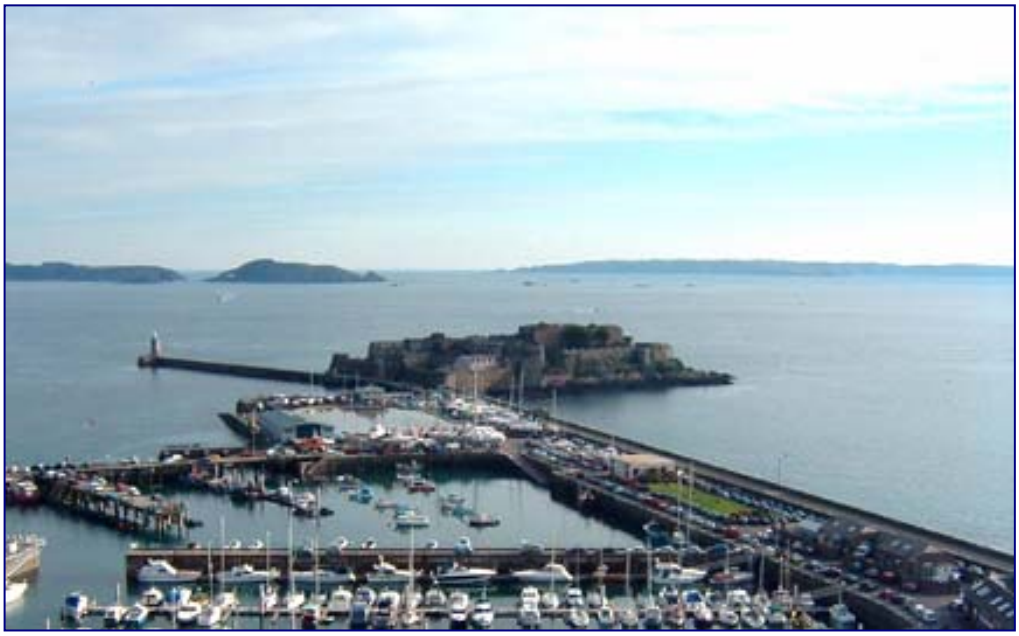
BAILIWICK OF GUERNSEY

DATA PROTECTION COMMISSIONER
REPORT FOR 2004



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: "Safe Harbor" – St. Peter Port harbour in the foreground, with the islands of Herm, Jethou and Sark in the background.

CONTENTS

FOREWORD

I am pleased to submit to the States my fourth public report on Data Protection in the Bailiwick of Guernsey; this has been prepared in accordance with paragraph 5 of Schedule 5 of the Data Protection (Bailiwick of Guernsey) Law, 2001.

The report covers the calendar year ending 31st December 2004, which started with a welcome visit from His Excellency the Lieutenant Governor in January; it was clear that His Excellency was most interested in the work of my office and in particular in the independence of the functions of the Commissioner.

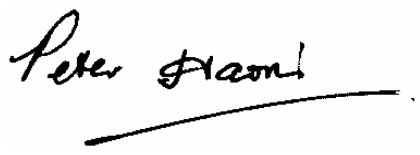
Following the publication in 2003 of the European Commission's declaration of the adequacy of the Bailiwick's Data Protection legislation, the next priority was to recommend the enactment of legislation to meet the revised European standards in the Directive on Privacy and Electronic Communications; as well as strengthening the protection for the privacy of telephone subscribers and e-mail correspondents, this legislation would control the sending of unsolicited communications, including "Spam" by organisations established within the Bailiwick.

My office dealt with an increased number of complaints during the year, most of which were resolved without the need for formal action, although it was found necessary to issue Notices in a small number of cases. A complaint about the unauthorised disclosure of information by a local voluntary body was upheld. Prosecution was contemplated in a number of cases, mainly concerned with non-notification, but it was eventually decided merely to issue cautions in a few specific instances.

Many people were troubled by the increasing volume of unsolicited communications. Where these emanated from within the British Isles, they were able to be dealt with by registration with the telephone or fax preference services, with some complaints involving unsolicited faxes being submitted to the UK premium service regulator. However, little can presently be done about bothersome calls or emails originating from outside the British Isles, unless a company established in the UK can be identified as having instigated such calls.

The Bailiwick was represented during the year at international conferences held in Argentina and Poland, where I was privileged to have been asked to present a paper. Nearer to home, the Assistant Commissioner and I attended a meeting in Jersey of the authorities from the British Isles, Ireland and Cyprus.

There has been continued interest in the provision of short training courses, given either by my staff or by specialists from the UK. In 2005 it is planned to establish local training courses facilitated by the Training Agency leading for the first time to a formal qualification in Data Protection.



Data Protection Commissioner, March, 2005.

THE BAILIWICK OF GUERNSEY

2004 saw the eight hundredth anniversary of the granting of independence to the Channel Islands by the British Crown. The Islands are located in the English Channel within the Gulf of St. Malo off the north-west coast of France. The islands form part of the British Isles but, as they do not form part of the United Kingdom, they are not Member States of the European Union. However, the islands remain as 'dependencies' of the British Crown (being neither part of the United Kingdom nor colonies) and enjoy full independence, except for international relations and defence, which are the responsibility of the United Kingdom Government.

The Channel Islands comprise two independent Bailiwicks – the Bailiwick of Guernsey and the Bailiwick of Jersey. This report concerns the Bailiwick of Guernsey (hereafter referred to as 'the Bailiwick'), which includes the main islands of Guernsey, Alderney, Sark, together with Herm, Jethou, Lihou, Brecqhou and some associated uninhabited islets and offshore rocks.

Alderney and Sark have their own legislative assemblies and, whilst much legislation is applicable to the individual islands, the Data Protection Law applies on a Bailiwick-wide basis and accordingly the responsibilities of the Data Protection Commissioner extend throughout the Bailiwick.

DEVELOPMENTS IN LEGISLATION

Data Protection Law

The Bailiwick has had Data Protection legislation since 1986. Commencement of that legislation in 1987 enabled the United Kingdom's ratification of the Council of Europe Convention 108 to be extended to the Bailiwick. However, the 1986 Law was not fully compatible with the European Data Protection Directive (95/46/EC), which meant that the Bailiwick was not able to achieve an adequacy status for the transfer of personal data from the European Union.

The Data Protection (Bailiwick of Guernsey) Law, 2001 ("the Law") came into force on 1st August 2002. The Law transposes all the relevant provisions of the European Directive (95/46/EC), resulting in the Bailiwick having been recognised by the European Commission as providing adequate protection for the trans-border flow of personal data.

Two periods of transitional relief were defined in the Law: after the first, which ends on 31st July 2005, existing automated processing must be up to the standards for new processing in the Law and subject access rights will extend to manual information held in relevant filing systems; after the second, ending on 24th October 2007, manual data held in relevant filing systems will be fully incorporated into the law.

Sixteen Statutory Instruments came into force at the same time as the commencement of the Law in August 2002, providing further detail on the implementation of the legislation, for example by specifying exemptions and detailing the notification regulations.

During 2004, two further Statutory Instruments were made: the first extended the exemption for processing of sensitive personal data [without necessarily obtaining consent] to elected representatives; this had the effect of requiring those elected representatives who processed such data to Notify under the Law. Accordingly, as an administrative convenience, the second Statutory Instrument exempted elected representatives who process personal data in their own right from the need to pay notification fees.

Privacy and Electronic Communications

In June 2004, the States of Guernsey approved the European Communities (Implementation of Council Directive on Privacy and Electronic Communications) (Guernsey) Ordinance 2004 ("the Regulations"). As the Regulations applied solely to Guernsey (including Herm and Jethou), similar Ordinances were drafted for Alderney and Sark.

The Regulations implement the European Directive 2002/58/EC which extends the definition of personal data to include all manner of electronic communications (including in particular e-mail and SMS messaging) and provides a statutory opt-out capability for individuals and businesses from receiving unsolicited marketing material by electronic or telephonic means.

As a result, there was increased publicity given to that fact that Bailiwick residents may take advantage of the preference services operated by the Direct Marketing Association in the UK and that organisations based within the Bailiwick and marketing to the UK must cleanse their marketing lists using the suppression databases available from that Association.

This topic is covered in more detail later in this report and a brief summary of the Regulations is given in the Appendix.

Rehabilitation of Offenders

Commencement of the Rehabilitation of Offenders (Bailiwick of Guernsey) Law was delayed for further consultation to take place on those occupations that were excepted in the legislation.

Nevertheless, the Code of Practice on the disclosure of criminal convictions in connection with employment that was developed by the Commissioner did receive a wide circulation and is ready to be put in place once the Commencement Ordinance has been made.

The Code of Practice was produced in three parts and is designed to complement the law by:

- providing guidance to employees who may need to obtain their record,
- specifying the procedures that should be used by employers who would be seeking such information and
- outlining the procedures to be followed by the Police who would be responsible for its provision.

Updating the Law

It is understood that the European Commission has written to the UK Government with a number of questions over the conformance of the UK legislation to the Directive. This is part of community-wide measures to reduce disparities between Member States in the way that the Directive has been transposed.

It is conceivable that the outcome of this process might be some proposals for changes to the UK Data Protection Act, 1998.

These developments will be monitored in the coming year in consultation with staff from the UK Department for Constitutional Affairs and any consequential recommendations for changes to the local legislation advised to the States via the Home Department in due course.

DATA PROTECTION ISSUES

ENUM

ENUM is an acronym for Electronic NUMbering and has been on the agenda of the International Working Group for Data Protection in Telecommunications for a number of years.

The ENUM proposal is fundamentally a technical solution to facilitate the convergence of the telephone system and the Internet and could prove to be a vital component of the Voice over IP protocol which promises to lower the cost of international telephone calls by routing them over the Internet.

Whilst offering a number of technical and economic benefits, the proposed system also carries risks, especially to the privacy of telephone subscribers, since the ENUM database would be a publicly available source of all telephone numbers.

A number of trials have been carried out internationally on the feasibility of such a scheme and in particular on its privacy aspects.

In May 2004, the UK ENUM Trial Group reported on the results of the UK Trial (www.ukenumgroup.org) and the DTI mounted a consultation exercise on the options for supervisory arrangements for the public ENUM data base between August and November 2004
(www.dti.gov.uk/consultations/consultation-1230.html)

The Bailiwick authorities were invited to submit comments in particular as to how they wished to participate in the supervision scheme for the ENUM database, bearing in mind that it would be structured in a similar way to the British Isles integrated telephone numbering system, that is presently controlled by OFCOM.

The Commissioner's comments focused on the Data Protection and privacy risks and how they might be addressed. These comments were submitted to the DTI through official channels in November. It is understood that similar concerns were voiced in the response from the UK Information Commissioner.

A final report on the outcome of the DTI consultation is awaited.

The Taxation on Savings Directive

On 3 June 2003, the European Union Council of Ministers adopted the Directive on Taxation of Savings Income in the form of Interest Payments [the "TOSD"] (Council Directive 2003/48/EC - see
http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/03/787&format=HTML&aged=1&language=en&guiLanguage=en).

This measure forms one of the elements of the "Tax Package" aimed at tackling harmful tax competition in the Community. On 19 July 2004, the Council adopted a Decision establishing the application date of 1 July 2005 (Council Decision 2004/587/EC).

Compliance with the "TOSD" requires the financial services institutions established in the Bailiwick to co-operate with the tax authorities in EU Member States in respect of interest paid on money deposited here by EU residents.

The Bailiwick authorities, in common with those in the other Crown Dependencies, decided by default to collect a retention tax on such deposits, but an option existed for the exchange of information in lieu of the payment of the retention tax.

