

BAILIWICK OF GUERNSEY



DATA PROTECTION COMMISSIONER REPORT FOR 2003



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.*

Cover Photograph:– “Trans-border flows” - the Water Ceremony at the start of the International Island Games in the Harbour of St. Peter Port, Guernsey on 28th June 2003.

CONTENTS

	Page
Mission Statement	1
Foreword	3
Introduction to the Bailiwick of Guernsey	4
Developments in Legislation	6
Data Protection Issues	8
Notification	12
Staffing and Staff Development	16
Raising Awareness	18
Enforcement	24
International Liaison	29
Objectives for 2004	37
Financial Report	38
The Data Protection Principles	39

FOREWORD

I am pleased to submit to the States my third public report on Data Protection in the Bailiwick of Guernsey that 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 2003, which has been a busy and productive year for my office. The highlight was the formal decision by the European Commission on 21st November 2003 that the Data Protection régime in the Bailiwick was deemed adequate to permit the transfer of personal data from the European Union to the Bailiwick.

This decision followed a sustained period of international negotiations and is good news for locally-established companies with international clients and for any local subsidiaries of organisations based in Europe or elsewhere in the world.

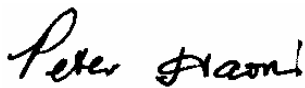
In May, the Guernsey Training Agency and I were pleased to host a Data Protection conference featuring internationally eminent speakers. The conference was well supported both by the public and private sectors and the delegates provided positive feedback on the quality of the content and presentation.

In June, the States of Guernsey approved the drafting of regulations to implement the European Directive on Privacy in Electronic Communications. This decision was mirrored in Alderney and Sark and it is expected that Regulations implementing the Directive should be enacted early in the New Year, further reinforcing the international reputation of Data Protection within the Bailiwick.

My office received a few complaints against data controllers during the year. Where these related to organisations based in the UK, they were passed onto the Information Commissioner's Office, with which we continue to have a close liaison. Complaints against local data controllers were all resolved without recourse to formal action. A number of significant Data Protection issues that arose in the UK during the course of the year are covered in this report, including the Court of Appeal judgement concerning subject access to manual records.

I have consulted the Law Officers, the Police and States Committees over the impact of the Rehabilitation of Offenders legislation. Once this law comes into effect, enforced subject access to criminal records will become an offence, so I have developed a statutory Code of Practice to be laid before the States in 2004 that will define the procedures for obtaining convictions information in relation to employment.

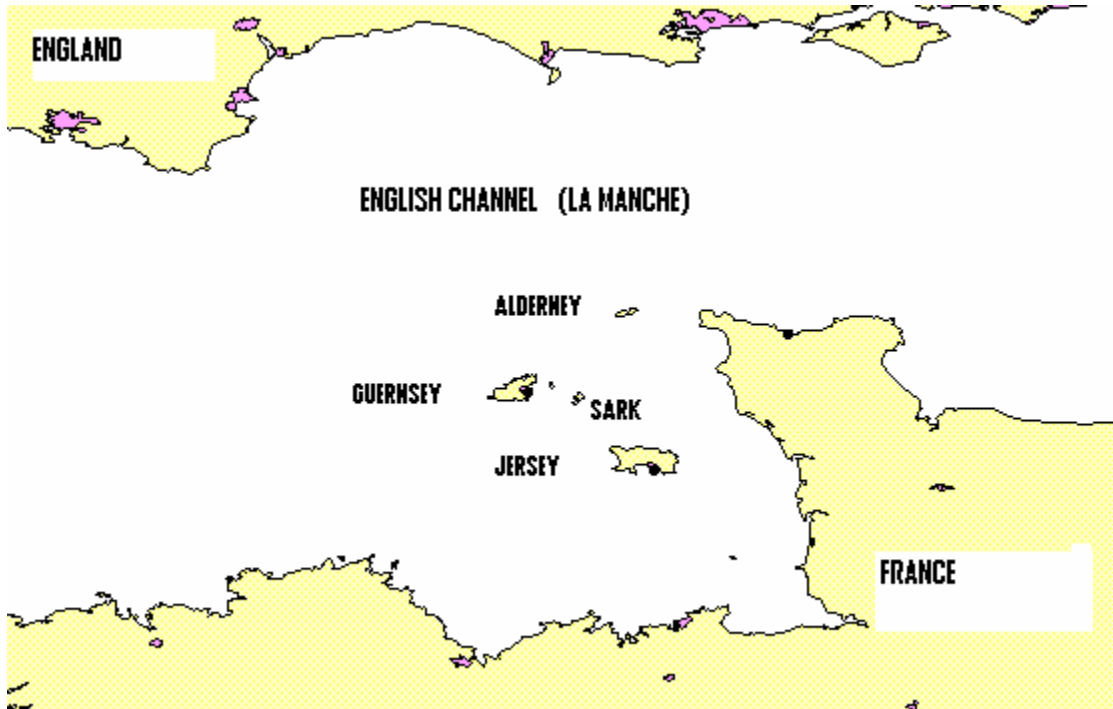
The coming year should see further development by the States of e-government solutions within its revised departmental structure; I look forward to working closely with the newly-formed Departments to ensure that the balance between operational efficiency and personal privacy continues to be maintained.



Data Protection Commissioner, April 2004.

INTRODUCTION TO THE BAILLIWICK OF GUERNSEY

The Channel Islands are a group of islands, islets and offshore rocks located in the English Channel within the Gulf of St. Malo off the north-west coast of France. Although the Islands form part of the British Isles they do not form part of the United Kingdom. They are divided into the Bailiwicks of Guernsey and Jersey.



This report concerns the Bailiwick of Guernsey (hereafter referred to as 'the Bailiwick'), which comprises the main islands of Guernsey, Alderney, Sark, together with Herm, Jethou, Lihou, Brecqhou and associated uninhabited islets and offshore rocks. The censal populations and areas of the inhabited islands are as follows:

Islands of the Bailiwick of Guernsey	Population (2001 census)	Area sq. miles
Guernsey (including Herm, Jethou & Lihou)	59,807	25.11
Alderney	2,294	3.07
Sark (including Brecqhou)	591	2.11
Entire Bailiwick	62,692	30.29

The Islands are 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. Guernsey, Alderney and Sark are each governed by separate elected Legislative Assemblies. The actual day to day administration, however, is conducted through various Committees formed predominantly by members elected from the Legislatures. The Committees are given specific portfolios of responsibilities and are supported by a dedicated Civil Service. Although much legislation is applicable to the individual islands, other legislation, such as that to do with Data Protection, applies on a Bailiwick-wide basis and the responsibilities of the Data Protection Commissioner similarly extend throughout the Bailiwick.

Guernsey is in the midst of a reform of its Machinery of Government that will see a more executive style of government, with the committees being replaced by a smaller number of larger departments under the overall control of a Policy Council.

One of the consequences of this reform will be that responsibility for liaison with the Data Protection Office will transfer in May 2004 from the Advisory and Finance Committee to the Home Department.

Accordingly, the staff of the Office will become seconded from the Home Department and the finance for the Office will be drawn from the budget of that department.

Both the staffing resource and the financial budget are 'ring-fenced' to ensure that they are dedicated to this Office so as not to compromise its independence.

Staff level discussions with the Chief Executive Designate of the Home Department have confirmed that this change of liaison department should make no material difference to the way in which the Office functions.

The merging of departmental responsibilities resulting from the reform of the Machinery of Government will not in itself permit additional data sharing since the fundamental Data Protection purpose limitation principle will still apply, irrespective of how the internal organisation of the departments is effected.

