information commissioner

Barrantagh Fysseree

Annual Report 2015-2016

GD 2017/0012

PO Box 69, Douglas, Isle of Man, IM99 1EQ T: +44 1624 693260 W: inforights.im E: ask@inforights.im

CONTENTS

THIS PAGE IS BLANK

Foreword

This is the first annual report of the Information Commissioner covering the twelve month period from appointment on 1st September 2015 to 31 August 2016. For completeness the report also covers the final five months of operation as Data Protection Supervisor from 1st April 2015 to 31st August 2015.

The period covers one of change in terms of legislation, functions and responsibilities of the Office and the duties of staff.

The Freedom of Information Act 2015 ('FOI') came into force on 1st September 2015 and changed the title from Data Protection Supervisor to Information Commissioner reflecting responsibility for oversight of FOI in addition to current responsibilities under the Data Protection Act 2002(DPA) and Unsolicited Communications Regulations 2005. In addition responsibility for oversight of the Code of Practice on Access to Government Information also transferred to the Office.

The full range of duties and functions of the Commissioner had to be prepared ready for commencement of the first phase of FOI requests on 1st February 2016 and therefore the Commissioner had five months to be ready. The Office consists of four staff of which only two are full time and staff willingly assumed new roles and duties and worked additional hours to ensure the Office met the deadline. It will be some time before the full impact of FOI upon my Office can be gauged, until then staff continue to work in temporary capacities with additional duties and responsibilities and I am indebted to them for their efforts in getting ready and their willingness to continue to work in temporary capacities.

I am also indebted to both the UK and Scottish Information Commissioners and their staff who have provided their time, advice and assistance in preparing for FOI.

In December 2015, agreement on the European General Data Protection Regulation (GDPR), was finally reached and the GDPR came into force on 24 May 2016. There is a two year transition before the GDPR becomes enforceable on 25 May 2018. In addition to the GDPR a new Directive, the Police and Criminal Justice Directive, relating to personal data processed for law enforcement purposes, was agreed at the same time and must be transposed into national law by 25 May 2018.

These new instruments are designed to reflect the realities of ubiquitous computing and modern global communications and seek to provide proportionate protection when personal data are processed. There are significant fines and penalties for non-compliance.

The GDPR is extra-territorial in scope and as such applies to any business outside the EU that provides goods or services to an EU resident. This means that all Island businesses that have customers in an EU Member state, including the UK, 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 GDPR by 25 May 2018.

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. The Island must introduce legislation essentially equivalent to the GDPR if it wishes to maintain this "adequacy finding".

In addition, the Police and Criminal Justice Directive also require a third country to be have an adequacy finding in order for personal data such as criminal records to be transferred to it from a law enforcement agency in an EU member state. This is an additional or different adequacy finding.

From the start of 2016, the Commissioner and Deputy have given numerous presentations and talks to various businesses and associations about these new instruments. We have developed GDPR advice and guidance which is available from dedicated GDPR pages on our website and now publish a GDPR newsletter.

We have also assisted associations to bring accredited data protection training courses to the Island and supported the development of local on-Island training.

The impact of these new instruments cannot be underestimated and it will therefore be the priority of my Office to continue to support businesses to understand and prepare for the GDPR.

Iain McDonald
Information Commissioner

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 purpose is 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. For designated Public Authorities under the Freedom of Information Act 2015 the definition of data is extended to all information held by such authorities.

The main functions of the Commissioner 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

UNSOLICITED COMMUNICATIONS REGULATIONS 2005

The Unsolicited Communications Regulations 2005 ('Regulations') 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.

The 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.

FREEDOM OF INFORMATION ACT 2015

The Freedom of Information Act 2015 ('FOI') came into force on 1st September 2015. The Commissioner is responsible for oversight of the Act and at the request of an applicant to review whether a Public Authority's response to a request complied with the provisions of FOI.

The Commissioner has the power to issue Notices including an Enforcement Notice to obtain compliance with the provisions of FOI. These powers are subject to Appeal to the High Court.

FOI made a number of amendments to the Data Protection Act to the extent that the Commissioner's powers, the tenure of Office, the appointment staff amongst other things are now set out in FOI.