If a financial institution wished as a matter of policy to opt for the automatic exchange of information, rather than the deduction of a retention tax, this would raise data protection issues, as their deposit-holders would have to consent to any resulting disclosure of information that was not mandated by Law.

The authorities decided to issue comprehensive guidance notes on the measures needed to comply with the Directive and the Commissioner was consulted on the Data Protection guidance notes to be included in that publication.

The final version of the guidance on this matter read as follows:

> *"Authorisation to report information ... can be in such form as the paying agent will require, but can normally be expected to take the form of a written agreement, letter or other document between the parties. Individual beneficial owners will be regarded as giving express authorisation by adopting a course of conduct in accordance with such documents. The collection of retention tax is a legislative requirement that flows from the Agreements and involves no disclosure by a paying agent of personal data about an individual client to the authorities in that individual's Member State of residence. Whilst it is open to any paying agent to decide that they will not, for administrative reasons, collect retention tax it is a requirement of data protection legislation to obtain the consent of the beneficial owner to the information exchange option.*
>
> *For existing investors, the paying agent should notify all beneficial owners that, under the legislation that flows from the Agreements, exchange of information is optional and subject to the express authorisation of the individual client. Such an authorisation should normally take the form of a written agreement [i.e. a positive opt-in] and the paying agent should not infer any such authorisation from a failure to respond to that notification.*
>
> *It is sufficient in the case of new contractual relationships for the paying agent to include a clear notice in the terms and conditions of the account, fund or other relevant instrument that information will be disclosed to the appropriate authorities detailing the interest payments received by beneficial owners resident in a EU Member State from that investment."*

Identity Cards

The following statements are reproduced from the Home Office web site: *(Home Office Press Notice 196/2004).*

"The UK Government published a consultation paper on Entitlement Cards and Identity Fraud on 3 July 2002. The consultation period ended on 31 January 2003. The Home Secretary set out government plans for an ID card scheme and published the public consultation and polling results on 11th November 2003. These can be found, along with subsequent documents, at www.identitycards.gov.uk.

'Legislation on Identity Cards: A consultation' was published on 26 April 2004 and views were sought on the draft legislation during a 12 week consultation period which ended on 20 July 2004. 766 responses were received to the consultation on legislation, including 109 from organisations.

The Home Affairs Select Committee published its report on identity cards on 30 July 2004, including its pre-legislative scrutiny of the Bill. The Committee concluded that the Government had made a convincing case for proceeding with the introduction of identity cards, and raised a number of detailed points.

The first phase of public research, between July 2002 and January 2003, showed that 79 per cent of respondents were in favour, or very much in favour, of the introduction of identity cards. Of the others, 13 per cent were against and 8 per cent were unsure. A summary of findings was published in November 2003.

The more recent phase of research, was carried out in June and July 2004. This asked more specific questions about the details of the Government's proposals. There was widespread awareness that the Government is considering the introduction of ID cards although a lesser understanding of the detailed proposals. For example, at least 70 per cent had not heard of the term 'biometric information' before. A sample taken from four ethnic minority groups was also asked about their overall support for the scheme. There was a clear majority in favour in all groups - especially with Chinese respondents (84 per cent). Support for ID cards had increased among all four groups since 2003.

This recent phase of research is published alongside responses from individuals and organisations to the consultation paper published in April 2004. These can be found at the web link above.

A development partner (PA Consulting) bringing in detailed expertise from outside Government was appointed in May 2004 to help determine the best way of designing and implementing the scheme."

It is evident that, although the cards are intended to be voluntary, there will be a number of compulsory elements, such as the use of electronic ID's for passports and driving licences and it is highly likely that there would be pressure on the Bailiwick authorities to introduce a similar scheme locally.

The UK Information Commissioner expressed a number of concerns about the proposals in the draft Bill, in particular:

- Continuing uncertainty about the lack of clear and limited statutory purposes for the proposals;
- The nature and extent of the personal information that will be collected and retained;
- Uncertainties and risks relating to administrative and technical arrangements;
- The provisions relating to access to and disclosure of personal information stored on the National Identity register;
- The need for stronger independent oversight;
- The absence of a "voluntary" option for driving licence and passport holders;
- The loss of some initial safeguards as and when the scheme becomes compulsory;
- The extent to which secondary legislation can be used to extent the scheme, thus fuelling anxieties about "function creep".

The Bailiwick Commissioner concurs with these concerns and it remains to be seen the extent to which these concerns are addressed when the final version of the Bill becomes Law.

NOTIFICATION

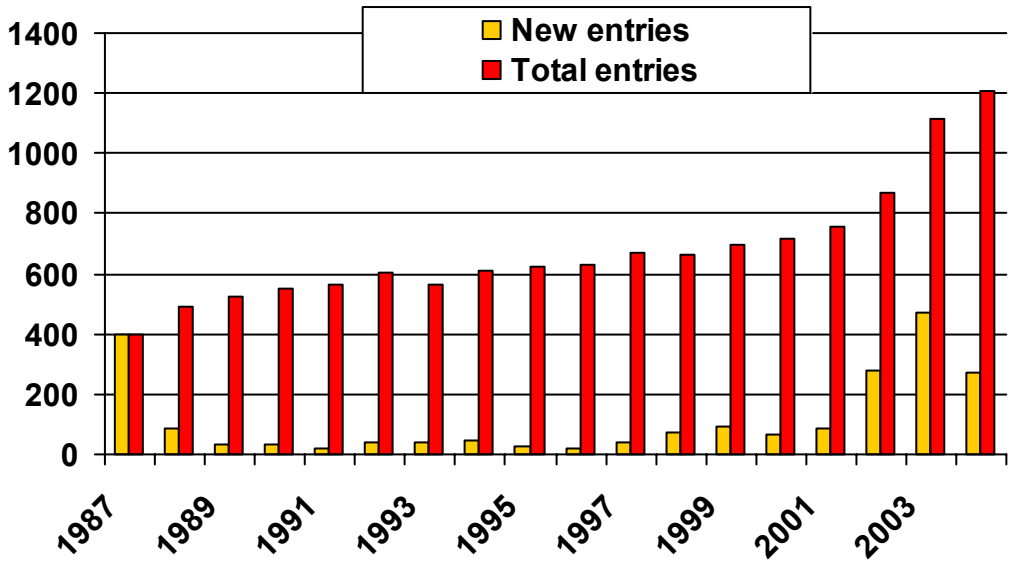
The Law requires Data Controllers to "Notify" the Commissioner of their processing of personal data. This Notification is on an annual renewable basis and covers all processing that is not exempt.

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.

Data Controllers Registered under the 1986 Law are deemed to have Notified until their existing (three-year) Registrations expire. The last of these remaining 184 Registrations will expire in July 2005, after which Data Controllers will be required to Notify annually.

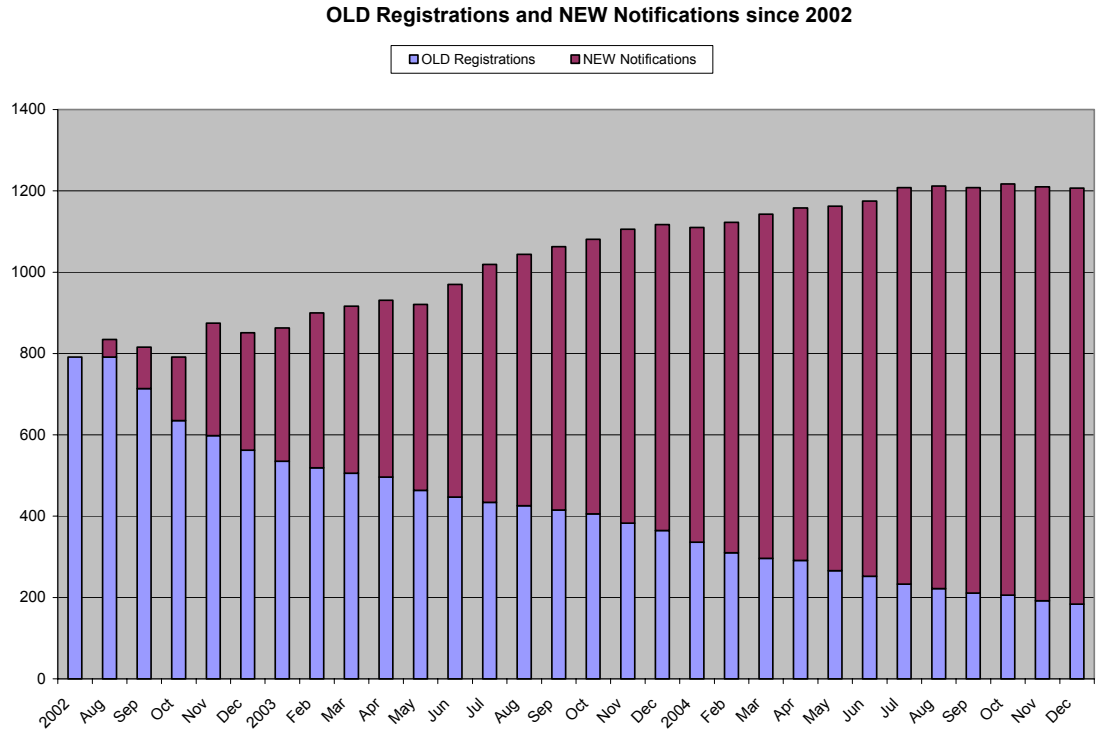
The chart reproduced below shows that the steep rise in New Notifications following the commencement of the Law in August 2002 declined as anticipated, with the total number of Notifications at the end of 2004 being 1210, only 91 higher than the corresponding figure at the end of 2003.

GROWTH IN DATA PROTECTION REGISTER ENTRIES



The chart shown overleaf shows a more gradual rise in Notifications under the New Law, corresponding to the lower number of Registrations under the Old Law that expired in 2004.

Of the 317 new notifications, 131 (41%) represented expiring Registrations from prior to 2002, whilst 186 (59%) were completely new. 39 of the expiring Registrations were not renewed and accordingly were closed during the year.



The automated facilities in the Internet Notification site that were developed in 2003 were fully exploited to minimise the administrative effort involved with the annual renewal process.

762 renewal notices were issued during the year. All those who had provided an e-mail contact address within their notification were sent their first renewal notice by e-mail.

Of the 423 (56%) reminders that were issued by email 106 (25%) needed a second reminder by post. This was mostly because an individual contact had moved and the old email address was no longer valid. Organisations are now being advised to provide a generic rather than a personal address for the receipt of communications, in order to minimise such problems in future, as failure to keep notification details up to date constitutes an offence under the Law.

During 2004, 223 notification and renewal fees (22%) were collected using direct debit. Although invitations were extended at renewal time to any non-direct debit registrants to sign up, there remains scope for this proportion to be considerably increased.

By the end of 2004, 900 notifications (88%) included an email address and 227 (22%) of the 1023 notifications on file had been set up for future collection by direct debit. This represents a marginal increase on the 2003 figures of 650 email addresses (87%) and 56 direct debit mandates (21%).

Failure to notify is a criminal offence under Section 21 of the Law. Towards the end of 2003 five data controllers who had failed to notify had been referred to the Law Officers. Early in 2004 they all eventually complied, but one received a Police caution.