Further pressure for information sharing may also result from the move towards citizen-centric e-government, but any additional sharing of information for purposes related to e-government would, as for any related to the reform process, require legislative changes.

It remains important to ensure that the privacy of citizens is not adversely impacted by any possibility of increased data sharing in the interests of operational efficiency that these or any other similar developments might entail.

DEVELOPMENTS IN LEGISLATION

Guernsey 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.

Data Protection Law

The 1986 law was superseded by the Data Protection (Bailiwick of Guernsey) Law, 2001 ("the Law") which, being based on the 1998 UK Act, was designed to be fully compliant with the EU Data Protection Directive of 1995 and came into force on 1st August 2002. 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; 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, providing further detail on the implementation of the legislation, for example by specifying exemptions and detailing the notification regulations.

Privacy and Electronic Communications

On 25th June 2003, the States of Guernsey resolved to enact regulations to implement the European Directive on Privacy and Electronic Communications. This Directive extends the definition of personal data to include all manner of communications, including e-mail and SMS messaging and provides a statutory opt-out capability from receiving unsolicited marketing material by electronic or telephonic means.

It has already been confirmed that Bailiwick residents may take advantage of the preference services operated by the Direct Marketing Association in the UK and that, once the local regulations are enacted, direct marketing organisations based within the Bailiwick and marketing in the UK should cleanse their marketing lists using the suppression databases available from that association.

Work on drafting these Regulations is due to commence early in 2004 and it is intended that they should follow closely the regulations that came into force in the UK on 11th December 2003. As well as dealing with unsolicited direct marketing, the separate regulations for Guernsey, Alderney and Sark, will impose privacy standards on the operators of telecommunications services in the Bailiwick and help to ensure that all licensed operators are covered by common privacy standards.

Rehabilitation of Offenders

Although the Rehabilitation of Offenders (Bailiwick of Guernsey) Law was passed in 2002, the commencement ordinance was not made by the Advisory and Finance Committee in 2003. This ordinance, which will specify in detail those occupations and professional appointments which are exempt from non-disclosure of spent convictions, is expected to be made early in 2004.

From the commencement of that law, it will become unlawful for spent convictions to be disclosed other than in circumstances specified in the ordinance; furthermore, commencement of Section 56 of the Data Protection Law will make it unlawful for an employer or prospective employer to require an employee to make a subject access request in order to reveal a police record that might include both unspent and spent convictions.

During 2003, the Commissioner consulted with the Law Officers, States Committees and the Guernsey Police in order to develop a statutory Code of Practice covering the disclosure of conviction information in connection with employment.

A draft version of this Code of Practice was circulated to States committees in December and will be published on a consultative basis early in 2004 with the aim of laying the final version before the States - in accordance with section 51(3) of the Data Protection Law - at about the same time that the Rehabilitation of Offenders Law and section 56 of the Data Protection Law are commenced.

This Code of Practice has been 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.

Simplification of the Operation of the Law

The UK Information Commissioner has stated that he wishes to simplify the operation of the UK Act and there have also been calls to clarify the interpretation of some of its provisions following the outcome of the Soham murder investigation.

These developments will be monitored in the coming year and any consequential recommendations for changes to the local legislation advised to the States in due course.

DATA PROTECTION ISSUES

A number of significant issues arose during 2003 that are dealt with in more detail below.

Anti-money-laundering and “know your customer”

In June, the Financial Action Task Force on Money Laundering issued an updated version of the “Forty Recommendations” and “Eight Special Recommendations” in relation to the combating of money laundering and the financing of terrorism.

These were incorporated in revised draft Guidance Notes issued by the Guernsey Financial Services Commission, prior to the making of new Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Regulations, 2003.

The Commissioner made representations to the Financial Services Commission over the draft Guidance Notes particularly in relation to the need for the definition of retention periods for personal data contained within transaction information and over the requirement for detailed originator and payee information to accompany all international wire transfers.

The Commissioner also proposed that a more risk-based approach should be taken in respect of anti-money laundering, rather than the blanket approach of harvesting all the “white data” in the hope of capturing the minute percentage of suspicious information therein.

The Financial Services Commission responded positively to these concerns and, in conjunction with other interested parties, produced an information leaflet for use by financial services institutions that explained the “Know Your Customer” procedures in layman’s terms.

Disclosure of passenger manifest details to the US authorities

In the aftermath of the terrorist attacks of 11 September 2001, the United States enacted legislation in November 2001, requiring that air carriers operating flights to, from or through the United States provide the United States’ Customs with electronic access to the data contained in their automated reservation and departure control systems, known as Passenger Name Records (PNR).

Whilst recognising the legitimate security interests involved, the European Commission informed the US authorities as early as in June 2002 that these requirements could conflict with Community and Member States’ legislation on data protection and with any provisions relating to the regulation of Computerised Reservation Systems (CRS).

The US authorities postponed the entry into force of the new requirements, but finally refused to waive the imposition of penalties on non-complying airlines beyond 5 March 2003. Several major European airlines have been providing access to their PNR since then.

On 18 February 2003, the European Commission and the US administration issued a joint statement, recalling their shared interest in combating terrorism, setting out initial data protection undertakings agreed by US Customs and recording the parties' undertaking to pursue talks with a view to allowing the Commission to make a decision in accordance with Article 25 (6) of the Data Protection Directive 95/45/EC, recognising the protection given to the transmitted data as adequate. The talks have thus aimed to bring the way the US use and protect PNR data closer to EU standards.

The European Data Protection authorities have constantly argued for the correct balance to be struck between combating terrorism and respecting personal privacy and this process has resulted in the filtering of irrelevant personal details from the PNR and undertakings that the data transferred will not be used for other purposes. However, the general approach of indiscriminate harvesting of such "white" data remains of concern and will continue to be a matter that requires careful monitoring in future.

Definitions of "personal data" and "relevant filing systems"

There is a scarcity of case law on Data Protection, so the judgment of Lord Justices Auld, Mummery and Buxton dated 8th December 2003 in the Court of Appeal in the case of *Durant v Financial Services Authority* is of particular interest and would be persuasive in the interpretation of the Law in the Bailiwick.

The judges considered that four important issues of law concerning the right of access to personal data were raised:

1. What makes "data" "personal" within the meaning of "personal data"?
2. What is meant by a "relevant filing system"?
3. Upon what basis should a data controller consider it "reasonable in all the circumstances" within the meaning of section 7(4)(b) to comply with the request even though the personal data includes information about another and that other has not consented to disclosure?
4. How much discretion does the court have as to whether to order compliance with a request if it finds the data controller has wrongly refused a request under section 7(4)?

The Court of Appeal's Findings

1. Personal data

The judges found that in conformity with the 1981 Council of Europe Convention (Convention 108) and the 1995 General Data Protection Directive (95/46/EC) the purpose of section 7 of the Act is to enable an individual to check whether a data controller's processing of his personal data unlawfully infringes his privacy and,

if so, to take steps, for example under section 14 or section 10, to protect it. It is not an automatic key to any information, readily accessible or not, of matters in which he may be named or involved. Nor is it to assist him, for example, to obtain discovery of documents that may assist him in litigation or complaints against third parties. It is likely in most cases that only information that names and directly refers to him will qualify.

2. "Relevant Filing System"

The judges noted that there was no material difference in the provisions of the Directive and of the Act. The court concluded that the intention "is to provide as near as possible the same standard of sophistication of accessibility to personal data in manual filing systems as to computerised records". It is right that the definition be broken down into three constituents:

1. Whether the material was a set of information relating to an individual;
2. Whether the material was structured either by reference to individuals or by reference to criteria relating to individuals;
3. Whether it was structured in such a way that specific information relating to a particular individual was readily accessible.

