end users and better facilities for the upload and maintenance of the information on the site by the staff of the Office.

In particular, in response to feedback from users, the Guidance Notes pages have been restructured into three pages, covering General Guidance, Guidance for Individuals and Guidance for Organizations and shortcuts to the Notification site: www.dpr.gov.gg have been reinstated.

Users of the former site are automatically redirected to the new site, which showed a steady growth in popularity following the completion of the changeover at the end of May 2005; prior to that time the new site had been running in parallel with the old site.

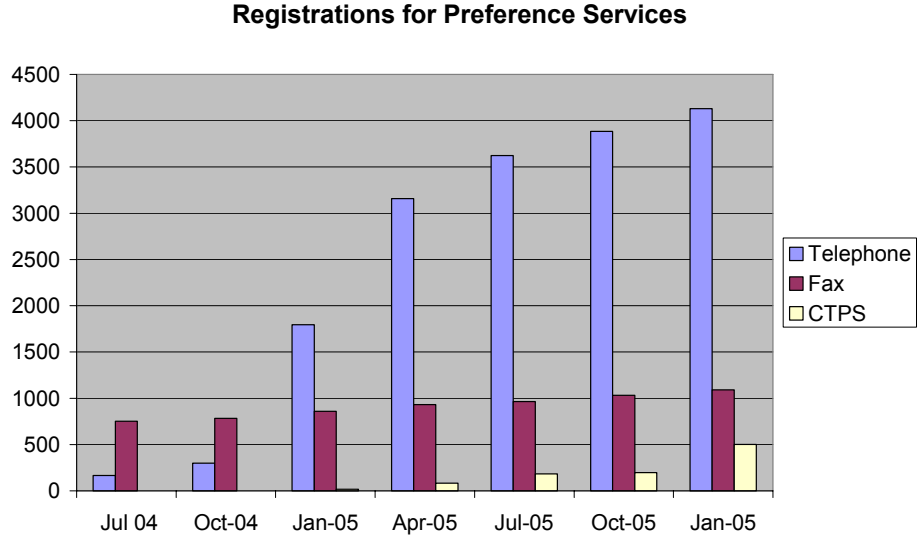
A chart of the average number of pages viewed per day between October 2004 and December 2005 is shown overleaf (unfortunately no statistics were available for the month of April 2005). Currently, it would appear that about 30 pages per day are being accessed, the most popular being the Guidance Notes pages.

It is reasonable to presume that the provision of ready access to information on the web site has reduced need for many people to make routine enquiries for information from the Data Protection Office.



Registrations with the Preference Services

Further publicity was given to the use of the Preference Services for reducing the receipt of unwanted telephone calls and junk faxes by means of dedicated pages in both the Cable & Wireless and Wave Telecoms phone books. By the end of 2005, the number of registrations for the TPS by private subscribers exceeded 4,000 for the first time and registrations on the Corporate TPS rose to 501, compared with 1,796 and only 19 at the end of 2004. Registrations with FPS rose from 860 to 1,092 during the same period.



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;

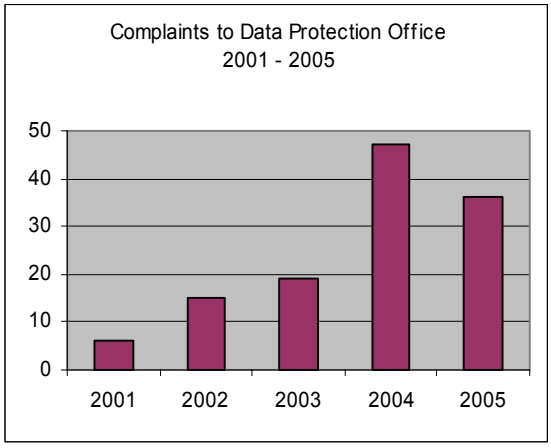
c) Failure to comply with a Notice issued by the Commissioner.

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.

Complaints

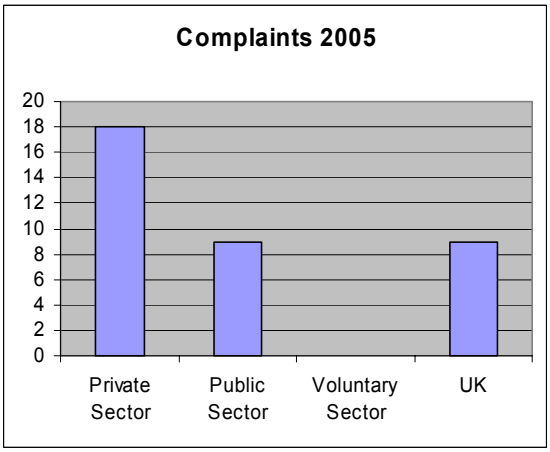
There were a total of 36 complaints received by the Commissioner during 2005.