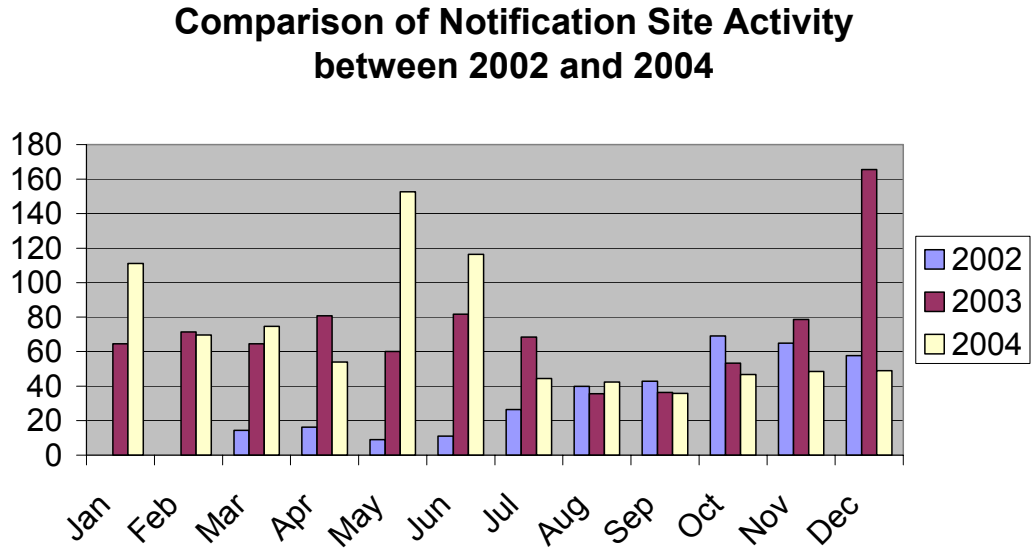
The small number of controllers who failed to notify in 2004 were issued with Final Reminders which resulted in them fully complying. Only one controller ignored the Final

Reminder and was referred to the Law Officers. This controller ultimately notified and also received a Police caution.

As there is now a general greater awareness of data protection requirements it is becoming more likely that any data controllers who, in future, ignore their notification obligations will be prosecuted.

The chart below illustrates the variation in the average daily activity on the online notification site: http://www.dpr.gov.gg , between 2002 and 2004, the vertical axis representing the average daily rate of successful requests for pages of data from the site each month.

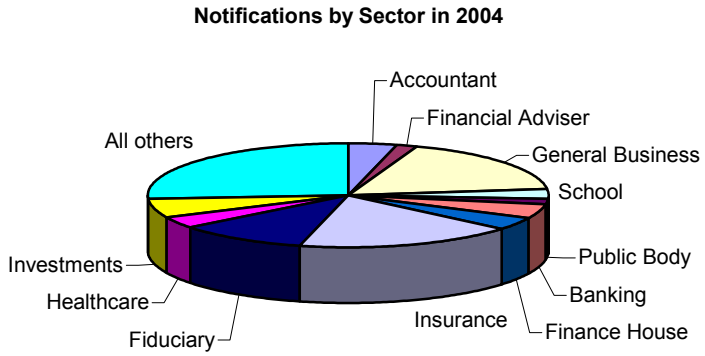
The variations generally correspond with the number of new Notifications and renewals that are dealt with in each month. There has been a gradual fall in activity as the number of old Registrations requiring replacement by new Notifications has decreased over time.



There remain a few instances where some UK data controllers find that they have mistakenly notified in Guernsey rather than in the UK. These problems, and a few where the reverse has occurred, are normally resolved fairly swiftly by liaison with the staff of the UK office.

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

The 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.



Greater proportions of notifications were derived from Insurance and General Business (18%), Fiduciary (10%) , Investments (6%), Finance House, Healthcare, Accountant and Banking (all at 5%), with All others comprising 26%.

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 8 to 42, (4% of the total).

In 2003, the Data Protection Office compiled 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.

During 2004 a further 144 organisations informed the Office of their exempt status making a total of 447. This represents 27% of the overall total [of 1647 exempt, registered and notified organisations].

STAFFING AND STAFF DEVELOPMENT

The establishment of the Office of the Data Protection Commissioner comprises three staff: 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 wholly responsible to him.

The Commissioner remains of the view that, whilst his office remains responsible only for the Data Protection law, the current establishment of one full time Assistant and one part time Administrator represents a satisfactory level of staffing resource, which enables him to undertake his current functions. There is no evidence at present that an increased establishment is required.

Anne Wiggins, the Assistant Commissioner, was successful in obtaining the ISEB Certificate in Data Protection. She attended the course and sat the exam at Mason's Solicitors in London in the earlier part of the year. The Certificate in Data Protection is a specialised qualification held by a limited number of people and it is thought that Anne may currently be the first person in Guernsey to obtain this qualification. It would, however, be beneficial for those with data protection responsibilities within their work role to have such a qualification. The Commissioner has liaised with the Training Agency about holding the course on island and it is anticipated that the first such course will take place sometime in 2005.

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 2004 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 564.

Involvement in Working Groups

The Commissioner and Assistant Commissioner also participated on various public sector working groups such as the E-Government Sub-Group for Citizen Access, the States Data Sharing Group, the E-Business Liaison Group and the Board of Health Registration of Care Workers' Group.

Making use of the media

Press releases

The Commissioner issued 15 press releases during 2004, which gave rise to 28 articles in the local Press and corresponding mentions and interviews on local radio and TV.

The topics covered included:

- **Scams**

  Premium telephone lines, bogus domain registry, "phishing" for e-bay and Paypal account information;

- **Manual Data**

  Guidance issued over the interpretation of the term "relevant filing system";

- **Privacy Regulations**

  Report of a seminar on the regulations, restrictions on e-mail marketing, privacy of telephone directory information, preference services and privacy statements on websites;

- **Rehabilitation of Offenders**

  The draft Code of Practice;

- **Euthanasia campaign**

  There were three articles on the investigations by the Commissioner into alleged breaches of the Data Protection principles by the organisers of the campaign.

Giving compliance advice

To assist data controllers with compliance, the office has also given advice and guidance on the following matters to various organisations:

- Standing orders
- Protocols
- Procedures
- Design of application forms
- Contracts with data processors
- Recording of telephone calls
- Subject access requests
- Transfer of personal data to other jurisdictions, especially "non-adequate" jurisdictions

All the guidance notes produced by the Data Protection Office were revised during the year and most were made available either as A5 booklets or in A4 format to facilitate easy download from the Commissioner's website.

There were five new publications:

***Personal Data and Filing Systems**:* this was published following a Supreme Court of Appeal judgement in the UK which affected the definitions of personal data and relevant filing systems to some extent.

***Trusts and Wills**:* this was complied in conjunction with the data protection authorities of Jersey and the Isle of Man. It had been identified that guidance was needed as to whether data protection law required that beneficiaries had to be informed of details of the terms of Trusts and Wills and if they should have access to these details.

***Privacy Statements on Websites**:* this was issued after a survey by the office suggested that 76% of websites in the Bailiwick were not data protection compliant.

***Privacy of Telephone Subscribers**:* this was needed following the commencement of the Privacy and Electronic Communications Regulations and the proposed introduction of a second telephone directory by another telecommunications provider.

***Dealing with Spam**:* specific guidance was needed to deal with this continuing and increasing problem.

A list of the available publications is given below:-

Guidance Notes published by the Commissioner

NAME AND DESCRIPTION OF BOOKLET
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*
Disclosures of vehicle keeper details *Explains when vehicle keeper details can be disclosed*
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 what 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*
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 has circulated the literature to a number of public, private and voluntary organisations throughout the Bailiwick. She keeps a record of the locations where the literature is sent so that a follow up can be undertaken to assess its uptake and impact.

Approximately 1,500 copies of the literature were distributed during 2004. In addition, Notification Guidance Handbooks were sent out to data controllers when their registrations under the 1986 law were about to expire and notification guidance is included in the literature that is available for downloading from the Commissioner's website.

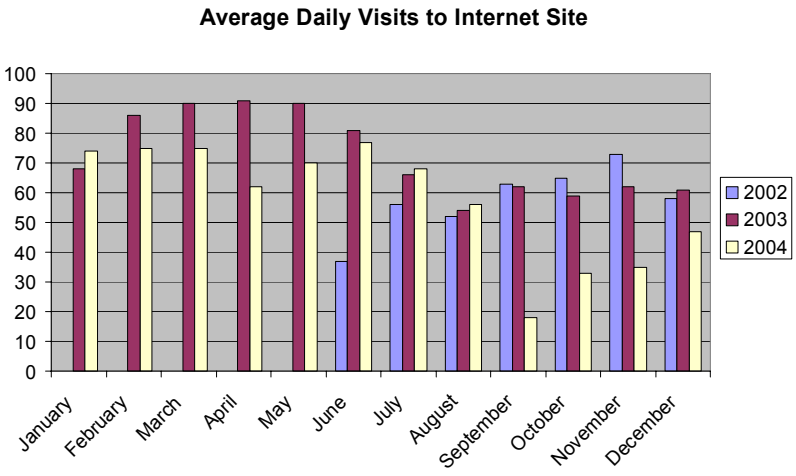
Further publications will be introduced throughout 2005. These will include more detailed guidance on the Privacy and Electronic Regulations, the monitoring of staff at work and guidance for employers in relation to staff references.

Developing the Internet Web Site

All of the information published by the Office is available on the Internet site: http://www.dataprotection.gov.gg . The chart below shows that the usage of the site in 2004 has varied between about 20 and 80 visits per day, a littler lower than in the previous two years.

The most popular sections of the site have been those devoted to the 2001 Law and to "Guidance Notes", where visitors are able to view or download an up-to-date copy of all of the guidance notes that have been published.

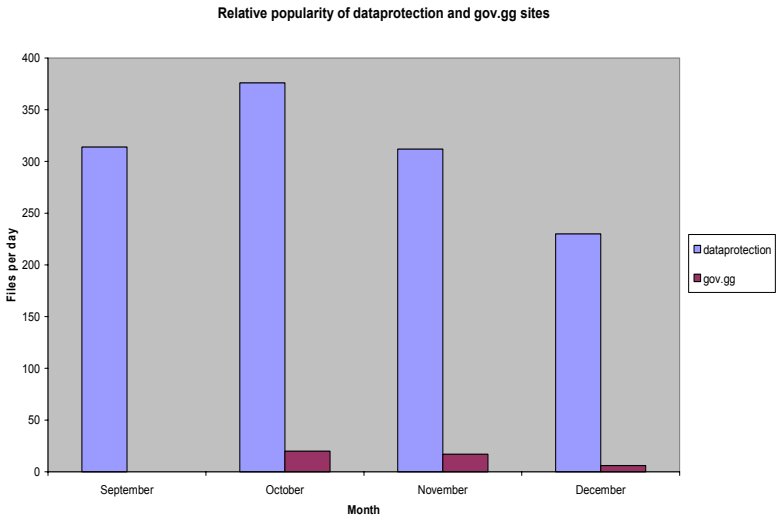
The site is updated on a regular basis and includes copies of all of the material which is published by the Data Protection Office, together with links to other data protection sites and information for data subjects about complaint handling.



In October 2004, a copy of the Data Protection web site was integrated into the States of Guernsey government portal: http://www.gov.gg.

The chart opposite illustrates that, as yet, this new site has attracted little attention. Time will tell whether the public prefers the integrated to the stand-alone site.

In the meantime, it is intended that both sites will as far as possible be kept in synchronism.



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.

