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

# Annual Report
# 2013-2014

**GD 2015/0003**

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

# CONTENTS

**FOREWORD** ..... **2**

**RESPONSIBILITIES** ..... **3**

DATA PROTECTION ACT 2002 ..... 3
THE DATA PROTECTION PRINCIPLES ..... 3
THE UNSOLICITED COMMUNICATIONS REGULATIONS 2005 ..... 3

**SIGNIFICANT ISSUES** ..... **5**

CHANGES TO LEGISLATION ..... 5
DATA SHARING ..... 6
SURVEILLANCE SYSTEMS ..... 6
SOCIAL MEDIA ..... 7
PRIVACY IMPACT ASSESSMENTS ..... 7
DATA LOSSES ..... 8
FREEDOM OF INFORMATION ..... 8

**REGISTER OF DATA CONTROLLERS** ..... **9**

INCOME FROM REGISTRATION ..... 11

**ASSESSMENTS** ..... **11**

**RAISING AWARENESS** ..... **13**

**OFFICE OF THE DATA PROTECTION SUPERVISOR** ..... **14**

STAFF ..... 14

**FINANCIAL REPORT** ..... **15**

**FUTURE OBJECTIVES** ..... **16**

# Foreword

This report covers the period from the 1st April 2013 to 31 March 2014.

Internationally the year was dominated by two issues: the proposal to replace the European Data Protection Directive 95/46/EC ('the Directive') with a General Data Protection Regulation and revelations made by Edward Snowden revealing the extent to which personal data was being intercepted by US and UK security services.

At one stage it seemed that the proposed Regulation had stalled, but the Snowden Revelations provided a new impetus. It now looks increasingly likely that the Regulation will be agreed in the autumn of 2015.

The Snowden revelations have made many appreciate that the risks involved are real and resulted in public trust and confidence in the ability of businesses and government to look after personal data being significantly damaged. Effective and consistent regulation will be vital in rebuilding public confidence in both the private and public sectors. New legislation, such as the proposed Regulation, is likely to require additional safeguards when data is transferred or held outside the European Union.

Data protection is now an essential component of the economy and it is vital that the Island maintains its "adequacy finding" from the European Union. Indeed the "adequacy finding" provides an opportunity for potential growth in E-business as business look to relocate data centres that serve EU residents. It is likely that legislation creating provisions equivalent to those of the Regulation will be required in the next few years if the Island is to retain it "adequacy finding."

The Office continues to work closely with other data protection authorities, in particular the UK, Ireland, Channel Islands and Gibraltar. During the year the Office applied and was accepted for membership of the Global Privacy Enforcement Network (GPEN). GPEN was originally established with support from the OECD and consists mainly of data protection or privacy agencies with enforcement powers in their respective jurisdictions. GPEN facilitates enforcement co-operation between members including collaborative working and also provides a forum for discussion on various privacy issues. Such networks will become increasingly important as data protection legislation moves towards consistent international standards.

Upholding information rights involves more than enforcement. 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. A significant part of our work continues to be the provision of advice and training which is intended to assist the development of products and services in a manner that respects privacy rights.

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 2012, the European Commission proposed replacing the current European Data Protection Directive 95/46/EC ('the Directive') with a General Data Protection Regulation. The European Parliament and the European Council of Ministers have now produced their versions. The next stage is for the parties to discuss and agree a final version. At present it is anticipated that agreement will be reached in the autumn of 2015 with the Regulation coming into operation in early 2016.

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.
- Will apply to data processors, that is, third parties processing on behalf of a data controller.
- Supervisory authorities to be fully independent of Government with powers to audit all data controllers.
- Supervisory authorities to have powers 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.

It is likely that the Island will be required 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.

A web page, reflecting developments, can be found at :
http://www.gov.im/odps/businessadvice/businessadvice1/future.xml

## DATA SHARING

The Supervisor regularly receives comments or hears claims that something could not be done as the Data Protection Act prevented the sharing of data.

