information commissioner

Barrantagh Fysseree

Annual Report 2018-2019

GD 2019/0088

CONTENTS

THIS PAGE IS BLANK

Foreword

This report covers the period from 1st April 2018 to 31st March 2019.

The year saw the most significant change to data protection legislation throughout Europe since the EU Data Protection Directive was agreed in 1995.

On 25th May 2018 the EU General Data Protection Regulation 2016/679 (GDPR) and the associated EU Police and Criminal Justice Directive 2016/680, known as the Law Enforcement Directive (LED), came into full operation.

In addition, modifications to Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, (the original data protection instrument dating from 1981) were agreed and Treaty No. 223, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, was opened for signature on 10 October 2018. The UK signed the treaty on the same date.

Whilst the GDPR applies to the 31 EEA states, Convention 108 applies to all European states and has extended to the Island since 1991. States outside of Europe can also ratify the Convention.

Versions of the GDPR and LED were applied to the Island by Orders made under the Data Protection Act 2018. The Applied GDPR and Applied LED came into force in the Island on 25 May 2018 and were followed by the GDPR and LED Implementing Regulations 2018 which came into operation on 1st August 2018.

Throughout the year, my Office has continued to give presentations and talks to various businesses organisations and associations in the Island. A range of guidance documents, have been produced and are available from our website and we continue to advise of developments via the website and social media.

We have observed adverse comment about the GDPR including claims that the GDPR was the reason why something did not occur or conversely why some action was taken. The GDPR is an evolution of laws that have existed for over 30 years and there has been little change to the basic principles, however the GDPR now provides supervisory authorities with powers to enforce the legislation.

The truth, therefore, is that a controller seeking to blame the GDPR was either not compliant with existing legislation or is using the GDPR as an excuse for its own failings.

While agreement to recruit a further three staff has been obtained, the Office continued to operate with a total of 4 staff, including the Commissioner. It has been a hectic year and I am indebted to my staff who have worked hard in challenging circumstances to effect the changes brought about by the new legislation and to manage the resultant increased work load.

Iain McDonald
Information Commissioner

RESPONSIBILITIES

DATA PROTECTION ACT 2018

The Data Protection Act 2018 ('the Act'), came into operation on the 15th May 2018.

The Act provides for Council of Ministers to make Orders to apply certain data protection EU instruments to the Island by Order and in doing so make any necessary implementing Regulations.

The following Orders and Regulations have been made:-

Data Protection (Application of the GDPR) Order 2018 (SD2018/0143)
Data Protection (Application of the LED) Order 2018 (SD2018/0144)
Data Protection Act 2018(Appointed Day) Order 2018 (SD2018/0142)

GDPR and LED Implementing Regulations 2018 (SD2018/0145)
Data Protection (Fees) Regulations 2018 (SD2018/0169)
GDPR AND LED Implementing Regulations (Amendment) Regulations 2018 (SD2018/0309)

APPLIED GDPR

The Applied GDPR is set out in the Annex to Data Protection (Application of the GDPR) Order 2018. In effect, it gives force to the provisions of the EU's GDPR but has a number of modifications and redactions that were necessary to give proper effect in the Island.

The Applied GDPR applies to the processing of personal data by most entities (controllers) and also third parties (processors) who process data on behalf of a controller.

APPLIED LED

The Applied LED is set out in the Annex to Data Protection (Application of the LED) Order 2018. The Order gives force to the provisions of the EU's LED but with a number of modifications and redactions necessary to give proper effect in the Island.

The Applied LED only applies to the processing of personal data for the purposes of crime prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties by certain competent authorities.

GDPR AND LED IMPLEMENTING REGULATIONS

The GDPR and LED Implementing Regulations are subordinate to the Applied GDPR and Applied LED.

Amongst other things, the regulations define a number of offences and set out the provisions for registration, the enforcement powers of the Commissioner, the purposes for processing special category personal data and the circumstances when the rights of a data subject may be restricted (exemptions) when necessary and proportionate to do so.

