



OFFICE OF THE
INFORMATION
COMMISSIONER

Annual Report

2017



OFFICE OF THE INFORMATION COMMISSIONER

Introduction and Our Mission	3
Governance Statement	5
Office Structure	7
Your Information Rights	8
Deputy Commissioner's Foreword	9
Our Aims	13
Operational Performance	14
Breach Reporting	16
Registration	17
Guidance	18
Enforcement	19
International Liaison	20
European Developments	22
Privacy Shield	24
Freedom of Information	25
Financial Information	28

Introduction and Our Mission

Despite starting the year as a pan-Island, Channel Islands regulatory body, this Annual Report details the work of the Jersey Office of the Information Commissioner (OIC) only during 2017. Following six successful years as a pan-Island authority, the respective governments of Guernsey and Jersey made the decision to separate at the end of the year in order that each jurisdiction could prepare for the implementation of new legislative regimes independently. The Guernsey Office of the Data Protection Commissioner will therefore be presenting their own Annual Report for the year 2017.

Statement of Purpose

To fully discharge our statutory duties, as an independent body, to enhance information governance in Jersey ensuring continued recognition as a well-regulated jurisdiction.

To assist organisations to meet their obligations; to regulate where the required standard has not been met and to ensure that individuals are confident and able to exercise their information rights.

Areas of Focus

DEVELOP – ensuring our staff are highly skilled and motivated, working effectively and efficiently across the Island.

EDUCATE – working with key organisations and individuals to promote awareness and understanding of information rights and responsibilities.

LEAD – ensuring, as the subject matter expert Jersey continued recognition on the European and international stage.

INFLUENCE – seeking to embed information rights in all relevant areas, especially new laws and policies across the private and public sector

VISIBLE – conducting our work in an open and transparent manner, ensuring relevant and useful information is proactively published on our website

ENFORCE – taking targeted and meaningful regulatory action in a fair and consistent manner

REGULATE – making effective use of our statutory powers to achieve consistency in approach in Jersey.

Governance Statement

The position of Information Commissioner was established in the Data Protection (Jersey) Law 2005 and the Freedom of Information (Jersey) Law 2011. From 25th May 2018, the position is appointed by the Data Protection Authority under the Data Protection Authority (Jersey) Law 2018.

Under the terms of the EU Directive 95/46, the Commissioner needed to be independent of government and this was enshrined in legislation. In Jersey, the sponsoring department for the Office was the Chief Minister's Department. The Information Commissioner was directly accountable to the States of Jersey for the exercise of statutory functions and subject to States audit. From 25th May 2018, the Information Commissioner is accountable to the Data Protection Authority.

Risks

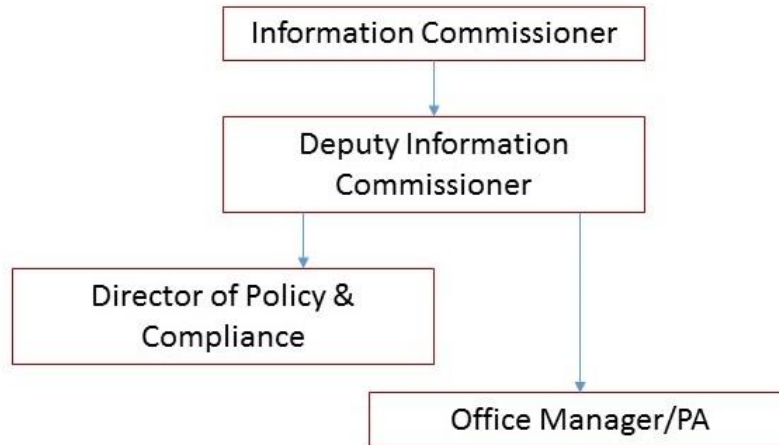
Risks are routinely assessed

1. **Budgeting 2017 and beyond:** The OIC has an agreed budget for 2018. Additional funding has been allocated to the OIC to assist with Data Protection (Jersey) Law 2018 preparation and implementation. Further detailed work will be required to establish the long-term resource requirements, as well as income options. In addition, long term funding for Freedom of Information in the Jersey office has yet to be agreed.
2. **Implementation of GDPR:** Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. While that obligation produced administrative and financial burdens, it did not contribute to improving the protection of personal data in all cases. The Directive abolished general notification obligations and replaced them with effective procedures and mechanisms that focus instead on those types of processing operations that are likely to result in a high risk to the rights and freedoms of individuals.

This would include processing involving using new technologies, or where the controller has not conducted a data protection impact assessment or where considerable time has elapsed since the initial processing. Accordingly, work is underway to establish a new, risk-based tiered model of registration to ensure that the OIC continues to be funded, whilst at the same time recognising that such a mechanism needs to be of value, to both the OIC and controllers.