CODE OF PRACTICE ON ACCESS TO GOVERNMENT INFORMATION 1995

On 1st February 2016 responsibility for oversight of the Code of Practice passed from His Worship the High Bailiff to the Commissioner.

LEGISLATION & CODES OF PRACTICE

The current list of legislation is shown below. Electronic copies together with case law and other relevant instruments and legislation are available from the Commissioner's web site under the Legislation menu at: www.inforights.im

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)

FREEDOM OF INFORMATION

Freedom of Information Act 2015

Secondary Legislation

Freedom of Information Act 2015 (Appointed Day) Order 2015 SD2015/0264
Freedom of Information Act 2015 (Amendment of Schedule 1) Order 2015 SD2015/0384

Code of Practice

Council of Ministers FOI Code of Practice

CODE OF PRACTICE ON ACCESS TO GOVERNMENT INFORMATION

2016 Code of Practice on Access to Government Information
2016 Guidance Notes on Code of Practice on Access to Government Information

DEVELOPMENTS

General Data Protection Regulation (GDPR)

In January 2012 the European Commission proposed replacing the current European Data Protection Directive 95/46/EC ('the Directive') with a General Data Protection Regulation (GDPR). In the four years since its initial proposal the GDPR has been subject to extensive scrutiny and lobbying.

The catalyst to this proposal was the 2009 Madrid Resolution setting down International Standards on the Protection of Personal Data and Privacy. The Madrid Resolution recognised the need for stronger consistent privacy rights in a global economy and in addition to the unanimous support of all international Data Protection Authorities it also has the support of ten of the world largest companies, the Council of Europe and the US Federal Trade Commission. The Madrid Resolution has been the catalyst to other initiatives including the modification of Council of Europe Convention 108 and the Asia Pacific Economic Co-operation's Cross Border Privacy Regulations. The Commissioner is a co-proposer of the Madrid Resolution.

The European Data Protection Supervisor, Giovanni Buttarelli, described the GDPR as:

"...the biggest attempt so far by a legislator to grapple with the realities of global, ubiquitous data in the internet era"

The GDPR introduces a number of game changing provisions including:-

- Extraterritorial Scope
  - Applies to businesses outside the EU providing services to an EU Resident
- Accountability
  - Onus upon data controller to demonstrate compliance
- Sanctions & penalties
  - Fines up to €20,000,000 or 4 % of global annual turnover
- New Regulatory Powers including :
  - Audit and inspection
  - Banning orders
  - Suspension of data transfer
- Data Minimisation
  - Data must be limited to that which is necessary for a purpose
- New rights
  - Free to exercise with one month for compliance
- Strict consent requirements
  - Clear language and as easy to withdraw
  - Strict requirements for Children
- Data Breach Notification
- Data Protection Officers
  - Report to highest level of management
  - Cannot have conflicting duties, for example data security, ICT
- New obligations including:
  - Data Protection Impact Assessments
  - Data Protection by design
  - Data Protection by default

With regard to “adequacy findings”, the GDPR provides that existing adequacy findings, such as that for the Isle of Man, will remain for the time being but must be reviewed within four years and every four years thereafter.

The Island’s adequacy finding has been in place since April 2004 and has been essential to business and Government as it has permitted personal data to be transferred between the Island and the EU, including the UK, without the need for additional safeguards and associated costs.

There are a number of factors that will be considered for an adequacy finding under the GDPR but the existence of essentially equivalent legislation and an independent supervisory authority are fundamental requirements.

Police and Criminal Justice Data Protection Directive

At the same time as the GDPR, the European Commission proposed a Directive for the processing of personal data by competent authorities for law enforcement purposes. This Directive is additional to the GDPR and is necessary as law enforcement is a reserved matter.

The Directive requires that where personal data are to be transferred to a third country, such as the Isle of Man, that third country must have an “adequacy finding” or other legally binding agreement.

This adequacy finding is not the same as an adequacy finding under the the GDPR. If the Island wishes to obtain personal data from an EU member state for law enforcement purposes, for example the criminal record of an EU resident, then it will have to obtain an “adequacy finding” under this Directive as well as the GDPR.

