OFFICE OF THE
Data Protection Supervisor
Oik Oaseir Coadey Fysseree Ellan Vannin

Annual Report
2012-2013

GD 0049/13

Laid before Tynwald
pursuant to section 48(1) of
the Data Protection Act 2002

CONTENTS

Foreword

This report covers the period from the 1st April 2012 to 31 March 2013.

On the international stage, the year has been dominated by the European Commission's proposal to replace the European Data Protection Directive 95/46/EC ('the Directive') with a General Data Protection Regulation, the United States Foreign Account Tax Compliance Act (FATCA) and the subsequent UK FATCA proposal.

The issues with regard to the proposed General Data Protection Regulation will continue for a considerable time and, given the significance to the Island, remain a priority. It is clear that the Island will be expected to introduce equivalent legislation if it is to maintain its "adequacy finding" which permits personal data to be transferred between the Island and the European Union, including the UK.

The global economy, and developments such as cloud computing, continues to present challenges to the effectiveness of data protection legislation and regulation. The Office will continue to work with other data protection authorities to protect personal data in a consistent manner.

In general, the Office continues to believe that the most effective way to protect personal data is to assist businesses and organisations to understand and comply with the data protection principles.

It is pleasing to report that most data controllers do seek to comply with the data protection principles and cooperate fully with the Office. Unfortunately, there is still a minority that appear to treat any enquiry, or assessment, with contempt. In such cases it becomes necessary to use enforcement powers and, during the year, two enforcement notices were issued.

One enforcement notice resulted in an Appeal to the Data Protection Tribunal but was subsequently withdrawn. When an Appeal is made, the burden of proof is upon the Supervisor and a considerable amount of time and effort went in to responding to that Appeal. In addition, legal costs in excess of £15,000 were incurred but these were subsequently recovered from the data controller.

The total number of assessments undertaken by the Office in 2012 was 28 with contraventions identified in 15 cases. The majority of complaints continue to concern the right of access to personal data. However, the number of contraventions has reduced and, hopefully, this trend will continue.

We continue to offer advice and training free of charge and I am pleased to report that during the year the demand for training was such that for several months all training days were fully booked. In cooperation with Government's Learning and Organisational Development Division, an awareness course for individual civil servants was also introduced.

The revised fees regulations appear to have had the desired effects. The intention was to reduce the number of register entries that lapsed. Previously approximately 13% of register entries lapsed and this has been reduced to less than 1.5%. It is expected that as data controllers become familiar with the new measures the number of lapsed entries will reduce further.

Finally, it would be remiss not to mention the contribution of staff. It has been a challenging year and these challenges could not have been met without the dedication and commitment of staff. I have every confidence that we will continue to work effectively in the next 12 months.

Iain McDonald
Data Protection Supervisor

RESPONSIBILITIES

DATA PROTECTION ACT 2002

The Data Protection Act 2002, came into operation on the 1st April 2003, and is based upon the UK's Data Protection Act 1998 and gives effect in the Island to Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The Office of the Data Protection Supervisor exists to protect and promote an individual's right to privacy with regard to the processing of their personal data by all businesses and organisations in the Island.

The Act applies to computerised records, structured manual records and health, education, social work and local authority housing records. The Act also modified the Access to Health Records and Reports Act 1993, to the extent that a living individual wishing to access their medical records does so via the provisions of the Data Protection Act.

The main functions of the Supervisor are set out in sections 47 to 49 of the Act and include:

- The promotion of good practice with regard to the requirements of the Act by data controllers
- Provision of advice and information regarding the obligations of data controllers
- Provision of advice and information regarding the rights of individuals
- Co-operation with other international data protection authorities

THE DATA PROTECTION PRINCIPLES

The Act sets out eight principles of good practice. In summary these are:

Personal data must be:

1. used fairly and lawfully;
2. used for specific and lawful purposes, in a manner that is compatible with those purposes;
3. adequate, relevant and not excessive;
4. accurate and where necessary kept up to date;
5. kept for no longer than necessary;
6. used in accordance with the rights of individuals under the Act;
7. kept secure to avoid unauthorised or unlawful use, accidental loss, or damage;
8. and not transferred to a third country without adequate protection

THE UNSOLICITED COMMUNICATIONS REGULATIONS 2005

The Office is also responsible for the enforcement of the Unsolicited Communications Regulations 2005 (the Regulations), which came into force in October 2005. These Regulations implement Article 13 of the Privacy and Electronic Communications Directive 2002/58/EC of the European Parliament and mirror some of the requirements of the UK Privacy and Electronic Communications (EC Directive) Regulations 2003.