3. **IT strategy:** In 2015, the OIC took the extremely important step of moving away from government IT support. Independence is a crucial part of a successful data protection and freedom of information regulation and we must hold our own data secure and independent. Preparation has started on the major internal IT reform needed to deliver Data Protection (Jersey) Law 2018.
4. **Increasing pressure on resources:** The significant increase in numbers of cases from spring 2017 onwards has in part been due to our ongoing work to ensure individuals know their rights and empowered to raise concerns. We continue to focus energy where possible on this important aspect of our role. Managing the volume of work as well as expectations at the same time as the OIC is going through significant changes will be a challenge for us all.
5. **Robust independence from government:** In order for us to be an effective regulator and to deliver on the Data Protection (Jersey) Law 2018 requirements, we need to ensure a workable and sustainable funding system as well as a clearer guarantee of independence across the Island. The implementation of the Data Protection Authority (Jersey) Law 2018, and the establishment of an overarching Board structure goes a long way to ensuring this independence.

Office Structure



A part-time role of Executive Officer was created in 2017 to provide casework support to the OIC during preparations for the implementation of Data Protection (Jersey) Law 2018.

In December 2017, the OIC commenced a recruitment program with a view to appropriately resourcing the OIC between 2018 and 2020 in light of the demands of GDPR and new local legislation.

Information Rights

The **Data Protection (Jersey) Law 2018** gives citizens important rights including the right to know what information is held about them, how that information is going to be handled, and the right to correct information that is wrong. The Data Protection Law in Jersey helps to protect the interests of individuals by obligating organisations to manage the personal information they hold in a fair and lawful way.

The **Freedom of Information (Jersey) Law 2011** gives people a general right of access to information held by most public authorities in Jersey. Aimed at promoting a culture of openness and accountability across the public sector, it enables a better understanding of how public authorities carry out their duties, why they make the decisions they do and how they spend public money by requiring the disclosure of information in those areas.

Acting Commissioner's foreword



2017 has been an interesting year to say the very least. As you will recall from last year, the General Data Protection Regulation (GDPR) was approved by the EU Parliament on 14th April 2016. It came into force twenty days after that and after a 2 year lead in period, will be directly applicable in all EU member states on 25th May 2018, replacing the Data Protection Directive 95/46/EC (the Directive).

The way organisations handle personal data has changed dramatically since the Directive came into being in 1995. The internet in particular, together with rapid advances in technology has allowed for greater accessibility, collection and use of our personal information to the point that the regulatory regime in Europe was deemed no longer fit for purpose. With a view to addressing the globalized nature of information sharing and how we live our lives in this digital era, the GDPR is the most significant reform of European data protection regulation ever seen. The apparent lack of control of personal information by organisations, evidenced by the significant rise and effect of data breaches, has resulted in a regime that is designed to enhance individual's fundamental rights of protection of their personal information and put the power back in the hands of the people.

As a 'third' country, largely dependent upon free flows of information between the Island and its European neighbours, GDPR is hugely important for Jersey. Back in 2005, Jersey implemented legislation in response to the Directive resulting in recognition as an 'adequate' jurisdiction for those purposes. The importance of retaining this position to protect the free flow of data cannot be understated, and 2017 saw the Island's government work to secure equivalent legislation to come into force at the same time as the GDPR.

In line with government objectives with the customer as the focus, data protection reform in Jersey needed to ensure that its citizens are provided with appropriate legal protections and remedies in this digitalized world. Secondly, the overwhelming need to retain the current adequacy status of the Island in respect of continuing data flows would be essential in preserving the Island's position as a well-regulated jurisdiction that is open for business. With data increasingly important to all business, government and domestic activity, providing a safe and strong regulatory environment must be recognised as a key requirement for a successful economy.

Despite an implementation plan with both Jersey and Guernsey working together to make the best use of resources, and with an understanding of the importance of a harmonised Channel Island approach, the Islands' respective governments made the decision to move forward separately. From November 2017, the focus of the Jersey OIC was to work with the States of Jersey in implementing a new legislative framework that reflected the requirements of the GDPR and ensured the continuing protection of its citizen's post-25th May 2018. Alongside the work of the States of Jersey Law Officers' Department, Law Draftsman and Digital Policy Unit, the OIC prepared an implementation program to create a new Data Protection Authority that could provide an unparalleled service to the local community. This has involved a program of recruitment, identifying potential new office premises, preparing new guidance to reflect the new local legislation and developing new IT systems to cope with the increased demand from our customers. This work will continue into 2018 and 2019 as we strengthen the office to provide the highest levels of data protection to the island.

It would be remiss of me to not mention the incredible contribution from the previous Information Commissioner, Emma Martins in this regard. Emma was responsible for laying much of the groundwork for this program of implementation, and her tireless work in preparing the landscape for the new Authority cannot be underestimated. I cannot thank Emma enough. Equally, my very small team have worked extremely hard to maintain a calm approach during what has been a hugely challenging period for the OIC. They have ensured that the office has run smoothly and that the high standard of service demanded has not faltered. Again, they deserve significant credit for this and I thank them wholeheartedly.