This compares with a peak of 47 that were received in 2004 and relatively smaller numbers that were processed in prior years, as is shown opposite.

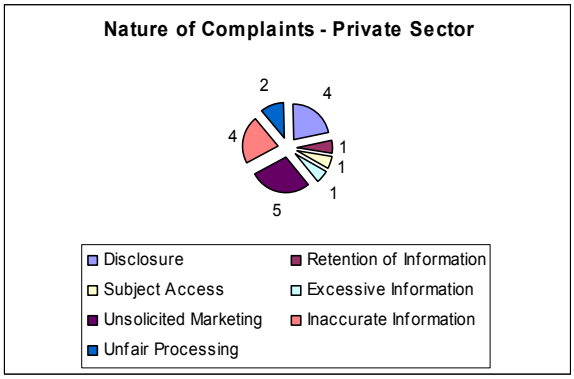


The breakdown of complaints received in 2005 and depicted opposite, shows that 18 related to the private sector, 9 to the public sector, none to the voluntary/charitable sector and 9 to UK organisations.

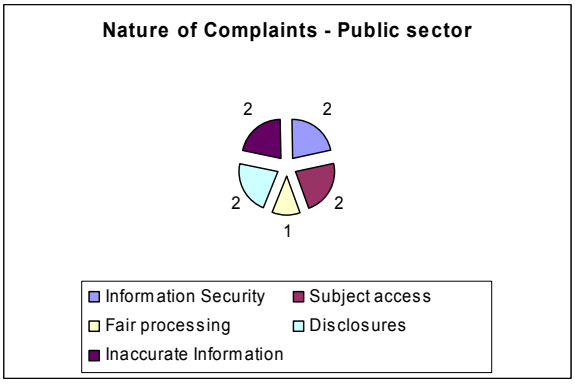
The 9 complaints against UK organisations, which were largely concerned with unsolicited marketing and junk faxes, were referred to the UK Information Commissioner's Office.



A breakdown of the complaints against the private sector can be seen opposite. The greatest number of complaints was concerned with unsolicited marketing (5), followed by inaccurate information and disclosure (4), unfair processing (2), holding of excessive information, retention of information and subject access (1).



The 9 complaints against the public sector were evenly split between subject access, information security, inaccurate information and disclosure (2), followed by one complaint of unfair processing.



Case Studies

A selection of these complaints is detailed below in the form of Case Studies.

Case Study 1

An Independent Financial Adviser complained to the Commissioner that one of his clients had been approached by an insurance agent who had previously provided services to this client. The client confirmed this complaint and stated that the "rogue" agent had details of a personal pension plan.
On investigation it was established that details of the personal pension plan had been obtained from a UK based Insurance Company by the "rogue" agent impersonating an employee of one of the UK Company's local agents. It appeared that information had been procured contrary to Section 55 of the Data Protection Law which would constitute the offence commonly referred to as "blagging".
The "rogue" agent resigned and stated that he had acted without the consent of his employer.
The matter was referred to the Law Officers, who concluded that, as the relevant data controller was established in the UK, any criminal offence would have been committed in contravention of the UK Act.
Accordingly, the matter was referred to the UK Information Commissioner.