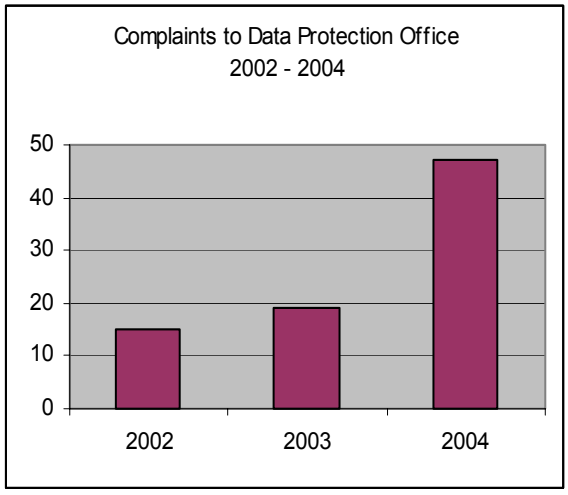
The Commissioner may serve an Enforcement Notice where he has assessed that a controller is not complying with the principles or an Information Notice where he needs more information in order to complete an assessment. With the advent of the Privacy in Electronic Communications Regulations, the Commissioner's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

Complaints by data subjects to the Commissioner concerning notification, or disclosure offences would be dealt with as potential criminal prosecutions by the Police and Law Officers.

Complaints about how data controllers process personal data are treated as "Requests for Assessment" by the Commissioner

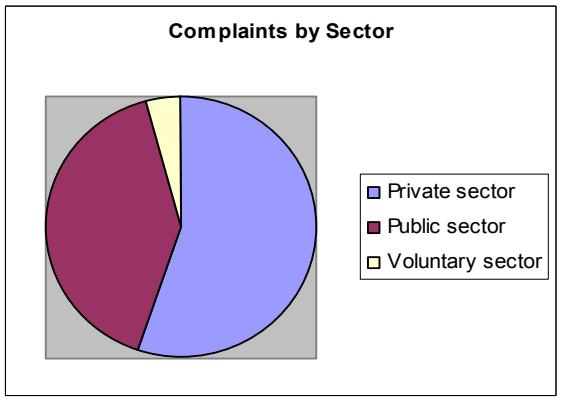
During 2004 a total of 47 such complaints were investigated. This is a significant increase compared with 2002 and 2003 and would suggest that the public are developing a greater awareness of their rights under the Law.

(These 47 complaints were in addition to the 297 calls from mainly elderly people who expressed deep concern over unwanted telemarketing calls they received. A fuller report of this issue is given in the Appendix).

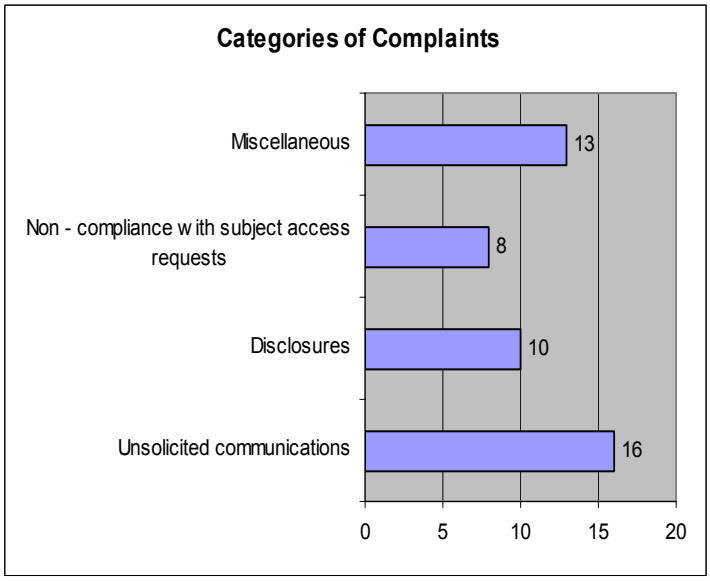


One complaint concerned three organisations and spanned both the public and private sectors.

Hence, the complaints comprised 27 about private sector bodies, 20 about public sector bodies and 2 about voluntary sector organisations.



The complaints can be categorized into unsolicited marketing communications, disclosures of personal information, non - compliance with subject access requests and miscellaneous.



The miscellaneous category comprises complaints to do with breaches of a combination of the data protection principles, mostly in relation to a lack of security and excessive processing of information.

Under section 43 of the Law the Commissioner is empowered to issue an Information Notice in pursuit of a complaint, or if he reasonably requires any information to determine if a data controller has breached any of the data protection principles.

Section 40 of the Law empowers him to issue an Enforcement Notice to require a data controller to comply with the data protection principles.

In 2004 the Commissioner needed to issue just two Information Notices and one Enforcement Notice. This means that, in the remaining cases, the data controllers concerned cooperated fully with the Commissioner without the need for formal action to be taken.

The 2002 and 2003 annual reports included summaries of all the complaints that were investigated. However, due to the larger number of complaints investigated in 2004, this report includes summaries of only a selection of those complaints in the form of Case Studies.

Case Study 1

Following complaints from two general election candidates in 2004 the Commissioner conducted an investigation into the data processing activities of the Guernsey4Dad organisation. This organisation campaigns to change the law in Guernsey to allow terminally ill, competent adults to choose a medically assisted death. It is affiliated to the VES (Voluntary Euthanasia Society) which is based in London.

The organisation ran a campaign in 2003 that sought to lobby sitting Deputies in support of an investigation into the legalisation of euthanasia and in March 2004, it ran a second campaign that involved the lobbying of election candidates and was timed to coincide with the run-up to Guernsey's general election in April 2004.

The first complainant was concerned to discover that his name appeared on a list of the supporters of the 2004 campaign although he had not signed up in support of that second campaign.

It was not clear whether the complaint related to a one-off error or was symptomatic of a more general problem with the compilation of the information in support of the 2004 campaign.

The second complainant raised a concern that he had received an unsolicited computer disc containing personal details of the respondents, when there appeared to be no evidence that their permission had been sought for such a disclosure in electronic form.

The organisers had sent pre-printed postcards by post to members of the public inviting them to show if they agreed with the statement; "*I support the legalisation of Doctor Assisted Dying"*.

In an accompanying letter, the organisers stated that they would forward the completed postcards to the candidates. There was no indication on the postcards or in the letter that information supplied by respondents was to be computerised or kept after the conclusion of the campaign, except a small opt-out box on the postcard stating; "*Please tick here if you do not wish to be updated on the campaign's progress*." There was also no indication that the respondents' personal details would be disclosed to third parties.

In actual practice the organizers had entered the names of respondents on a computer database and sent a copy of the spreadsheet and computer disk to most of the candidates, although some candidates did not receive anything. The candidates were urged to make contact with the respondents.

The Commissioner sought to resolve the matter informally and requested a copy of the organisation's database and a face to face meeting in order that he could investigate the allegation. However, the organisers chose to liaise with the Commissioner through a UK based legal representative, the database copy was not forthcoming and the request for a meeting was declined.

The Commissioner therefore had to seek information by referring to section 24 of the Law and when the information supplied was not sufficient to conduct a thorough assessment, an Information Notice, under section 43 of the law, had to be issued.

The outcome of the investigation was that there appeared to have been breaches of data protection principles in relation to how the organisers processed data during the 2004 campaign; in particular there were substantive breaches of the first principal concerned with fair and lawful processing, and the seventh principle concerned with data security.

Furthermore, it was determined that the data in question were sensitive personal data as individuals were invited to join a political lobby group and to make known their views on euthanasia (which is essentially a philosophical belief). Data protection law lays down stringent conditions for the processing of sensitive personal data.

Because of the nature of the contraventions, it was considered that continued processing of the data could cause damage or distress to anyone whose name had been incorrectly included in the data, or had been unaware that the data would be further processed, retained or disseminated electronically.

It was concluded that as the declared purposes of the 2003 campaign [lobbying Deputies] and of the 2004 campaign [lobbying election candidates] had been achieved and as there was an absence of any 'fair obtaining' notices or a published data retention policy there could be little justification for the continued processing of any personal data related to those campaigns, especially in view of the fact that the collection of the data appeared to have been unfair.

The Commissioner was minded to issue an Enforcement Notice under Section 40 of the Law requiring the organisers to destroy all personal data held by them that related to the campaigns.

However, he was prepared to consider an alternative proposition whereby the organisers undertook to communicate with the respondents, seeking their explicit consent to the holding and further processing of their personal details in electronic form and by electronic means for the limited and specified purposes associated with the campaign until its conclusion.

The organisers also had to give assurance that any future processing of personal data connected with their campaigns would be conducted in accordance with the Data Protection principles and that a privacy statement would be included on their web site.

In an effort to mitigate the damage caused by the unlawful disclosure of those data to the election candidates, the Commissioner sought the recall of the personal data that was originally disclosed to the candidates.

Case Study 2

The Commissioner received a complaint from an Open Market owner/occupier whose details were being published by the Housing Authority on the Internet.

The third data protection principle states that data must be relevant, adequate and not excessive for the purpose for which it is being processed.

It is a legal requirement that the Open Market Register is made available for public inspection. The Housing (Control of Occupation) (Implementation) Ordinance, 1982 provides that it should be made available for inspection in loose leaf form, in which various details, including the ownership of open market properties, are inscribed. The provision of the register on the Internet would not be considered inconsistent with these legal provisions.

However, the prime purpose of the aforementioned Law is to record those properties which are "Open Market" and the publication of ownership of properties is only incidental to that purpose.

The loose leaf register only permits a search to be conducted by reference to the actual properties. The Internet version had a facility which enabled a search to be made with reference to the names of property owners. This prompted a complaint and a general enquiry from members of the public who expressed concerns that the online search facility by reference to name rather than property was an invasion of personal privacy.

In the course of the investigation into the matter it was noted that it was the original intention of the Housing department to exclude ownership details from on-line publication but that this was not carried through to implementation.

The Housing Department voluntarily had the "search by name" facility disabled from use by the general public. The Commissioner did permit the continued use of this facility by a defined set of enquirers for specified purposes, e.g. conveyancing clerks.

Case Study 3

A States employee complained that, by printing his name on a work parking permit, his workplace was excessively processing his personal information and thus invading his privacy.

When contacted by the Data Protection Office the department in question accepted that there was no need to print employee names on the permits and proceeded promptly to rectify the situation.

Case Study 4

An individual working for a company based at Guernsey Airport complained that personal information was being obtained from employees that he claimed to be unduly excessive and invasive. He also stated that the company he worked for was not registered with the Data Protection Commissioner.

This investigation brought up certain issues.

A list was obtained of all companies based at the airport and was checked against the data protection register. The companies who had not met their data protection obligation to notify were contacted and subsequently complied.

It was established that the personal information being collected was for the purpose of police vetting checks and these were being carried out on the directions of the Department of Transport (DfT) in the UK.

The Commissioner was concerned to discover that the DfT had instructed the vetting to be undertaken by *Disclosure Scotland* and not the Guernsey Police. *Disclosure Scotland* provides basic disclosures, (records of unspent criminal convictions) and was, in all probability, being used by the DfT as the Criminal Records Bureau in the UK was at that time providing only Full Disclosures (spent and unspent convictions).

The Commissioner advised that the Guernsey Police should be requested to carry out the checks as they were able to provide a more comprehensive, efficient and cheaper service than *Disclosure Scotland*.

This met with disapproval from the DfT who claimed that any criminal record checks the Guernsey Police made from the Police National Computer (PNC) would not be as comprehensive as those made by *Disclosure Scotland* as no Scottish convictions would be recorded. The DfT strongly advised the airport administration to continue using *Disclosure Scotland*.

The Commissioner, in turn, informed the airport administration that the Guernsey Police do have the same access to convictions information as the *Criminal Records Bureau* and *Disclosure Scotland*. He advised that Scottish convictions were recorded on the PNC.