We are undoubtedly moving into an exciting but hugely challenging era. The expert input of the Channel Islands Brussels Office has been invaluable and will continue to be so as we work towards a positive adequacy review.

The European Commission have stated they will be reviewing all 'third' country adequacy findings together and this piece of work will be completed in 2020. I am optimistic that we are in good shape and that the Commission will view Jersey's new data protection framework favourably. However, it remains an absolutely crucial point for the Island and will be high on the agenda as we move forward into a post-GDPR era. The importance of maintaining a high level of data protection compliance in a way that enhances the economic benefit of the Island cannot be underestimated.

Achieving our primary goals and providing the best regulatory framework in the wake of GDPR and Data Protection (Jersey) Law 2018 implementation means changing the way we do things as a regulator. Historically we have operated a tiny office and have largely been forced to be reactive to data protection complaints and issues. However it is clear that maintaining this approach will not suffice if we are to deliver even the basics of data protection compliance in a GDPR world. To be an effective and efficient regulatory body means increasing our resources, changing our practices, taking a proactive approach and building a strong authority that can support business as well as provide an effective enforcement function should the need arise. We are committed to develop a regulatory regime that focuses on encouraging ethical business practice and delivering ethical business regulation. We will strive to engage more with the all our stakeholders so we can understand the key issues a guide those stakeholders accordingly. We want to encourage data protection compliance naturally and promote a regime where businesses see good data protection as good business sense, thus reducing the fear of regulatory action for failures, and creating an environment of trust, both with the regulator and their customers.

There is no doubt that 2018 will be a bumpy ride for many, including my office. 'Rome however was not built in a day', and we are under no illusions that many businesses will struggle to be 'ready' for Data Protection (Jersey) Law 2018 implementation on 25th May. However, the Island's community should rest assured that we will do our utmost to support those businesses and help organisations to develop a glide path to compliance over the coming years.

Notwithstanding, there will be those who continue to brush the importance of data protection under the metaphorical carpet and will do nothing. While our primary aim is to be a more engaging and supportive regulator, the new regime also brings increased enforcement capability for our office.

In cases where data protection compliance is ignored, wilfully neglected, or deliberately flouted, then it is those organisations who should worry the most. Ultimately, it is our role to protect the personal information of the citizens of Jersey, and we will do this without fear or favour, exercising our powers to their full extent where warranted and necessary.

As a final note, do not be scared of the Data Protection (Jersey) Law 2018 road ahead. Sadly, there are organisations out there who seek to profit from the GDPR and local new law build up by promoting a culture of fear amongst particularly the small and more vulnerable business community. In my view, this is unnecessary, unethical and unhelpful. Instead, we hope to see a collaborative approach where we all work together to achieve the common goal of presenting Jersey as a well-regulated Island that takes data protection and privacy seriously. We wish you luck for the new regime ahead!

