

Annual Report

2018

For the period 25 May 2018 – 31 Dec 2018



Contents

Foreword	2
Introduction	3
About the Authority	4
Organisational chart	5
Strategic aims	6
Strategic activity – highlights	7
Case studies	9
Key statistics	11
Appendix 1: Reform and governance strategic activity details	12
Appendix 2: Regulatory approach strategic activity details	14
Appendix 3: Raising awareness strategic activity details	17
Appendix 4: Relationships strategic activity details	19
Appendix 5: Members’ Report and Audited Financial Statements	21

Foreword

A flying start. Elaborating those three words, this first Annual Report sets out what has been achieved on the journey to the establishment of an effective independent Data Protection Authority for the Bailiwick of Guernsey.

25 May 2018 saw two events on the same start date. The coming into force of a new and complex Law, based on the EU's General Data Protection Regulation. And the creation – to use the language of GDPR - of a new Supervisory Authority. An ambitious programme for any jurisdiction. Simultaneously, the challenges of getting to grips with new rights for individuals, new requirements for those processing personal data and new regulatory powers and duties. Plus the strategic, governance, financial and administrative responsibilities involved in setting up any new organisation.

This has also been a time of massive cultural change as data protection has globally come of age. There can be very few who do not now recognise the absolutely central role of data – the 'new oil' – in all aspects of economic and governmental activity and in the social well-being of all citizens. Technology has brought many benefits and these will continue and will accelerate. But the risks – of harm to individuals and of societal harm – have also increased and go to the very heart of how we live our lives. Data protection seeks to minimise those harms, while not stifling beneficial innovation.

The ODPA has numerous new responsibilities and we are seeking to make the best possible use of the carrots and sticks available to us. As teachers, we must educate. As police-officers, we must enforce the law. And as referees, we must deal with complaints. In broad terms we want to help those who want to get things right, but be tough on those who do not.

Challenges still lie ahead. A new team has to get to full strength. Many parts of the Law have yet to be tested. We do not yet find ourselves on a firm financial footing. There are still those who have yet to understand the crucial role of data protection for the prosperity of financial services and other enterprises based in the Bailiwick. Public bodies are having to change. Above all this, the European Commission's imminent assessment of the 'adequacy' of the Bailiwick's data protection regime will present a day of judgment.

We are on our way and – as this report spells out – a huge amount has been achieved. I pay tribute to the excellent members of the Authority's Board who bring a wealth of experience and insight. And the whole Bailiwick is extremely fortunate to have Emma Martins as its Commissioner, leading a carefully-selected team of such obvious talent and commitment.

Richard Thomas CBE, Chair, The Data Protection Authority (Bailiwick of Guernsey)

Introduction

I am pleased to present this Annual Report for the Office of the Data Protection Authority for the period 25 May – 31 December 2018 in accordance with the requirements of Schedule 6, para.13 of *The Data Protection (Bailiwick of Guernsey) Law, 2017*.

The General Data Protection Regulation came into effect across the European Union on 25 May 2018. On the same day, our own equivalent legislation came into effect for the Bailiwick. It marked what was probably one of the most significant dates in the history of data protection; not just for the Bailiwick or Europe, but globally. The data economy is increasingly borderless and the reach of this enhanced regulatory framework goes well beyond national or geographical borders.

The commitment to a continued high-quality regulatory environment for data is important to ensure the free flow of data necessary for business, as well as enhanced individual rights; both of which are key for economic success and social justice for the Islands in this digital era.

The comprehensive reform programme to ensure the Bailiwick is able to meet these new standards was well underway at the time the new legislation took effect and has continued to make good progress. With the new Chair and Authority Members already in place, the inaugural Authority meeting was held on the 25 May 2018.

Shortly after that we relocated to new office accommodation which provides sufficient space for the required additional members of staff as well as a board room which is also used as a small events space, supporting the delivery of our communications programme.

With independence such a crucial requirement of the new Authority, we moved away from reliance on government for financial administration, budgeting, audit and HR to ensure the Authority has autonomy in these areas. The first full financial audit is due in 2019.

We have thought carefully about our overall direction and are developing a strategic plan from which all our activities will flow. We will perform our duties with clarity about our wider strategic direction and how we can enhance the Bailiwick's reputation.

