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

Annual Report

2014-2015

GD 2016/0011

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

This page is blank

CONTENTS

Foreword

This report covers the period from the 1st April 2014 to 31 March 2015.

With regard to legislation, the year continued to be dominated by the proposal to replace the European Data Protection Directive 95/46/EC ('the Directive') with a General Data Protection Regulation. Discussions have now entered the "trilogue" phase, when the European Commission, European Parliament and the European Council of Ministers collectively debate and agree its content. It is anticipated that agreement will be reached by the end of 2015 and the regulation should be finalised and complete its passage through the European Parliament by June 2016.

It has been confirmed that the Regulation will be extraterritorial in scope and apply to businesses outside the EU that provides goods or services to EU residents. This means that all Island businesses that have customers in an EU Member state, or process personal data on behalf of an EU business, or obtain personal data from an EU Business will have to be fully compliant with the Regulation when it comes into full force in 2018. There will be significant fines and penalties for failing to comply.

The Island's "adequacy finding" has been in place since 2004 and has been important to the Island's economy as it permits EU based businesses to transfer personal data to and from the Island. If this finding did not exist then those businesses would incur additional costs and may decide not to do business in the Island. The fines and obligations in the new Regulation will inevitably result in EU businesses carefully considering where they transfer personal data to. If the Island is to retain its "adequacy finding" then it will have to introduce equivalent legislation; indeed if the Island wants to seek growth and employment in E-business then maintaining the "adequacy finding" will be essential.

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 became a member of the Global Privacy Enforcement Network (GPEN). GPEN was originally established with support from the OECD and consists of agencies that have data protection or other privacy enforcement powers in their respective jurisdictions. GPEN facilitates enforcement co-operation between members including collaborative working and consistent interpretations which is important for the protection of individuals as personal data is increasingly transferred around the world.

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.

This is the last annual report of the Data Protection Supervisor as the Office is to be renamed Information Commissioner and have additional functions under the Freedom of Information Act. A business case has been developed accordingly.

Finally, it would be remiss not to mention the contribution of staff. During the year there was a personal tragedy that affected everyone. However we have worked through the associated problems and are now preparing for the challenges of FOI. We are very grateful for the assistance provided by our friends and colleagues in other data protection authorities during this time.

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 the web site at:
https://www.inforights.im/legislation/data-protection-act/

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 and a further Directive to protect personal data processed by law enforcement agencies. Agreement is finally expected by the end of 2015, with the Regulation coming into operation in the summer of 2016. The Regulation and Directive would be enforceable in 2018.

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.

The impact will be significant and should not be underestimated. The Regulation will apply to many of the Island's businesses and there is a two year transition period to adjust or risk loss of business and /or substantial fines from European Supervisory Authorities.

Government will also be affected. EU data controllers, for example UK data controllers such as NHS trusts, UK Police, HMRC, Immigration, etc. will be required to ensure that any transfer of personal data to the Island is protected to the standards set down in the Regulation. Therefore, when Government seeks to obtain, or have access to, personal data processed by any of these bodies additional scrutiny will occur and could lead to access being denied as these bodies will not want to risk incurring a substantial fine and/or prosecution.

Government will therefore need to ensure that the Island affords a similar level protection and should move to introduce equivalent legislation at the earliest opportunity.

FREEDOM OF INFORMATION

Under the Freedom of Information Act the Supervisor becomes the Information Commissioner and, in addition to his duties and responsibilities under the Data Protection Act 2002 and Unsolicited Communications Regulations 2005, assumes responsibility for FOI oversight.

Responsibility for oversight of the Code of Practice on Access to Government Information will also pass to the Supervisor.

It is not possible to gauge the impact of FOI but assumptions based on experiences in the UK and Scotland can be made. Using such assumptions an initial business case was provided to Treasury.

The Office is fortunate to already possess a good degree of FOI knowledge which reduces the need for additional staff and training. During the initial phases it has been assumed that the additional responsibilities can be managed by changing the roles and duties of both the Office Manager and Compliance Officer to that of Casework Officers and increasing the number of hours worked.