Paul Vane

Acting Information Commissioner

Our Aims

Priorities

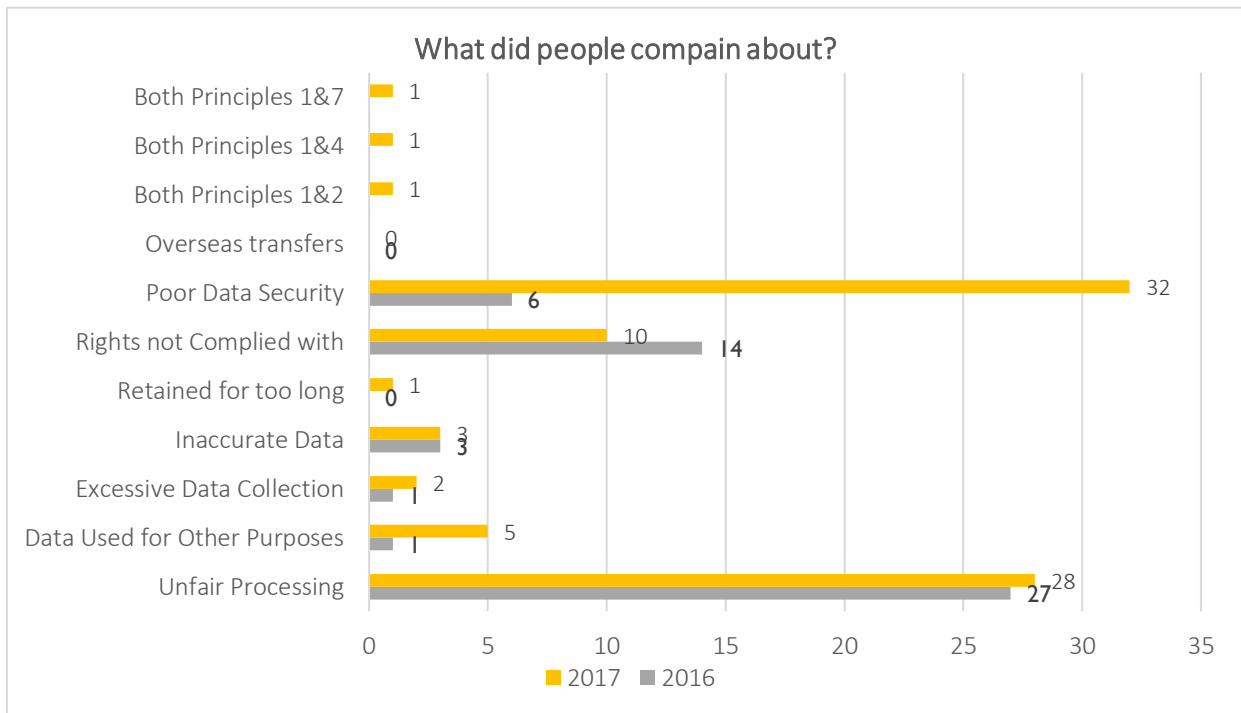
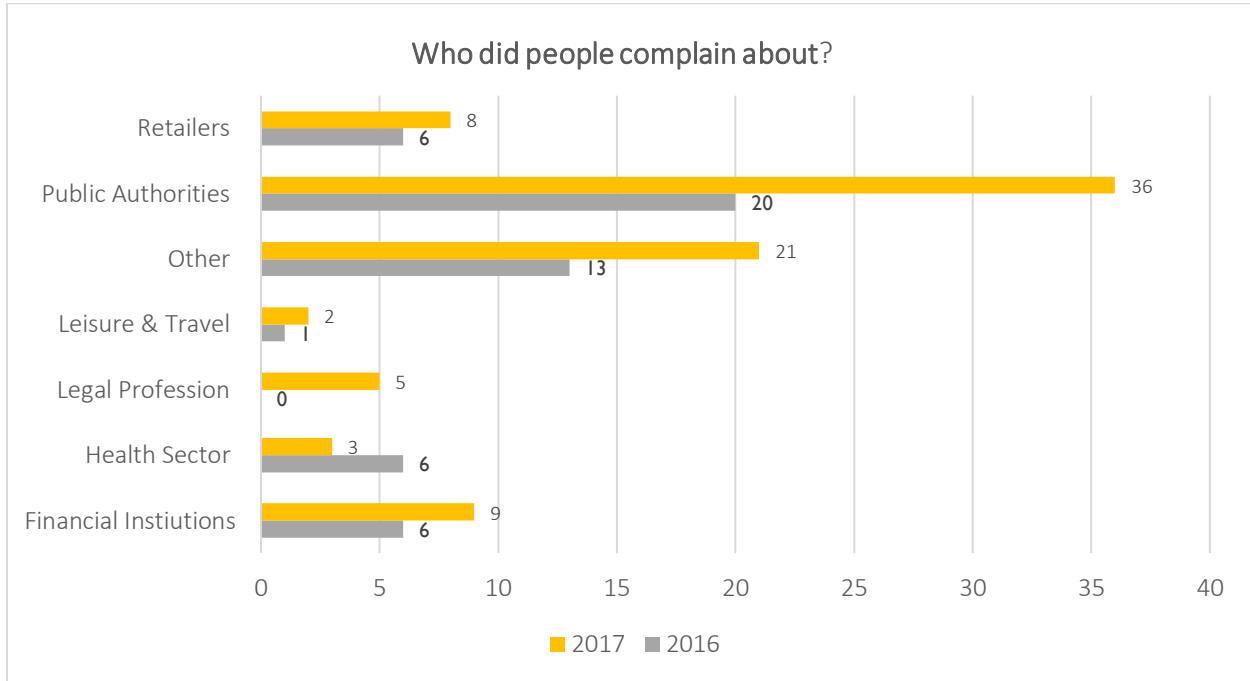
- To be a well-led and managed organisation, one that staff are proud to work for and that makes a real difference to Jersey.
- To ensure that Jersey is recognised on the European international stage as well regulated jurisdictions, both now and once the EU Regulation is implemented.

What we want to achieve

- To raise the profile of information governance, highlighting the role it plays in successful organisations while protecting the privacy of the individuals with which the organisation deals.
- To ensure that all those that handle personal information do so lawfully and responsibly.
- To encourage government organisations to embrace openness and transparency in all their activities whilst respecting an individual's right to privacy.
- To ensure that individuals are aware of their information rights and are confident in exercising them.
- To provide an effective and efficient registration service that is consistent throughout Jersey.
- To ensure there exists a mechanism for purposeful, targeted and meaningful regulatory activity.
- To reach a point where information rights are embedded in new laws, technology and public policy.
- To be a model of good regulation;
 - Transparent
 - Accountable
 - Proportionate
 - Consistent
 - Targeted
 - Independent

Operational Performance

Complaints



A total of 89 data protection related complaints were recorded in Jersey during 2017, representing a 71% increase on the 52 complaints recorded in 2016. As expected, Jersey's biggest business sectors received the most complaints, but there has been a notable increase in the number of complaints involving the health sector.

