information commissioner

Barrantagh Fysseree

Annual Report 2016-2017

GD 2018/0021

CONTENTS

THIS PAGE IS BLANK

Foreword

This is the second annual report of the Information Commissioner. The Information Commissioner was appointed on 1st September 2015 and the first report covered the period up to the 1st September 2016. However, in order to bring the report into line with previous reports and allow for comparisons with previous years to be made, the reporting period has been extended to 31st December 2017. This report therefore covers the the period from 1st September 2016 to 31st December 2017.

The period has again been dominated by the EU General Data Protection Regulation 2016/679 (GDPR) and the associated EU Police and Criminal Justice Directive 2016/680, otherwise known as the Law Enforcement Directive (LED).

Earlier this year the Economist reported that data, regularly referred to as the currency of the 21st century, had overtaken oil as the world's most important commodity. The numerous attempts to obtain personal data by hacking, phishing etc., demonstrates how valuable personal data is; individuals are now more likely to be a victim of identity theft or identity fraud than any other crime.

It is against this backdrop that the GDPR and LED have been created, establishing strong enforcement powers, penalties and sanctions that require data protection compliance to become the responsibility of the boardroom. In short, the GDPR and LED are designed for the reality of ubiquitous computing and data processing in the 21st century.

To raise awareness of the GDPR, my Office has given numerous presentations and talks to various businesses organisations and associations in the Island. We have also produced a range of GDPR guidance documents, which are available from our website, and continue to advise of developments as they occur via the website, social media and our GDPR newsletter.

In May, my Office organised a conference entitled "Getting ready for GDPR". The conference was oversubscribed but the 300+ attendees heard from recognised UK and EU experts in the field. Feedback has been excellent and we are indebted to all the speakers and colleagues from other data protection authorities who gave freely of their time.

The UK has confirmed that it is introducing both the GDPR and LED and, having recognised the vital importance of data flows with the EU, has also confirmed that these laws will remain in place after Brexit. If the Island wishes to maintain its current "adequacy finding" that facilitates the flow of essential personal data to and from the UK and EU, then it must introduce equivalent legislation.

During 2017, the Freedom of Information Act 2015 ('FOI') was extended to all Government Departments, Statutory Boards, publicly-owned companies and other public bodies. There have been eight requests for review by the Commissioner within the year which is consistent with the projections my Office made in 2012. However, my Office does read the public authorities' published responses to FOI requests and is somewhat surprised that more reviews have not been sought.

The Office consists of the Commissioner and three staff. I am indebted to my staff who have worked in temporary capacities with additional duties and responsibilities since September 2015 and for their continued willingness to do so. There is no doubt that the advent of GDPR and LED, coupled with FOI responsibilities, will have a significant impact on the Office requiring additional resource. However, until the new laws are published and duties defined, we are unable to identify what those resources are. It is difficult to see how the Office can be prepared by May 2018.

Iain McDonald
Information Commissioner

RESPONSIBILITIES

DATA PROTECTION ACT 2002

The Data Protection Act 2002 ('the Act'), which came into operation on the 1st April 2003, 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 of the Act 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 under the Act 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.

During the year FOI was extended to all Government Departments and Statutory Boards. FOI will extend to Local Authorities with effect from 1st January 2018.

In addition, with the appointment of a Tynwald Commissioner for Administration at the end of 2017, FOI will be extended to the Information Commissioner in 2018.

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 for which the Office is responsible 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 or via the Isle of Man Legislation website: https://legislation.gov.im/cms/

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)

The GDPR becomes enforceable throughout the European Economic Area on 25 May 2018.

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:-

- Territorial Scope
    - Applies to businesses outside the EU providing goods or services to EU residents
- Accountability
    - Onus upon controller to demonstrate compliance
- Sanctions & penalties
    - Fines up to €20,000,000 or 4% of 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
    - Enhanced 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

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.

The GDPR provides that existing adequacy findings will remain for the time being but must be reviewed by the European Commission within four years, with ongoing monitoring and periodic review (at least every four years) thereafter.

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.

In January 2017, the European Commission commenced its initial review of existing adequacy findings and has entered into correspondence with Isle of Man Government.

Police and Criminal Justice Data Protection Directive (LED)

At the same time as the GDPR, the European Commission proposed an additional Directive (LED) for the processing of personal data by competent authorities for law enforcement purposes. The LED applies only to EU Member States and is necessary as law enforcement is a reserved matter.