The Guernsey Police also raised concerns that *Disclosure Scotland* was not contacting them when making checks and were relying solely on the information held on the PNC. It was pointed out the PNC does not include Summary offences such as Disorderly Conduct and Possession of an Offensive Weapon in a Public Place whereas the local Police have knowledge of these offences.

The concerns of the Commissioner and the local Police were passed on to the President of the Home Affairs Committee.

Case Study 5

A UK resident (the complainant) asked the Commissioner for assistance in gaining access to his personal information. He was an ex-employee of a Guernsey company and had worked in one of its UK branches. He wanted access to certain documents that were carried out into the practices and procedures of the branch where he worked and he claimed that there were opinions expressed about his professional competence in these documents.

The company withheld access to certain documents claiming legal professional privilege and that, as the documents were not part of a "relevant filing system", they did not constitute data in terms of the Data Protection Law.

The Commissioner's investigation revealed that:

(a) The complainant already had a significant amount of documents released to him but the two most relevant documents had been withheld.

(b) One of the documents was a report of an investigation into the competence of another employee and, as this would not constitute the personal data of the complainant, he would not have the right of access to it.

(c) There was however an opinion expressed about the complainant's competence in the report. This part of the report could include personal information about the complainant.

(d) As a result of the opinion expressed in (c) an investigation was carried out into the complainant's professional practice. The report that resulted could also include personal information about the complainant.

(e) The company had appointed an agent to carry out the investigation into the UK branch. It received reports from the agent upon the conclusion of the investigation.

(f) The reports were in paper form and not electronic form; they were stored in A4 ring binders and were referenced according to the name of the branch. They could not be readily retrieved or accessed by reference to an individual.

(g) Accordingly, these documents did not appear to constitute a "relevant filing system." Section 1 (1) (c) of the Data Protection Law states that information in manual records must form part of a relevant filing system to constitute data.

(h) As the requested documents did not fall within the definition of a relevant filing system the Commissioner had to advise the complainant that he did not have the right of access to the requested documents from the Guernsey company.

(i) However, as it was possible that the documents were held in electronic form at the UK branch, the matter was referred to the UK Information Commissioner's Office for further investigation.

Case Study 6

An individual complained to the Commissioner about having had a provisional offer of employment withdrawn.

The prospective employer received references on behalf of the job applicant from a former employer. There was a note attached to the references advising that the referee should be contacted.

It was alleged that the referee informed the prospective employer verbally that the applicant had been subject to a disciplinary hearing and had difficulty relating to colleagues.

This was discussed with the applicant who stated that this information was inaccurate.

On advice from the Data Protection Office the applicant made a subject access request for a copy of her personnel file from the former employer. This was made available and it was clear that there was no record of a disciplinary hearing on file and past appraisals had stated that the applicant had a good relationship with colleagues.

It is understood that the offer of employment was reinstated and that the individual was subsequently appointed to the post.

Case Study 7

An individual complained that he had received an unsolicited email from a local company. He claimed that he had previously written to the company and instructed them that no further marketing emails were to be sent to his business.

The investigation revealed that the complainant had various email addresses and had only made an application in respect of one of these addresses. He was advised to inform the company of all his email addresses so that these could be suppressed from its mailing list.

Case Study 8

An individual complained about receiving marketing materials and products which she had not requested from a local company. When she approached the company about this she was informed that she must have ordered the products as they had been paid for. This caused her concern as she considered that her personal details, including her financial details, had been cross fertilised with those of another person or persons. She also continued to receive unwanted products after informing the company that she did not want them. Another concern was that her details might have been passed to third parties without her consent.

The company had informed the complainant that the products she received had been ordered by another customer with the same postal address as her own and this was why her account had been used. The other customer had ordered multiple products which were not all in stock and so were dispatched on different occasions. The last item was dispatched before the complainant had instructed that no further material be sent to her.

In addition to an apparent breach of section 11 of the Law there also were apparent breaches of the data protection principles especially the accuracy, security and fair obtaining principles.

The Commissioner asked the company to supply details of the organisational and technical measures employed to ensure that customers' details were processed accurately and securely. The company supplied evidence which showed that it did have a sound procedure for the processing of orders and that staff training was of a satisfactory level. It therefore seemed evident that that there had been a one off operational error in the case of the complainant where the placing of an order was concerned.

The Commissioner also asked for assurance that the complainant's details had been removed from the company's database and had not been passed to any third party. It had been noted that customers were not given the opportunity to opt out of receiving promotional materials from the company or third parties on the company's order forms and website.

The Commissioner asked for this to be rectified and give the company a specific time period to comply with his instructions.

When this did not happen an Enforcement Notice was issued. The company then promptly responded and complied with all the Commissioner's instructions by removing the complainant's details from their database and by redesigning the website and order forms so that the fair obtaining element of the first data protection principle was met.

INTERNATIONAL LIAISON

International Working Group on Data Protection in Telecommunications

The Commissioner [also representing Jersey and the Isle of Man] attended the 35th meeting of this group that was held Buenos Aires in April 2004.

The main topics for discussion centred on developments in e-government and the privacy aspects of the Internet and of Mobile Communications. The topics being addressed by the Working Group included:

- Regional availability of documents on the Internet as opposed to global availability;
- Prevention of unsolicited e-mail ("spam");
- Media privilege and privacy;
- Intrusion detection systems;
- The ENUM protocol for Internet-based telephony.

The 36th meeting was held in Berlin in September, 2004 but was not attended by any delegate from Guernsey or from the other Crown Dependencies; however the Commissioner was asked to provide contributions, by email, to the text of the resolutions discussed at that meeting.

The meeting dealt with many issues, including:

- Measures to combat cyber-fraud in a privacy-friendly way;
- Efforts towards the integration of cyber-security into national curricula;
- Privacy issues related to web-based e-mail services;
- Geolocation technology;
- Further developments with spam;
- "Phishing" and solutions for e-mail authentication;
- Transmission of location data for commercial purposes;
- Processing of personal data in 'Whois' databases;
- Privacy and Public key Infrastructure.

The Commissioner intends to attend the next meeting of the Working Group in Madeira in April, 2005.

Further details of the working group are available (mostly in German) at:

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

European Spring Conference

The Spring Conference of European Data Protection Commissioners was held in Rotterdam and was attended by the Data Protection Supervisor from the Isle of Man, who also represented the Bailiwick. The conference was structured into 6 sessions; the first five sessions concentrated on specific topics:

- The Roles of Data Protection Authorities;
- Communication and Interaction with the Outside World;
- Compliance and Enforcement;
- Internal Organisation and Effective Privacy Governance;
- European Co-operation and law enforcement;

with the last session being devoted to more general topics.

The Assistant Commissioner plans to attend the next meeting, which will be held in Krakow, Poland in April 2005.

British and Irish Data Protection Authorities

This meeting of the supervisory authorities from the UK, Ireland and the Islands was held in Jersey and included for the first time the Cyprus Commissioner.

The Commissioner and Assistant Commissioner attended from Guernsey.

It had previously been agreed, on the instigation of the UK and Irish Commissioners, that Cyprus and Malta should be invited to participate in these meetings, as they were also relatively small island authorities with a legislative and supervisory environment very similar to those in effect in the Crown Dependencies.

Both Cyprus and Malta had received assistance from the UK and Irish Commissioners in the months prior to their accession to the European Union.

The items covered in the meeting included:

- Implementation of the Privacy and Electronic Communications Directive;
- Citizen identity cards and e-government;
- Know Your Customer banking regulations;
- Biometrics and genetic information.

The Commissioner and Assistant Commissioner plan to attend the next meeting, which is due to be held in Cyprus in May, 2005.

26th International Conference of Data Protection Authorities

This annual conference was held from 14-16 September 2004 in Wroclaw, Poland.

The theme of the conference was "The right to privacy – the right to dignity".

Topics covered at the conference included:

- Privacy and the use of RFID technology;
- The individual's awareness of the right to privacy;
- The employee's privacy protection versus the employer's interests;
- Co-operation between Data Protection authorities at national and international level;
- Economic approach to privacy protection – balancing costs and profits;
- Privacy and the media;
- Counteracting privacy violations on the Internet;
- Privacy protection and political marketing;
- The threats to privacy in the time of e-democracy;
- Biometric identification;
- Short privacy notices;
- The Individual's privacy versus the need to deal with the past;
- Transborder data flows and the challenges of the global economy.

Full details of the conference may be found on the internet site: http://26konferencja.giodo.gov.pl/zaproszenie/j/en/

The Guernsey Commissioner was asked to speak on the topic of the economic costs and benefits of Data Protection. A copy of his paper is included in the Appendix to this report.

The public sessions were followed by a closed session of accredited Commissioners, in which the Guernsey Commissioner participated and at which Formal Resolutions were made on:

1. The accreditation of Korea as a national authority, Catalonia as a sub-national authority and the European Data Protection Supervisor as a supra-national authority;
2. The Draft ISO Privacy Standard (ISO/IEC (PAS) DIS 20886);
3. An amendment to the privacy aspects of automatic software updates – this resolution was originally adopted at the 2003 conference in Sydney, but then amended following representations by Microsoft.

The Commissioner plans to attend the 27th international conference, which is to be held also from 14-16 September 2005 in Montreux, Switzerland, of which further details may be found on: www.privacyconference2005.org

Liaison with the UK Government

2004 saw the retirement of Mr. Graham Sutton, who had been primarily responsible for dealing with Data Protection policy within the Department for Constitutional Affairs (and prior to that at the Lord Chancellor's Department and the Home Office), since the early 1990's. Mr. Sutton had provided invaluable assistance during the drafting Guernsey's Data Protection legislation and was instrumental in promoting the case to the European Commission for an early determination of the adequacy of the Data Protection régime within the Bailiwick to be made.

During his time with those departments he had built up excellent working relationships with the authorities in the Crown Dependencies and we look forward to continuing support and good relations with his successors.

OBJECTIVES FOR 2005

The primary objectives for 2005 will encompass the following areas:-

- ***Legislation***

  Completion of the Statutory Code of Practice on the Disclosure of Criminal Convictions in connection with Employment and commencement of section 56 of the Data Protection Law.

  Considerations of any recommendations that may arise from reviews of the UK Act or legislative developments elsewhere.

- ***Adequacy***

  Ensuring 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***

  Continuation of the close liaison with the Jersey Registrar, the Isle of Man Supervisor, the UK and Irish Commissioners and attendance at meetings with officials from the UK Department of Constitutional Affairs as the need arises.

  Attendance at relevant UK, European and international conferences will continue as a means of enhancing the international recognition of the Bailiwick and updating our knowledge of international developments.

- ***Raising Awareness***

  Continuation of the media awareness campaign and the mounting of seminars and talks for the public and private sectors.

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

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

  The publication of new literature and the reviewing and revision of existing literature.

  The continued publicising of the Preference Services and the undertaking of periodic surveys to determine their use and effectiveness.

- ***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.

- ***Government***

  Liaison with the newly constituted departments will be maintained, to ensure that data sharing protocols are redefined to reflect the newly established organisation of the Guernsey government departments, whilst maintaining the separation of purposes.

  The provision of data subject access to government information will be kept particularly under review, especially in the light of the fact the there is no freedom of information legislation in force. Efforts will be made to promote a code of practice for the release of information that would render the enactment of such legislation unnecessary.