Case Study 2

The Commissioner received a complaint that a States Department had not made information available in response to a subject access request made under Section 7 of the Law.
In order to investigate the matter, the Commissioner requested details of information held by the Department, but this request was refused.
The Commissioner was concerned by this apparent lack of cooperation from the Department and subsequently served an Information Notice on the Department in accordance with Section 43 of the Law.
The Department responded by threatening to appeal the Notice, claiming weaknesses in the Notice and alleged anomalies in the Law in relation to its applicability to States Departments. A supplementary Information Notice was issued against the relevant Minister.
The legality of this Notice was also challenged, but a resolution of the matter was ultimately reached by the Department "voluntarily" providing the Commissioner with access to the information that he had requested.
The Commissioner completed his assessment and found that in his opinion there were weaknesses in the way that the Department had handled the subject access request and that the Department held information that was eligible for disclosure to the complainant.
The Commissioner recommended that improvements were made to the departmental procedures such that they conformed to his published guidance on: "Dealing with Subject Access Requests".
The complainant resubmitted his subject access request and in response the Department disclosed certain information to him. This did not constitute all of the information that had been identified by the Commissioner.
However, as it appeared that the complainant was seeking this information in order to initiate legal proceedings against the Department, the Commissioner decided not to take further enforcement action but that it was up to the complainant to take court action under Section 7(9) of the Law if he felt that the Department had failed fully to comply with his subject access request.
This case raised a number of ambiguities in relation to the applicability of the Law to States Departments and the Commissioner will be recommending that these issues are addressed by proposed amendments to the legislation.

Case Study 3

An individual complained to the Commissioner's office about the circulation of "Notes" of a meeting that had occurred. These "Notes" made reference to family members and comments were made about child protection and welfare issues. The "Notes" were circulated to all who had attended the meeting as well as to other professionals from the educational, health and social work fields.

The complainant had been aware that the meeting had happened but had failed on a number of occasions to obtain a copy of the "Notes". Eventually later after much insistence, a copy of the "Notes" was made available and their content caused much distress to the complainant.

An internal investigation conducted by the Data Controller concerned concluded that the "Notes" were inaccurate and that they should have been given the status of "Minutes" rather than "Notes". A letter of correction was sent to each recipient to attach to their copy of the "Notes".

The Commissioner's Office asked the Data Controller to ensure that all the recipients confirm in writing whether they had attached the letter of correction to the "Notes", destroyed the "Notes" or returned them to their author.

The Commissioner found that the Data Controller had issued Guidelines to staff concerning the conduct of meetings especially in regard to child protection matters. The Guidelines were found to be satisfactory, but this particular meeting had not been conducted in accordance with those Guidelines.

This case identified a number of breaches of the data protection principles.

The sixth principle states that personal data should be processed in accordance with the rights of individuals. Such rights include the right to access one's personal data and to prevent any processing that causes damage or distress and the right to have inaccurate personal data corrected or deleted.

The fourth principle states that personal data must be processed accurately.

The seventh principle states that appropriate technical and organizational measures must be taken to process personal data. The issue of appropriate Guidelines to ensure that accurate and secure processing of information occurs is dictated by this principle.

It is the duty of all data Controllers not merely to have in place appropriate Guidelines, policies and procedures but also to ensure that staff are made aware of them so that they may be incorporated into everyday practices.

Case Study 4

A financial institution (Company A) complained to the Commissioner that a client had been contacted, without consent, by a past employee offering services from a new financial company (Company B). The contact had been by means of an unsolicited email.
Company A claimed that the past employees may have taken information with them to use for the benefit of Company B to market its clients. The Commissioner advised that the recipient of the email (the client) should make the complaint and a written complaint was duly received.
Based on the information received it appeared that a section 55 offence of the Law may have been committed by the past employees if there had been a disclosure of personal information without the consent of the Data Controller (Company A) to Company B.
In addition, it was considered that if an unsolicited email had been sent for the purposes of direct marketing this would constitute a breach of section 20(2) of the European Communities (Implementation of Council Directive on Privacy and Electronic Communications) (Guernsey) Ordinance, 2004. It is obligatory to obtain consent from clients before they are marketed by email.
Company A produced evidence that it had provided guidance to its employees in regard to the processing of clients' information; this evidence comprised staff training records, contracts of employment, continuing Confidentiality and Declaration of Secrecy in respect of information obtained during the individual's employment with the bank.
As there was an alleged criminal offence under section 55, the Commissioner approached the Law Officers to request the Police to undertake an investigation.
The Police interviewed the Director of Company B, his partner and another person (C) who had all once worked together at Company A. The Director and C had dealt with the client while working at Company A. They considered that they had had a good working relationship with him, had socialized with him and considered him to be a friend. They stated that during a dinner appointment they spoke about this client and considered that he might be a potential client for Company B.
Once the client was made aware of the criminal investigation, he withdrew the complaint against his "two friends" as he did not wish for them to be prosecuted.
As the client withdrew the complaint and it appeared that he may have been pressurized into making it, the Commissioner was advised not to pursue any further action against Company B.
Company A was advised by the Commissioner to ensure that in future clients were fully informed as to the nature of any complaint that they were being asked to make.
This case highlights some issues of which all Data Controllers should be aware and take note.
To send an unsolicited email for the purpose of direct marketing is a breach of the Electronic Communications Regulations. The Commissioner would require such practice to cease. In the event that any Data Controller would ignore this instruction the Commissioner would issue an Enforcement Notice to ensure compliance. To ignore an Enforcement Notice is an offence.
Employees owe a duty of fidelity to their employers and so any information they obtain in the course of their employment must not be used outside the organization for personal benefit or for any detriment to others. This applies to information retained in the employee's memory as well as information in tangible form that can be removed by the employee. Any resulting disclosure of personal information without the consent of the Data Controller would be an offence under section 55 of the Data Protection Law.