Council of Europe Convention 108

The Council of Europe includes all 46 European States and it is under its auspices that Conventions such as the European Convention on Human Rights are established.

Council of Europe Convention 108 is the original data protection instrument dating from 1981 and applies to the automatic processing of personal data. It was extended to the Island in January 1993.

The Council of Europe proposed to modify Convention 108 in January 2012 at the same time as the European Commission proposed the GDPR, but put its proposal in abeyance while the GDPR was negotiated.

A revised Convention 108 is near to agreement. Some countries, notably Russia, have expressed reservations but it is hoped that agreement will be reached in the near future. In broad terms the revised Convention 108 can be considered to be a high level GDPR.

Importantly, after Brexit, Convention 108 will continue to apply to the Island and the UK.

E Privacy Regulation

The EU has commenced the process of replacing the current E Privacy Directive, from which the Island's Unsolicited Communications Regulations 2005 derive, with a Regulation on Privacy and Electronic Communications.

It is intended that this new Regulation will enter into force in May 2018 to coincide with the GDPR and ensure definitions, in particular consent, are consistent. Further information on is available at: https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

The Island's related legislation will also require updating.

BREXIT

There is confusion with regard to Brexit and the above mentioned EU legislative changes.

However, the UK has confirmed that as it will be an EU member state when these changes come into full force in May 2018, the UK will be implementing these laws as required.

After Brexit, the UK will need to maintain essentially equivalent legislation in order to trade with the EU and obtain personal data, such as criminal records.

In addition, as Convention 108 will continue to apply to the UK, any new data protection legislation created in the UK, as a result of the proposed Great Repeal Act, is unlikely to differ significantly from the GDPR.

ISSUES

FREEDOM OF INFORMATION

The immediate priorities for the Commissioner after appointment on 1st September 2015 was to prepare guidance for the public and technical advice and guidance for Public Authorities, establish internal procedures for dealing with requests and publish this information in a new website prior to the commencement of FOI requests on 1st February 2016.

There was a significant amount of work to be undertaken but it was completed on schedule thanks to the commitment of staff.

Assistance was provided by both the UK Information Commissioner's Office and, as the Island's FOI Act is more akin to Scotland's, the Scottish Information Commissioner's Office (SIC). The Commissioner and Deputy visited the SIC in St Andrew's and over a two day period were provided with a wealth of information upon which our advice, guidance and internal procedures have been modelled.

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."*

In my last report I stated that certain Government Departments failed to comply with this fundamental right, and in particular mentioned the Department of Health and Social Care. Since then further failure to comply with the right of access occurred and led to my Office preparing draft summonses.

However I am pleased to report that the DHSC has now put into place new governance procedures which appear to be working satisfactorily.

SURVEILLANCE SYSTEMS

The use of surveillance systems continues to produce complaints and raise compliance concerns.

During the year my Office learned of some suggestions for the deployment of body worn video (BWV) which raised concerns. These concerns are not in relation to use by the Constabulary where strict codes of practice have been developed.

The suggestions included members of the public routinely using BWV. Other suggestions included use by "secret shoppers" to monitor staff performance and evidence the "customer experience." There are obvious implications for the individual's right to privacy and in some instances the suggested uses could be seen as inflammatory and rather than protect an individual lead to confrontation or the commission of an offence.

In the Commissioner's opinion new legislation regulating the wide use of modern surveillance technology should now be considered.

Compliance advice can be found at:

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

AUDIO RECORDINGS

A questions as to whether an individual may make a recording of a meeting came to the fore during the year.

With regard to the provisions of the Data Protection Act, provided an individual only records a meeting for their own domestic purposes then the exemption for such purposes set out in the Act applies.

However the Commissioner recommends that individual's should advise that they intend to record and preferably reach agreement with the other parties to the meeting as to how any recording should occur and be subsequently used.

DATA PROTECTION BY DESIGN AND DEFAULT

Last year I reported that the UK Information Commissioner had 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

Article 35 of the GDPR sets out when a data protection impact assessment must be undertaken. For new projects, the Commissioner recommends that the code of practice should be followed.