UNSOLICITED COMMUNICATIONS REGULATIONS 2005

The Unsolicited Communications Regulations 2005 ('Regulations') came into force in October 2005. 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.

However, the Schedule to these Regulations modified the Data Protection Act 2002 to provide the Commissioner with powers to enforce the Regulations. With the coming into operation of the GDPR and Implementing Regulation 2018 on 1st August 208 the Data Protection Act 2002 was repealed which has resulted in the Commissioner having no powers to enforce the Regulations.

An amendment Order is expected to be made before the end of 2019 to rectify the problem.

The Commissioner's advice with regard to direct marketing can be found at:-
https://www.inforights.im/organisations/direct-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.

FOI now extends to all Government Departments and Statutory Boards, Local Authorities, certain publicly-owned companies and other public authorities including:- HM Attorney General's Chambers, the Chief Constable, the Clerk of Tynwald, General Registry, Industrial Relations Officers, The Manx Museum, Public Services Commission, Road Transport Licensing Committee and the Information Commissioner.

A person dissatisfied with the response of a public authority to a request for information may make a complaint to the Commissioner. As expected, few complaints under FOI legislation have been made in the past 12 months. The decisions of the Commissioner can be found at:-
https://www.inforights.im/organisations/freedom-of-information/decision-notices/

No decision has been appealed to the High Court.

Good practice advice as well as guidance foR public authorities can be found at:-
https://www.inforights.im/organisations/freedom-of-information/good-practice-advice/
https://www.inforights.im/organisations/freedom-of-information/guidance-for-public-authorities/

CODE OF PRACTICE ON ACCESS TO GOVERNMENT INFORMATION 1995

The Commissioner also has oversight of the Code of Practice.

No complaints under the Code of Practice have been made to the Commissioner.

LEGISLATION & CODES OF PRACTICE

The full list of legislation for which the Office is responsible is shown below. Electronic copies together with case law and other relevant instruments are available from the Commissioner's web site at: www.inforights.im

DATA PROTECTION

Data Protection Act 2018

Orders and Regulations
Data Protection (Application of the GDPR) Order 2018 (SD2018/0143)
Data Protection (Application of the LED) Order 2018 (SD2018/0144)
Data Protection Act 2018(Appointed Day) Order 2018 (SD2018/0142)

GDPR and LED Implementing Regulations 2018 (SD2018/0145)
Data Protection (Fees) Regulations 2018 (SD2018/0169)
GDPR AND LED Implementing Regulations (Amendment) Regulations 2018 (SD2018/0309)

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

Data Protection Legislation

In brief the new data protection legislation requires a controller to comply with the principles and the rights of data subjects set out in the Applied GDPR. Detailed guidance is available from the website at www.inforights.im

The Principles of Data Protection

There are 7 principles set out in Article 5 of the Applied GDPR.

Six principles which apply to the processing of personal data:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality

and an overarching principle of **'accountability'** which requires a controller to be able to demonstrate compliance with the personal data processing principles.

Rights

The rights of individuals, set out in Articles 13 - 22 of the Applied GDPR, are:

- Right to information about processing
- Right of access
- Right to rectification
- Right to erasure ('right to be forgotten')
- Right to restriction of processing
- Right to data portability
- Right to object to processing

General rules applying to the rights

- Controllers must "facilitate" individuals to exercise their rights.
- A Controller must comply with a right "without undue delay" and usually within ONE month of receipt of the request.
- In most cases no fee can be charged.

ACTIVITIES

DATA PROTECTION

Raising Awareness/ Training

During the year both the Commissioner and Deputy have provided numerous presentations to a range of associations including:-

- Association of Isle of Man Compliance Professionals
- Chamber of Commerce
- Chartered Insurance Institute
- Institute of Directors

Presentations were also made to smaller specialist groups.

Advice and Guidance

All guidance produced is made available on our 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 reviewed and amended to reflect case law, emerging views and technology changes. We provide updates via a RSS news feed.

In the past year, the time available to produce guidance has been limited due to case workload. When possible we have focused on providing new guidance on pages on the website.