Case Study 5

Some Sark residents claimed that the circulation of minutes of an informal meeting violated their privacy and that of their children. As it had taken place without the knowledge of the Committee responsible (the Data Controller) any disclosure of information without the consent of the Data Controller by its staff would constitute an offence under section 55 of the Data Protection Law. For this reason the Commissioner treated the complaint as a Request for Assessment.
After an assessment of the minutes he concluded that they did contain the personal information of some adults and children.
Although there here had been an attempt to conceal the identity of the children mentioned some complainants stated that many people could recognize the children because Sark is a small community.
Some complainants claimed that they suffered distress as confidential information concerning their children was now in the public domain. It was also claimed that some of this information had not even been made known to the parents. One claimed of being approached by a significant number of people asking if the information in the minutes was true.
Another complainant claimed that the minutes were widely distributed and not kept confidential.
The Chairman of the meeting informed the Commissioner that the intention had been to keep the minutes confidential and to circulate them only to members of staff and the Committee.
It was established that the minutes had been faxed from a local pub.
The Commissioner requested the Law Officers to assess the findings with a view to prosecution. This request was refused on the grounds that it would not be possible to find out with any certainty who had faxed the minutes.

Case Study 6

An Alderney resident claimed that a member of the Policy and Finance Committee had disclosed information about him to a third party. This information related to the possession of a work permit.

On enquiry the Commissioner was informed that work permits are administered by the Policy and Finance Committee. They appear as a standard item on the agenda of the monthly Committee meeting; it is within the remit of the Chief Executive to make a decision on individual applications but he will at times ask the Committee to decide.

Any applications granted by the Chief Executive are not considered to be confidential from the Committee. The Chief Executive will give information about the work permit status of an individual to a Committee member upon request if there is a justifiable reason.

Moreover it is an offence under the Employment Permits (Alderney) Law, 1975 for a person to make a misrepresentation to an employer that he does not need a work permit.

In this particular case the Committee member had reason to suspect that the complainant was making such a misrepresentation, and took steps to insure that the Law was being complied with. In doing so he did not contravene the Data Protection Law as section 29 of this law provides for disclosures to be made in connection with the prevention and detection of crime. In addition the complainant did not suffer any detriment as he was merely advised to make a retrospective application.

The Employment Permits Law provides for an Inspector to be appointed by the Chief Executive to ensure that only individuals in possession of a work permit, or exempt from having one, are employed. An Inspector has now been appointed and this should remove the need for Committee members to police the work permit legislation personally.

INTERNATIONAL LIAISON

International Conference of Data Protection Authorities

The 27th International Conference of Data Protection and Privacy Commissioners was held in the Montreux Convention Centre, Switzerland, from 14th to 16th September 2005.

The theme of the conference was: "The protection of personal data and privacy in a globalised world: a universal right respecting diversities."

The Commissioner and the Assistant Commissioner participated in this conference, which was attended by over 300 delegates from the major countries in the world. The Commissioner was invited to chair one of the sessions, entitled: "What can organisational and evaluation techniques offer to guarantee Data Protection?"

Other topics covered during the two days of the public conference sessions included:

- Humans and the web – a civilizatory view;
- One law of Data Protection in different legal, economic, political and cultural systems: utopia or reality?
- The principles of Data Protection – an adequate answer to the internet?
- New invasive technologies – are new Data Protection standards needed?
- The economy facing a vast variety of Data Protection rules – towards a simplification of regulations and procedures?
- 10 years after the adoption of the EU Directive 95/46/EC – what are the experiences, what are the prospects?
- The importance of self-regulation in the implementation of the Data Protection principles;
- The effectiveness of Data Protection supervision;
- The regulation of trans-border flows facing globalisation;
- How can the requirements of Data Protection be reconciled with the fight against terrorism?
- The role of the private sector in Data Protection to fulfil public tasks – when private companies become "Big Brother";
- Bio-banks and related challenges;
- Political marketing - towards a code of conduct?
- The contribution of international organisations to the enforcement of Data Protection law;
- Police cooperation in a federal state.