Complaints about poor data security saw a significant rise from the previous year, however the pattern of complaints broadly follows a similar trend to 2016, which is undoubtedly a reflection of heightened awareness of the Law and numerous campaigns off and on island regarding 'cyber security'

A perceived lack of compliance with the rights of data subjects whilst an area of concern for individuals, has decreased from the previous year. Organisations should have clear procedures in place regarding subject access requests, covering such areas as the acknowledging of requests, the identification of relevant personal data and responding in a timely manner. Organisations should also be aware that existing timescales are subject to change in 2018 and take this opportunity to review processes accordingly.

Unfair processing still represents just over a third of annual complaints, indicating that organisations should be very aware of fair processing and data subjects understanding of processing.

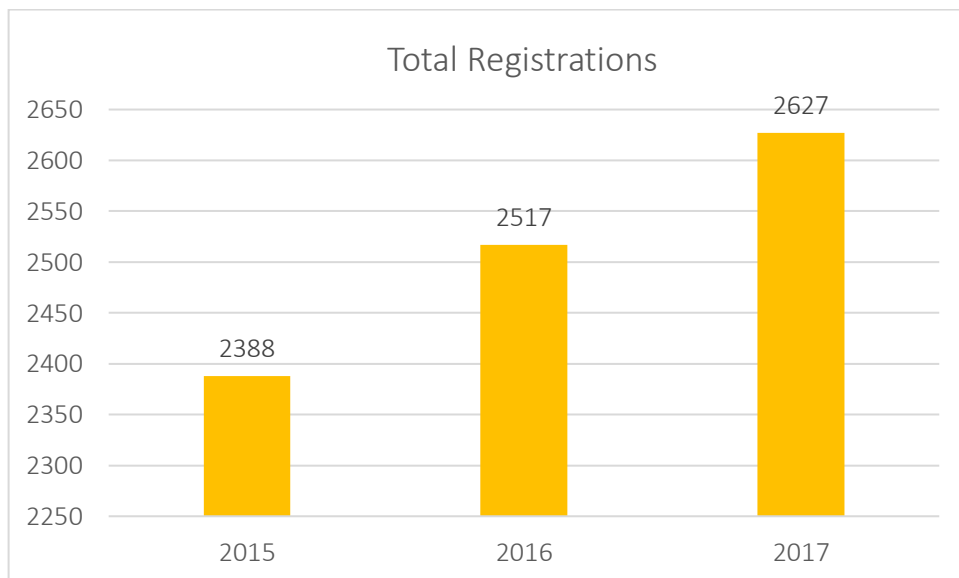
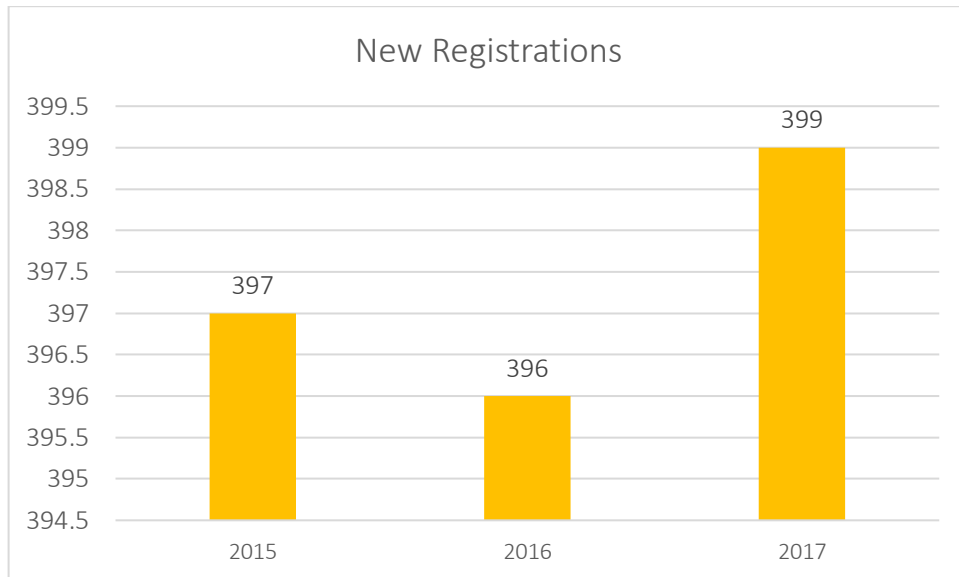
Breach Reporting

It is of note that whilst there was no requirement to notify the Office of a data breach, we regularly received such reports and, where appropriate, provided guidance as to next steps that an organisation should consider if an incident occurs. A key feature of the new data protection reform is mandatory breach reporting with organisations being compelled to report a data breach within 72 hours of discovery and it is encouraging to see organisations embracing this reporting requirement in advance and putting in place processes and procedures to capture issues and deal with them appropriately. This self-reporting also accounts for the increase in data security issues dealt with compared with 2015 and gives something of an indication as to how the reform will have an impact on this Office.