The Court found that the Directive supported a restrictive interpretation of "relevant filing system", and that "the protection given by the legislation was for the privacy of personal data, not documents".

3. Redaction

The Court found the protection that the Act gives to other individuals is qualified. The principle of proportionality means that the interest of the data subject in gaining access to his personal data must be balanced against that of the other individual in the protection of his privacy.

The balancing exercise only arises if the information relating to the other person forms part of the "personal data" of the data subject. The provisions of the Act appear to create a presumption that information relating to a third party should not be disclosed without his consent. The presumption may, however, be rebutted if the data controller considers that it is reasonable "in all the circumstances" to disclose it without such consent. The circumstances that go to the reasonableness of such a decision include, but are not confined to, those set out in section 7(6).

4. The Court's Discretion

The last issue to be considered by the Court was the extent of the Court's discretion under section 7(9) of the Act to order a data controller to comply with a request for information under that section where the data controller has failed to do so in breach of the Act.

The Court noted that the question of the exercise of discretion did not arise in this case but agreed with the observations of Mundy J in the case of *R (on the application of Alan Lord) v The Secretary of State for the Home Department* [2003] EWHC 2073, at paragraph 160, that “the discretion conferred by that provision is general and untrammelled”.

The Commissioner welcomes the contribution that this judgment will make to case law on Data Protection. It is intended to issue updated guidance incorporating the consequences of judgement as soon as possible during the early part of 2004.

Retention of criminal intelligence in connection with vetting

Following the conviction of Ian Huntley for the Soham murders, it emerged that the Humberside Police had destroyed vital criminal intelligence information that related to allegations against him, ostensibly because of the data retention provisions in the Data Protection Act.

As a consequence there were initially calls for the Act to be amended, but later it emerged that this failure appeared to be due to misinterpretations of the law rather than to deficiencies in the law itself.

Nevertheless, it is likely that there will be some relevant findings from the enquiry set up after the conclusion of the case and these will be evaluated and taken into consideration in any policy advice that may be given to the States once they have been published.

Bogus Data Protection Agencies

The activities of the self-styled notification agencies have created considerable problems in the UK and some have extended their operations to cover the Bailiwick. There have been many complaints about the “official-looking” notices that are sent to businesses demanding that they notify and pay an inflated fee. The UK Commissioner has been working closely with Trading Standards Offices, the Office of Fair Trading and Police forces with a view to prosecuting these agencies. Any organisation in the Bailiwick that receives a communication from a “Data Protection Agency” based in the UK should ignore it.

‘Blaggers’

There has been some evidence of tracing agents using deception or impersonation to obtain information about people. This is colloquially known as ‘blagging’ information. A training video is available to assist those who might be the target of such blaggers on how to deal with them. The UK Commissioner has already successfully prosecuted some of the perpetrators.

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.

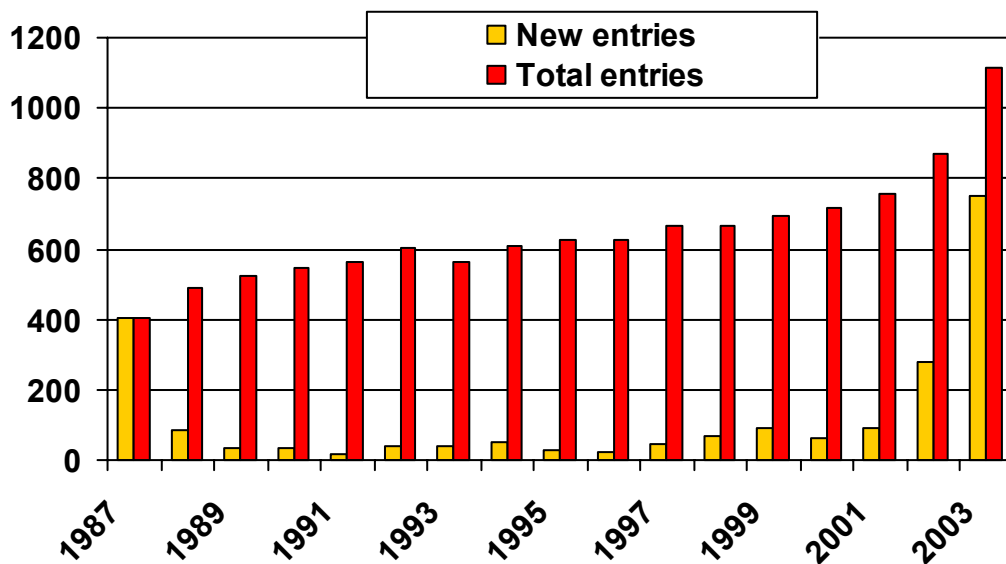
Exemptions from Notification exist for manual data, certain charitable and not-for-profit organisations and for the processing of data associated with the core business purposes of accounts, staff administration and marketing.

Controllers Registered under the 1986 Law are deemed to have Notified until their existing (three-year) Registrations expire.

The chart reproduced below shows that Registrations grew slowly from an initial figure of 400 in 1987, when the 1986 Law came into force, rising to just over 800 by the commencement of the 2001 law in August 2002. Since then, Notifications have risen by nearly 50%, reaching over 1100 by the end of 2003.

This is despite the fact that some multiple registrations by controllers under the 1986 law are being replaced by single notifications under the 2001 law and would appear to be as a result of the increased profile of Data Protection and especially the awareness and compliance campaigns that were mounted during the year.

GROWTH IN DATA PROTECTION REGISTER ENTRIES

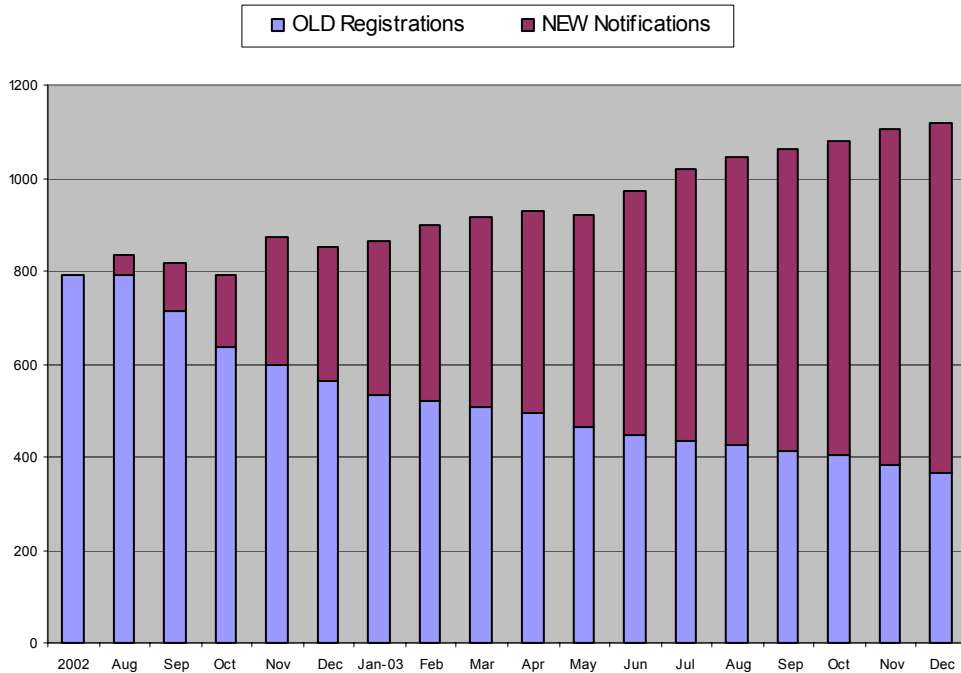


It is anticipated that this increasing trend will probably level off during 2004.