These Regulations impose certain requirements upon organisations that utilise electronic means for direct marketing and provide individuals with rights to prevent or opt out of such marketing.

CURRENT LEGISLATION

The current list of legislation is shown below. Electronic copies together with case law and other relevant instruments and legislation are available from our web site at:
http://www.gov.im/odps/legislation/welcome.xml?menuid=52

DATA PROTECTION

Data Protection Act 2002

Subordinate Legislation
Data Protection (Corporate Finance Exemption) Order 2003 (SD 23/03)
Data Protection (Crown Appointments) Order 2003 (SD 24/03)
Data Protection (Designated Codes of Practice) Order 2003 (SD 25/03)
Data Protection (Fees) Regulations 2011 (SD 426/11)
Data Protection (Functions of Designated Authority) Order 2003 (SD 26/03)
Data Protection (Notification) Regulations 2003 (SD 16/03)
Data Protection (Processing of Sensitive Data) (Elected Representatives) Order 2003 (SD 28/03)
Data Protection (Subject Access Exemptions) (Adoption etc.) Order 2003 (SD 22/03)
Data Protection (Subject Access Modification) (Education) Order 2003 (SD 21/03)
Data Protection (Subject Access Modification) (Health) Order 2003 (SD 19/03)
Data Protection (Subject Access Modification) (Social Work) Order 2003 (SD 20/03)
Data Protection (Subject Access)(No. 2) Regulations 2003(SD 786/03)
Data Protection Act 2002 (Appointed Day) (No. 1) Order 2003 (SD 15/03)
Data Protection Act 2002 (Appointed Day) (No. 2) Order 2003(SD 701/03)
Data Protection Tribunal Rules 2003 (SD 27/03)

UNSOLICITED COMMUNICATIONS

Unsolicited Communications Regulations 2005
Unsolicited Communications Order 2005
Privacy and Electronic Communications Directive (2002/58/EC)

SIGNIFICANT ISSUES

CHANGES TO LEGISLATION

In the foreword, I mentioned that the year has been dominated by the European Commission's proposal to replace the European Data Protection Directive 95/46/EC ('the Directive') with a General Data Protection Regulation.

While considerable progress was made during the year, it seems unlikely that the Regulation will be agreed before the European Parliament dissolves in 2014. However, it is expected that the proposal will be agreed by 2015.

Once the Regulation is agreed it is inevitable that the Island will need to update its legislation accordingly if it is to maintain the "adequacy finding" from the European Commission which allows personal data to be transferred between the Island and Europe. At present, the draft Regulation proposes that new "adequacy findings" will be required within five years of the Regulation coming into force.

Proposed measures include:

- Data Controllers outside the EU, as well as those within the EU, who provide services to individuals resident in the EU must comply with the Regulation.
- Data processors, that is, third parties processing on behalf of a data controller, must also comply with certain provisions.
- Measures to ensure supervisory authorities are fully independent of Government with additional powers to investigate and audit all data controllers.
- Supervisory authorities to be able to impose fines up to €1 billion or up to 5% of turnover for serious breaches of the Regulation.
- Requirement to notify data breaches.
- A requirement for data controllers to undertake privacy impact assessments and to seek authorisation from the supervisory body prior to the commencement of processing.
- Data controllers must advise data subjects of data retention periods.
- Individuals may make a complaint to the supervisory authority in their home country even when a data controller outside the EU processes their data.