To be clear, if it is lawful to share data then the Data Protection Act does not prevent that data sharing from occurring. The Supervisor is aware of instances where there was no statutory power to share data but is not aware of any case where the provisions of the Data Protection Act have prevented any data from being lawfully shared when it was necessary and justified to do so.

Sadly, the Data Protection Act continues to be used by others as an excuse for their own failings.

The Supervisor recommends that anyone seeking to share data should follow the Code of Practice published by the UK Information Commissioner which can be found at:

https://ico.org.uk/for-organisations/guide-to-data-protection/data-sharing/

The code of practice provides practical advice to all organisations, whether public, private or third sector, that share personal data and covers systematic data sharing arrangements as well as ad hoc or one off requests to share personal data.
Adopting the good practice recommendations in the code will help organisations to collect and share personal data in a way that complies with the law, is fair, transparent and in line with the rights and expectations of the people whose data is being shared.

## SURVEILLANCE SYSTEMS

The installation of surveillance systems continues to be a regular source of complaint and concern.

Increasingly systems are being installed on domestic properties and some have led to disputes between neighbours.

Complaints include body worn cameras used, for example by door security, and include audio recordings and there have also been complaints about images from CCTV systems that have been uploaded onto social media.

Complaints are also being received about other forms of surveillance in particular the tracking of employees via GPS technology either in vehicle or by mobile phone.

These systems must comply with the Data Protection Act and in the case of use by public authorities the European Convention of Human Rights. The Office has published guidance, "Surveillance camera systems - complying with the Data Protection Act", which can be found at:
http://www.gov.im/odps/businessAdvice/businessAdvice1/tribunal.xml

The UK Information Commissioner has recently updated its guidance to include other forms of surveillance. The revised code of practice can be found at:

https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

In addition any data controller who proposes to use such systems to monitor staff must consider the employment codes of practice:

https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

One simple question asked in the employment practices code is:

*"Can established or new methods of supervision, effective training and/or clear communication from managers, rather than electronic or other systemic monitoring, deliver acceptable results?*

## SOCIAL MEDIA

Social media has become a source of complaint.

The most common complaint is from employees who have been subject to disciplinary action as a result of a comment made on, or information obtained from, social media. Typical examples include adverse comments about the employer or information showing that an employee who was absent from work due to illness taking part in some activity.

Social media is not private and an employer is not contravening the Data Protection Act by acting on information obtained from social media.

During the year, the Supervisor visited Facebook's headquarters in Dublin. It was reassuring to learn of the significant measures Facebook has taken to protect privacy in co-operation with the Irish Data Protection Commissioners' Office.

## PRIVACY IMPACT ASSESSMENTS

Privacy impact assessments have proved a useful tool to help organisations which process personal data to properly consider and address the privacy risks that the proposed processing may entails.

The proposed European Data Protection Regulation may require public sector bodies to undertake such assessments while, in the UK, the Ministry of Justice now requires UK Government Departments to do so.

To assist organisations the UK Information Commissioner has published a code of practice for undertaking such Privacy Impact Assessments, which can be found at:

https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

The Supervisor recommends that data controllers, particularly in the public sector, follow the above code of practice.

## 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

## FREEDOM OF INFORMATION

The Freedom Of Information Bill (FOI) proposes that the Supervisor will become the Information Commissioner and, in addition to his duties and responsibilities under the Data Protection Act 2002 and Unsolicited Communications Regulations 2005, assume responsibility for FOI oversight.

It is also anticipated that responsibility for oversight of the Code of Practice on Access to Government Information will pass to the Supervisor.

The impact of this proposal has been considered and a business case prepared for Government. The Office possesses a good understanding of the operation of FOI in the UK and the Supervisor believes that during the initial commencement phases these additional responsibilities can be managed with the addition of one member of staff. When the initial phases have been completed this will be reviewed.

As the responsibilities are demand led this will be reviewed after two years.

At present, it is expected that the Freedom of Information Act will come into operation, in part, in early 2016.