The LED 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" under the LED, or another legally binding agreement.

The LED adequacy finding is not the same as the 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 the LED as well as the GDPR.

Council of Europe Convention 108

The Council of Europe includes all 47 European States and Conventions, such as the European Convention on Human Rights, are established under its auspices. Council of Europe Convention 108 is the original data protection instrument and has applied to the Island since January 1993.

Convention 108 is being revised. Some countries, notably Russia, have expressed reservations but it is hoped that agreement will be reached by the end of 2018. In broad terms, the revised Convention 108 can be considered to be a high level GDPR.

After Brexit, the obligations under Convention 108 will continue to apply to the UK and the Isle of Man.

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 expected that this new Regulation will enter into force in early 2019. The Island's related legislation will also require updating.

Programme for Government

In the Programme for Government approved by Tynwald in 2017, Isle of Man Government committed to introduce equivalent legislation to that of the GDPR and LED by 25 May 2018. The Chief Minister has taken political responsibility to do so.

ACTIVITIES

FREEDOM OF INFORMATION

While Freedom of Information had been a priority in the previous year, due to the importance of GDPR and the resources available to the Office less priority had to be given in 2017.

This meant that, while some revision to guides was undertaken during the year, work was mostly limited to that required when making a decision.

DATA PROTECTION

Raising Awareness/ Training

The advent of GDPR has meant that both the Commissioner and Deputy have provided numerous presentations during the year 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

Presentations were made to smaller specialist groups such as the ISO27001 group and other groups such as the Women's Institute.

The Commissioner has also assisted some professional associations to arrange on-Island training for their members which has led to a number of individuals obtaining recognised Data Protection qualifications. The Commissioner has also supported a number of local training initiatives.

Conference

In May 2018, the Commissioner organised a conference in the Villa Marina entitled "Getting Ready for the GDPR".

Chaired by David Smith, a former UK Deputy Information Commissioner, the conference brought together a number of expert speakers from business and legal backgrounds as well as representatives from other data protection regulatory authorities and the European Commission to assist Isle of Man businesses understand how they are affected by the GDPR and what steps they should be taking now to ensure compliance by May 2018.

The conference was sold out with over 300 attendees. Feedback has been excellent.

The Commissioner is indebted to all the speakers who gave of their time freely and also to staff who took on the arduous task of organising and administering all aspects of the conference in addition to normal duties.

Advice and Guidance

All guidance produced is available on the website to assist both organisations and individuals in their understanding of, and compliance with, the Act, FOI 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. Updates are also provided via a RSS news feed.

In the past year, we have focused on providing new guidance to assist businesses with the GDPR. The following guidance has been produced:-

Two short overview guides entitled:-

New Data Protection Laws -10 things you need to know and do
New Data Protection Laws Summary

and a series of guidance notes under the title "A closer look" which consider different aspects of the GDPR in more detail. To date the series includes:-

A closer look at Rights and Remedies
A closer look at Records of Processing
A closer look at Data Protection Officer
A closer look at Principles
A closer look at Definitions
and
A closer look at Transparency

This is in addition to the guides produced in 2017:-

GDPR Toolkit: Part 1: Know Your Data: Mapping the 5 W's
GDPR Toolkit: Part 2: Accountability questionnaire for the Board

Positive feedback on these guidance notes has been received from significant controllers and experts in the UK and Ireland.

It is intended to produce a small business guide in early 2018 with further specific guides produced once the Island's new legislation is finalised.

GDPR Newsletter

The Commissioner also produces a GDPR newsletter which provides updates when significant developments occur. 8 editions have been produced to date and the newsletter is circulated by email to over 400 recipients as far afield as Brazil and Sweden.

Social Media

The Office now has a LinkedIn page and also provides updates and commentary on relevant issues via that medium.

ISSUES

Surveillance Systems

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

As the cost and ease of installation of such systems has reduced the use of these systems has become more prevalent. We have seen an increase in installations of CCTV on domestic properties, of "dashcams" in vehicles and the use of body worn video cameras.

During the year the Office has received many complaints from the public about the use of such systems, together with queries or complaints about the use of covert CCTV in public spaces, GPS trackers installed covertly in vehicles and location tracking apps installed on the private phones of employees.

It is very clear that surveillance is an emotive subject.