We recognise that breach reporting will be an additional duty for data controllers under the new Laws. It is our aim to ensure the process is as straight forward as possible whilst ensuring meaningful engagement and the highest levels of data security. Work has started to plan a new reporting system for our own Office and we are talking to government and the Jersey Financial Services Commissions to ensure a consistent approach in this area.

We are clear that we want breach reporting to be viewed as positively as possible by all parties; it will provide the regulator with accurate information about data security incidents and allow organisations affected to enter its constructive communications aimed at support and learning. Whilst there may be occasions where regulatory action is taken because of a breach, any punitive sanctions will be targeted based on non-compliant activity that is deliberate, wilful, negligent, repeated or particularly harmful. Failure to report a breach that comes to our attention later will also carry with it the risk of formal sanction.

Registrations



With regard to registrations, Jersey recorded an increase in both the number of new registrations received and the total of live registrations active at the end of 2017.

Guidance

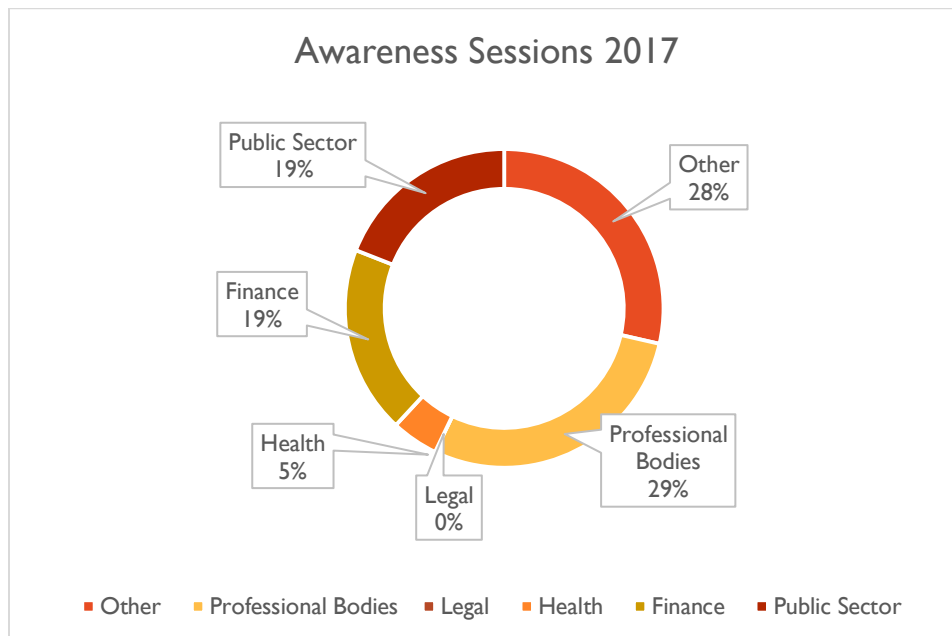
Guidance documents

Following the review and updating of our guidance notes in 2015 and 2016, we dedicated more time formulating the help and guidance relating to Data Protection (Jersey) Law 2018; exploring a bespoke website option, designing and publishing easy to read guides and publications.

Awareness sessions

The Deputy Commissioner and staff are regularly invited to undertake speaking engagements and provide awareness sessions to industry representatives and professional bodies. During 2017, a total of 21 sessions were delivered to a mix of audiences in Jersey.

The increase in awareness sessions gradually rose throughout the year – ranging from simple talks to the general public to detailed, technical seminars to industry.



Enforcement

No formal undertakings were issued in 2017 in relation to complaints. We were able to help guide all of the 89 cases to closure without the need of enforcement action being pursued by the Commissioner, either through enforcement notices or formal undertakings.

It remains the case that much of the workload relates to general enquiries, the breadth and depth of which varies significantly. Where formal complaints are made we make every effort to work with all parties towards a successful resolution. We recognise that this is not always possible, and we have observed an increase in cases where there are complex interlinked issues regarding employment grievances or legal proceedings in a family or civil context. Such matters are very resource-intensive and highlight the need for careful consideration of Data Protection (Jersey) Law 2018 obligations for our Offices.

International liaison

Representatives of the Office of the Information Commissioner attended two conferences in 2017. The Deputy Commissioner benefited from the International Conference of Data Protection and Privacy Commissioners in Hong Kong.