A total figure of 1200 - 1300 Notifications would appear to be a reasonable number for an area of the size, population and economic activity of Guernsey.

The chart below shows the continued rise in New Notifications displacing those Old Registrations that have expired. Because Registrations under the 1986 Law have a 3-year life and continued to be issued and renewed until the end of July 2002, the last of those Old Registrations will not finally disappear until mid-2005.

OLD Registrations and NEW Notifications since 2002



The Internet Notification process was further enhanced early in the year to provide better support for the annual renewal process.

This meant that all data controllers who had provided an e-mail contact address within their Notification were sent their first renewal notice by e-mail and those who paid by direct debit had their Notification automatically renewed.

This resulted in a significant improvement in the efficiency of the renewals process; by the end of the year, over 87% (650) of Notifications included an e-mail address and over 80% of the 161 e-mail renewals issued from September to December 2003 led directly to a renewal without the need to issue a postal reminder.

In addition, of the 263 Notifications that were renewed between August and December, 56 (21%) had been set up by direct debit and were able to be renewed automatically.

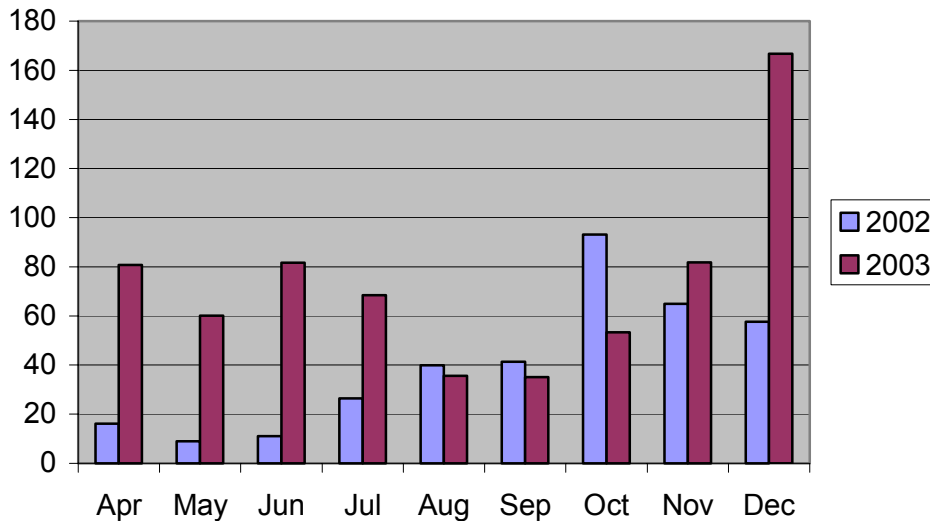
A facility was also developed to allow data controllers to amend the details of their notifications on-line, by opening existing register entries for update. This further reduced the administrative effort of the Office and also assisted data controllers in the keeping of their entries up to date as is required by the Law.

The chart below illustrates the variation in the average daily activity on the online notification site: <http://www.dpr.gov.gg>, between April and December in 2002 and 2003. The vertical axis represents the average daily rate of successful requests for pages of data from the site.

The figures for 2002 show a sharp rise following the launch of the site in July with activity peaking in October.

The figures for 2003 show a reasonably constant activity apart from what seems to be a seasonal decline during the summer months of August and September and a sharp increase in December, possibly due to the larger number of renewals that fell due in that month.

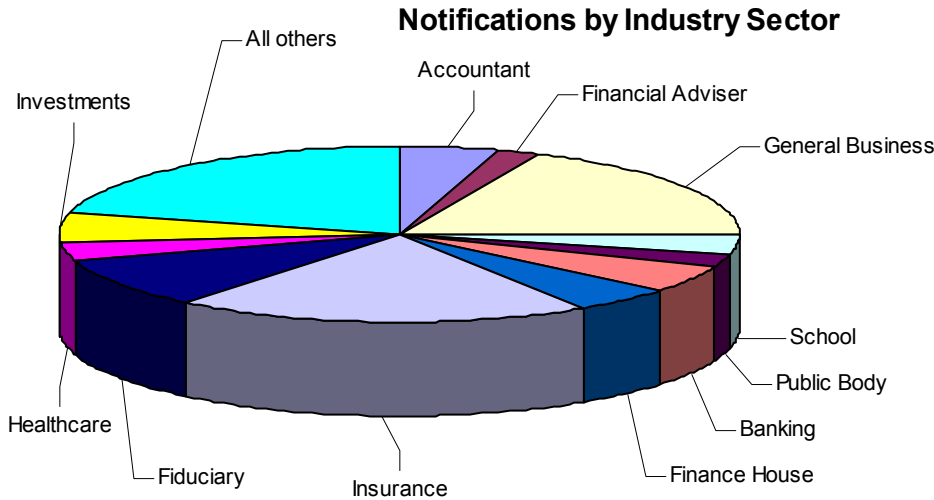
**Comparison of Notification Site Activity
between 2002 and 2003**



There remain problems in that Internet search engines looking for “Data Protection” tend to find the Guernsey Data Protection Notification site in preference to that of the UK Information Commissioner, for searches ‘within the UK’. This means that, despite the prominent warnings that are displayed on the Notification site, some UK 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.

A similar problem that led to UK-based callers to the Directory Enquiry services being directed to Guernsey rather than the Information Commissioner’s Office in Wilmslow appears now to have been largely resolved, as far fewer calls originating from the UK were received in 2003.

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 above shows the cumulated distribution of notifications at the end of 2003 by industry sector, continuing a similar pattern to that of 2002.

The largest number of notifications was derived from Insurance (20%), followed by General Business (18%), Fiduciary (9%), Finance House, Accountant, Investments and Banking (all at 5%), with All others (21%).

Exemptions from the need to notify may be claimed by controllers 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 those whose processing is limited to manual data.

The compliance drive netted an additional 130 Notifications in 2003 and also resulted in 303 organisations being added to the database of exempt controllers. 37 organisations, who might otherwise have claimed an exemption, chose to Notify voluntarily. This relieves them of the alternative obligation under section 24 of the Law from making equivalent particulars of their processing available to any person on demand.

STAFFING AND STAFF DEVELOPMENT

The establishment of the Office of the Data Protection Commissioner presently comprises three staff: the Commissioner and Assistant Commissioner - who work full time - and the Personal Assistant to the Commissioner who works part-time. The Commissioner is a statutory public appointment and members of his staff are seconded from the Civil Service, but wholly responsible to him.

Following the implementation of the reforms to the Machinery of Government, the Commissioner's staff will be seconded from the newly-created Home Department, rather than from the Advisory & Finance Committee.

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 the minimum level of staffing resource necessary for him to undertake his current functions. There is no evidence at present that an increased establishment is required.

The Assistant Commissioner, Anne Wiggins was appointed in August 2002. Her role is to assist the Commissioner in promoting and enforcing the Law, with primary responsibility for raising awareness amongst both individuals [data subjects] and organisations [data controllers]. She achieves this by the design and production of leaflets and the running of short in-house courses for data controllers.

In addition, she investigates compliance matters, having contacted and followed up numerous compliance issues with specific industry sectors in the past year. As part of her compliance activities, she is also responsible for the generation and completion of draft notifications.