Whilst it is the case that the regulated community need to commit to delivering on the new legal standards, it is also the case that we, as the regulator, need to commit to delivering on our obligations in an accountable, fair and consistent matter. The long-term funding model for the office is yet to be agreed, but whatever model the States of Guernsey settle on, we will continue to build the regulatory office constantly mindful of the need for us to make effective use of our resources. The breadth and depth of data protection regulation means that we have to regulate in a smart way if we are to secure good outcomes. We are consciously targeting resources at actively engaging with and supporting the regulated community, and we are working towards launching several initiatives in 2019, including drop-in sessions for local businesses, a free events programme, study visits, and a schools programme.

In seeking to embed a culture of data protection into the Islands, we want to leverage the opportunities that present themselves in this data driven economy without compromising on the highest standards of data protection. Against the global backdrop of economic and political uncertainty, we want to ensure that the Bailiwick maintains a high-quality, stable and forward-looking regulatory environment which recognises that innovation and good governance are mutually dependent.

Lastly, I want to thank my team who have worked so tirelessly and with such commitment and focus. We are extremely fortunate to have an exceptionally experienced Chair and Authority Members who have already contributed so much in ensuring we are a fit for purpose regulatory office that supports our jurisdiction's social and economic wellbeing. The task in hand is considerable and I am extremely proud of the progress that has been made. All data protection authorities are faced with an environment of unprecedented social and technological change. The need for us to fulfil our role with independence and integrity has never been greater.

Emma Martins, Data Protection Commissioner (Bailiwick of Guernsey)

About the Authority

The Office of the Data Protection Authority (ODPA) is the independent regulatory authority for the purposes of *The Data Protection (Bailiwick of Guernsey) Law, 2017* and associated legislation.

The Law creates the independent Data Protection Authority which is tasked with the development and implementation of the new regulatory regime necessary to oversee the requirements of the Law. Comprising a Chair and between four and eight Members, the Authority provides governance to the Office of the Data Protection Authority (ODPA).

The ODPA is the operational body that carries out the regulatory functions of the Law delegated by the Authority. These include recording data breaches, investigating complaints, running education programmes and examining proposed legislation and how it may affect individual privacy. The ODPA strives to empower individuals to exercise their rights as well as to support organisations to meet their compliance requirements and take action where they fall short.

The Office of the Data Protection Authority:



Empowers individuals and protects their rights



Promotes excellence in data protection

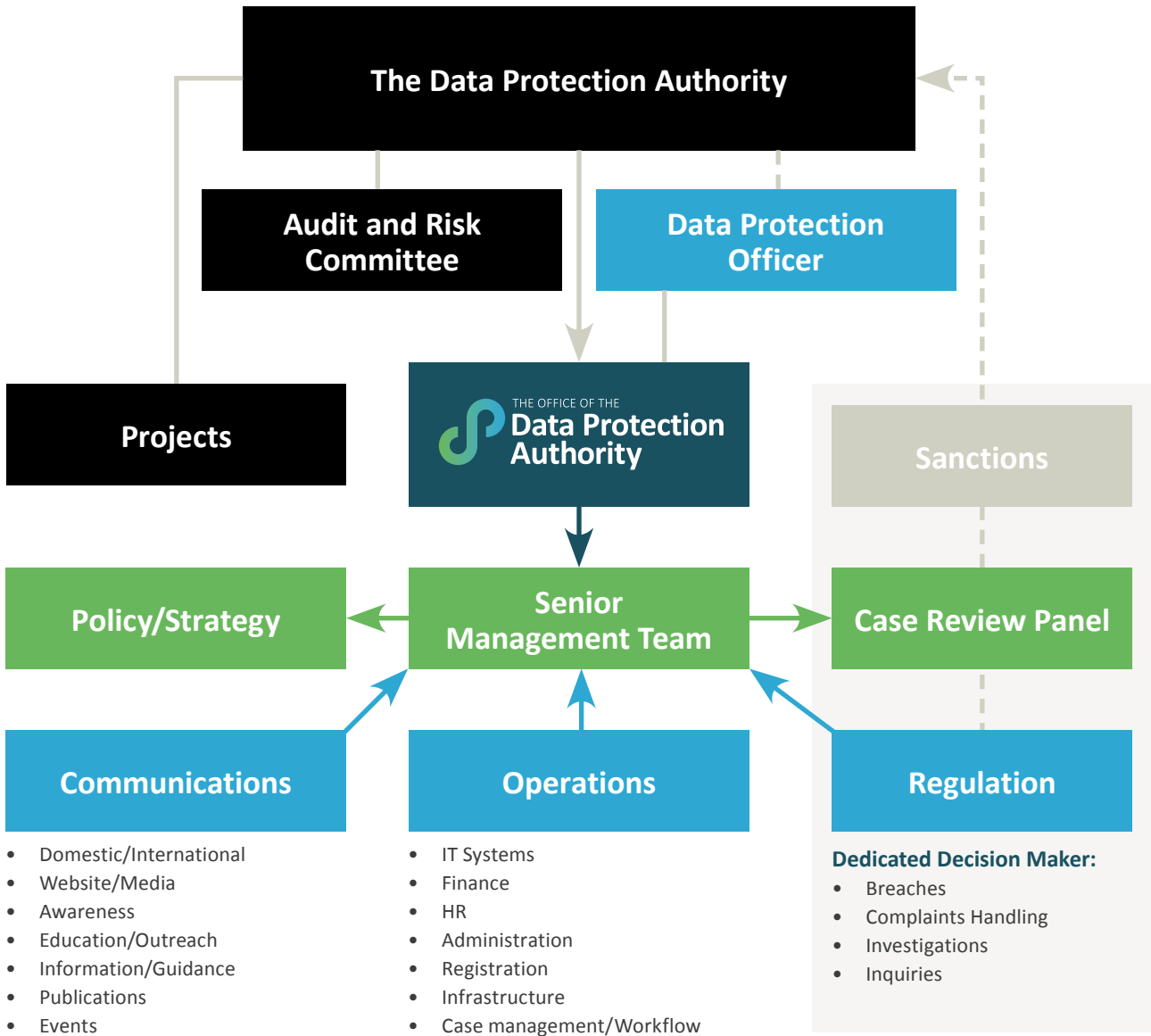


Supports the data economy to embrace innovation



Regulates data protection legislation through an ethics-based approach

Organisational chart



The Data Protection Authority

- Chair – Richard Thomas CBE
- Voting Member – John Curran
- Voting Member – Christopher Docksey
- Voting Member – Simon Entwisle
- Voting Member – Mark Lempriere
- Voting Member – Jennifer Strachan
- Commissioner as *ex-officio* and non-voting Member – Emma Martins

The Office of the Data Protection Authority

- Chief Executive / Data Protection Commissioner – Emma Martins
- Deputy Commissioner – Rachel Masterton
- Chief Operating Officer – Tim Loveridge
- Office Manager – Mike Appelqvist
- Operations and Compliance Manager – Lawrence West
- Communications Manager – Leanne Archer
- Executive Officer – Lesley Le Bailly

Strategic aims

For the purposes of this report we present the ODPa's strategic aims for 2018 across four themes:

1. Reform and governance

- 1.1. We will play an integral part in the successful reform of the Bailiwick's data protection regime, ensuring enhanced rights for our citizens as well as continued 'adequacy'.
- 1.2. We will work to support the creation of a robust and effective governance structure including supporting the constitution of the new Authority and associated financial and operational control mechanisms for our Office.

2. Regulatory approach

- 2.1. We will ensure, through effective structuring and resourcing of our Office, that we are capable of delivering our statutory requirements, demonstrating the highest standards of data protection regulation for the Bailiwick.
- 2.2. We will ensure regulatory action is targeted, proportionate and fair in the knowledge that most organisations want to do the right thing.
- 2.3. We will adopt a risk-based approach to deliver cost-effective outcomes. This will be done in the knowledge that choices have to be made because of resource pressure and we commit to making those decisions intelligently and openly.

3. Raising awareness

- 3.1. We will support organisations and individuals to embrace and deliver on the higher standards the reform entails and society demands.
- 3.2. We will raise the profile of data protection, demonstrating its role as a key builder of trust between organisations and the individuals with which they interact, aiming for enlightened self-interest as a motivator for regulatees, not simply a way of avoiding sanction.
- 3.3. We will improve standards of data protection practice through clear, meaningful and inspiring communications, engagement and influence.

4. Relationships

- 4.1. We will maintain existing connections and work to develop new key, strategic relationships within the data protection regulatory community, and beyond, in the knowledge that there is increasing overlap with regulatory and other bodies in the areas such as consumer rights and cyber security.
- 4.2. We will engage in constructive relationships with all stakeholders to improve overall compliance without compromising our independence, recognising that effective data protection requires multi-disciplinary skills and approach.

Strategic activity - highlights

Below is what the ODPa achieved in line with its strategic aims for 2018, more detail can be found in Appendices 1 - 4:

1. Reform and governance

- 1.1. We will play an integral part in the successful reform of the Bailiwick's data protection regime, ensuring enhanced rights for our citizens as well as continued 'adequacy'.
- 1.2. We will work to support the creation of a robust and effective governance structure including supporting the constitution of the new Authority and associated financial and operational control mechanisms for our Office.