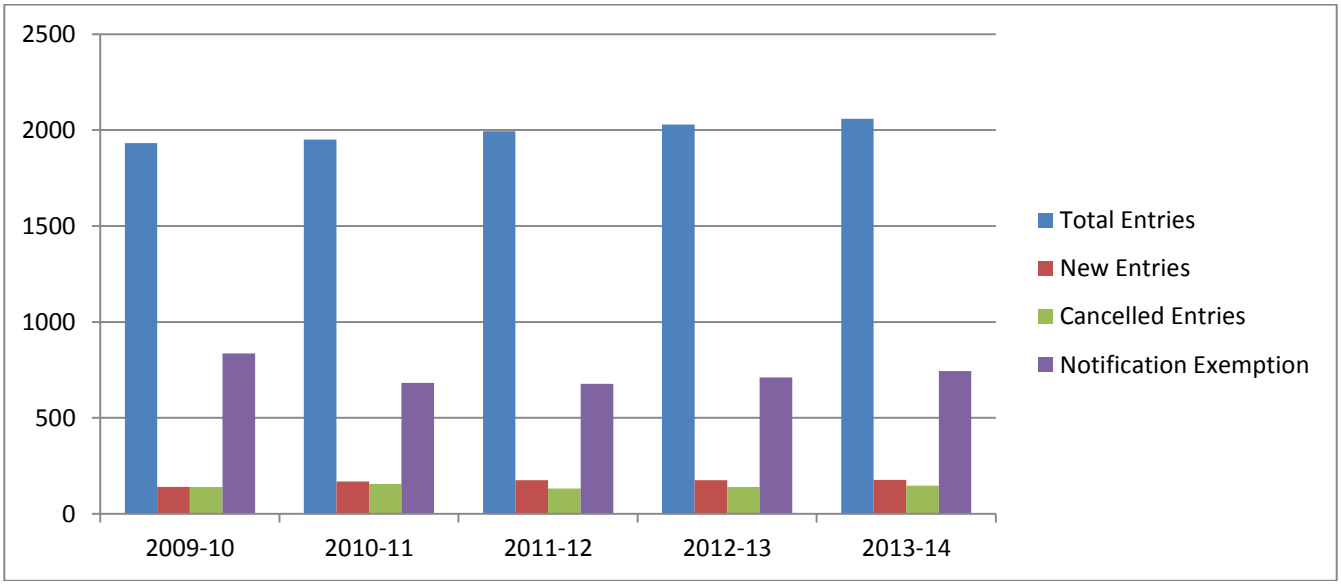
# REGISTER OF DATA CONTROLLERS

The Supervisor is responsible for the maintenance and administration of the Register of Data Controllers. In the year 2013-2014, 178 new entries were made in the register while 148 entries were cancelled, representing a small increase of 30 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:

| | Total Entries | New Entries | Cancelled Entries | Notification Exemption |
|---|---|---|---|---|
| 2004-5 | 1273 | 406 | 72 | 327 |
| 2005-6 | 1483 | 207 | 93 | 496 |
| 2006-7 | 1795 | 217 | 107 | 645 |
| 2007-8 | 1896 | 189 | 41 | 765 |
| 2008-9 | 1932 | 184 | 148 | 810 |
| 2009-10 | 1932 | 141 | 141 | 836 |
| 2010-11 | 1950 | 169 | 155 | 682 |
| 2011-12 | 1993 | 175 | 132 | 678 |
| 2012-13 | 2028 | 176 | 141 | 711 |
| 2013-14 | 2058 | 178 | 148 | 744 |