The public conference concluded on 15th September and was followed by a closed session, restricted to Commissioners from accredited countries and territories – essentially those with Data Protection or privacy legislation that complied with accepted international standards.

The closed session of the conference endorsed three resolutions:

- On the use of Personal Data for political communication;
- On the use of Biometrics and
- The Montreux declaration.

The Commissioner was a joint sponsor and co-author of the "Montreux Declaration" which was addressed to international bodies and reiterated the need for concerted international action to improve the protection of personal data throughout the world.

Full details of the presentations given at the conference and the text of the resolutions are available at: www.privacyconference2005.org

The Commissioner intends to participate in the 28th Conference, which is planned to be held in Argentina in November 2006 and Canada has offered to be the host for the 29th conference in September 2007.

European Spring Conference

The annual Spring Conference of European Data Protection Authorities took place in Krakow, Poland on 25th – 26th April 2005. It was attended by representatives of EU level bodies and national delegates from 34 countries, including all the Member States of the EU. The Bailiwick was represented by the Assistant Commissioner.

The Commissioner first participated in the Spring conference that was held in Bonn in 2002 and the Assistant Commissioner attended the 2003 conference in Seville.

The 2005 conference was mainly devoted to the 10th anniversary of the adoption of European Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Sessions and discussion took place on the following:

- The impact of the Directive on personal data protection in the EU and Third Countries;
- Whether any amendments of the Directive were necessary;
- How decisions of the European Court of Justice impact on the application of the Directive;
- How the Directive may be interpreted in a world of advancing technology, increasing terrorism and social and cultural changes;
- Transfer of personal data to third countries (i.e. any country outside the EEA);
- The rights of individuals to access their personal data;
- Methods of increasing the awareness of individuals about data protection.

As is customary, a short meeting of the European Commissioners was also held during the International Conference of Data Protection Commissioners in Montreux and was attended by the Commissioner.

The Assistant Commissioner is planning to attend the 2006 European Spring Conference, which is due to be held in Budapest.

International Working Group on Data Protection in Telecommunications (IWGDPT)

This Working Group was originally formed in 1983 on the initiative of the Berlin Commissioner to study the impact on privacy of the growth in telecommunications and to recommend actions to the annual international conference of Data Protection and privacy Commissioners. The Working Group normally meets twice per year – each spring at the invitation of one of the member countries and each autumn in Berlin.

The Commissioner participated in both meetings of this Working Group, which were held in Funchal and Berlin.

35 delegates from 24 countries attended the meeting in Funchal from 31st March to 1st April 2005 and 46 delegates from 26 countries attended the meeting which took place in Berlin from 6th – 7th September 2005.

The major topics covered in the meetings were:

- Geo-location technology;
- Privacy and public key infrastructure;
- Data Protection and electronic voting;
- E-health and privacy;
- E-government;
- Privacy aspects of web-based services (e.g. Google Mail);
- Privacy and copyright management;
- Developments with Spam;
- Personal data in WHOIS databases;
- IP telephony;
- RFID;
- Web-logging;
- Peer to peer computer networks;
- Telecommunications-related Video-surveillance;
- Voice analysis/stress detection technology;
- Electronic wristbands;
- Working group on internet governance;
- Satellite technology (e.g. Google earth);
- The Council of Europe media division.

Papers adopted and published by the Working Group are available online at:

http://www.datenschutz-berlin.de/doc/int/iwgdpt/index.htm

The Commissioner plans to attend the next meetings of the Working Group in Washington (April 2006) and Berlin (Autumn 2006) and the Working Group has accepted an invitation from the Commissioner to meet in Guernsey in April 2007.

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

These meetings originated from the regular liaison meetings between the UK, Irish, Isle of Man, Guernsey and Jersey Authorities which took place when these Islands were drafting their original data protection legislation in the 1980's. The meetings continued whilst revised legislation compliant with the European Directive was being contemplated, drafted and subsequently implemented in the UK, Ireland and the Islands.