Anne is normally the first point of contact for complaints from data subjects and she deals with the initial work on any resulting assessments of processing.



In April, she participated in the European Spring Conference of Data Protection Authorities that was held in Seville and represented Jersey and the Isle of Man as well as the Bailiwick. This was an opportunity to interact with members of supervisory authorities throughout Europe and to appreciate the common problems that are faced in many countries.

Also in April, she spent two days at the office of the UK Information Commissioner in Wilmslow, Cheshire. The full and varied programme which was organized for her enabled her to acquire knowledge of the structure and systems of the Commissioners office as well as meeting key members of his staff. She is thankful to him and his staff for providing this very valuable and positive experience.

In July, she attended the three day conference at St John's College, Cambridge which is organized annually by Privacy Laws and Business. The theme of the conference was incorporating risk management into everyday practice. This gave her an opportunity to meet people from many public and private sector organisations and to learn how they are incorporating the requirements of data protection legislation into their work situations.

Towards the end of the year, Anne enrolled on an ISEB Data Protection course at Mason's in London. Successful completion of this course will not only give her a formal qualification, but will also provide an opportunity for her to assess the suitability of the course for local compliance officers who may wish to gain a qualification in Data Protection.

During the year, Wendy Ozanne was promoted to the post of Personal Assistant to the Commissioner.

In that role she combines her previous duties of administrative support to the office with more specific duties in support of the Commissioner, such as arranging appointments and travel, dealing with the office financial management and managing the Commissioner's correspondence.

Wendy is the initial contact for personal and telephone callers to the office and she has primary responsibility for the maintenance of the Notification system and the collection of Notification fees.

She has also attended Civil Service Board training courses on the use of the States corporate SAP accounting system and reconciles the entries in that system with the Commissioner's bank account.



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 2003 has included the following activities:-

- Organising Data Protection Conferences
- Delivering presentations and training
- Involvement in working groups
- Making use of the media.
- Giving compliance advice
- Developing the Internet web site

Local Data Protection Conferences

Les Cotils Conference

This Data Protection Conference was organised by the Commissioner, the Data Protection Adviser and the Training Agency on 13th and 14th May 2003 at Les Cotils Conference Centre.

The Public Sector day on 13th May was chaired by the Data Protection Adviser and attended by 74 delegates, including some public servants from Jersey. The Private Sector day on 14th May was chaired by the Commissioner and attended by 47 delegates. Papers were presented by:

- Robert Titterington - the draughtsman responsible for the Data Protection Law,
- Louise Townsend and Rosemary Jay from Mason's solicitors,
- Sandra Cavill from the Office of the UK Information Commissioner,
- Stewart Dresner, from Privacy Laws & Business,
- Diana Alonso Blas, from the European Commission,
- The Commissioner and Assistant Commissioner.

The Data Protection Supervisor from the Isle of Man, the Registrar and Deputy Registrar from Jersey also took part and chaired some of the discussions.

Delegates' responses from both days were positive, with the main comments being "interesting", "professional", "valuable", "helpful" and "well-presented".

The support and organisation provided by the Training Agency was of a high standard.

Conference for Board of Health Staff

This conference, which took place at the Peninsula Hotel on 03 December 2003, was organised by the Commissioner and the Board of Health (BoH) . It was structured into two half day sessions which were attended by thirty eight delegates from the BoH and other health organisations. Ann Jones, Assistant Information Commissioner for Wales and David Evans, Compliance Manager, Health Sector, Office of the UK Information Commissioner delivered the sessions at the invitation of the Commissioner, who participated in the discussion and workshop sessions. The conference was well received by the delegates and resulted in further training needs for health service staff being identified.

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 was around 770.

Involvement in Working Groups

The Commissioner and Assistant Commissioner also participated on various 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 a number of press releases throughout 2003; these gave information about:

- the data protection obligations of data controllers in relation to Closed Circuit Television Systems (CCTV)
- the Commissioner's visit to Zurich where he participated at the International Working Group on Data Protection in Telecommunication
- the data protection conferences organised by the Commissioner's office and Guernsey Training Agency for the public and private sectors.
- assurances that data protections principles would be upheld in the reorganisation that would be brought about by the future Machinery of Government changes
- bogus data protection letters from UK agencies to businesses and organisations within the Bailiwick

- the approval by the European Commission of the Bailiwick's data protection legislation
- the anti-spam regulations which came into force in the UK in December and how these would affect Bailiwick residents

Press articles

There was a total of twenty-two articles published in the local press which concerned the following data protection issues:

- the legal obligations of data controllers in regard to registering details of their personal data processing with the Commissioner and their use of CCTV;
- bogus data protection letters from UK agencies to businesses and organisations within the Bailiwick;
- the Commissioner's visit to Zurich for the "anti-spam" discussions – this report was supplemented by an editorial in the Comment column which supported the Commissioner in undertaking his international co-operation activities in the fight against "spam";
- the approval by the States for the drafting of the Privacy and Electronic Communications "anti-spam" regulations;
- the conditions under which postal, telephone and e-mail communications may be intercepted by public bodies within the Bailiwick;
- how the Commissioner's office carries out its compliance responsibilities;
- the progress of the European Commission in deciding the adequacy of the Bailiwick's data protection legislation;
- the advantages and disadvantages of introducing Identity Cards within the Bailiwick;
- the Commissioner's views on the USA's demand that European airline carriers transfer personal data of passengers travelling to, from and through the United State so as to combat terrorism and other international crime;
- the data protection function of getting the balance right between protecting individuals' rights to privacy and protecting the general public – this was in the wake of the Soham trials;

The Commissioner was interviewed on a number of occasions on local radio and television on some of the issues raised in the press releases and the press reports.

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

The following literature has been produced by the Data Protection Office. The brochures are free of charge and are available in hard copy but may also be downloaded from the Commissioner's website.

Advice Booklets (A5)

- Notification – a Simple Guide
- Baby mailing preference service (how to stop unwanted mail about baby products)
- Be Open ...with the way you handle information (obtaining data fairly and legally)
- CCTV – Guidance for Users
- CCTV Checklist
- Data Controllers (how organisations must process personal data)
- Your rights under the Law: Guidance for individuals
- Mailing, telephoning, fax and e-mail preference services
- No Credit (how to access, and correct, details held by credit reference agencies)
- The Data Protection Law and You (advice for small businesses)
- Violent warning markers: use in the public sector

Guidance Handbooks (A4)

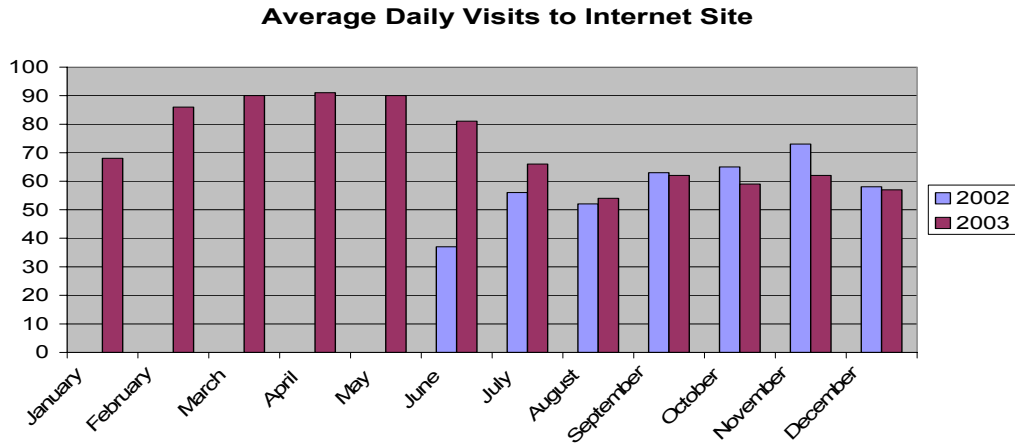
- Charities
- Data Controllers
- Financial Institutions
- Notification Exemptions
- Notification Handbook
- Small Businesses
- States Committees

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 4,000 copies of the literature were distributed during 2003. In addition, Notification Guidance Handbooks were sent out to data controllers when their registrations under the 1986 law were about to expire.