The Commissioner and the Director of Policy and Compliance attended the British, Irish and Islands' Data Protection Authorities (BIIDPA) meeting which was held in Gibraltar.

Discussions at these meetings are informal in nature and provide the right platform for the exchange of useful information to ensure a consistent approach to the treatment of issues that are of common interest. For a number of years now, Jersey has played an active role in discussions between the British, Irish and Islands' Data Protection Authorities. Representatives of the regulators from the UK, Ireland, the Jersey, Guernsey, the Isle of Man, Gibraltar, Malta and Cyprus meet annually to discuss the challenges facing each jurisdiction, to share best practice and ensure cooperation where appropriate.

The Director of Policy and Compliance also benefited from attendance at the Global Privacy Enforcement Network (GPEN) The Privacy Enforcement Network was established to foster cross-border co-operation among privacy authorities.

European Developments

The European Commission put forward its EU Data Protection Reform Package in January 2012. More than 90% of Europeans say they want the same data protection rights across the EU – and for these rights to apply regardless of where their data is processed.



The General Data Protection Regulation (GDPR) is viewed as an essential step to strengthen citizens' fundamental rights in the digital age and facilitating business by simplifying rules for companies in the Digital Single Market. A single law will also do away with the current fragmentation and costly administrative burdens. The Directive for the police and criminal justice sector protects citizens' fundamental right to data protection whenever personal data is used by criminal law enforcement authorities. It will in particular ensure that the personal data of victims, witnesses and suspects of crime are duly protected and will facilitate cross-border cooperation in the fight against crime and terrorism.

On 15 December 2015, the European Parliament, the Council and the Commission reached agreement on the new data protection rules, establishing a modern and harmonised data protection framework across the EU. The European Parliament's Civil Liberties Committee and the Permanent Representatives Committee (Coreper) of the Council then approved the agreements with large majorities. The agreements were also welcomed by the European Council as a major step forward in the implementation of the Digital Single Market Strategy.

On 8 April 2016, the Council adopted the Regulation and the Directive. In addition, on 14 April 2016, the Regulation and the Directive were adopted by the European Parliament.

On 4 May 2016, the official texts of the Regulation and the Directive were published in the EU Official Journal in all the official languages. While the Regulation will enter into force on 24 May 2016, it shall apply from 25 May 2018. The Directive enters into force on 5 May 2016 and EU Member States have to transpose it into their national law by 6 May 2018.

This included introduction of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). It also included Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. Jersey has committed to implementation of the requirements of both the Regulation and the Directive in 2018.

Privacy Shield Overview



The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce, and the European Commission and Swiss Administration, respectively, to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce. On July 12, 2016, the European Commission deemed the EU-U.S. Privacy Shield Framework adequate to enable data transfers under EU law (see the adequacy determination). On January 12, 2017, the Swiss Government announced the approval of the Swiss-U.S. Privacy Shield Framework as a valid legal mechanism to comply with Swiss requirements when transferring personal data from Switzerland to the United States.

The Privacy Shield program, which is administered by the International Trade Administration (ITA) within the U.S. Department of Commerce, enables U.S.-based organisations to join one or both of the Privacy Shield Frameworks in order to benefit from the adequacy determinations. To join either Privacy Shield Framework, a U.S.-based organisation will be required to self-certify to the Department of Commerce and publicly commit to comply with the Framework's requirements. While joining the Privacy Shield is voluntary, once an eligible organisation makes the public commitment to comply with the Framework's requirements, the commitment will become enforceable under U.S. law. This is an area we expect to come under increasing scrutiny and key developments will be added to the news pages of the Offices' websites.

Freedom of Information

The Freedom of Information (Jersey) Law 2011 provides public access to information held by Scheduled Public Authorities (SPAs). It creates a legal basis that entitles members of the public to request information from SPAs. The Law covers any recorded information that is held by a SPA in Jersey. SPAs are listed within Schedule 1 of the Law as:

- The States Assembly including the States Greffe
- A Minister
- A committee or other body established by resolution of the States or by or in accordance with standing orders of the States Assembly
- A department established on behalf of the States
- The Judicial Greffe
- The Viscount's Department
- Andium Homes Limited (registered as a limited company on 13th May 2014 under Registration number 115713).
- The States of Jersey Police Force
- A Parish (effective from 1st September, 2015)

Recorded information includes printed documents, computer files, letters, emails, photographs, and sound or video recordings. It is defined in the Law as meaning 'information recorded in any form.'