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/

Data Breach notification form part of the GDPR and the Commissioner recommends that data controller should ensure appropriate procedures are in place to report and investigate such breaches.

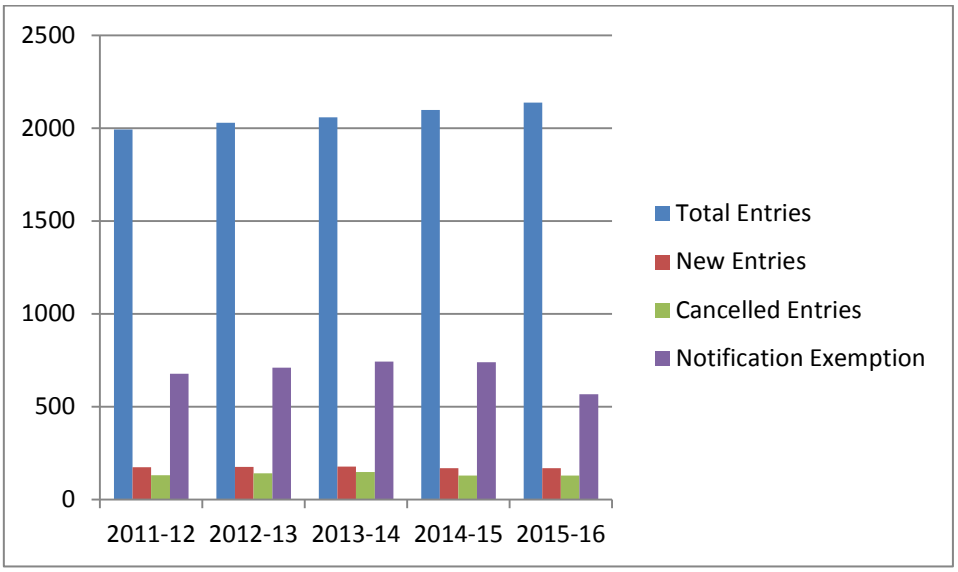
REGISTER OF DATA CONTROLLERS

The Commissioner is responsible for the maintenance and administration of the Register of Data Controllers. In the year 2015-2016, 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
2015-16	2138	169	129	567

REGISTER OF DATA CONTROLLERS

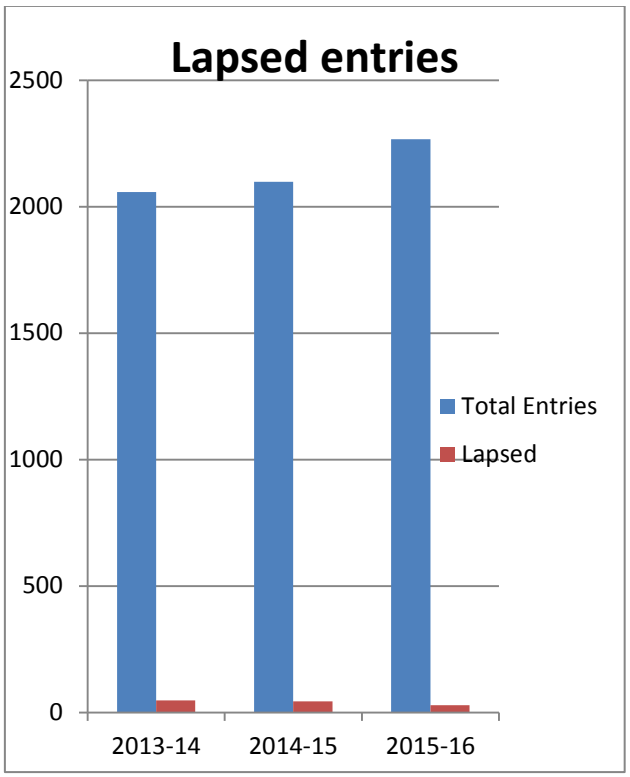


The growth in the number of register entries broadly reflects economic activity and it is therefore pleasing to see some continued albeit modest growth in the register.

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 do not 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, however, electronic copies are emailed on request.

Under the GDPR the onus to maintain "processing records" similar to the register entry falls to the data controller and not the Commissioner.