In 2004, membership was broadened to include the island authorities from the EU accession territories of Cyprus and Malta, which had received special assistance from the Irish and UK Commissioners with their preparations for enacting data protection legislation that was compliant with European standards.

It has been found that many common problems arise in small communities and that these relatively informal meetings help to ensure a consistency of approach and a greater understanding of the application of the Data Protection principles to these similar situations.

The annual liaison meeting was held in Cyprus in May 2005 and was attended by the Commissioner and the Assistant Commissioner.

The agenda included:

- The restructuring of the UK Information Commissioner's activities;
- Simplification of Privacy / Fair Processing Notices;
- Update on Binding Corporate Rules
- International Travel Issues (PNR, biometric travel documents, etc);
- The Privacy and Electronic Communications Directive and its applicability to the various territories;
- Powers of the Commissioner in relation to government departments.

There was no meeting in the Autumn, but the UK Commissioner hosted a one-day special conference on "Data Protection – the next 21 years?", which was held in Manchester in November 2005 and was attended by the Commissioners from Guernsey, Jersey, the Isle of Man and Ireland, together with representatives of the public and private sectors in the UK, and a small number of European counterparts.

This conference included presentations and discussion groups covering:

- Changes to the operating environment in the future;
- Data protection challenges and reform options in post-liberal democracies;
- Better compliance by data controllers;
- Better powers for the Information Commissioner;
- Better remedies for the individual.

It is planned that the next meeting of the Authorities will be held in the Spring of 2006 in the Isle of Man.

Liaison with the UK Government

Regular meetings used to be held between the Data Protection authorities from the Islands, the UK Commissioner's office and the Whitehall officials responsible for advising on UK Government policy. These meetings commenced in the 1980's firstly at the Home Office, secondly at the Lord Chancellor's Department and thereafter at the Department of Constitutional Affairs.

The meetings were particularly valuable during the drafting stages of Data Protection legislation and prior to the adequacy assessments by the European Commission.

There were no formal meetings held in 2005 between the Islands' authorities and the officials responsible for dealing with Data Protection policy within the Department for Constitutional Affairs, but contact has been maintained and informal discussions held during regional and international conferences which have been attended by all parties.

In particular, the opportunity was taken during the conference held in Jersey in January 2005 concerning the Data Protection (Jersey) Law 2005, to discuss current developments with the Jersey Commissioner and the official from the Department of Constitutional Affairs, who was a guest speaker at that conference.

In addition, the Commissioner has been briefed on the UK Government's response to the European Commission's review of the Data Protection Directive; there have been no indications that any amendments to the UK legislation are currently being planned.

Data Protection Forum

The Data Protection Forum is a UK-based association which provides a focus for the collection, formulation and exchange of information on data protection.

Membership comprises a cross section of those involved with data protection and includes private sector members from financial services, retail, accountancy, travel, charities and public sector members from the police, local authorities, universities, as well as lawyers, consultants and consumers.

The Forum is based on the idea that co-operation between organisations in all areas would be advantageous and so aims to bring together companies, public sector and consumers to discuss privacy and personal data issues in order that mutual assistance and support may be provided.

Meetings are normally held in London four times a year and information is provided on a dedicated website (www.dpforum.org.uk).

In June, 2005 the Commissioner was invited to deliver a presentation to some 200 members of the Forum and spoke on the topic of "exporting personal data". The meeting was held at British Airways Waterside headquarters near Heathrow.

Afterwards, the Commissioner shared a "Question-Time style" panel with his fellow Commissioners from the UK, Republic of Ireland, Jersey, the Isle of Man and New Zealand. The audience responded with a set of many varied and topical questions but, in contrast to Question Time, there was much discussion but little dissent within this panel!

This meeting was widely reported, including an article in the British Airways staff magazine (see below).

Expert visit on data protection

BRITISH Airways hosted a meeting of data protection experts this week at the airline's Waterside headquarters.

Five information commissioners – experts in the field of data protection – formed the panel of the event where they presented to and took questions from an audience of privacy professionals from organisations in the UK, including BA, and public and private sectors.

They are all members of the Data Protection Forum, a UK-based organisation that BA is also a member of, promoting best practice for the protection of personal data.

"Personal data" is information relating to a living individual who can be identified from the data. Examples within the airline of personal data are people online records and passenger name records. Personal data is subject to the UK Data Protection Act and similar legislation in many other countries.