The Office Manager's hours will increase from half time to three quarter time while the Compliance Officer's hours will increase from 0.8 to full time.

The duties of the Deputy Supervisor (Deputy Commissioner) will also change with particular responsibility for the management of the assessment process and drafting of decision notices.

No new staff will be recruited.

It is intended that the above arrangements will be reviewed again in the autumn of 2017.

BLAME DATA PROTECTION

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

Usually these excuses claim that something could not be done or had to be done in a particular way because of Data Protection. Such claims are not unique to the Island and when examined have always been found to be without substance.

To be clear, the Data Protection Act is designed to protect individuals. Provided it is lawful to do so, there is no provision that prevents personal data from being processed. Instead, the Act sets out eight good practice principles to follow when processing personal data.

RIGHT OF ACCESS TO PERSONAL DATA

The right of access to personal data together with fair processing, that is the right to know who is processing personal data and for what purposes, are referred to in the Act as the "subject information provisions."

The Act states, in subsection 23(5), that *"…the subject information provisions shall have effect notwithstanding any statutory provision prohibiting or restricting the disclosure, or authorising the withholding of information."*

Certain Government Departments have continued to fail to comply with this fundamental right, in particular the Department of Health and Social Care. This is unacceptable and during the year the

Supervisor has made it clear that he is prepared to prosecute the Department and the Officers responsible for that failure in the future.

SURVEILLANCE SYSTEMS

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

As the costs reduce, the number of installations have increased which in turn has led to more disputes for example between neighbours over what is being recorded and why. Concerns have also been expressed about in-vehicle dashboard mounted cameras, body worn cameras and video taken by smart phone.

The Court of Justice of the European Union in the Rynes case, confirmed that where a surveillance system captures images beyond the curtilage of an individual's property then that system is not exempt and is subject to the data protection principals, the right of access etc.

It follows that the principles and rights set out in the Act apply to other surveillance systems including body worn cameras and in-vehicle dash cams.

Compliance advice can be found at:

https://www.inforights.im/information-centre/data-protection-unsolicited-communications/guidance-for-organisations/surveillance-technology-cctv/

SOCIAL MEDIA

Social media continues to be a source of complaint.

The most common complaints continue to come from employees who have been subject to disciplinary action in relation to 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 BY DESIGN AND DEFAULT

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

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

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

DATA BREACH NOTIFICATION

When a loss of personal data 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 guidance on managing a security breach which can be found at:

https://www.inforights.im/information-centre/data-protection-unsolicited-communications/guidance-for-organisations/security-of-personal-data-getting-it-right/managing-a-data-security-breach/