Current guidance includes:-

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

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
A closer look at Transparency

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

Registration

Under the Data Protection Act 2002, the Commissioner was responsible for the maintenance and administration of the Register of Data Controllers. Prior to 1st August 2018, there were 2109 entries in that register.

Under the GDPR and LED Implementing Regulations 2018, the Commissioner became responsible for the maintenance and administration of a new Register of Controllers and Processors. This is a basic register which simply identifies the controller or processor, states their nature of business, any trading names and websites and provides contact details.

The new data protection legislation also provided a transitional period, up to 31st January 2019, which permitted a Data Controller to choose either to make a new application to the new register or renew its entry in the Register of Data Controllers.

In advance of 1st August 2019, the Office has had to specify, create and test the new register, create documentation and on line application forms and correspondence for new applications and subsequent renewals while continuing to manage and maintain both registers. This work was completed "in house" and on time with assistance from GTS to build the database.

The system, processes and procedures including documentation have undergone a number of refinements over the year but, in general, the system has worked well. There have been a few negative comments but there have also been numerous positive comments.

By 31st July 2019, there were in excess of 2000 entries in the new Register with approximately 500 entries remaining in the old Register. The old Register will close on 31st January 2020.

Direct comparisons between the Registers is not possible due to a difference in exemptions from registration requirements and that processors are now also required to register. However it seems there are several hundred new entries which also suggest that the GDPR awareness initiatives undertaken by the Office over the previous years have worked.

Personal Data Breaches, complaints, investigations, etc.

Whilst the period of this report is up to 31st March 2019, in order to give a picture of the effect of the new data protection legislation the following table sets out the number of matters the Office has handled in the 12 months since the data protection legislation came into force.

Matter	Number made
Personal data breaches	208
Data Protection infringement complaints	60
Data Protection Investigations	2
Data Protection Impact assessments	5
Information Notices issued	3
Enforcement Notices issued	1
Reprimands	9
Appeals to Data Protection Tribunal	2
FOI decision notices	6
Code of Practice decisions	0

Personal data breaches

This is a new provision in the data protection legislation.

The nature of breaches reported have ranged from a breach affecting one individual to a breach affecting several thousand and involving multiple jurisdictions.

The primary purpose of personal data breach notification is to prevent or mitigate harm to an individual as a result and notification to the Commissioner, who has independent oversight, ensures a controller does take appropriate action. Considering and responding to a personal data breach notification is therefore prioritised by the Office. This work consumes a considerable amount of staff resource on a daily basis.

In most cases controllers do take appropriate action to prevent harm without the need for the Commissioner to order action to be taken.

However personal data breach reports also reveal poor practice and infringement of data protection legislation. These are considered further after any harm issues have been prevented or mitigated. On two occasions, investigations have been undertaken as a result of the gravity of the infringements.

Data Protection infringement complaints

The advent of the GDPR has resulted in the public becoming more aware of their data protection rights. In particular individuals are exercising their right of access to personal data.

This is reflected in the number of complaints made to the Office which is almost double the previous year. Approximately 60 % of complaints received concern the right of access to personal data.

In general, controllers do co-operate with the Commissioner as they are required to do by Article 30 of the Applied GDPR. However, on three occasions it was necessary to issue Information Notices and on one occasion an Enforcement Notice.

Data Protection impact assessments

This is a new provision in the data protection legislation.

Where new processing of personal data is likely to result in a high risk to individuals, a controller must undertake a data protection impact assessment (DPIA) and consult the Commissioner.

The five DPIAs received during the year came from public bodies. The Commissioner has eight weeks to consider the DPIA and provide written advice. The Commissioner has given advice that has resulted in changes to proposed processing. On one occasion the Commissioner advised that the proposed processing would infringe the legislation.

The DPIA and resultant consultation process does require significant resource to consider and provide appropriate written advice, but has proven useful in preventing infringements and unnecessary harm to individuals.