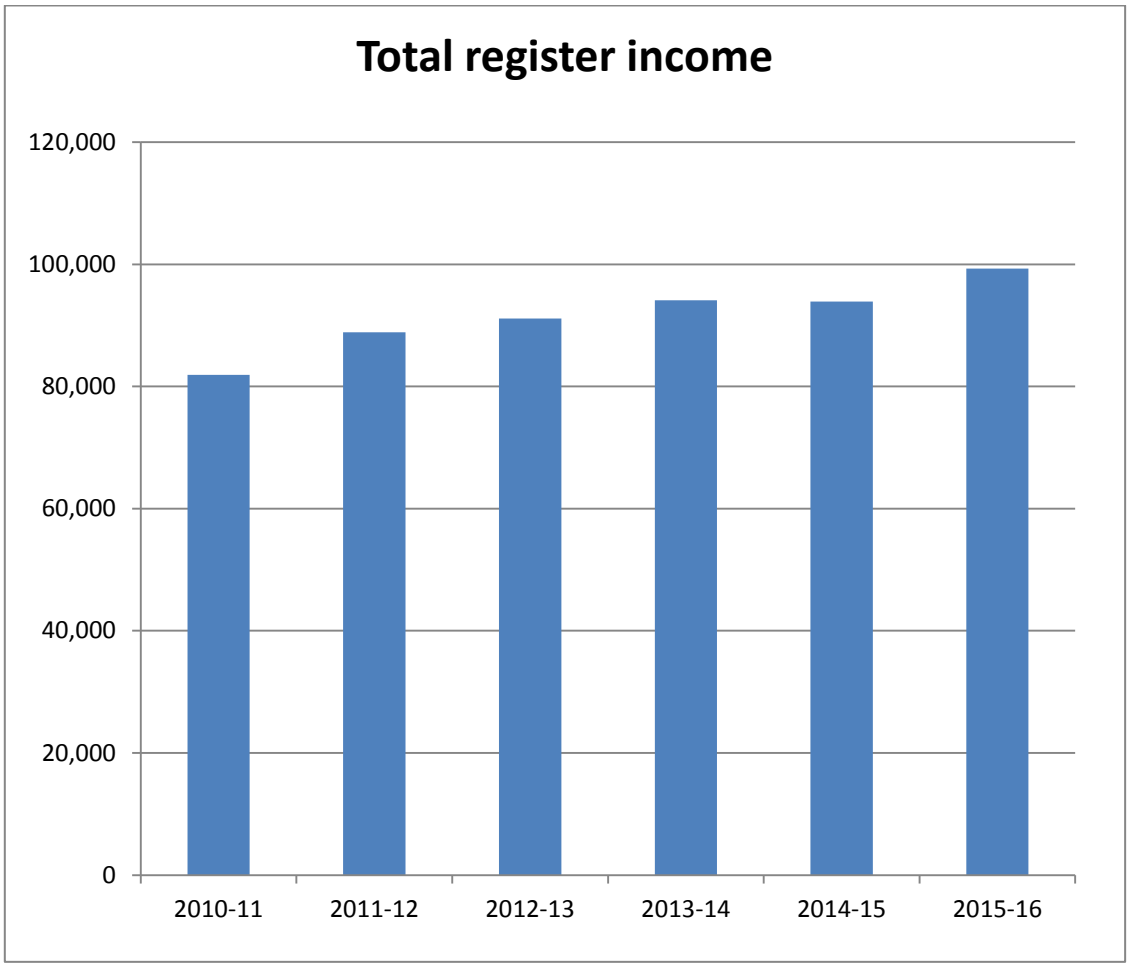
The fees regulations introduced in October 2011 have been effective in reducing the number of lapsed register entries and thereby reduced costs and overheads. Prior to introduction, approximately 13% of all register entries lapsed. In 2015-16, only 29 entries, representing 1.28% of entries, lapsed.



INCOME FROM REGISTRATION

In 2015-2016, income from registration totalled £ 99,292, an increase of £6,402 on the previous year. The chart below shows the fee income levels over the past six years. Fees remain at £70 for a new notification and £50 for a renewal. Currency conversion accounts for the small apparent discrepancy in income.