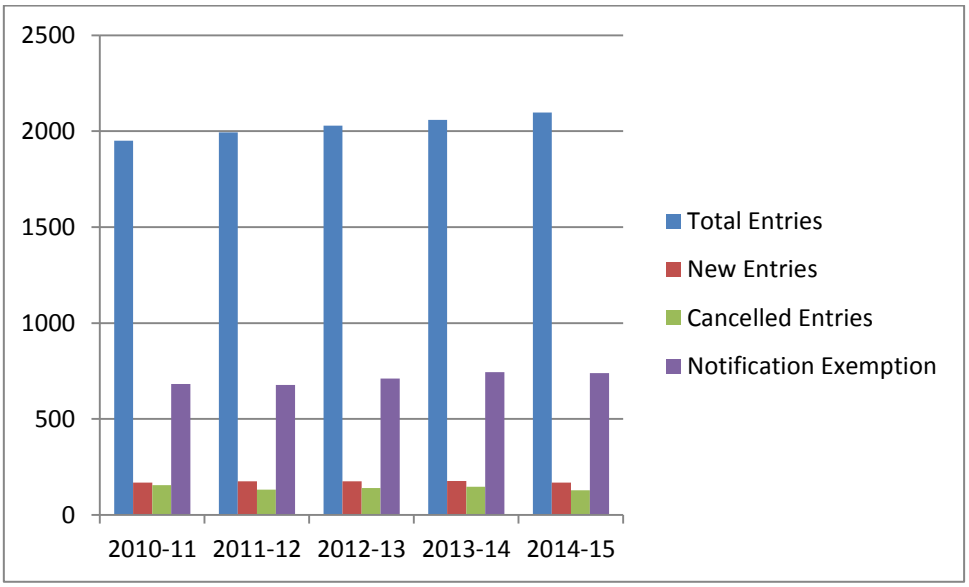
REGISTER OF DATA CONTROLLERS

The Supervisor is responsible for the maintenance and administration of the Register of Data Controllers. In the year 2014-2015, 169 new entries were made in the register while 129 entries were cancelled, representing a small increase of 40 in the total number of register entries. The current list of data controllers is available on our web site at: https://www.inforights.im/information-centre/data-protection-unsolicited-communications/register-of-data-controllers/