The Office has created a dedicated web page, to reflect developments with the proposed Regulation, which is updated regularly:

http://www.gov.im/odps/businessadvice/businessadvice1/future.xml

DATA LOSSES

When a loss does occur, it is important that a data controller takes immediate steps to protect individuals from any further damage or distress. In most cases, the data controller should inform the individual that the loss has occurred. There are four key steps to take when a data loss or breach occurs:

- **Containment and recovery** – the response to the incident should include a recovery plan and, where necessary, procedures for damage limitation.
- **Assessing the risks** – you should assess any risks associated with the breach, as these are likely to affect what you do once the breach has been contained. In particular, you should assess the potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to happen.
- **Notification of breaches** – informing people about an information security breach can be an important part of managing the incident, but it is not an end in itself. You should be clear about who needs to be notified and why. You should, for example, consider notifying the individuals concerned; other regulatory bodies; other third parties such as the police and the banks; or the media.
- **Evaluation and response** – it is important that you investigate the causes of the breach and also evaluate the effectiveness of your response to it. If necessary, you should then update your policies and procedures accordingly.

The Office has produced a guidance on managing a security breach which can be found at : http://www.gov.im/odps/businessAdvice/businessAdvice4/seventhprinciple.xml

CLOUD COMPUTING

Cloud computing presents many opportunities to data controllers to reduce costs and manage its computing resources and data. However, it also presents a number of risks and it is important that these risks are fully considered and properly managed. The Office has produced a guide to Cloud Computing which can be found at:

http://www.gov.im/odps/businessAdvice/businessAdvice4/seventhprinciple.xml

The UK Information Commissioner has also produced a detailed guide, which can be found at:

http://www.ico.org.uk/for_organisations/data_protection/topic_guides/online/cloud_computing.aspx

SURVEILLANCE SYSTEMS

The installation of surveillance systems, including CCTV cameras and Automatic Number Plate Recognition cameras (ANPR) is a constant source of complaint to the Office. As the cost of such systems reduces, and the ease of installation increases, we are receiving more and more complaints.

Complaints have included installations in public areas, such as civic amenity sites, and on lamp-posts, and in private houses and in vehicles. Other complaints include cases where there is no signage to indicate the data controller responsible for the system.

Surveillance systems do have a function in detecting crime but other solutions, such as improved lighting, may provide a better and cheaper solution. There is also the capacity for "function creep" in the use of these systems. The privacy concerns are such that the proposed European Regulation includes specific provisions for surveillance systems and requires public installations to be subject to privacy impact assessments.

The Office has published guidance, "Surveillance camera systems - complying with the Data Protection Act", which can be obtained from our document library at:

http://www.gov.im/odps/businessAdvice/businessAdvice1/tribunal.xml

The UK Information Commissioner also publishes a CCTV code of practice that can be found at:

http://www.ico.org.uk/for_organisations/data_protection/topic_guides/cctv.aspx

Surveillance Cameras on Public Transport

The main issue dealt with in relation to surveillance systems during the year was the use of surveillance cameras installed on the interior and, in particular, the exterior of buses operated by the Department of Community Culture and Leisure (DCCL).

Contrary to claims made elsewhere the issues were not a matter of interpretation but ones of fact.

The facts are:

1. There is no legal requirement for buses to have cameras installed and new buses do not come fitted with cameras as standard. Many operators do not have external cameras while others have a forward facing camera only. Indeed Transport for London, for example, only requires bus operators to have a forward facing camera.

2. In the case of buses ordered by the DCCL, cameras are installed to a specification originally created for the Department of Transport in January 2010. In addition to internal cameras, the specification has cameras mounted to obtain external images from the front, rear and both sides of the bus.

3. No thought had been given by the DCCL to the distance over which images should be obtained. Each external camera has a wide field of view and obtained, and recorded, good quality images over considerable distances.

4. The general public had not been informed that external surveillance cameras had been installed or what these cameras recorded. However, the police had been informed and regularly sought access to the images obtained.

5. Most buses, but not all, have internal cameras and signage advising passengers accordingly.

There were, therefore, clear contraventions of the first data protection principle with regard to fair processing and the third data protection principle with regard to excessive processing.

After protracted correspondence, an Enforcement Notice was issued in November 2012 requiring:
"

1. *(a) Ensure that appropriately sized and worded fair processing notices have been placed in a prominent position on the interior of all buses where interior surveillance systems are in use.*

(b) These notices must be clearly visible to passengers and must be able to be easily read by such persons.