On several occasions individuals have claimed that the installation of CCTV on a domestic property had been suggested as a means to resolve a dispute between neighbours. However, the complaints that my Office has received indicate that rather than resolve a dispute, installation can cause escalation particularly where individuals feel they are being watched or monitored on their own private property by a neighbour's CCTV cameras and are not willing, or do not feel able, to speak to their neighbour about the installation due to the dispute.

Similarly my Office has received complaints about the use of "dashcams". Where an individual installs a dashcam only for their own private purposes, for example to use as evidence if their vehicle is involved in an accident, then the exemption from complying with the requirements of the Data Protection Act in respect of "Domestic Purposes" applies.

However, when a dashcam is installed with the intention of capturing images of perceived 'bad driving' or 'poor parking', for example, and the subsequent proactive disclosure of those images to the Police where no request for evidence or information has been made, or through publication on social media, then the Domestic Purposes exemption does not apply. Individuals using dashcams in such circumstances must, therefore, as data controllers, fully comply with the Data Protection Act, including registration, fair and transparent signage on the vehicle, permitting the exercise of rights by individuals whose personal data has been processed, in particular, the right of access.

In 2005, the then UK Information Commissioner produced a report that found that the UK was sleep walking into a surveillance society; it seems the Isle of Man, promoted as being one of the safest places in the British Islands to live, is in danger of doing the same.

It is a concern, therefore, that during the year there seems to have been support from various quarters for the installation of surveillance systems. This could be seen as encouraging vigilantism. Proportionality and necessity must be at the forefront of any decision to install or use any surveillance system, whether by data controllers or individuals, to ensure that, as far as possible, the privacy of individuals is maintained.

In the Commissioner's opinion, consideration of the issue is overdue and new legislation regulating the increasing use of modern surveillance technology is required.

Compliance advice can be found at:

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

Legal Professional Privilege

During the year the subject of legal professional privilege arose on a couple of occasions.

While a claim to legal professional privilege can be made to prevent the disclosure of information to a data subject in response to a subject access request, that does not prevent the Commissioner, in discharging his duties under the Act, from being furnished with that information in order to consider whether or not the exemption has been correctly applied.

Section 53 of the Act, specifically provides for that information to be furnished to the Commissioner.

Similar issues have arisen in the UK and it is notable that UK's Data Protection Bill includes additional provisions which clarify how that information will be treated.

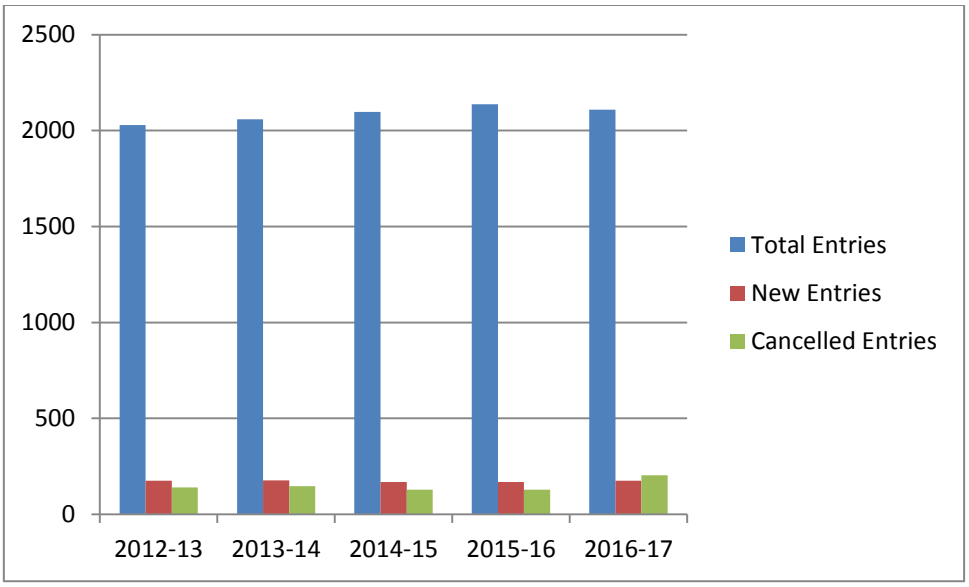
REGISTER OF DATA CONTROLLERS

The Commissioner is responsible for the maintenance and administration of the Register of Data Controllers. In the year 2016-2017, 175 new entries were made in the register while 204 entries were cancelled, resulting in a decrease of 29 in the total number of register entries. In addition the Commissioner holds a list of a further 601 controllers that have claimed exemption from Notification.