Sarah Bains and Paul Byrne of Im information security represent BA on the forum, and at the event Sarah was elected chairman of the organisation – which provides information on current privacy issues as well as opportunities to discuss practical approaches to compliance.

Sarah said: "Data protection awareness and compliance within BA is key to assuring that all personal data is kept safe and secure and processed in accordance with privacy legislation and guidelines."

Also present were 20 of BA's own data protection coordinators who work throughout the airline, managing queries from their departments and assisting Sarah and Paul on compliance matters.

The event coincided with a programme of data protection awareness within BA to highlight elements including data retention, disposal, classification and completion of mandatory computer-based training by all managers and staff handling personal data.

If you would like to know who the data protection co-ordinator is for your area, please see the intranet – "Company Procedures/ Are You Managing Risk?/ Information Security/ Law inc Data Protection/ Data Protection Coordinators."

Ready, steady, shred: Richard Thomas, UK information commissioner; Dr Peter Harris, data protection commissioner, Guern-sey; Iain McDonald, data protection supervisor, Isle of Man; Emma Martins, data protection registrar, Jersey; Marie Shroff, New Zealand privacy commissioner; Geoff Want, director safety, security and risk management and Gordon Penfold, head of Im business development.

Following this event, the regulatory authorities which attended were given honorary membership of the Forum and it was suggested that such an event might be repeated in the future.

The Bailiwick was represented at the September and December meetings of the Forum by the Assistant Commissioner. It is considered that 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 was invited to become a member of the British Computer Society [BCS] Information Privacy Expert Panel [IPEP], which is a small group of up to 16 members that was formed to provide expert guidance on Data Protection and Privacy matters to the BCS Security Forum Strategic Panel and onwards to Government, industry, the media and the general public.

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 Commissioner attended two meetings of this panel in 2005 and has been invited to attend four meetings in 2006. The cost of attendance at these quarterly meetings of the IPEP and at any related meetings is borne by the BCS.

OBJECTIVES FOR 2006

The primary objectives for 2006 will encompass the following areas:-

- ***Legislation***

  The Statutory Code of Practice on the Disclosure of Criminal Convictions in connection with Employment will be completed to tie in with the commencement of the Rehabilitation of Offenders Law and section 56 of the Data Protection Law.

  Advice will be given to the States on the need for changes to the local Data Protection legislation.

- ***Adequacy***

  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***

  The liaison with the Jersey Commissioner, the Isle of Man Supervisor, the UK and Irish Commissioners, the Commissioners from Cyprus and Malta and the maintenance of contact with officials from the UK Department of Constitutional Affairs will continue.

  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 of the Telephone and Fax Preference Services and periodic surveys to determine their use and effectiveness will be undertaken.

- ***Compliance***

  Targeted compliance activities will be organised to increase the notification level of local organisations. More rigorous enforcement will take place, 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 be done.

- ***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.

- ***Conference organisation***

  The preliminary organisation of the meeting of the IWGDPT in Guernsey in April 2007 will be completed, together with an investigation of the feasibility of holding a Data Protection conference immediately preceding that meeting.

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	**2005**	**2004**
	£	**£**
Data Protection Fees [1]	41,686	37,622
EXPENDITURE		
Rent	16,276	15,526
Salaries and Allowances[2]	137,251	129,782
Travel and Subsistence	9,751	7,366
Furniture and Equipment [3]	14,237	13,107
Publications	2,609	2,199
Post, Stationery, Telephone	4,253	3,881
Heat Light, Cleaning	4,874	5,054
TOTAL EXPENDITURE	**£189,251**	**£176,915**
EXCESS OF EXPENDITURE OVER INCOME	**£147,565**	**£139,293**

NOTES

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

Income includes accrued income (on a monthly basis) from previous years: £1,543.75 being the final accrual of the triennial registrations from January to July 2002 and £18,144.58 from annual notifications and renewals throughout 2004.