2. *(a) Ensure that appropriately sized and worded fair processing notices have been placed in a prominent position on the exterior of all buses where exterior surveillance systems are in use.*

(b) These notices must be clearly visible to pedestrians and persons in other vehicles and must be able to be easily read by such persons.

(c) The external fair processing notices must clearly advise data subjects that images of members of the public outside the vehicle are being processed

3. *Ensure that further information is made available to data subjects to enable processing in respect of them to be fair, for example by making the information, including sample images, available by other means such as via the website.*

4. *Confirm the field of view of the forward facing and side view cameras, i.e. the extent and distance to which these will obtain personal data, and provide a date by which the data controller will have tested, adjusted and confirmed that all externally mounted cameras only record images to this specified field of view. This date must be no later than three months from the date of this Notice.* "

DCCL appealed the Enforcement Notice to the Data Protection Tribunal.

This would have been the first time the Tribunal had been required, but DCCL withdrew its appeal before the Tribunal sat.

In withdrawing the appeal against the issue of the Enforcement Notice, DCCL committed to the installation of fair processing notices, drafted specifications for the field of view for the cameras and introduced new retention periods for the images. Minor changes were made to the Enforcement Notice with regard to the date for compliance and an amended Enforcement Notice was issued. The content of both Enforcement Notices is available on the website.

Unfortunately, this matter took over 8 months to resolve and, taking into account the basic nature of the compliance issue, a disproportionate amount of time was expended and unnecessary, significant

expenditure of public money incurred. DCCL has reimbursed £15,335 which was most of this Office's legal costs.

It was also claimed that with regard to the use of such surveillance systems the UK Information Commissioner holds a different view to the Supervisor. While the Supervisor cannot speak for the UK Information Commissioner, he can advise that this matter has been discussed with UK Information Commissioner and other Commissioners and staff on several occasions and the UK Information Commissioner's Office is currently reviewing the use of CCTV on Public Transport.

KNOW YOUR CUSTOMER FILES IN SKIP

One of the more bizarre issues during the year was the discovery of thousands of customer files in a skip in a lay-by on Belmont Terrace. The files, which belonged to a financial services company, contained significant personal data of previous customers including copies of passports, bank account details, etc. It was obvious that the files had been lying in the skip overnight.

However, having been contacted by the Supervisor, the company acted responsibly and without hesitation to ensure the files were quickly secured and arranged for the files to be removed and properly destroyed via incineration on the same day.

The issue arose due to a failure to appreciate the importance of the content of the files. However, the exemplary manner in which the company responded to the issue mitigated the risk and there was no need to use enforcement powers.

FREEDOM OF INFORMATION

Many individuals and organisations contact the Office on the assumption that the Office has responsibility either for Freedom of Information or the current Code of Practice on Access to Government Information.