There is no notification requirement in the current format under the GDPR.



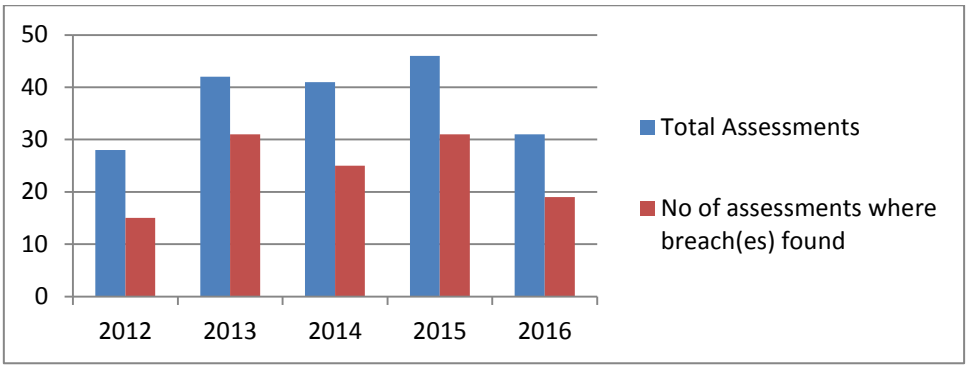
ASSESSMENTS and REVIEWS

DATA PROTECTION ASSESSMENTS

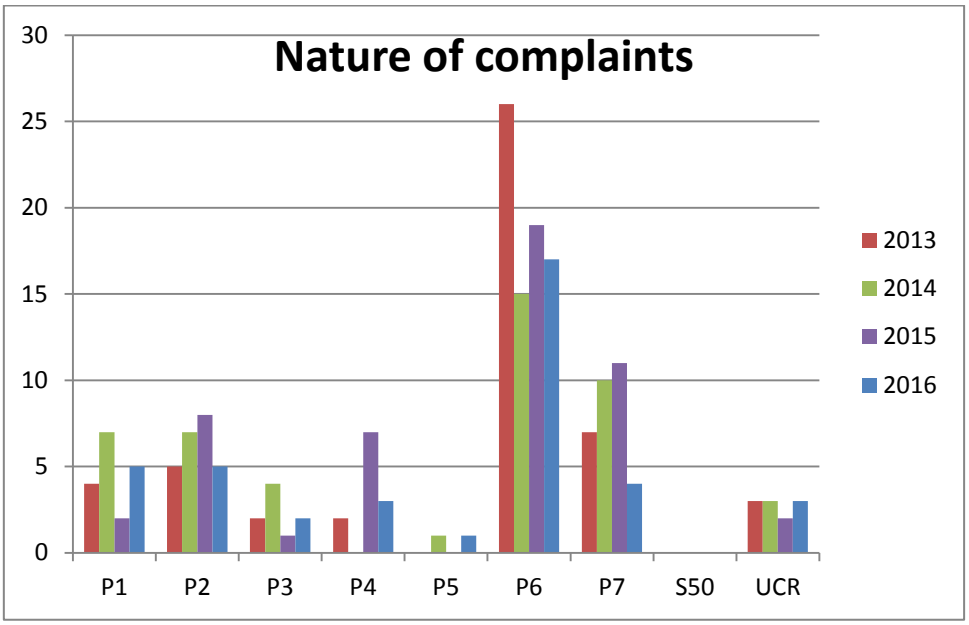
When an individual makes a complaint, that is a request for assessment under section 38 of the Data Protection Act, my Office is required to form a view as to whether the processing of personal data is likely, or unlikely, to be in compliance with the provisions of the Act or in accordance with the Regulations.

Complaints involving the private sector continue to be resolved quickly without the need to exercise the Commissioner's enforcement powers.

During 2016, the number of formal requests for assessment totalled 31 and breaches were identified in 19 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 61% of all assessments.

On average assessments were completed within 26 days of opening which is a decrease on previous years. The longest assessment took 120 days to complete.