Developing the Internet Web Site

All of the information published by the Office is available on the Internet site: <http://www.dataprotection.gov.gg>, for which access statistics are available from June 2002.



The chart above shows that the usage of the site in 2003 has varied between about 55 and 90 visits per day. 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 Commissioner’s office, together with links to other data protection sites and information for data subjects about complaint handling.

The range of information available on the Internet site continues to grow, but it was not possible to undertake the redesign of the site during 2003 as a major redevelopment of the overall ‘Guernsey.government’ portal, <http://www.gov.gg> was in progress.

Further work is anticipated in 2004 on improving the linkage between the Guernsey.government portal and the ‘dataprotection’ site, in particular by the provision of a search facility.

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.

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.

An Information Notice was served on one data controller who did not provide the Commissioner with a description of personal data processing upon request. This prompted the data controller to provide the requested information.

Towards the end of 2003 five data controllers were referred to the Law Officers in connection with notification offences. These are currently being investigated by the Police.

Brief details of the assessments undertaken during the year are as follows:

Introduction

During 2003 the Commissioner received nineteen complaints regarding how personal data were being processed. One of these complaints was ongoing from the previous year and is included in the eight official Requests for Assessment investigated by the Commissioner. Two complaints were forwarded to the Office of the United Kingdom Information Commissioner. Three complaints were treated as general enquiries as the Commissioner considered that to do so was in the general public interest. Enquiries were made into the remaining six complaints but these were not pursued.

Official Requests for Assessment

1. An individual who was undergoing divorce proceedings complained that her husband's advocate had acquired itemized billings of telephone calls that she had made. The Commissioner's office received full co-operation from the organisation concerned. It was established that the calls were made during a period when the couple were still co-habiting. The

Commissioner found the complaint was ill-founded as no unlawful disclosure had been made by the organisation.

2. A voluntary organisation complained that an ex-employee had removed a card index system which contained names of customers. The Commissioner was unable to help in this case as the manual data concerned were subject to the transitional provisions allowed for in the Law, and so would not be subject to data protection requirements until 31 July 2005.
3. An individual received an adverse report from an organisation which prevented him from setting up a new business venture. He suspected that the negative report was a result of inaccurate data contained within his personal file. He was advised to make a subject access request so that he would have the opportunity to have any inaccurate information corrected and to have his comments added to any statement which was in dispute. On gaining access to records inaccuracies of information did come to light. Following a without prejudice face to face meeting the individual provided the organisation with additional information with which the relevant records were updated.
4. An Alderney resident and a local politician raised concerns that hotels and guest houses in Alderney were being officially requested to collect excessive amounts of personal data on their guests. It was established that the information collected exceeded its intended purpose which was statistical analysis. The Commissioner referred the matter to the Law Officers who suggested to the States of Alderney that the appropriate legislation be amended to draft an Ordinance that would specify the purpose of the collection of information. It was also suggested that the Ordinance might only need to be made if a voluntary code of practice failed.
5. An individual complained that a number of health professionals had made disclosures of her health records to her estranged husband without her consent. She also expressed concern that she had been given an inaccurate diagnosis which prejudiced how she was treated by different doctors.

On advice from the Commissioner she made subject access requests to the relevant health professionals. She received copies of her medical records from some doctors but others did express concern that the release of the records might be of some detriment to her. There is a provision in the secondary legislation which exempts data controllers from complying with subject access requests if it is considered that to do so would serious physical and / or mental harm to the data subject.

Following further discussion with the Commissioner the individual decided not to proceed further with the complaint.

6. An individual complained to the Commissioner that a local credit reference agency had not removed spent information from his personal file. The Credit Reference Agencies' Code of Practice in the UK states that all information over six years old should be deleted from credit files. After liaison between the Commissioner and the credit reference agency concerned the file was deleted.
7. A finance company did not renew a client's credit facility and added an extra sum of money to the final settlement figure. Another person, acting as the authorized agent for the client, wrote to the finance company and asked for an explanation as to why these actions had been taken; he also asked why his offer as a guarantor had been refused.

The finance company responded by saying that they could not discuss matters with the authorized agent due to "recent legislation being imposed on the finance industry by the Guernsey Financial Services Committee (Data Protection)." Subsequently the Financial Services Commission referred the agent to the Data Protection Office.

The finance company was contacted and advised of their obligations under the law in relation to subject access rights. This resulted in the finance company agreeing to discuss the matter with the authorized agent.

8. An individual complained that on receipt of the revised Postcode Finder he discovered that the road where he lived had been renamed. He claimed that this would cause him, and anyone else similarly affected many problems, such as difficulty in buying goods on the internet and undergoing security checks.

The Postcode Finder had been revised by Guernsey Post following a collation exercise done by Guernsey Digimap Services (GDS) between the "official road names" used in the Digital Map and those held by Guernsey Post.

The Commissioner's Office liaised with Guernsey Post, the relevant Parish Constables and GDS about this matter and it was agreed that all queries relating to road name changes would be investigated. GDS contacted all parochial authorities requesting updates to the "official road names" that had been used. In the meantime the complainant received assurance from Guernsey Post that address information would not be passed on to any third parties until all corrections to road names had been processed; therefore the accuracy of his personal data was unlikely to be compromised in any way.

Referred Complaints

Two complaints, each received from elected States members within the Bailiwick of Guernsey, were referred to the Office of the UK Information Commissioner.

The first complaint concerned a UK based organisation using a personal e-mail address of a Bailiwick resident for the purpose of unsolicited marketing.

The second complaint also concerned using a personal e-mail address by a training agency for the purpose of unsolicited marketing. The company concerned was allegedly based in Guernsey but there was uncertainty about this as there was a diversion when the local telephone number was used and the e-mail address was a UK based ISP. The company was not listed in the local directory.

The investigation into these complaints continued into 2004.

General / Public Interest Enquiries

- On opening a deposit account with a bank an individual wished to nominate his employees to be signatories to the said account. When he complained that the bank was asking for excessive information to verify the identity and addresses of his staff the bank stated that they acting in accordance with what Guernsey Financial Services Commission (GFSC) required. He was also informed that the bank would retain any information obtained during the verification process.

The Commissioner decided to treat this matter as a general issue rather than a complaint against the specific bank. On contacting the GFSC it was learned that the GFSC was in liaison with the Association of Guernsey Banks and the Financial Intelligence Service (FIS) about preparing a leaflet on how banks could give clearer guidance to their customers on the procedures to be used in respect of Due Diligence checks. This leaflet has since been published. The GFSC informed the Commissioner that it would contact the Law Officers and the FIS on the issue of record retention.

- The Commissioner was contacted and subsequently interviewed by a local radio station as one of their reporters had found a patient's notes in a hospital car park and handed them in. This incident raised public concerns over the protection of patient confidentiality as well as the security measures taken by health personnel when they were transporting clinical notes between sites.

After liaison between the Commissioner and the appropriate authority the security policy of the organisation was assessed and it was advised that staff should be given more explicit guidance when carrying clinical notes on their person and / or in their cars. This advice was actioned.