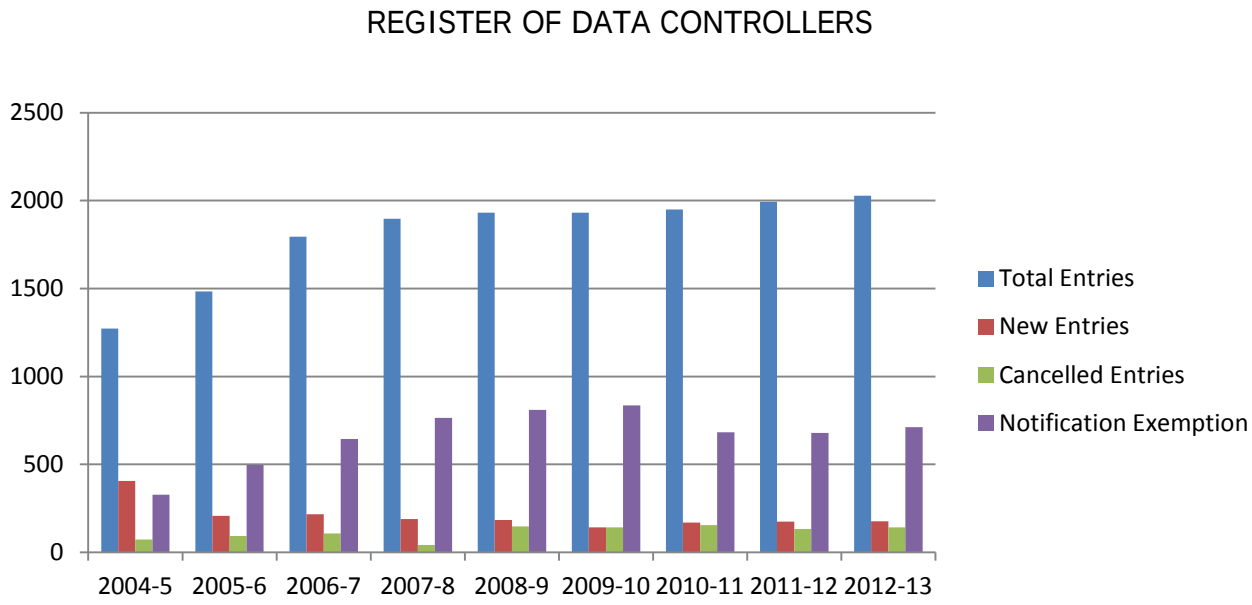
While this assumption is understandable, the Office does not have any responsibility for FOI or the Code of Practice.

REGISTER OF DATA CONTROLLERS

The Supervisor is responsible for the maintenance and administration of the Register of Data Controllers. In the year 2012-2013, 176 new entries were made in the register while 141 entries were cancelled, representing a small increase of 35 in the total number of register entries. The current list of data controllers is available on our web site at:
http://www.gov.im/odps/datacontrollersregister.xml

The following table and chart shows the growth in the Register since 2004:

Year	Total Entries	New Entries	Cancelled	Net Increase	Notification Exemption
2004-5	1273	406	72	334	327
2005-6	1483	207	93	114	496
2006-7	1795	217	107	110	645
2007-8	1896	189	41	148	765
2008-9	1932	184	148	36	810
2009-10	1932	141	141	0	836
2010-11	1950	169	155	14	682
2011-12	1993	175	132	43	678
2012-13	2028	176	141	35	711



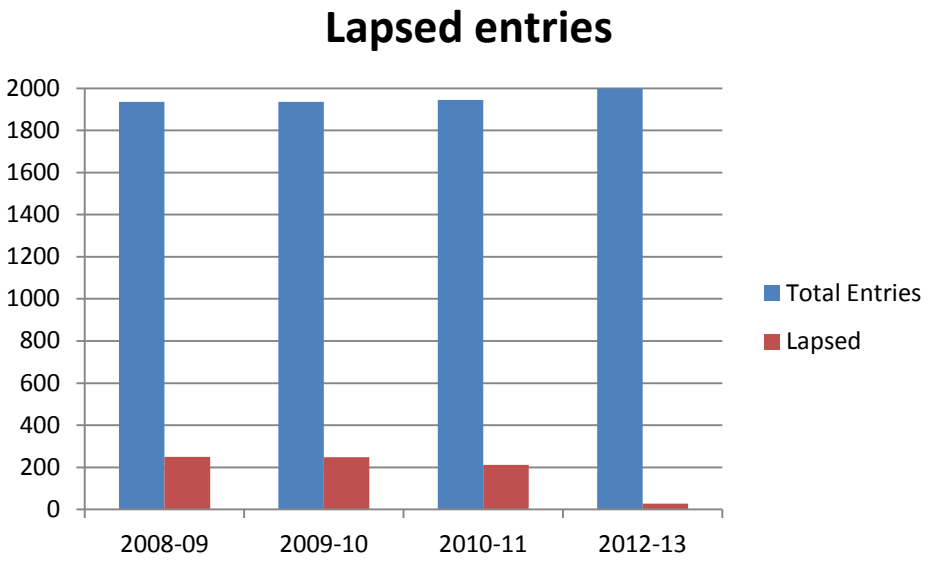
The growth in the number of register entries broadly reflects economic activity and it is therefore pleasing to see some continued modest growth in the register.