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

	2011	2012	2013	2014	2015	2016
Av. Days to complete	33	30	44	41	28	26
Maximum time to complete	166	241	207	167	191	120

The Office continues to believe that enforcement 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/

FREEDOM OF INFORMATION REVIEW OF DECISIONS

In the period from 1st February 2016 to 31 August 2016, the Commissioner received three requests to make a decision pursuant to section 42 of the Freedom of Information Act 2015.

By 31st August 2016 one decision had been made. The decision notices can be found at:

https://www.inforights.im/information-centre/freedom-of-information/decision-notices/

The first decision partially upheld the review applicant's complaint as the Cabinet Office had incorrectly applied exemptions. However it was clear that another exemption could apply to the request and therefore the Commissioner required the Cabinet Office to review its response to the FOI request again.

CODE OF PRACTICE ON ACCESS TO GOVERNMENT INFORMATION

Pursuant to paragraph 12 of Part 1 of the code of practice, I can report that:-

a) No outstanding matter was passed over to me by His Worship the High Bailiff on 1st September 2015,
b) no complaints were referred to me between that date and 31 January 2016, and
c) for the period 1st February 2016 to 31 August 2016 no matter was reported to me.

RAISING AWARENESS

TRAINING

With the implementation and additional workload of FOI the Office has for the time being stopped the provision of training to organisations.

However the advent of GDPR has meant that the Commissioner and Deputy have given a number of presentations and in some instances several presentations to a range of associations including:-

- Association of Isle of Man Compliance Professionals
- Chamber of Commerce,
- Chartered Insurance Institute
- Institute of Directors,
- Isle of Man Law Society
- MICTA
- Society of Trust and Estate Practitioners

Additional presentations were made to smaller specialist groups such as the ISO27001 group.

ADVICE AND GUIDANCE

All guidance we produce is made available on our website to assist both organisations and individuals in their understanding of, and compliance with, the Acts or Regulations. New guidance is introduced as necessary, with existing guidance being regularly reviewed and amended to reflect case law, emerging views and technology changes. We provide updates via a RSS news feed.

In the past year, in addition to the FOI guidance mentioned previously we have focused on providing new guidance to assist businesses with the GDPR.

INFORMATION COMMISSIONER'S OFFICE

STAFF

The Office is currently maintained by a staff of 4 people. The current job titles and grades are shown below:-

Job Title		Actual FTE	Grade Analogy
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 over 10 years since there has been any change in personnel. This stability and detailed knowledge is important as the Office takes on additional responsibility for Freedom of Information and the implementation of the GDPR.

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 Malta and was attended by the Commissioner and counterparts from the UK, Ireland, Gibraltar, Channel Islands, Malta and Cyprus.

The Deputy Commissioner attended the European Data Protection Authorities Spring Conference which was hosted by the Hungarian Commissioner's Office in Budapest while the Commissioner attended the International Data Protection Authorities Conference hosted by the Moroccan Commissioner in Marrakesh. Both conferences were dominated by consideration of the impact of the GDPR.

FINANCIAL REPORT

The figures for the financial years 2015-2016 and budget for 2016 -2017 are as follows:

	2015 - 2016			2016-2017
	Budget	Actual		Budget
Income	(£'s)	(£'s)		(£'s)
New notification fees	8,000	11,810		8,000
Renewal fees	75,000	87,482		76,660
Other income				
Total Income	83,000	99,292		84,660
Revenue Expenditure				
Employee Costs	206,244	182,862		261,531
Infrastructure Expenses	0	0		0
Supplies and Services	30,000	20,814		24,208
Total Expenditure	236,244	203,676		285,739
Net Figure	153,244	104,374		196,079

The Employee Costs budget provision for 2016-17 now includes salaries, pensions, ERNI, training costs and expenses.

The Office continues to operate well within its allocated expenditure budget and exceed its income target.

However the additional responsibility of FOI and the advent of GDPR significantly change the duties and responsibilities of the Office. At present it is not possible to predict what additional resources my Office will require in 2018 or what income, if any, may be generated.

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 continues 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 continue with the introduction of FOI while keeping up to date with developments regarding the modernisation of the Council of Europe Convention 108 and the European General Data Protection Regulation and providing guidance and advice.