REGISTER OF DATA CONTROLLERS

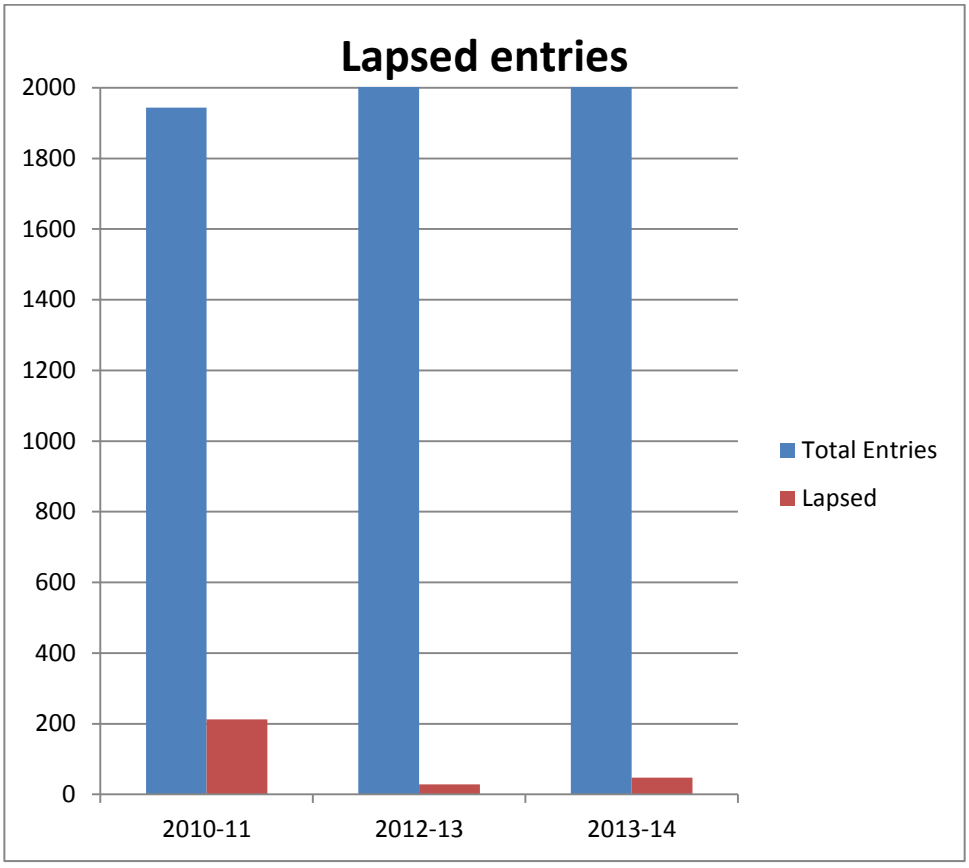



The growth in the number of register entries broadly reflects economic activity and it is therefore pleasing to see some continued modest growth in the register.

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.

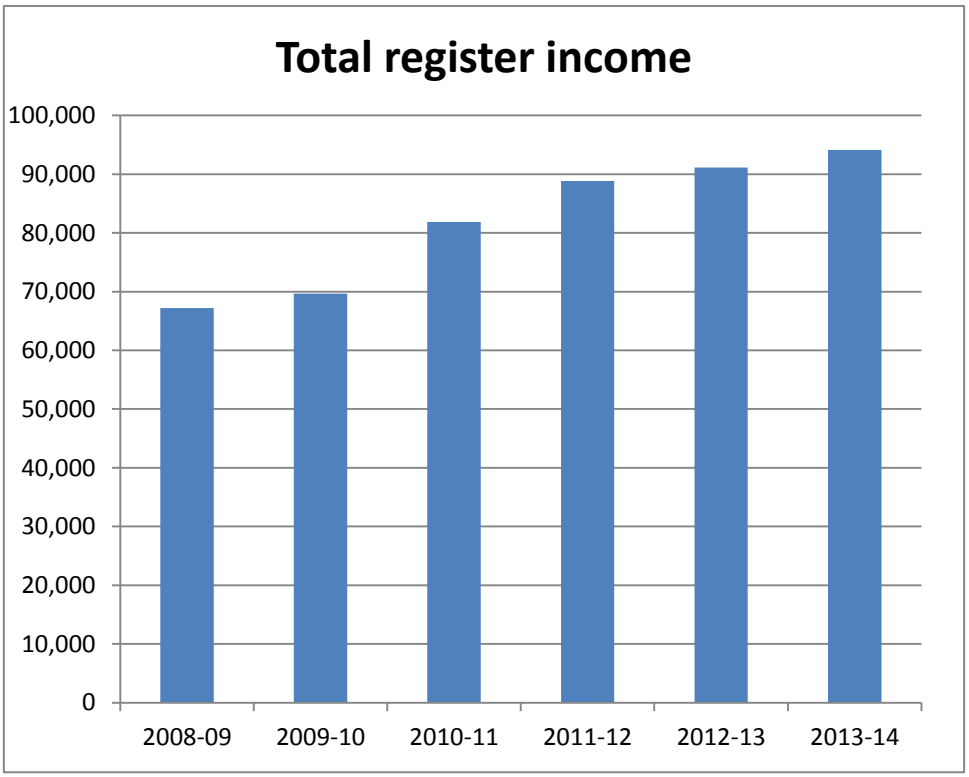
The register entry is renewable annually and, to assist data controllers comply with their registration obligations, renewal letters are sent out six weeks prior to the renewal date, with further reminders sent by email as the expiry date approaches. Renewal letters no longer include a copy of the current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