It is our view that the Register is more or less complete, that is, most data controllers now have a register entry. However, my Office will continue to proactively target specific business groups to ensure they are registered and aware of their obligations.

The register entry is renewable annually and, to assist data controllers comply with their registration obligations, renewal letters are sent out six weeks prior to the renewal date, with further reminders sent by email as the expiry date approaches. Renewal letters no longer include a copy of the current register entry as data controllers should have retained the copy provided on completion of the previous year's renewal process.

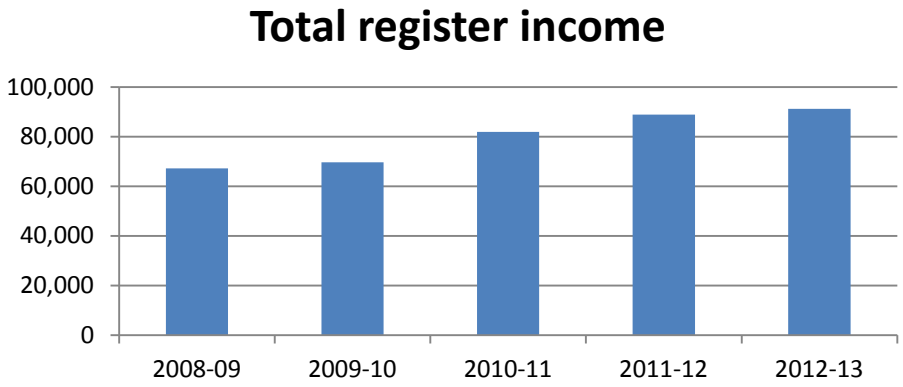
The new fees regulations introduced in October 2011 appear to have been effective in reducing the number of lapsed register entries.

The chart below shows that in the three years prior to the introduction of the new regulations, approximately 13% of all register entries lapsed. Whilst it will take two years for this approach to take full effect, results show that the number of lapsed entries has significantly reduced by 90% to less than 1.5% of all entries. In addition, most entries that do lapse apply for a new entry within a few days.



INCOME FROM REGISTRATION

In 2012-2013, income from registration totalled £91,120, an increase of almost £3,500 on the previous year. The chart below shows the increase in fee income over the past five years.