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

	Total Entries	New Entries	Cancelled Entries
2004-5	1273	406	72
2005-6	1483	207	93
2006-7	1795	217	107
2007-8	1896	189	41
2008-9	1932	184	148
2009-10	1932	141	141
2010-11	1950	169	155
2011-12	1993	175	132
2012-13	2028	176	141
2013-14	2058	178	148
2014-15	2098	169	129
2015-16	2138	169	129
2016-17	2109	175	204

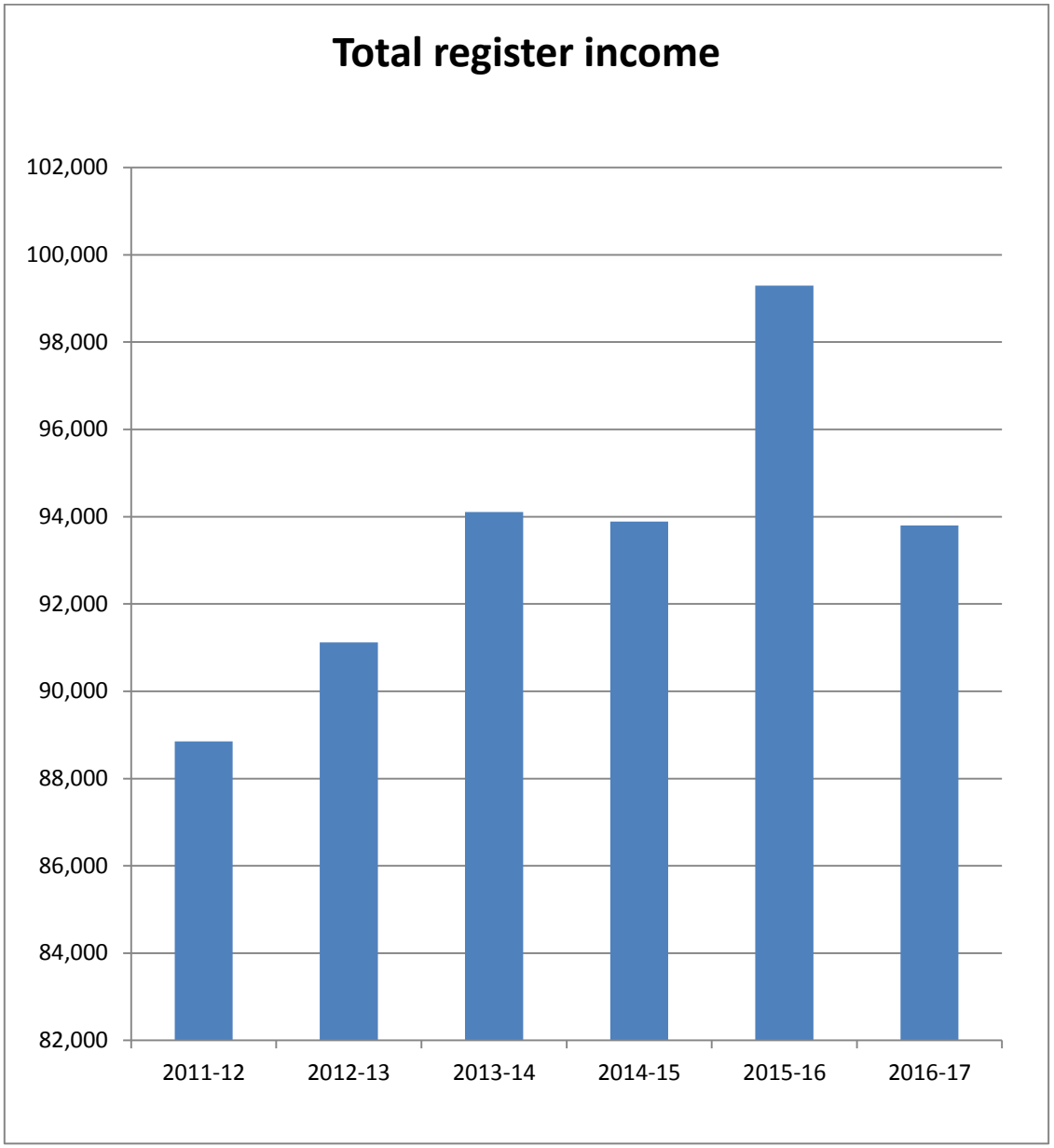
REGISTER OF DATA CONTROLLERS



Under the GDPR the onus to maintain "processing records" falls to the data controller and not the Commissioner and there is no requirement for a register to be maintained in the existing format. However, other jurisdictions have decided to retain a register containing basic information about the controller and the Commissioner has recommended that a basic register should be maintained.