The fees regulations introduced in October 2011 have been effective in reducing the number of lapsed register entries and thereby reduced costs and overheads. Prior to introduction, approximately 13% of all register entries lapsed number has reduced to less than 1.5% .



## INCOME FROM REGISTRATION

In 2013-2014, income from registration totalled £94,109, an increase of approximately £3,000 on the previous year. The chart below shows the increase in fee income over the past six years.

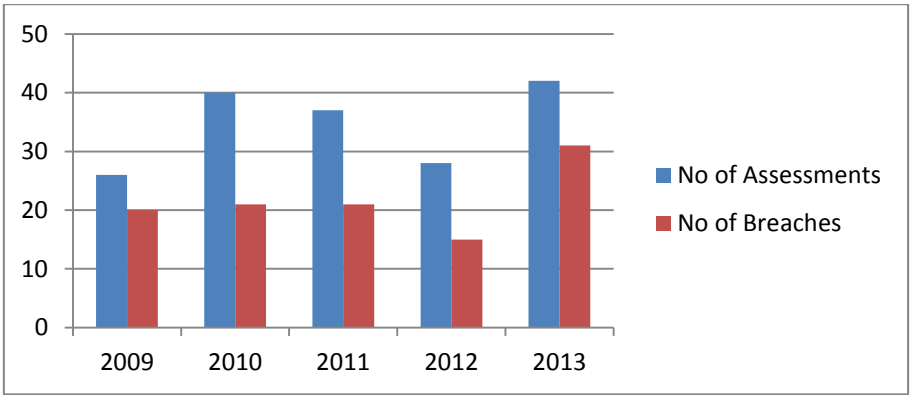



## ASSESSMENTS

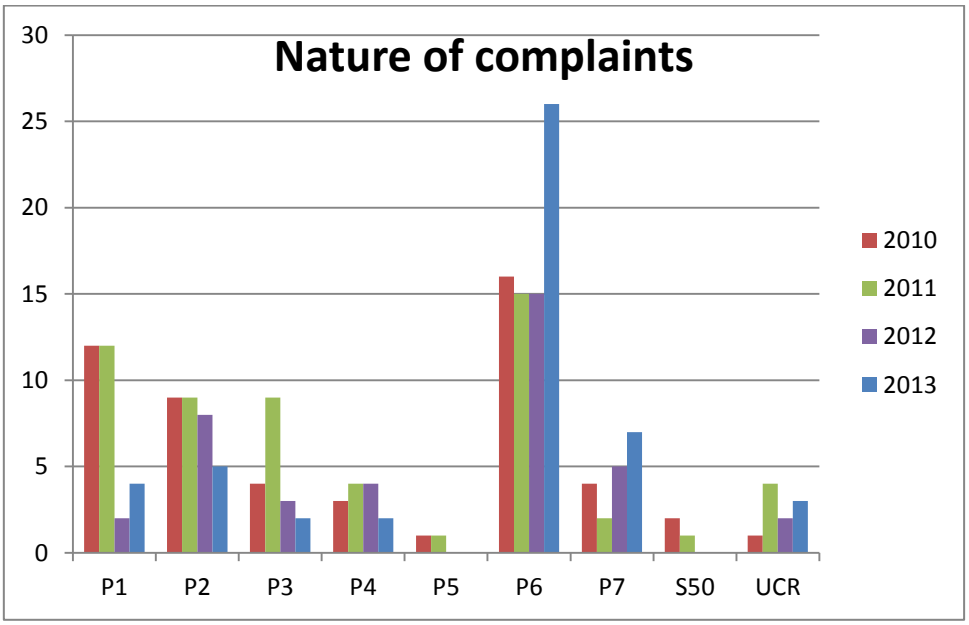
When an individual makes a formal complaint, a request for assessment under section 38 of the Act, my Office is required to form a view as to whether the processing of personal data is likely, or unlikely, to be in compliance with the provisions of the Act or in accordance with the Regulations.