What the ODPa did

- Became an independent regulator on 25 May 2018.
- Held three board meetings of The Data Protection Authority (25 May 2018, 11 September 2018 and 6 December 2018).
- Completed their move into new fit-for-purpose premises (July 2018).
- Completed systems and data migration projects to achieve fully independent status (July 2018).
- Recruited three new permanent members of staff (Tim Loveridge, Mikael Appelqvist, and Leanne Archer).
- Set up separate banking arrangements and auditors, independent of the States of Guernsey (July/August 2018).
- Submitted a proposal of how their activities could be funded by the regulated community instead of the States of Guernsey, to the Committee *for* Home Affairs (November 2018).

2. Regulatory approach

- 2.1. We will ensure, through effective structuring and resourcing of our Office, that we are capable of delivering our statutory requirements, demonstrating the highest standards of data protection regulation for the Bailiwick.
- 2.2. We will ensure regulatory action is targeted, proportionate and fair in the knowledge that most organisations want to do the right thing.
- 2.3. We will adopt a risk-based approach to deliver cost-effective outcomes. This will be done in the knowledge that choices have to be made because of resource pressure and we commit to making those decisions intelligently and openly.

What the ODPa did

- Made the deliberate choice to seek informal resolution to investigations, wherever possible.
- Made thoughtful, evidence-based, impartial determinations in all cases.
- Started developing a project on investigation, case-handling, and compliance best practice.
- Focused efforts and resources on investigating the most harmful complaints.
- Introduced a secure online system for breach reporting.

3. Raising awareness

- 3.1. We will support organisations and individuals to embrace and deliver on the higher standards the reform entails and society demands.
- 3.2. We will raise the profile of data protection, demonstrating its role as a key builder of trust between organisations and the individuals with which they interact, aiming for enlightened self-interest as a motivator for regulatees, not simply a way of avoiding sanction.
- 3.3. We will improve standards of data protection practice through clear, meaningful and inspiring communications, engagement and influence.

What the ODPa did

- Raised awareness of new Law through effective PR, and engagement with regulated community through commissioner/deputy commissioner's attendance or speaking at 18 local events (May-Dec 2018).
- Published a suite of guidance documents around key areas of the law (May 2018).
- Published statistics about self-reported personal data breaches with key message of enlightened self-interest included each time (regularly from June 2018 onwards).
- Established an ODPa motto 'Excellence through Ethics' (July 2018).
- Focused on sharing message of importance of ethical data use, through key channels (July – Dec 2018).
- Developed and published a Communications Strategy (September 2018).
- Started work on scoping the re-development of ODPa's web services and associated internal systems (September 2018).
- Continued to focus on producing and updating key guidance documents, written in plain English.
- Started posting regular, high-quality content on an ODPa LinkedIn page (September 2018).
- Started producing a monthly newsletter (October 2018).
- Started work on developing a free public events programme (November 2018 onwards).

4. Relationships

- 4.1. We will maintain existing connections and work to develop new key, strategic relationships within the data protection regulatory community, and beyond, in the knowledge that there is increasing overlap with regulatory and other bodies in the areas such as consumer rights and cyber security.
- 4.2. We will engage in constructive relationships with all stakeholders to improve overall compliance without compromising our independence, recognising that effective data protection requires multi-disciplinary skills and approach.

What the ODPa did

- Started establishing memoranda of understanding with key entities.
- Continued to work closely with the regulated community, focusing on positive engagement.
- Represented the Bailiwick at the British, Irish and Islands' Data Protection Authorities (BIIDPA) forum in June 2018
- Visited the UK Information Commissioner's Office (ICO) communications team in July 2018.
- Visited the European Data Protection Supervisor communications team in October 2018.
- Represented the Bailiwick at the International Conference of Data Protection & Privacy Commissioners (ICDPPC) in October 2018.
- Visited the Irish Data Protection Commission's senior management team in November 2018.

Case studies

To promote awareness of the diverse range of complaints received by data protection authorities, below are three anonymised examples:

1. Employment scenario

Complainant (data subject): Mr A, an employee of Company B

Controller: Company B

Mr A was under disciplinary action by his employer and was currently off work. All correspondence was being sent to his home address. He moved house and believed he had advised his employer that he had done so. Personal data relating to this disciplinary action was sent to his old address by his employer. It was opened by the new occupant who advised Mr A that he had done so in error.