- An enquirer concerned about people's rights and civil liberties asked whether civil servants and politicians would have access to individuals' personal data via the States computer systems and the computer system of a locally owned airline, especially with regard to their movements.

The Commissioner wrote to the President of the Advisory and Finance Committee and the airline's Managing Director. The responses that the Commissioner received showed that the complainant's concerns were ill-founded.

The Commissioner also gave assurance that any States employee obtaining and / or disclosing personal data made without the consent of the relevant States Committee would face prosecution. Further assurances were also given about the data protection training that civil servants receive and the independence of the Data Protection Commissioner

The complainant was advised that for an Assessment of Processing to take place he would have to provide firm evidence of a contravention of the law. No response to that effect was received.

Complaints not pursued

Six complaints were not pursued by the Commissioner as the complainants did not supply necessary information and / or documentary evidence to enable the complaints to be accepted as official Requests for Assessment.

INTERNATIONAL LIAISON

A major focus of the International visits made in 2003 was to facilitate obtaining a positive decision from the European Commission on the adequacy of the Data Protection régime in the Bailiwick.

In January, the Commissioner and a legislative draughtsman were invited to visit the offices of the European Commission in Brussels, for a day-long examination of the Bailiwick's Data Protection legislative and enforcement régime.

Immediately prior to this meeting, the Commissioner took the opportunity to attend a conference in London organised by the newly-appointed UK Information Commissioner, Richard Thomas, on the Government proposals on 'entitlement cards'; following an address by the Home Secretary, many speakers expressed concerns over the potential privacy implications of the cards and the likelihood of "function-creep" once they were introduced.

The Commissioner and the legislative draughtsman also met officials from the Data Protection Unit within the Lord Chancellor's Department [now the Department of Constitutional Affairs], which represents the UK Government on Data Protection matters in Europe, for a briefing on the UK position in relation to the adequacy question prior to travelling to Brussels.

The EU officials in Brussels posed numerous questions, all of which were satisfactorily addressed by the Bailiwick representatives. The officials outlined the 'comitology' process leading to a final decision of the European Commission and explained that it involved a protracted time-scale:

- firstly, the working party established under Article 29 of the Directive, comprising the European supervisory authorities, would be asked for their opinion;
- following that, the committee established under Article 31 of the Directive, comprising representatives from the EU Member States would be asked to endorse the Opinion of the Article 29 working party;
- next, a draft decision would be prepared and circulated amongst the EC Directorates, a process known as 'inter-service consultation';
- finally, the draft decision would be laid before the European Parliament for any comments prior to its being formally published in the Official Journal.

The delegates from the Bailiwick were advised that the soonest that they could expect the official decision would be by the end of the year, on the assumptions that no delays were encountered in this comitology process.

The fact that the official decision was indeed published in the Official Journal on 25 November means that the finding of adequacy for the Bailiwick represents the fastest adequacy decision taken by the Commission to date.

It is to be hoped that the process used for Bailiwick will be able to be used as a means of expediting similar decisions for the other Crown Dependencies.

International Working Group on Data Protection in Telecommunications

The Commissioner [also representing Jersey and the Isle of Man] attended the 33rd meeting of this group that was held in Zurich in March 2003.

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 34th meeting was held in Berlin in September and was attended by the Assistant Supervisor from the Isle of Man, who was also asked to represent the Bailiwick.

A particular topic at this meeting concerned the privacy aspects of ‘RFID’ tags; this new technology offers the possibility that individual articles may be tagged with unique codes that would permit them to be tracked not only during manufacture but also after purchase.

A draft resolution on RFID was prepared for consideration by the Annual conference in Sydney and then refined following comments received thereafter. The final version of this resolution is reproduced on page 34.

European Spring Conference

The Spring Conference of European Data Protection Commissioners was held in Seville, Spain on 3-4 April 2003. It was attended by eighty-eight delegates from twenty-five European data protection supervisory authorities, the European Commission, the Council of Europe and the Data Protection Secretariat. The Bailiwick of Guernsey was represented by Assistant Data Protection Commissioner, Anne Wiggins, who was also asked to represent Jersey and the Isle of Man.

The conference was structured into 6 sessions, the first five sessions concentrated on specific topics and the last session was devoted to general topics:

Session 1 – “Roles of Data Protection Authorities”

Session 2 – “Implementation of Directive 95/46/EC”

Session 3 – “The current situation of data protection in candidate countries”

Session 4 – “International transfers of personal data”

Session 5 – “Data protection in the Telecommunications Sector”

British and Irish Data Protection Authorities

This meeting of the supervisory authorities from the UK, Ireland and the Islands was held in Wilmslow on 23rd July and chaired by the UK Information Commissioner. It was an opportunity to meet the regional assistant commissioners for Northern Ireland and Wales, whose offices were in the process of being established.

The items covered in the meeting included:

- The Privacy and Electronic Communications Directive;
- Citizen identity and e-government;
- Know Your Customer;
- Biometrics and genetic information.

Rights to Privacy

This seminar entitled “Privacy: Thai and Farang [foreign] experiences” was hosted by the Thailand Office of the Information Commission in Government House, Bangkok on 2 September.

The Commissioner and the Jersey Registrar had been invited to lead the seminar by presenting the way in which the Channel Islands had addressed compliance with European directives on privacy and data protection. The seminar was well attended and included the government lawyer who was drafting the Thai Data Protection Law.

The illustration opposite shows the Guernsey Commissioner and the Jersey Registrar, with Mr. Niti Wirudchawong, the organiser of the seminar, preparing the material in Government House.



The ensuing debate highlighted some cultural differences between Western and Asia/Pacific societies that can pose difficulties with privacy legislation that is concerned with personal data. Asian culture tends to value the rights of the family higher than those of the individual, leading to potential conflict with the traditional Western view of individual privacy and subject access rights.

The Body as Data

This international conference, on the Data Protection implications of Genetics and Biometric Data was held in the impressive 'BMW Edge' conference centre in Melbourne, Victoria on 8th September and attended by about 140 delegates, about half of whom were from Australasia.

The conference included papers on the privacy aspects of genetics and biometrics and the Commissioner was invited to participate as a member of the "panel of experts" that facilitated the discussion session following the presentation of papers.



Picture courtesy of the Victoria Privacy Commissioner

Further details of the conference are available on www.privacy.vic.gov.au by following the 'conferences' link.

25th International Conference of Data Protection Authorities

This annual conference was held from 10-12 September 2003 at the Convention centre in Darling Harbour Sydney. It was attended by over 360 delegates, comprising Data Protection and Privacy Commissioners from Europe, Asia, the Americas and Australasia, representatives from a number of other countries that were in the process of implementing privacy legislation and many interested parties from government and commerce in Australia.

The theme of the conference was "Practical Privacy for people, government and business", the aim being to get Data Protection and Privacy Commissioners, and other government regulators, practitioners, analysts and consumers talking together about what makes good privacy, where the problems are and where the opportunities are to implement good privacy practice.

Full details of the conference may be found on the internet site:
<http://www.privacyconference2003.org>

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

1. Improving the communication of data protection and privacy information practices;
2. The Transfer of Passengers' Data;
3. Data Protection and International Organisations;
4. Radio-Frequency Identification;
5. Automatic Software Updates.

Improving the communication of data protection and privacy information practices

1. The conference calls the attention of organisations, in both public and private sectors, to the importance of:
 - improving significantly their communication of information on how they handle and process personal information;
 - achieving global consistency in the way they communicate this information;and by these means
 - improving individuals' understanding and awareness of their rights and choices and their ability to act on them; and
 - putting an incentive on organisations to improve, and make more fair, their information handling and processing practices as a consequence of this awareness.