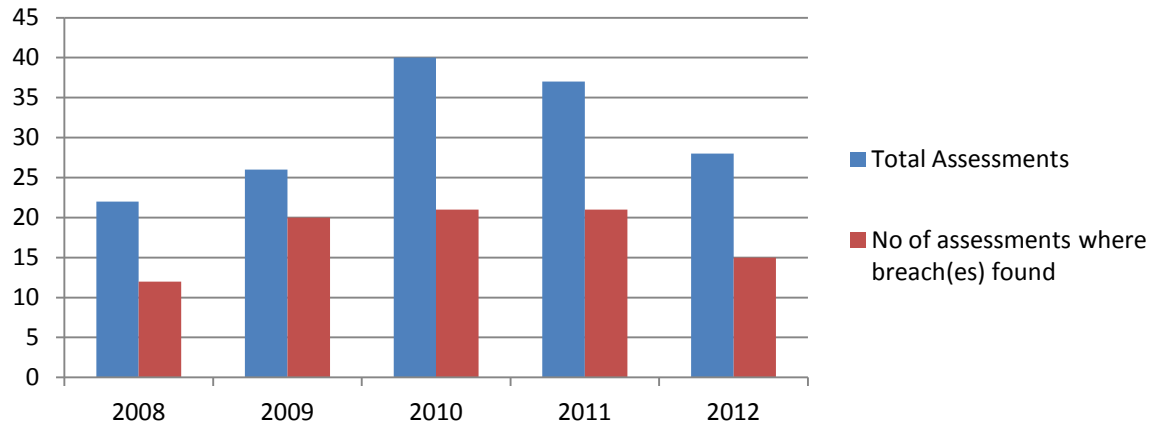


ASSESSMENTS

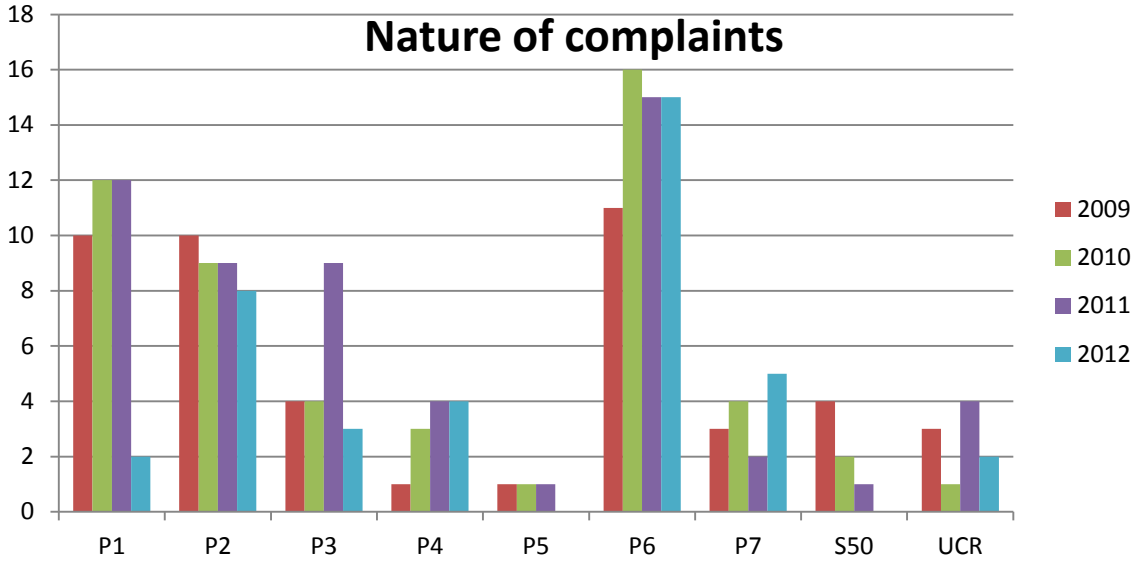
When an individual makes a formal complaint, a request for assessment under section 38 of the Act, my Office is required to form a view as to whether the processing of personal data is likely, or unlikely, to be in compliance with the provisions of the Act or in accordance with the Regulations.

However, I am pleased to report that due to the nature of the existing relationship this Office enjoys with the business community most complaints continue to be resolved quickly and amicably without the need to resort to the formal process.

During 2012, the number of formal requests for assessment totalled 28 and breaches were identified in 15 cases. The following chart shows the number of requests made and breaches identified in each of the past five years:



The following chart shows the trend in complaints over the past four years and identifies the nature of a complaint in terms of the data protection principles, an offence under section 50 of the Act or the Unsolicited Communication Regulations.



The majority of complaints continue to concern whether or not a data controller has complied with the individual right of access to personal data. In terms of the data protection principles, this is a question of compliance with the sixth data protection principle (P6).

However, whilst breaches were identified in 54% of all assessments, I am pleased to be able to report that breaches were identified in only 33% of complaints concerning the right of access.

Although assessments were completed, on average, within 30 days of opening, disappointingly, the longest assessment took 241 days to complete.

The following table indicates that overall performance has remained consistent with previous years:

	2008	2009	2010	2011	2012
Av. Days to complete	35	33	34	33	30
Maximum time to complete	99	91	146	166	241

Despite the frustrations mentioned in the foreword, the Office continues to believe that enforcement notices should only be used as a last resort when a data controller's actions indicate that there is little or no intention to comply with the provisions of the Act.

The Office has had cause to issue 2 Enforcement Notices in the past year.

However, an alternative to enforcement is that of an undertaking, which is not a formal regulatory power but a form of action used to bring about compliance with the Act and related laws. The Office required 3 data controllers to provide undertakings in lieu of enforcement.

Undertakings and enforcement notices are published on our website at:
http://www.gov.im/odps/businessadvice/businessadvice5/complaintstoregistrar.xml

RAISING AWARENESS

TRAINING

One of the most satisfying aspects to the year has been the attitude of businesses who have demonstrated a continuing commitment to understanding their obligations and achieving compliance with the provisions of the Act. The Office continues to offer and provide free training and advice to all organisations, regardless of whether they are in the public or private sector, or run by individuals for the benefit of the population, such as sports clubs and charities.