FINANCIAL REPORT

The Data Protection Office is funded by a grant from the States of Guernsey that is administered from 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 (2004) and were so included for the Advisory and Finance Committee (2003 and prior years), have been as follows:

INCOME	**2004**	**2003**
	£	**£**
Data Protection Fees [1]	37,622	23,937
EXPENDITURE		
Rent	15,526	15,526
Salaries and Allowances	129,782	114,988
Travel and Subsistence	7,366	15,648
Furniture and Equipment	13,107	33,045
Publications	2,199	3,255
Post, Stationery, Telephone	3,881	5,295
Heat Light, Cleaning	5,054	5,366
TOTAL EXPENDITURE	**£176,915**	**£193,123**
EXCESS OF EXPENDITURE OVER INCOME	**£139,293**	**£169,186**

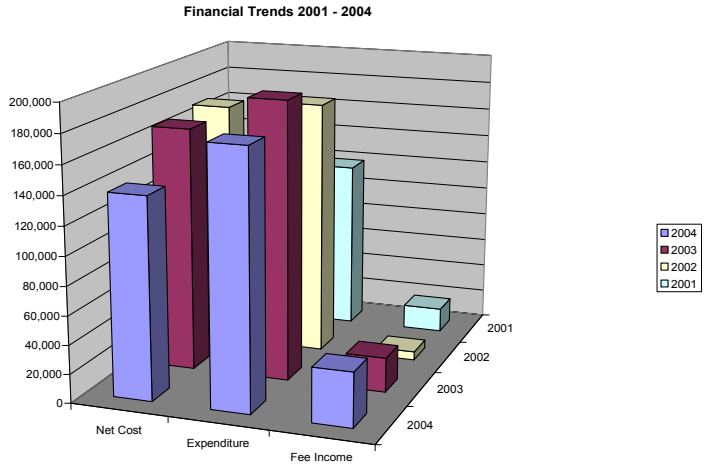
NOTES

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

The Income for 2004 includes accrued income from previous years: £4,900 from triennial registrations from January to July 2002 and £14,992 from annual notifications and renewals throughout 2003.

The cash received for 2004 was £35,875 representing receipts for the 1025 annual notifications and renewals that were processed during 2004.

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



It can be seen that the fee income apparently fell between 2001 and 2002 but this was on account of the fact that it was the first year in which fee income was accrued; whereas expenditure for 2002 was inflated by the employment of temporary assistance with the implementation of the Law.

The 2003 expenditure included one-off costs incurred in the upgrading of the Notification System to deal more effectively with renewals and a recovery of the development costs of the notification system originally funded in 2002 directly from the Advisory and Finance Committee's unspent balances.

Accordingly, the 2004 figures are likely to be most representative of the level of future income and expenditure, although it is prudent to anticipate the need for the phased replacement of certain items of equipment in 2005 and in subsequent years.

The employment of consultants is an area that may show wide variations from year to year, depending in particular on the need for external legal assistance. This might arise specifically if any action were contemplated for which it would not be practical or possible to obtain legal advice from the Law Officers, or if any data controllers were contemplating appeals against any decisions of the Commissioner.

APPENDIX

The European perspective - is Data Protection value for money?

Dr. Peter R. Harris

Data Protection Commissioner, Bailiwick of Guernsey
P.O. Box 642, St. Peter Port, Guernsey, Channel Islands GY1 3JE
dataprotection@gov.gg

Abstract
This paper aims to examine the economics of the regulation of the processing of personal data in the context of the 1995 European Directive on Data Protection. The major elements of the Directive and their impact on costs are identified and quantified where possible. Reference is made to published assessments of cost published by the UK Government in 1997 and 2003 and to the expenditure of the Commissioners in the UK and Ireland. These are compared and contrasted with a number of mostly intangible benefits associated with the relatively strong regulatory environment that results from implementation of the Directive. The question is raised as to whether the costs of strong regulation are justified by the economic benefits that ensue.

1. Introduction

Both business and government exploit Information and Communications Technologies to obtain process efficiency, and aim to maximise the use of information sharing to combat fraud and to provide tailored personalised services to individual customers.
Free market economics relies on competition to drive down prices, but needs adequate regulation to ensure fairness of trading and consumer protection.
The regulation of the processing of personal data interferes in the free market by enforcing individuals' rights and imposing standards of processing on organisations, so it is perhaps not surprising that anyone who regulates personal data processing may be required to provide an economic justification for their existence.
Regulation is also required of the public sector's use of technology to ensure that human rights are not compromised by the unwarranted sharing or unnecessary publication of personal information by government.
In Europe, regulation has tended to develop on the basis of statutory powers vested in independent public officials, whereas elsewhere in the world there may have been a greater tendency to encourage self-regulation.
There appears to be a generally held belief that Data Protection is a "good thing", but very little evidence as to whether the costs of compliance are balanced by the overall economic benefits to society.

1.1. OECD

The Organisation for Economic Co-operation and Development was established to promote policies designed to encourage economic development and a rising standard of living on a multilateral, non-discriminatory and global basis.
The Recommendation concerning the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[1] was adopted by the Council of the OECD on 23rd September 1980.
This document was designed to stimulate international trade by defining eight principles of good practice that should apply to the protection of privacy.

[1]The text of the declaration may be found at:
http://www.oecd.org/document/20/0,2340,en_2649_34255_15589524_1_1_1_1,00.html

Broad political attention was first given to privacy online at the OECD Conference "Dismantling the Barriers to Global Electronic Commerce" held in Turku, Finland, on 19-21 November 1997 and in the following year, the Ottawa Ministerial Declaration reaffirmed a " commitment to the protection of privacy on global networks in order to ensure the respect of important rights, build confidence in global networks, and to prevent unnecessary restrictions on transborder flows of personal data".
Much of the work of the OECD in this area is detailed in: "*Privacy Online: OECD Guidance on Policy and Practice"* [2], and further information may be found on the OECD website[3]. In the privacy sphere, the OECD has sought to build bridges based on voluntary compliance with their recommendations rather than by establishing binding international treaties. However, it is evident that the members of the OECD believe that globally uniform standards of privacy protection would benefit international economic activity.

1.2. Council of Europe

At about the same time as the OECD was developing its eight principles, the regulation of Data Protection throughout Europe was being initiated by the publication of the 1981 Council of Europe Convention 108[4]; this came into force in 1985, has since been ratified by 31 Parties - including all the present EU Member States - and has also been signed by 7 other countries.
Convention 108 defined common minimum standards that were to be applied to the automated processing of personal data: it established the 5 principles of data quality, introduced the concept of special categories of data and established the rights of individuals in respect to information processed about them. Parties to the Convention were encouraged not to inhibit trans-border flow of personal data to another Party for reasons connected with privacy protection.
Some countries already had Data Protection legislation prior to Convention 108 and the subsequent implementation of national legislation in other countries diverged significantly between different European countries. The definitions of personal data were not consistent, some including manual records, for example, whilst others specifically excluded sound and image data. Some countries extended protection to legal persons, whilst others restricted protection to data about living individuals.
The result was that, despite the binding nature of the Convention, the flow of data between States was being impeded, owing to the different levels of protection in force and prohibitions by those with the strongest legislation from transfers to those States and territories with a lower standard of protection.

1.3. The Data Protection Directive

In the late 1980's, the economic consequences of the divergence of Data Protection standards were potentially quite acute and beginning to threaten the proper functioning of the Internal Market within the [then] European Economic Community. There was at least one instance, for example, where computerised personnel records of workers in one Member State were prevented from being transferred to the head office of the company that was established in another Member State. It was evident that the unequal protection of personal data was having an adverse effect on the economic progress on the Internal Market.
The European Commission responded to these by drafting a Data Protection Directive in 1990. This was not finally adopted until 1995[5] and imposed a common generally higher standard of protection and regulation across all Member States. The twin objectives of the Directive expressed in Article 1 were:

1. to protect the rights of individuals with respect to the processing of their personal data; and
2. to facilitate the free movement of personal data between Member States.

Although it was the first objective that received much attention, it was the second that held out the prospect of major economic benefit.

---

[2] A description of this publication may be found at:
http://www.oecd.org/document/49/0,2340,en_2649_33703_19216241_1_1_1_1,00.html
[3] Further information on the privacy policy of the OECD and the privacy statement generator may be found at www.oecd.org/privacy .
[4] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data http://conventions.coe.int/Treaty/en/Treaties/Word/108.doc
[5] Directive 95/46/EC on the protection of individuals with the regard to the processing of personal data and on the free movement of such data OJ L 281 23.11.95 p 31-50. http://europa.eu.int/comm/internal_market/privacy/law_en.htm

However, the economic benefits came at the costs of compliance with the more uniform, but higher, standards of the national legislation resulting from the Directive and it is worth asking whether the facilitation of trade within the European Union has come at the cost of inhibiting the development of trade with Third Countries.

2. Elements of Cost

Costs may be classified as tangible or intangible as shown in the table below:

TANGIBLE	INTANGIBLE
Supervisory Authority	Impact on competitiveness
Notification Fees	Limitation on sharing of data
Compliance	Excessive bureaucracy
Subject Access	

The tangible costs of Data Protection comprise two main elements:

a) The cost of running the supervisory authority and the payment of any fees for notification; and
b) Compliance with the Data Protection principles, in particular the costs of the provision of data subject access.

Intangibles include:

c) The perception that compliance might reduce competitiveness, by limiting what can be done with customers' information; and
d) Inefficiencies introduced by restrictions on the sharing of data and the additional bureaucracy associated with compliance activities.

The major elements of the Directive that are of particular relevance to this paper are:

1. compliance with the Data Protection principles,
2. respecting the rights of data subjects,
3. administration of the notification process,
4. controlling data transfer to third countries and
5. exercising the functions of the supervisory authority.

2.1. Compliance with the Principles

The costs of compliance are borne by both the public and private sectors. In the private sector all businesses need to have regard to the privacy rights of their staff, but the main element of cost is likely to be determined by the extent to which an organisation transacts business with private individuals and then whether these transactions involve the processing of sensitive personal data.
In January 1994, the UK Home Office undertook a survey about the economic impact of the Directive [that was at that time still in a draft form] on 625 organisations, drawn from central government, local government, charities, private sector organisations and trade associations. The conclusions of that initial study[6] were that set-up costs would amount to £2.24 billion (€3.34bn) and that annual expenditure on data protection would rise by a factor of 25 to £308 million (€460m). However, that estimate received some criticism (for example in Data Protection News[7]) and a report by Ashton Business School and the Universities of Tilburg and Leiden[8] found in 1994 that : *"The financial impact of the proposed Directive will be very small for the majority of organisations studied in the public and private sectors in the Netherlands."*

[6] Costs of Implementing the Data Protection Directive. Paper by the United Kingdom. Home Office 1994.
[7] Data Protection News, Issue 20 Winter 1994/95, published by Hoskyns (CAP Gemini Sogeti)
[8] Report to the European Commission: An Evaluation of the Financial Impact of the Proposed European Data Protection Directive, Ashton Business School, 1994

The Home Office published a subsequent regulatory assessment of the costs of implementing the Directive in 1997 [9] that estimated the start-up costs to be £1.150bn. (€1.720bn.), representing slightly more than 0.1% of GDP for the UK for that year; the annual costs were estimated to be £0.742bn. (€1.110bn), representing just less than 0.1% of the GDP. If anything, these assessments may have underestimated the impact of the inclusion of manual records in the compliance costs. The post-implementation appraisal of the Data Protection Act 1998, undertaken by the Lord Chancellors' Department in September 2000[10] did not specifically address the economics, but did include a "… *concern over the economic impact of the provision of information. As well as the cost of providing the information, the provision of information on the telephone when selling a product or service measurably resulted in abandoned calls and lost sales…".*
Compliance with national legislation will require the data controller to manage their use of personal data. This will normally include direct costs from the need to appoint data protection officers and indirect costs associated with the provision of training and the implementation of business procedures to ensure the correct processing of data. Legislation may also limit the extent to which personal data may be shared within the organisation for different purposes from those for which it was originally collected. This will imply the need for additional resources to be devoted to increased dialogue with individual clients in order to obtain consent for the processing activities associated with these different purposes. The level of these costs depends very much on the business sector of the organisation, but could amount to a few percent of turnover.
The elements of costs that particularly affect the public sector, apart from human resource aspects, particularly relate to the control of information sharing between government departments and the security of transactions with the citizen.
These compliance costs may be quite substantial, involving the appointment of data guardians, the development of information handling and sharing protocols and the organisation of staff training programmes. These issues are coming into prominence in tandem with the drive towards the electronic delivery of more joined-up services and can be minimised by taking the opportunity to ensure that compliance is built-in at the earliest stage to the design principles for e-government.