INCOME FROM REGISTRATION

In 2016-2017, income from registration totalled £ 93,800 a decrease of £5,492 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.



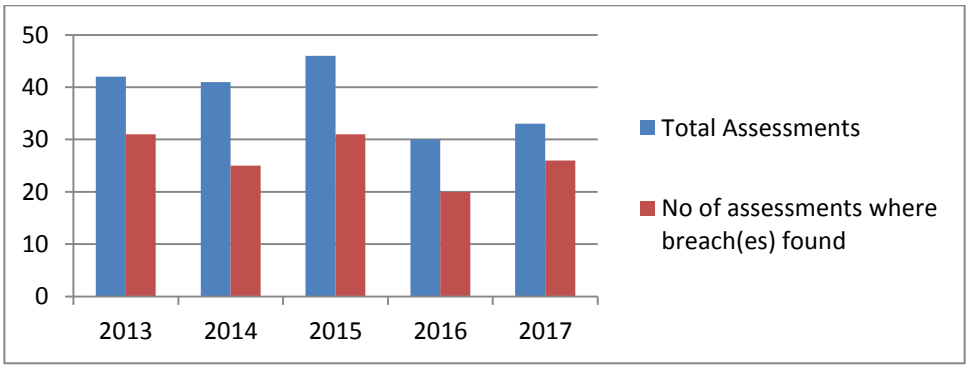
ASSESSMENTS and REVIEWS

DATA PROTECTION ASSESSMENTS

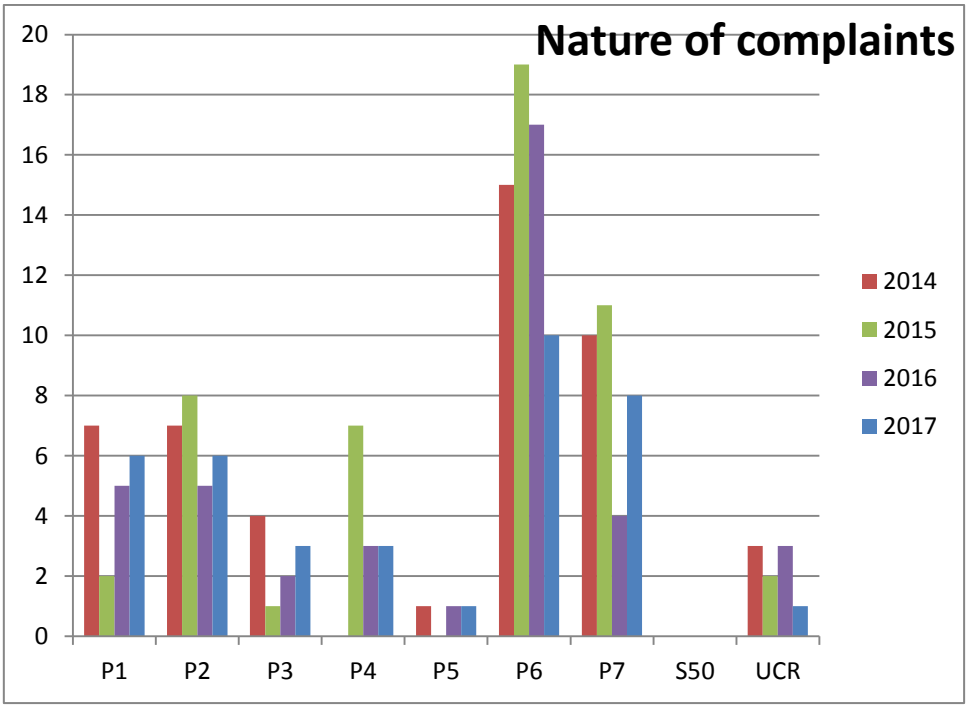
When an individual makes a complaint, a request for assessment under section 38 of the Data Protection Act, my Office is required to form a view as to whether the processing of personal data is likely or unlikely to be in compliance with the provisions of the Act or in accordance with the Regulations.