In 2012, 22 training sessions were provided, with the number of attendees totalling over 330. Private sector organisations accounted for 8 of these sessions, with 122 staff attending.

The Office also continues to provide presentations to a number of professional bodies and seminars upon request, and presentations were made at 5 events at the invitation of the host.

ADVICE

The Office regularly provides advice to individuals regarding their rights and to organisations regarding their obligations under the Act or Regulations.

All guidance we produce is made available on our website to assist both organisations and individuals in their understanding of, and compliance with, the Act or Regulations. New guidance is introduced as necessary, with existing guidance being regularly reviewed and amended to reflect current views, or technology changes.

We also update via the RSS news feed, for example, any developments in the proposed European Regulations are reported via the RSS news feed to alert subscribers.

OFFICE OF THE DATA PROTECTION SUPERVISOR

STAFF

The Office is maintained by a staff of 4 people:

Job Title		Actual FTE	Grade Analogy
Data Protection Supervisor	Full time	1.0	OS7
Deputy Data Protection Supervisor	Full time	1.0	HEO
Office Manager	Part time	0.5	EO
Compliance Officer	Full time	0.8	AO

The Office with an actual FTE of 3.3 continues to operate inside its authorised total of 3.5.

For comparison, in 2003, the authorised total number of staff was 6 with a full time equivalent (FTE) of 5.5.

It is now 7 years since there has been any change in personnel. This stability is important and has allowed staff to develop extensive knowledge of data protection legislation and issues. We regularly receive comments and compliments from both individuals and businesses on the quality of advice and assistance provided.

INTERNATIONAL COOPERATION

The Office continues to enjoy close working relationships with its international colleagues. In particular, the Office regularly works with and assists its counterparts in the Channel Islands and the UK. During the year, the Office attended an annual Crown Dependencies update meeting at the Ministry of Justice, but due to other commitments, did not attend either the International or European Conferences.

In July 2012, the Islands Data Protection Authorities meeting was hosted in the Isle of Man. This was attended by data protection authorities from Bermuda, Channel Islands, Cyprus, Gibraltar, Ireland, and United Kingdom. The main topic of discussion was the proposed changes to Data Protection legislation in Europe. The Hon. Steven Rodan, Speaker of the House of Keys, provided a Tour of Tynwald during the lunch break.

FINANCIAL REPORT

The figures for the financial years 2012-2013 and budget for 2013 -2014 are as follows:

	2012 - 2013			2013-2014
	Budget	Actual		Budget
Income	(£'s)	(£'s)		(£'s)
New notification fees	4,000	12,320		4,000
Renewal fees	64,000	78,800		64,000
Other income		18		
Total Income	68,000	91,138		68,000
Revenue Expenditure				
Employee Costs	164,506	158,681		163,794
Infrastructure Expenses	8,180	0		0
Supplies and Services	44,314	21,909		53,206
Total Expenditure	217,000	180590		217,000
Net Figure	149,000	89452		149,000

For comparison, the bottom line budget and actual expenditure figures for the previous four financial years are shown below:

	Vote	Actual
2008-09	259,904	216,470
2009-10	266,075	216,141
2010-11	255,327	199,179
2011-12	217,000	174,482

I am pleased to report that this Office continues to operate well within its allocated expenditure budget but also continues to exceed its income target.

As part of the Office's commitment to openness and transparency, details of the income and revenue expenditure, broken down into categories, is now published on the website on a quarterly basis. This information can be found in the "About us" section at http://www.gov.im/odps/about_us/

FUTURE OBJECTIVES

Our future policy will continue to revolve around the belief that the most effective way to protect an individual's rights is to actively assist businesses and organisations to understand and comply with the law.

Our priority over the next year will be to keep fully abreast of all developments regarding the modernisation of the Council of Europe Convention 108 and the proposed European General Data Protection Regulation, understand the potential effect upon the Island and advise Isle of Man Government and Businesses accordingly.