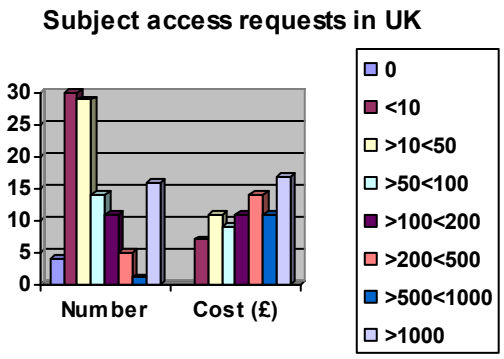
2.2. Individual Rights

Individuals have rights to access and to have corrected personal data processed about them by data controllers. The exercise of these rights can have costly consequences for an organisation. In order to be able to respond adequately to a subject access request, the organisation must have effective information handling processes in place.
The provision of information to data subjects is often seen as one of the more onerous requirements on data controllers. However, the extent of this burden varies substantially, depending on the type of business conducted by the organisation. Arguably, the more efficient the organisation, the lower would be the costs of the provision of information, since it should be more readily available.
In July 2002, the Department of Constitutional Affairs within the UK Government published the results of a consultation exercise on subject access that had been undertaken in the previous autumn[11]. Some of the findings of this report are illustrated in the chart opposite.
Whilst 27% of those organisations that responded had to deal with less than 10 access requests per year, 14% received over 1000 annual requests.
Only 9% of the requests were dealt with at a cost less than the subject access fee (of £10 or about €15), with over 20% costing in excess of 100 times that fee. These figures may have been skewed by the fact that over one third of the respondents were from the public sector or public bodies.
A significant element in the compliance costs arises from the inclusion of the majority of manual records within the definition of personal data.

---

[9] Regulatory Impact Assessment of Directive 95/46/EC, Home Office December 1997 www.dca.gov.uk/ccpd/dpara.htm
[10] Data Protection Act 1998 Post-Implementation Appraisal CP(R)99/01 originally published by the Lord Chancellor's Department, December 2001 http://www.dca.gov.uk/ccpd/dparesp.htm
[11] Response to the Consultation Paper - Data Protection Act 1998:Subject Access, July 2003 www.dca.gov.uk/consult/foi/dpsaresp.htm

This means that organisations that hold a lot of manual records may spend a lot of effort bringing together all of this material in response to a subject access request. Recently, the Supreme Court of Appeal in the UK delivered a ruling[12] that substantially limited the types of manual data that were subject to the Law. This ruling, if carried through to general application, should have the effect of considerably reducing the burden on organisations in complying with subject access requests that might have involved searching relatively unstructured manual filing systems and accordingly reducing the high costs that have previously been quoted by some data controllers.



A similar survey conducted in 2003 throughout the European Union, "The Euro-barometer Report [13] on Data Protection in Europe" found that in 2002 49% of respondents received fewer than ten access requests per year, with less than 1% receiving in excess of 500 such requests. The vast majority (96%) of respondents received no Data Protection complaints during 2002. So, whilst the cost of dealing with an access request or a complaint may be significant when it occurs, the incidence of such requests is generally quite low, meaning that for most organisations the economic impact is also low.

2.3. Notification

The Directive requires data controllers to notify the supervisory authority of the details of their processing of personal data. Arrangements for notification vary substantially between different countries and in some cases (such as in the UK) a fee is charged; this is currently about €50 per notification.
The annual cost of the notification fee is a relatively insignificant expense, compared to the administrative time that may be required to generate the information required for a notification and the ongoing effort needed to ensure that it remains up to date. This activity would typically involve maintaining records of all systems that process personal data and being aware of all planned upgrades to such systems throughout an organisation. An integral part of the UK notification process involves the completion of a questionnaire on the security measures that are in place to protect the processing of personal data.
The costs of the overall notification process will vary and clearly could be significant for a large or complex organisation that transacts business with individuals.

2.4. Restrictions on Data Transfer abroad

The Directive prohibits the transfer of personal data to a territory without adequate protection. Very few Third Countries have yet achieved an adequacy finding[14], so transfers in general outside the EEA can only occur under the additional protection of contractual clauses or under the authority of the national supervisory body. Contracts can take some time to negotiate and can at times be in conflict with the national law of the "Third Country", hence the need for these contracts can inhibit trade, especially between the Pacific rim and Europe, and has proved a potential barrier to activities such as outsourcing back office operations to Asian countries. The Euro-barometer report on Data Protection in Europe shows that only 10% of the companies surveyed transferred personal data outside the European Economic Area in 2002. Data Protection constraints may have been a contributory factor in this.

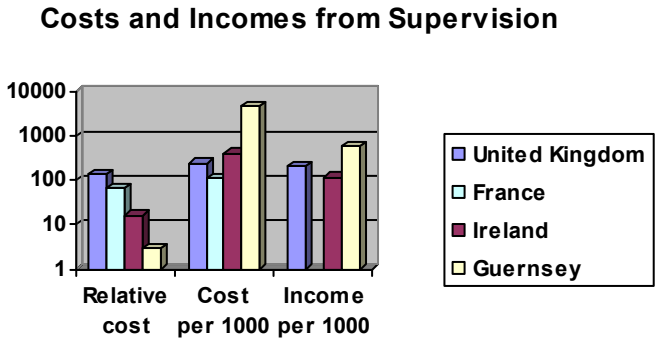
---

[12] Michael John Durant v Financial Services Authority [2003] EWCA Civ. 1746, Court of Appeal (Civil Division) decision of Lord Justices Auld, Mummery and Buxton dated 8th December 2003.
http://www.courtservice.gov.uk/judgmentsfiles/j2136/durant-v-fsa.htm
[13] EOS Gallup Europe Flash Eurobarometer 147 "Data Protection in the European Union":
http://europa.eu.int/comm/public_opinion/flash/fl147_exec_summ.pdf.
[14] Commission decisions on adequacy may be found at:
http://europa.eu.int/comm/internal_market/privacy/adequacy_en.htm

The European Commission's Analysis and impact study on the implementation of the Directive[15], published in 2003 found that: " *late transposition by Member States and differences in the ways the Directive is applied at national level have prevented Europe's economy from getting the full benefit of the Directive."* There was particular divergence between the national laws and practice of Member States with regard to international transfers of data and so a similar argument could be applied to postulate the harmful effects on international trade.

2.5. Supervision

In Europe, the supervisory régime is dominated by the Directive 95/46/EC.
This lays down that supervision should be by an independent statutory authority, not under direct political control. Within Europe, the Data Protection or Privacy Commissioner's office is normally funded by central or regional government and in some cases may charge fees for its services such as for maintaining a register of data controllers. Such fees payable by law to a public body are essentially a form of indirect taxation and so any fee income should ideally be disregarded when international comparisons of the costs of the supervisory régimes are made.
The federal or regional structure of some European states further complicates a comparative study of costs as does the different functions performed by such supervisory bodies – in the UK, for example, the Information Commissioner is responsible for enforcing Freedom of Information legislation as well as Data Protection. The chart below illustrates the comparative costs of regulation in the UK, France, Ireland and Guernsey.
In the UK, which is the largest non-federal Member State in the EU, the Information Commissioner's Office spent about €14m in 2003,[16] which is €240.00 per thousand head of the population. That cost was largely offset by income of about €12.5m. (€212 per thousand).
Similarly, the 2003 budget of the CNIL in France was €6.5m[17], representing €108 per thousand head of the population for a mandate that was more specifically concerned with privacy.
By way of contrast, in the Republic of Ireland, which is one of the smaller Member States, the Data Protection Commissioner's Office[18] spent about €1.6m in 2003 (€404.00 per thousand) as against an income of €0.45m. (€115 per thousand).
In Guernsey[19], which has a population of only 60,000, last year I spent about €288,000 (€4,800 per thousand) against a income from fees of €35,000 (€583 per thousand).
These figures serve to illustrate the economies of scale that can apply to larger countries.



3. Benefits

So, let us look at the benefits of regulation, under similar headings that we used for examining the costs.

[15] European Commission's First Report on the transposition of the Data Protection Directive, 26 May 2003
http://europa.eu.int/comm/internal_market/privacy/lawreport/data-directive_en.htm
[16] Annual Report and Accounts of the UK Information Commissioner for 2003
http://www.informationcommissioner.gov.uk/cms/DocumentUploads/AR03.pdf
[17] CNIL 24e rapport d'activité 2003, Annexe 4
[18] Fifteenth Annual Report of the Data Protection Commissioner for the Republic of Ireland for 2003
http://www.dataprivacy.ie/images/annual_report_2003.pdf
[19] Bailiwick of Guernsey Data Protection Commissioner's report for 2003
http://www.dataprotection.gov.gg/Reports/2003%20Report.pdf

3.1. Compliance with the Principles

Compliance with the principles can have a significant impact on business processes and business organisation. Organisations that show that they are compliant with the principles should derive a number of benefits, including:

- Better staff relations, through improved transparency of personnel records and improved training;
- Better customer relations, through improved record keeping and up-to-date information and enhanced consumer confidence;
- Fewer complaints from clients, resulting in lower overhead costs;
- More efficient operations through better organised filing systems and improved business processes;
- Improved opportunities to transact international business, especially with customers resident in EU Member States.

3.2. Individual rights

Incorporation of respect for human rights, especially the right to privacy, into national law contributes to the establishment of a fair, just and open society.
This legislation means that citizens who transact business with government will have increased confidence that their personal information will be respected and will not be unnecessarily shared without their consent.
It has been widely predicted that e-commerce will continue to grow to encompass more and more consumer-led transactions. E-commerce itself offers amazingly low transaction costs, especially where services, such as theatre bookings, tickets for public transport and music downloads are concerned. The economic consequences of the widespread adoption of e-commerce are immense. However, its growth has not nearly been as rapid as was predicted and one reason for this is the lack of trust by consumers in doing business over the Internet.
Consequently, it can be argued that exploitation of the strong regulation of Data Protection can have a pivotal role to play in facilitating the increased confidence amongst consumers that their personal data will not be abused from the use of electronic transactions.
Organisations established throughout Europe are able to exploit their compliance with strong Data Protection legislation to offer improved levels of consumer protection and should therefore be able to gain substantial competitive advantage from e-commerce applications. The high profile given to personal privacy within Europe can mean that European consumers may be discouraged from doing business over the Internet unless they can be sure that the privacy of their business is protected by adequate legislation in the destination country.

3.3. Notification

There are no particularly obvious direct economic benefits from the notification process. Indeed there are many who think that notification is a waste of time. Although it does consume some resources, the side effects of notification can be a greater awareness amongst the business community of Data Protection matters and the incentive to establish an organisational focus for everything concerned with personal data. As an example, completion of the security questionnaire that is associated with the notification processes forces an organisation to consider its security procedures and is in itself an educational exercise.
Notification can also reduce the need to respond to the more straightforward requests for information about processing, as the answers to such requests may be found in the published notification; hence individuals can know at the outset the types of information processed and purposes for which they are processed prior to deciding whether it is necessary to make a detailed subject access request.