In general, complaints involving the private sector continue to be resolved quickly without the need to exercise the Commissioner's enforcement powers. There was, however, one significant exception during the year which required the issue of an Information Notice and took a considerable time to resolve.

During 2017, the number of formal requests for assessment totalled 33 and breaches were identified in 26 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 91% of all assessments relating to SARs. Two undertakings were signed by data controllers which failed to comply with subject access requests.

On average, assessments were completed within 19 days of opening which is a decrease on previous years. The longest assessment took 96 days to complete.

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

	2012	**2013**	**2014**	**2015**	**2016**	**2017**
Av. Days to complete	30	44	41	28	26	19
Maximum time to complete	241	207	167	191	120	96

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.

Unfortunately, during the year it has been necessary to commence proceedings for the failure to notify. This is the first occasion since the current Act came into force in 2003 that it has become necessary to take proceedings for this particular offence. The matter is currently before the courts and, as such, no further comment can be made.

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 September 2016 to 31 December 2017, the Commissioner received eight requests to make a decision pursuant to section 42 of the Freedom of Information Act 2015.

By 31st December 2017, 4 decision notices had been issued. The remaining four review requests were received during December 2017 and decisions will be made in 2018.

The decision notices can be found at:

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

It was anticipated that it would take some time for requests for Review by the Commissioner to be made. However it is surprising to report that, despite the number of requests for information that were made to Public Authorities during the year, only 10 requests for Review by the Commissioner were received.

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 matter was referred to the Information Commissioner in the period 1st September 2016 to 31st December 2017.

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 and LED.

INTERNATIONAL COOPERATION

The Office continues to enjoy close working relationships with its international colleagues. In particular, the Office works closely with colleagues from the UK, Ireland, the Channel Islands and Gibraltar.

The annual Island Data Protection Authorities meeting was held in Gibraltar and was attended by the Commissioner and counterparts from the UK, Ireland, Gibraltar, Channel Islands and Malta.

The Deputy Commissioner and a casework Officer attended the European Data Protection Authorities Spring Conference which was hosted by the Cypriot Commissioner's Office in Limassol while the Commissioner and Deputy attended the Information Commissioner's International Conference which was jointly hosted by the UK and Scottish Information Commissioners in Manchester.

While the Commissioner did not attend the International Data Protection Authorities Conference which was held in Hong Kong he did take part in a conference call.

The Office is a member of the Global Privacy Enforcement Network and the Deputy Commissioner and a casework officer attended the inaugural GPEN Enforcement Practitioners Workshop which followed the European Case handling Workshop hosted by the UK Information Commissioner in Manchester. The Deputy Commissioner, in collaboration with a colleague from Norway, gave a presentation at the case handling workshop. A number of issues of common interest are discussed between GPEN members via conference calls and on a dedicated website.

The Commissioner is also a member of the Common Thread Network which consists of a number of Commonwealth Data Protection Authorities. This is a relatively new organisation which is growing in numbers and has the aim of assisting the development of data protection throughout the Commonwealth. A presentation of the work of the Common Thread Network is to be made at the Commonwealth Heads of Government meeting in London in April 2018.

FINANCIAL REPORT

The figures for the financial years 2016-2017 and budget for 2017 -2018 are as follows:

	2016 - 2017			2017-2018
	Budget	Actual		Budget
Income	(£'s)	(£'s)		(£'s)
New notification fees	8,000	9,800		8,000
Renewal fees	76,660	84,000		78,353
Other income				
Total Income	84,660	93,800		86,353
Revenue Expenditure				
Employee Costs	261,531	227,530		246,911
Infrastructure Expenses	0	0		0
Supplies and Services	24,208	21,028		24,206
Total Expenditure	285,739	248,558		271,117
Net Figure	201,079	154,758		184,764

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 will be required during 2018 or what income, if any, will be generated under the new legislation.

As part of the Office's commitment to openness and transparency, details of the income and revenue expenditure, broken down into categories and is 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 individuals' rights is to actively assist businesses and organisations to understand and comply with the law.

Our priority over the next year will continue to be assisting businesses with understanding their obligations under the new Data Protection legislation while managing the changes that transition to the new legislation brings for the Office.