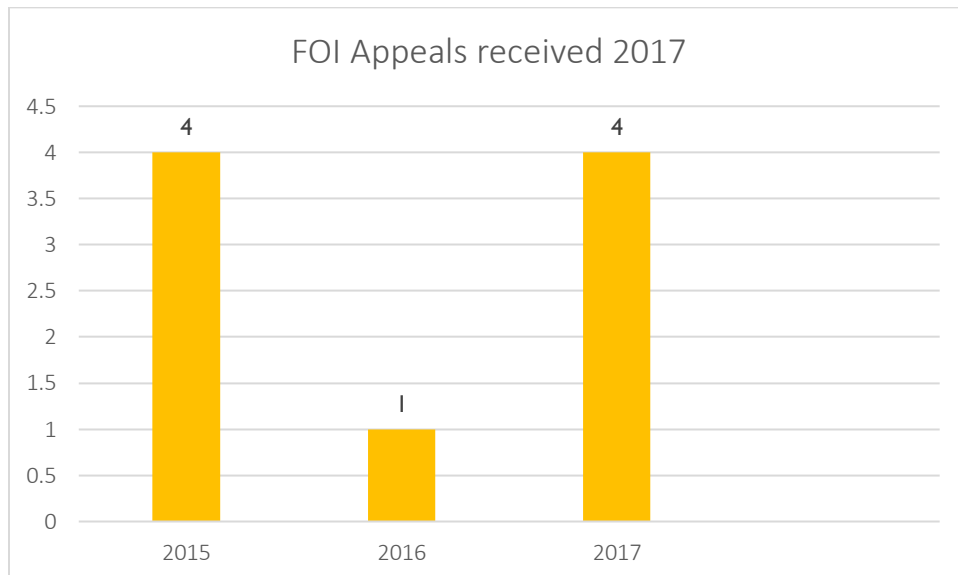
The Law does not give people access to their own personal data (information about themselves) such as their health records or credit reference file. If a member of the public wants to see information that a SPA holds about them, they are directed to make a subject access request under the Data Protection (Jersey) Law 2005.



The Law came into force on 1 January 2015. A total of 736 requests were received by the Central FOI Unit during 2016 and 809 requests in 2017. Representing a 9.9% increase between 2016 and 2017. Responses to FOI requests are published on the States of Jersey website

(www.gov.je/Government/FreedomOfInformation/Pages/index.aspx).

In respect of the Office of the Information Commissioner, four appeals under the Freedom of Information (Jersey) Law 2011 were submitted to the Commissioner during 2017, the same number from the first full year of FOI.



It is noted that whilst there was a 6.5% increase in the total annual number of FOI requests received between 2015 (691) and 2016 (736) the number of formal appeals to the Commissioner fell from four in 2015 to one in 2016. In considering the low number of appeals, the Commissioner supports the view of this being partly influenced by greater communication between requestors and SPAs as well as greater public awareness of the Law. In addition, this also reflects the work of both the central FOI Unit and the Office towards increased transparency across scheduled public authorities.

The Commissioner is also aware of the intention to consider amendment and further development of the Law and looks forward to an opportunity to contribute towards this work for the benefit of the public and increased transparency of government. However, in doing so, it should be recognised that any amendment and development may result in the need for discussion regarding the resourcing and skilling of FOI practitioners engaged across the process.

In final consideration of the FOI Law it has to be noted that significant effort is extended by the Commissioner's staff in providing informal advice and assistance to both members of the public and SPAs at various stages of the FOI process prior to any formal appeal. This includes time taken for discussion, advice and mediation aimed at provision of information to the public along with greater public understanding of the machinery and workings of government. Whilst such work cannot necessarily be easily recorded, the benefits are recognisable in increased public awareness and improved transparency, which is to be welcomed.

Financial Information

	<u>2016</u>	<u>2017</u>
<u>Income</u>		
Registry Fees	125,452	125,519
Guernsey Recharge	105,968	67,057
Total Income	231,420	192,576
Contribution from the States of Jersey	308,900	399,700
Net Income	540,320	592,276
<u>Operating Expenses</u>		
Manpower costs		
Staff Salaries, social security & pension contributions	356,128	360,413
Supplies & services		
Total costs (to include but not limited to)	125,462	163,250
IT development, maintenance & software		
Books & publications		
Legal fees		
Conference & training fees		
Pan-Island Travel		
Meals & entertainment		
Public Relations		
Public Relations	768	0
Administrative costs		
Total costs (to include but not limited to)	11,227	12,040
Printing & stationery		
Telephone charges		
Postage		
Other administrative costs		
Premises & maintenance		
Total costs (to include but not limited to)	43,976	44,252
Utilities (incl. electricity & water)		
Rent		

ANNUAL REPORT 2017

Finance costs

Finance costs	2,759	11,758
---------------	-------	--------

Total operating costs

	540,320	591,713
--	---------	---------

Excess of income over expenditure

0	563
---	-----

One Liberty Place
St. Helier
Jersey
JE2 3NY

Tel: 01534 716530

www.oicjersey.org



OFFICE OF THE
INFORMATION
COMMISSIONER