3.4. Restrictions on Data Transfer abroad

As has been previously mentioned, the prohibition of data transfers to non-adequate jurisdictions can initially have negative economic consequences as it can restrict trade, by making it more difficult to do business with organisations based in such territories.
This is very much a short-term view. In whatever field standards are introduced they have the effect of partitioning the universe into the compliant and the non-compliant. Once it has been recognised that the standards are worthwhile, they become more universally adopted, with the result that economic costs of non-compliance far outweigh the costs of compliance.
Essentially, this means that the pressure on a country to enact legislation to provide adequate Data Protection is increased as a result of the economic effect of the trade sanctions that it suffers. Certainly, it was economic arguments that were primarily used to justify updating the Data Protection legislation in Guernsey, such that we were able to obtain a finding of adequacy.
However, with much of the United States, Latin America, Africa and Asia not yet deemed "adequate" by the European Commission, we are still some way from reaching a critical mass of "adequate" economies that would enable sufficient pressure to be imposed to facilitate the free movement of personal data on a global scale. Indeed, there is a danger that the reverse could apply – strong economic pressure by those with "weak" protection might be applied in an effort to dilute the level of protection that applies in Europe and those other countries that enjoy "strong" protection.

3.5. Supervision

The supervisory body imposes a direct and an indirect load on the taxpayer. What benefits accrue from having an independent supervisor? For the regulation of business, it of little concern whether the regulator is a government servant or not. For the regulation of government, of course, it is vitally important that regulation can be seen to be independent and promoting the right balance between the legitimate needs of the state and the fundamental rights of the individual. Striking this balance is particularly relevant at the present time in dealing with the responses to international terrorism and money laundering and in the debate over biometrics, identity cards and the interception of communications.
One of the major functions of the supervisory body is that of increasing public awareness – this translates into enhanced public confidence and improved quality of life. Intangible benefits, but benefits none the less. More tangible is the power of the regulator to intervene, to respond to complaints, to enforce compliance - normally without the need to exercise the legal process by engaging in prosecution or litigation. This may be bad news for the legal profession, but it is good news for the economy, as most problems can be fixed by intervention rather than confrontation. By way of example, in 2003 the UK Information Commissioner processed approximately 12,000 complaints, involving nearly 5,000 assessments of processing, but undertook only eight prosecutions.

4. Conclusions

The protection of privacy has long been recognised as having important economic consequences and has been high on the agenda of intergovernmental organisations such as the OECD and the Council of Europe for over 25 years. The processing of personal data in Europe is subject to strong regulation driven by the EU Directive that interferes in the free market by imposing high standards on the processing and protection of Personal Data in both the private and public sectors.
Strong regulation appears to have a significant economic cost, which although amounting to a fraction of a percent of a nation's Gross Domestic Product, may have a greater indirect effect by inhibiting the capacity of that nation to trade internationally. However, this cost is balanced by the increased consumer trust in dealing with an economy that respects privacy.

Although the European Commission has undertaken an analysis of the implementation of the Directive, this did not extend to an economic appraisal. However, it is understood that the Commission is in the process of commissioning a study into the costs of compliance, the results of which should be available in 2005. Whilst some countries have followed the European approach, many other countries have favoured a regulatory approach that depends more on voluntary compliance, with sectoral legislation addressing areas of particular concern. This difference in approach could inhibit the flow of personal data between the "strong" and "weak" regulatory environments and is particularly relevant to consideration of the needs of international ecommerce.

In its 2004 economic survey of the Euro area[20], the OECD reports: *"Goods, services and financial market integration must be deepened with a view to raising that area's growth potential"*. Implicit in that statement is the need for common global privacy standards to facilitate trans-border flows of personal data. The final report of the World Summit on the Information Society[21] the important role of privacy protection is recognised in Principle 35. "*Strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICT's. A global culture of cyber-security needs to be promoted, developed and implemented in cooperation with all stakeholders and international expert bodies. These efforts should be supported by increased international cooperation. Within this global culture of cyber-security, it is important to enhance security and to ensure the protection of data and privacy, while enhancing access and trade. In addition, it must take into account the level of social and economic development of each country and respect the development-oriented aspects of the Information Society*."

There is currently very little data available on the costs of complying with privacy regulation and even less on its economic benefits. The benefits of strong regulation are mostly intangible, but contribute towards the creation of a fair and open society. The question remains – are the costs balanced by the benefits?

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.

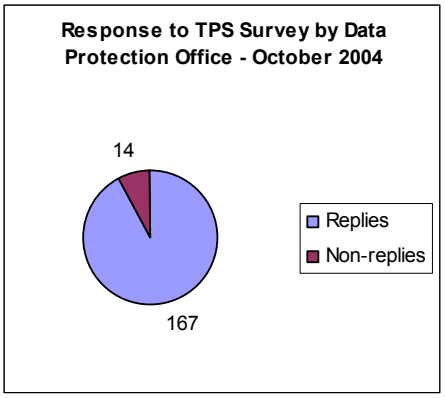
[20] www.oecd.org/dataoecd/17/33/33626607.pdf
[21] Final Report of the Geneva Phase of the Summit WSIS-03/GENEVA/DOC/0009 (rev. 1) http://www.itu.int/wsis/documents/doc_multi-en-1191|0.asp

FIRST BATTLE AGAINST NUISANCE CALLS WON

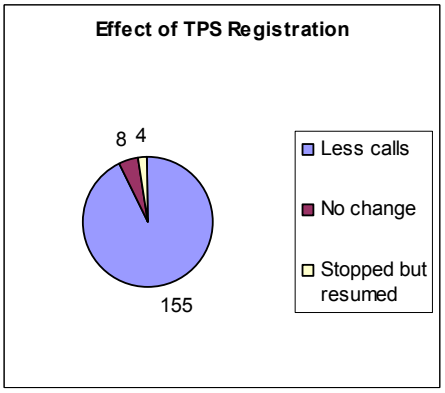
Anne Wiggins
Assistant Data Protection Commissioner

Results of an interim research project undertaken recently by the Data Protection Office have suggested that the Telephone Preference Service (TPS) is very effective in its aim of reducing the numbers of unsolicited telephone calls received by individuals.

A questionnaire was sent to 180 individuals whom the office had registered with the TPS during October 2004. There was an excellent response with 167 forms being returned, this represents almost a 92% response rate.



Out of the 167 individuals who responded 155 stated that they received less calls, this represents a 93% improvement.



Many people have expressed gratitude for the improvement in their lives due to the reduction of these unwanted telephone calls.

Some typical comments were:

"It is certainly a wonderful improvement and I am very grateful"

"Very satisfied. Recently all we have had is one call"

"Am very pleased and relieved as they were becoming a real problem"

"Thankfully these calls appear to have ceased and I have had none for the last three weeks"

"I have been very pleased with the effectiveness of this service"

"We no longer receive any of these unwanted calls. Your service is excellent. Thank you very much"

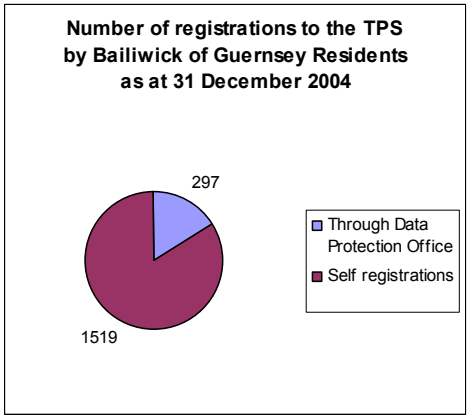
Although calls do not stop completely many people notice a significant improvement. The calls that persist come from outside the Bailiwick and the United Kingdom, mostly from America, and so are not subject to the Privacy and Electronic Regulations which are in force in the former jurisdictions.

The TPS is operated by the Direct Marketing Association in the UK. It maintains a register of telephone numbers which companies must, according to the Regulations, screen on a monthly basis. It is unlawful to make marketing calls to any number listed on the register. It is a service provided free of charge and available to Bailiwick of Guernsey residents.

As the Regulations are in force in the Bailiwick local companies must also screen the TPS register before making any marketing calls. Non-compliance with this rule would result in the Commissioner taking enforcement action.

Companies are increasingly telephoning individual households with offers and information about products and services. Such calls are not always welcome.

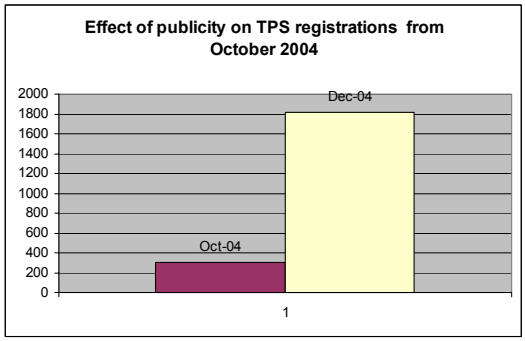
A local press article in early October 2004 highlighted the plight of many elderly people who were subjected to receiving unwanted telephone calls. The contact details for the TPS were widely circulated in the wake of this report and a lot of elderly people contacted the Data Protection Office stating that they were experiencing difficulty in trying to register. Therefore the office decided, with their permission, to undertake registration on their behalf. Between 10 October 2004 and 31 December 2004 a total of 279 telephone numbers were registered in this way.



The office is happy to continue to make registrations on behalf of the elderly. They may contact the Data Protection Office on tel: 742074.

Many more people in the Bailiwick have registered directly with the TPS following the publicity last October. Then only 240 Bailiwick telephone numbers were registered but this had risen to 1,816 in January 2005, representing over a 750% increase.

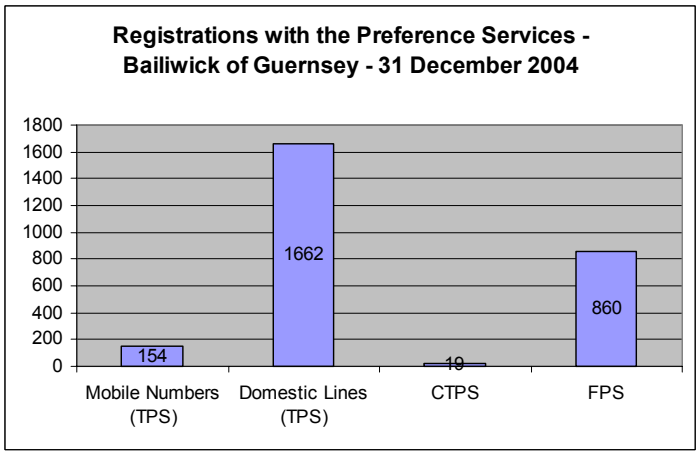
The TPS may be directly contacted on 0845 070 0707 or registrations may be made on line at www.tpsonline.org.uk. An information leaflet on the TPS is available from the Data Protection Office.



Mobile telephone numbers may be registered on TPS as can business telephone numbers, (Corporate Telephone Preference Service - CTPS) and fax numbers (Fax Preference Service - FPS). So far there have not been so many registrations made to these services as to the TPS.

The chart opposite suggests that businesses within the Bailiwick are not making best use of the Corporate Telephone and Fax Preference Services (CTPS and FPS). It is recommended that all telephone and fax numbers that are used should be registered if marketing calls are not required. Registration is available through the DMA website.

The Data Protection Office intends to continue doing periodic surveys to assess the use and ongoing effectiveness of these services.



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