Most complaints involving the private sector, continue to be resolved quickly and amicably without the need to resort to the formal process.

During 2013, the number of formal requests for assessment totalled 42 and breaches were identified in 31 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, a subject access request or SAR. In terms of the data protection principles, this is a question of compliance with the sixth data protection principle (P6).

Breaches were identified in 74% of all assessments. With regard to compliance with an SAR, breaches were identified in only 42% of cases

On average assessments were completed, within 44 days of opening which is an increase of 14 days over previous years. The additional time reflects the complexity of complaints. The longest assessment took 207 days to complete.

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

| | **2008** | **2009** | **2010** | **2011** | **2012** | **2013** |
|---|---|---|---|---|---|---|
| **Av. Days to complete** | 35 | 33 | 34 | 33 | 30 | 44 |
| Maximum time to complete | 99 | 91 | 146 | 166 | 241 | 207 |

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. It was not necessary to issue an Enforcement Notice or Undertaking in the past year.

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

# RAISING AWARENESS

## TRAINING

Businesses 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 2013, 28 training sessions were provided, with the number of attendees totalling over 380. Private sector organisations accounted for 12 of these sessions, with 200 staff attending.

The Office also continues to provide presentations to a number of professional bodies and seminars upon request, and presentations were made at 11 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 8 years since there has been any change in personnel. This stability has helped staff gain detailed knowledge of data protection legislation and issues which will be important as the Office takes on additional responsibility for Freedom of Information.

## INTERNATIONAL COOPERATION

The Office continues to enjoy close working relationships with its international colleagues. In particular, the Office works closely with colleagues form the UK, Ireland Channel Islands and Gibraltar who hosted the annual Island Data Protection Authorities meeting

# FINANCIAL REPORT

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

| | 2013 - 2014 | | | 2014-2015 |
|---|---|---|---|---|
| | Budget | Actual | | Budget |
| **Income** | (£'s) | (£'s) | | (£'s) |
| New notification fees | 4,000 | 12,460 | | 4,000 |
| Renewal fees | 64,000 | 81,649 | | 64,000 |
| Other income | | 15,369 | | |
| **Total Income** | 68,000 | 109,478 | | 68,000 |
| | | | | |
| **Revenue Expenditure** | | | | |
| Employee Costs | 172,614 | 159,436 | | 182,760 |
| Infrastructure Expenses | 0 | 0 | | 0 |
| Supplies and Services | 44,386 | 14,572 | | 34,240 |
| **Total Expenditure** | 217,000 | 174,008 | | 217,000 |
| **Net Figure** | 149,000 | 64,530 | | 149,000 |

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

| Year | Vote | Actual |
|---|---|---|
| 2008-09 | 259,904 | 216,470 |
| 2009-10 | 266,075 | 216,141 |
| 2010-11 | 255,327 | 199,179 |
| 2011-12 | 217,000 | 174,483 |
| 2012-13 | 217,000 | 180,590 |

With a net cost figure of £64,530 compared to its target figure of £149,000, the Office continues to operate well within its allocated expenditure budget and 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 the developments regarding the modernisation of the Council of Europe Convention 108 and the European General Data Protection Regulation.