Appeals to Data Protection Tribunal

There is a new provision in the Regulations that provides for a person to make a complaint to the Data Protection Tribunal if they believe the Commissioner has not taken appropriate steps to investigate a complaint. Such Appeals are free of charge and it is inevitable that when the Commissioner does not uphold a complaint that a person may seek to Appeal to the Tribunal and it is right that a complaint procedure does exist.

One such Appeal has been made during the year. In all Appeals, as set out in the Tribunal Rules, the burden of proof lies with the Commissioner. Several days were spent responding to the Appeal. The Tribunal found that the Commissioner had taken appropriate steps to investigate the complaint.

An Appeal against an Information Notice was also made to the Tribunal which also took several days to respond to. The Appeal was subsequently withdrawn.

The Tribunal Rules have not been updated to reflect the provisions of the new data protection legislation. These Rules do need to be updated and in the opinion of the Commissioner should provide for an Appellant to demonstrate substance to an Appeal before the Commissioner is required to respond.

FREEDOM OF INFORMATION : REVIEW OF DECISIONS

In the period from 1st August 2018 to 31st July 2019, the Commissioner received 6 requests to make a decision pursuant to section 42 of the Freedom of Information Act 2015.

The decision notices can be found at:

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

CODE OF PRACTICE ON ACCESS TO GOVERNMENT INFORMATION

No matter was referred to the Information Commissioner under the code of practice in the period.

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

As a result of the new data protection legislation the Commissioner has approval to recruit a further 3 full time staff, a senior Compliance Officer at HEO analogy and 2 Compliance Officers at EO analogy. Staff will be recruited over the next twelve months.

PREMISES

The Office now occupies the whole of the first floor of Prospect House. During the year the floor was upgraded to provide space for additional staff, a meeting/training room and an interview room.

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.

In 2018, it was the Isle of Man's turn to host the annual Island Data Protection Authorities meeting. This was held in the I Museum and was attended by colleagues from the UK, Ireland, Gibraltar, Channel Islands and Malta. The GDPR, LED Adequacy and Brexit were the main items of discussion. Representative of the UK DCMS took part via conference call in some of the Brexit discussions.

The Commissioner and Deputy took part in a presentation made by the Common Thread Network (data protection authorities in the Commonwealth) to the Commonwealth Heads of Government meeting in London. The Commissioner is a member of the Common Thread Network which has the aim of assisting the development of data protection throughout the Commonwealth.

Officers attended the European Data Protection Authorities Spring Conference in Albania.

The closed session of the International Data Protection Authorities Conference was held in Brussels but the Commissioner was not represented.

In addition to the above, the Commissioner is a member of the Global Privacy Enforcement Network A number of issues of common interest are discussed between GPEN members via conference calls and on a dedicated website.

FINANCIAL REPORT

The figures for the financial years 2018-2019 and budget for 2019 -2020 are as follows:

	2018 - 2019			2019-2020
	Budget	Actual		Budget
Income	(£'s)	(£'s)		(£'s)
New notification fees	8,000	61,160		134,900
Renewal fees	80,080	55,200		134,900
Other income		117		
Total Income	88,080	116,477		269,800
Revenue Expenditure				
Employee Costs	248,953	245,865		372,994
Infrastructure Expenses	0	0		0
Supplies and Services	24,206	18,779		46,806
Total Expenditure	273,159	264,644		419,800
Net Figure	185,079	148,167		250,000

The variance in actual income from budgeted income for 2018/19 is due to the budget figures being set prior to the effect of the new data protection legislation registration provisions. The "New notification fees" total is higher as many Controllers opted to be registered on the new Register of Controllers and Processors rather than renew their existing entry on the Register of Data Controllers.

The budget income for 2019/20 is dependent upon a revised Fees Order being made and approved. To date no such Order has been made. The Commissioner provided a fees proposal in early 2018. The lack of income will be offset by the fact that additional staff have not as yet been recruited.

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 be to introduce new staff so that the Office can commence effective monitoring of compliance with the data protection legislation and provide more guidance, via the website and in person, for controllers and processors.