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
2014-15	2098	169	129	740

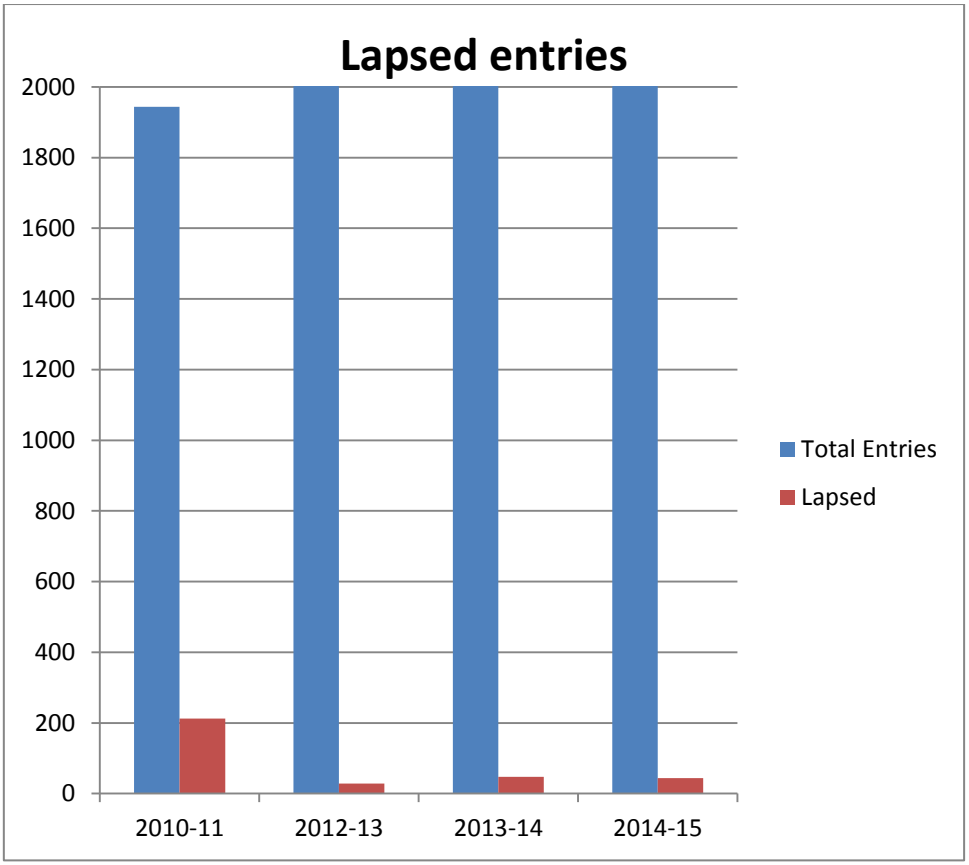
REGISTER OF DATA CONTROLLERS



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

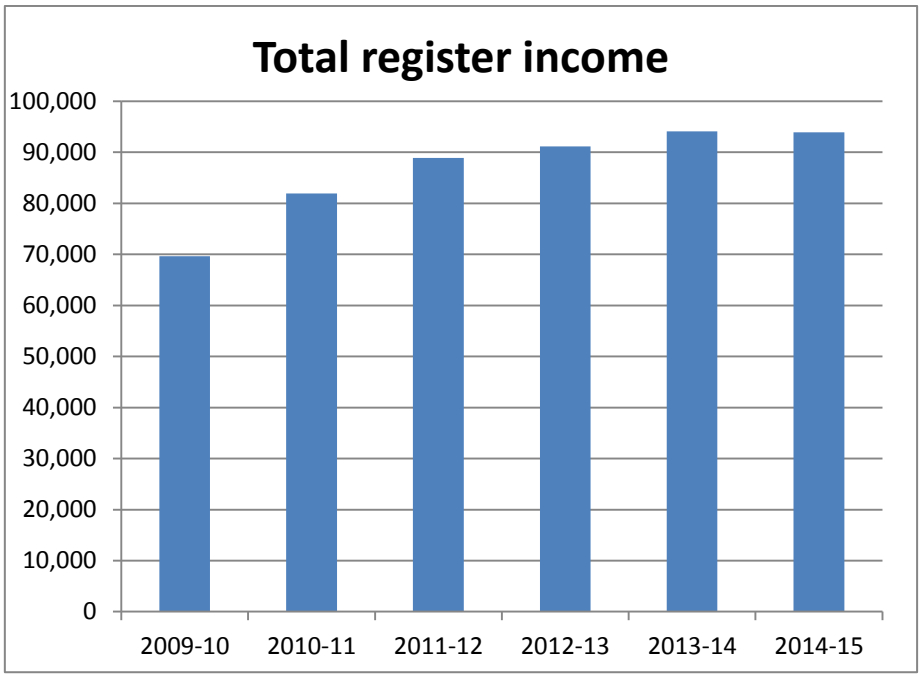
The register entry is renewable annually and, to assist data controllers comply with their registration obligations, renewal letters are sent out six weeks prior to the renewal date, with further reminders sent by email as the expiry date approaches. Renewal letters no longer include a copy of the current 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 and that number has reduced to less than 1.5%.



INCOME FROM REGISTRATION

In 2014-2015, income from registration totalled £93,890, a decrease of just over £200 on the previous year. The chart below shows the fee income levels over the past six years.