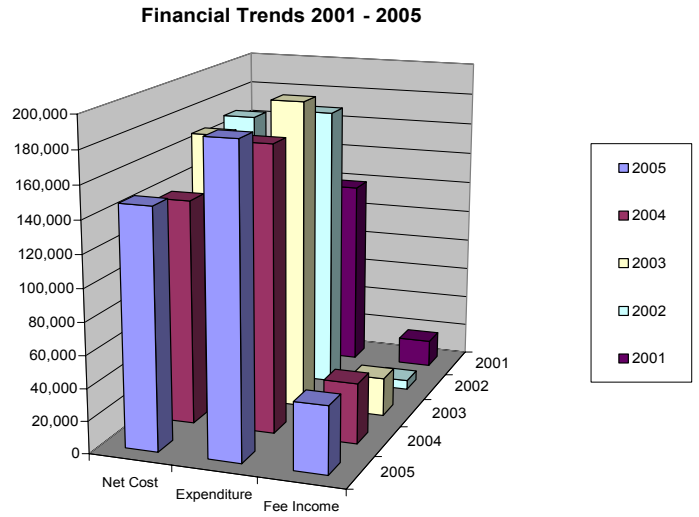
The cash received for 2005 was £42,665 (£35,875 in 2004) representing receipts for the 1219 annual notifications and renewals that were processed during 2005.

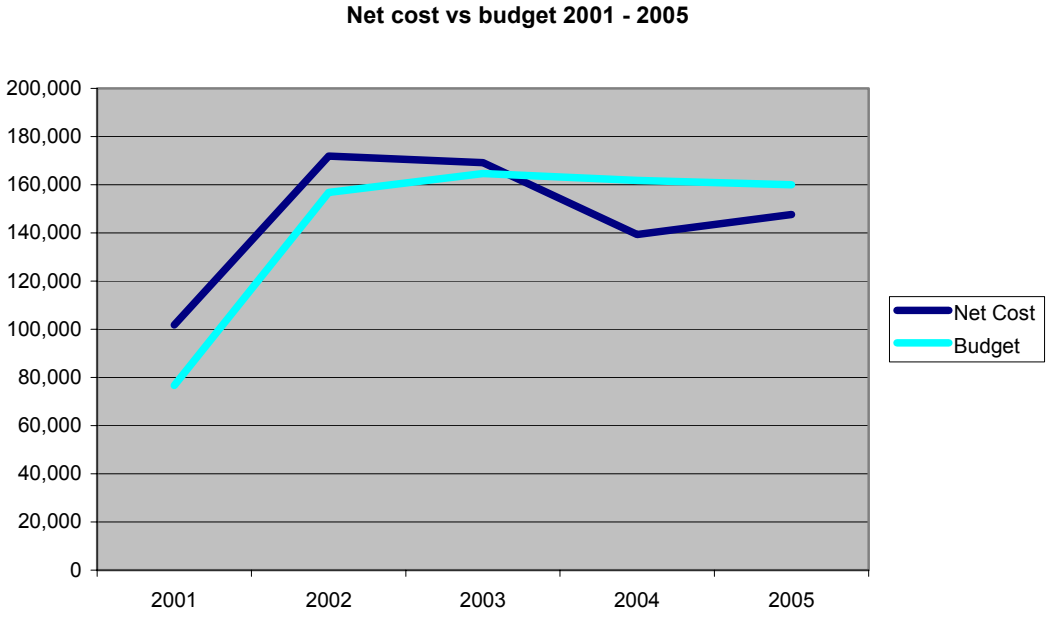
[2] This includes an amount of £6,270 for consultancy (£6,315 in 2004) concerned with the provision of legal advice that was not available from the Law Officers.

[3] This includes an amount of £3,048 for replacement of the four year old file server and a one-off payment of £1,200 towards the implementation of online payments system, but

no balancing allowance for the return of the old equipment to the ITU for potential use elsewhere.

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





Expenditure for 2005 was kept under strict control and the net cost of the Office again remained below the authorised budget for the year. Whilst there remains little scope for any further reduction in expenditure, it is intended that proposals will be put to the States

in 2006 for a modest increase in Notification fees, which should reduce the net cost and mean that all of the non-salary costs of the Office should be fully recovered through fees.

The Office was subject to an Internal Audit in October. This had been requested by the Commissioner, who was keen to ensure that the Office should be audited at least once during each Commissioner's normal term of office. The auditors were requested in particular to recommend improvements to operating procedures; the resulting report assessed the Office as "satisfactory", with 9 recommendations on procedural matters being made. Of those, five were accepted and implemented, two were partially accepted and two rejected as impractical at present.

One of the recommendations that was accepted related to the recording and reporting of any materially significant gifts or hospitality and it was agreed that a statement would in future be included in each Annual Report.

In accordance with that recommendation, it is confirmed that no gifts or hospitality were received by the Commissioner or his staff during 2005.

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 via:

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

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