[N.B. the remainder of this conference resolution is available on:

<http://www.privacyconference2003.org/commissioners.asp>]

The Transfer of Passengers' Data

- A. The Conference notes that:
 1. In the course of the legitimate struggle against terrorism and organized crime measures are being considered in some countries that could threaten fundamental rights and freedoms, in particular the right to privacy.
 2. There is a danger of undermining democracy and freedom by measures designed to defend it.
 3. Legal requirements on airlines and other transports to provide access to, or transfer data from, comprehensive passenger data stored in reservation systems could conflict with international data protection principles or those providers' obligations under national data protection laws.
- B. The Conference therefore affirms that:
 1. In the fight against terrorism and organized crime, countries should determine their responses paying full regard to fundamental data protection principles, which are integral parts of the values being defended.

Where regular international transfers of personal data are necessary, they should take place within a framework taking data protection into account, e.g. on the basis of an international agreement stipulating adequate data protection requirements, including clear purpose limitation, adequate and non-excessive data collection, limited data retention time, information provision to data subjects, the assurance of data subject rights and independent supervision.

Data Protection and International Organisations

The conference calls upon:

- (a) international and supra-national bodies to formally commit themselves to abiding by principles that are compatible with the principal international instruments dealing with data protection and privacy;
- (b) international and supra-national bodies that hold or process personal data to establish appropriate mechanisms to ensure compliance with applicable data protection principles, such as the establishment of internal but operationally independent supervisory authorities with control powers;
- (c) international and supra-national bodies that have a role in promulgating standards, rules or common practices which affect personal data handling within the jurisdictions of their constituent members to develop and adopt suitable mechanisms to ensure that data protection considerations are effectively taken into account, such as the use of privacy impact assessments and consultation with recognised data protection authorities;

and requests the host of the 25th International Conference to draw this resolution to the attention of the relevant bodies.

Radio-Frequency Identification

The Conference highlights the need to consider data protection principles if RFID tags linked to personal information are to be introduced. All the basic principles of data protection and privacy law have to be observed when designing, implementing and using RFID technology. In particular

- a) any controller – before introducing RFID tags linked to personal information or leading to customer profiles – should first consider alternatives which achieve the same goal without collecting personal information or profiling customers;
- b) if the controller can show that personal data are indispensable, they must be collected in an open and transparent way ;
- c) personal data may only be used for the specific purpose for which they were first collected and only retained for as long as is necessary to achieve (or carry out) this purpose, and
- d) whenever RFID tags are in the possession of individuals, they should have the possibility to delete data and to disable or destroy the tags.

These principles should be taken into account when designing and using products with RFID.

Automatic Software Updates

1. The Conference notes with concern that software manufacturers worldwide increasingly use non-transparent techniques to transfer software updates to users' computers. In doing so they
 - can read and collect personal information stored on the user's computer (e.g. browser settings, and information on the user's browsing habits) without the user being able to notice, to influence or to prevent it,
 - may gain at least partial control over the target computer thereby restricting the ability of the user to meet his legal obligations and responsibilities as a controller to ensure the security of any personal data he may be processing,
 - change the software installed on the computer which will then be used without any required testing or clearance and
 - may bring about malfunctions in the updated computer without the possibility to identify the update as the cause.

This may cause particular problems in government institutions and private companies to the extent that they are under specific legal obligations how to process personal information.

1. The Conference therefore calls on software companies
 - a. to offer procedures to update software online only at the user's initiative or request, in a transparent way and without allowing unchecked access to the user's computer;
 - b. to ask for the disclosure of personal data only with the informed consent of the user and insofar as it is necessary to carry out the online update. Users should not be forced to identify (as opposed to authenticate) themselves before they can initiate the download process;
 - c. to provide for freedom of choice by offering online updates only as an alternative to other (offline) means of software distribution such as CD-ROM.
3. The conference encourages the development and implementation of techniques to update software which respect the privacy and autonomy of computer users.

Liaison with the UK Government

Staff of the then Lord Chancellor's Department ("LCD") hosted a meeting for the Data Protection authorities from Guernsey, Jersey and the Isle of Man ("the Islands") at the end of April 2003.

The main topic of discussion was the implementation of the European Directive on Privacy and Electronic Communications (2002/58/EC), for which a representative from the Department of Trade and Industry was present.

It was made clear that access to the telephone and fax preference service opt-out lists from the Islands was essential in order to ensure that unsolicited communications emanating from the Islands could be properly regulated.

Also discussed were the responses to the LCD Consultation Paper on Subject Access and progress by the European Commission with the adequacy assessments of the Islands' Data Protection régimes.

The staff from the LCD updated the Island authorities on other developments in the EU and in the Council of Europe. Mention was made of the possibility of a free-standing provision on Data Protection in discussions being undertaken on a revised treaty proposed under the Convention on the Future of Europe.

Following the reorganisation of government in the UK, the Lord Chancellor's Department was renamed the Department for Constitutional Affairs.

Responsibility for Freedom of Information, Data Protection and Data Sharing now rests with the Information Rights Division within the Constitution Directorate of that department.

The department has moved to the MWB Business Exchange in Greycoat Place, but the senior staffing is unchanged and continues to be an invaluable source of assistance on UK government policy and on European and international developments.

OBJECTIVES FOR 2004

Legislation

Completion of the drafting of regulations that implement the European Directive 2002/58/EC with the aim of commencing these regulations in the first half of the year.

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 Determination

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.

International Liaison

The Commissioner will liaise with the Jersey Registrar, the Isle of Man Supervisor and attend meetings with officials from the UK Department of Constitutional Affairs and with the British and Irish Commissioners as issues arise. Attendance at relevant UK and international conferences will continue as a means of maintaining 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 with the aim of assessing the feasibility of running 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.

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.

Government

Further advisory work will be undertaken, specifically as a consequence of the Commissioner's advisory role in relation to the States Digimap Management Board and the Commissioner's and Assistant Commissioner's participation in a number of other ad-hoc data sharing groups.

FINANCIAL REPORT

The Data Protection Office is funded by a grant from the Advisory and Finance Committee that 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 accounts for the Advisory and Finance Committee, have been as follows:

<u>INCOME</u>	2003	2002
	£	£
Data Protection Fees ¹	23,937	5,902
<u>EXPENDITURE</u>		
Rent	15,526	22,853
Salaries and Allowances	114,988	120,014
Travel and Subsistence ²	15,648	13,219
Furniture and Equipment ³	33,045	11,020
Publications	3,255	2,693
Post, Stationery, Telephone	5,295	3,919
Heat Light, Cleaning	5,366	4,015
TOTAL EXPENDITURE	£193,123	£177,733
EXCESS OF EXPENDITURE OVER INCOME	<u>£169,186</u>	<u>£171,831</u>

NOTES

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

The Income for 2003 includes accrued income which was received during 2002 of £12,644 from triennial registrations and renewals under the 1986 Law and [from August 2002] annual notifications under the 2001 law. The income for 2002 did not include any income accrued from previous years.

The cash received for 2003 was £26,285 representing the 751 annual notifications and renewals that were processed during 2003.

² This also includes an apportionment of the costs associated with the Data Protection Conference held in Guernsey of £3,740.

³ This includes one-off costs of £8,160 incurred in the upgrading of the Notification System to deal more effectively with renewals and a £13,600 recovery of the development costs of the notification system originally funded in 2002 directly from the Advisory and Finance Committee's unspent balances.

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.

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