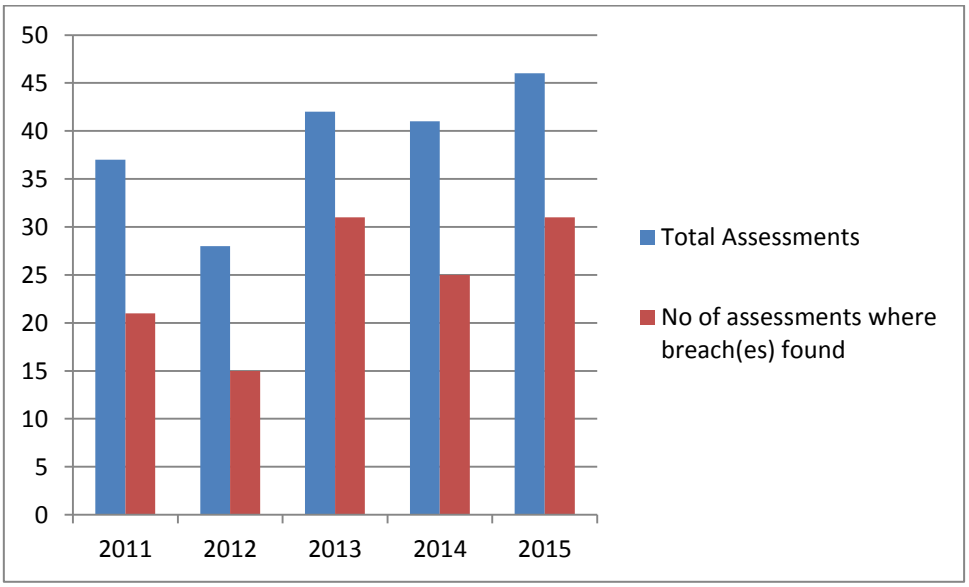


ASSESSMENTS

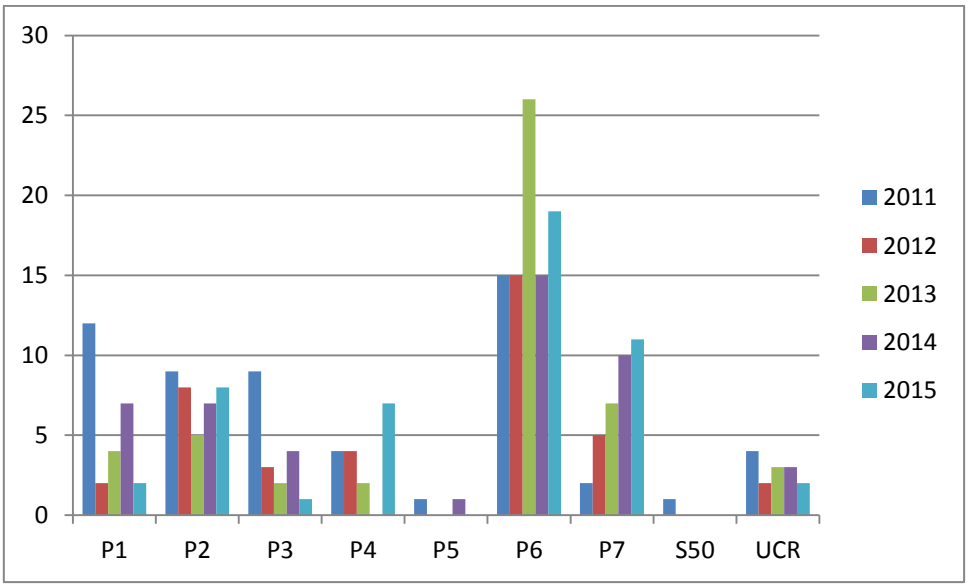
When an individual makes a formal complaint, a request for assessment under section 38 of the Act, my Office is required to form a view as to whether the processing of personal data is likely, or unlikely, to be in compliance with the provisions of the Act or in accordance with the Regulations.

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

During 2015, the number of formal requests for assessment totalled 46 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 67% of all assessments. With regard to compliance with an SAR, breaches were identified in 74% of cases

On average assessments were completed within 28 days of opening which is a decrease on previous years. The longest assessment took 191 days to complete.

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

	2010	**2011**	**2012**	**2013**	**2014**	**2015**
Av. Days to complete	34	33	30	44	41	28
Maximum time to complete	146	166	241	207	167	191

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.

Undertakings and enforcement notices are published on our website at:
https://www.inforights.im/document-library/data-protection-enforcement-notices/

RAISING AWARENESS

TRAINING

Businesses have demonstrated a continuing commitment to understanding their obligations and achieving compliance with the provisions of the Act.

The Office continued 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.

However with the advent of FOI, training will be curtailed in the short term.

In 2014, 19 training sessions were provided, with the number of attendees totalling 300. Private sector organisations accounted for 13 of these sessions, with 189 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 revised staffing under FOI will be:

Information Commissioner	Full time	1.0	OS7
Deputy Commissioner	Full time	1.0	SEO
Casework Officer	Full time	1.0	EO
Casework Officer	Part time	0.75	EO

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

It is now 9 years since there has been any change in personnel. This stability is 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.

The annual Island Data Protection Authorities meeting was held in Guernsey and was attended by UK, Ireland, Jersey, Malta, Cyprus and Bermuda.

The Supervisor also attended the European Data Protection Authorities Spring Conference which was hosted by the UK Information Commissioner in Manchester and a GPEN meeting which was also hosted by the UK Information Commissioner.

In addition the UK Information Commissioner kindly hosted an FOI workshop in October for the Islands. This invaluable workshop included representatives from the Scottish and Irish Information Commissioner's offices.

FINANCIAL REPORT

The figures for the financial years 2013-2014 and budget for 2014 -2015 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 https://www.inforights.im/information-centre/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 the introduction of FOI and keeling up to date with developments regarding the modernisation of the Council of Europe Convention 108 and the European General Data Protection Regulation.