Mr A subsequently discovered that people were gossiping about his disciplinary action. Until then, it had been kept confidential. This gossip negatively affected his future employment prospects.

Outcome

Mr A had no way of proving that gossip about his disciplinary action had emanated from the new occupant of his old house. Even if he was able to, the damage was done.

- Mr A's complaint was addressed with his employer, Company B (the controller). The controller's HR department denied that Mr A had advised them of his change of address. Mr A had no proof that he had notified the HR department. It is incumbent upon employees to advise employers of a change of address in writing and to obtain confirmation that this has been recorded. Had this been done this data breach, with serious consequences, would not have occurred, or if it had, action could have been taken.
- No formal action could be taken against the controller.

2. Sole trader scenario

Complainant (data subject): Mr C, a sole trader, contracted by Company D

Controller: Company D

Company D is a building consultancy using several building contractors, including Mr C. They were aware that different rates might be charged by the same contractor for different clients. Company D, however, disclosed to a client the lower rates that Mr C had charged to another client. As Mr C is a sole trader, his rates were classed as personal data.

Outcome

- An investigation concluded that, whilst the action of the controller was inappropriate and it was clear that the controller should have not disclosed Mr C's personal data, it had admitted its conduct.
- It was decided that no further action should be taken, as the controller had admitted the oversight, learnt from the mistake and was unlikely to repeat it.
- Additionally, it was concluded that Mr C had not suffered much in the way of privacy damage.

3. Public figure

Complainant (data subject): Ms E, a TV presenter

Controller: Company F, a telecoms provider

Ms E was employed as a TV presenter. Wishing to separate her personal life from her professional life, her home telephone number was ex-directory. A member of the public became very attracted to Ms E and was constantly sending her messages to her work email address, hanging around outside the studio and posting messages about her on social media. This unwanted attraction was tantamount to stalking.

Company F published a new telephone directory with Ms E's name, home telephone number and home address appearing in both the hard copy directory and online, contrary to her previously stated instructions. When Ms E discovered this, she contacted Company F immediately and her details were removed from the online directory. However, the hard copy directory had already been widely distributed. Company F advised Ms E that they could not assist further. She complained to the regulator.

Outcome

- It was recognised that the issue was causing Ms E a great deal of stress, not only in respect of her own safety but of that of her family. There was also the potential for harm.
- An investigation was launched to ascertain how the error had occurred and determined that it was human error, not a failure in process. Appropriate action was taken against Company F.
- In communicating with senior employees of Company F, the regulator was very concerned at the apparent lack of appreciation of Ms E's distress and concern. In such an instance, public and customer relations are paramount and, although the distributed directories could not be amended, the regulator suggested that the distress might be mitigated by some form of recompense. Company F eventually took this on board.

Key statistics

For period 25 May 2018 – 31 Dec 2018

570	Number of additional local organisations who fulfilled their legal obligation to register with the ODPA
66	Number of email enquiries ODPA answered, on average each month
14	Number of speaking engagements by the commissioner and deputy commissioner
£554,129	The ODPA's operating budget
3	Number of board meetings held by The Data Protection Authority
3	Number of additional staff recruited to ODPA
34	Number of data protection complaints received
30	Number of investigations conducted
1	Number of inquiries conducted
0	Number of investigations resulting in a determination that an operative provision has been or is likely to be breached <small>Note: zero determinations made owing to ODPA's desire to find informal resolutions.</small>
0	Number of inquiries resulting in a determination that an operative provision has been or is likely to be breached <small>Note: zero determinations made owing to ODPA's desire to find informal resolutions.</small>
0	Number of sanctions imposed by the Authority under section 73 <small>Note: zero as ODPA has not made a determination under section 71, thus not triggering sections 76 and 73.</small>

Appendix 1

Reform and governance strategic activity details

Legislation

Part XI of *The Data Protection (Bailiwick of Guernsey) Law, 2017* (the Law) sets out the statutory obligations in respect of the Data Protection Authority (the Authority).

Section 60 refers to the establishment and constitution of the Authority as a body corporate with perpetual succession and a common seal.

Section 61 sets out the general functions of the Authority.

Section 62 requires the Authority to be independent and free from direct or indirect external influence in the exercising or performing of its duties.

The Authority

The Law came into force on the 25 May 2018. The Law created the Data Protection Authority and at its meeting on 16 May 2018, the States of Deliberation approved the appointment of the following Authority members, with effect on and from 25 May 2018:

- Chair – Mr Richard Thomas CBE
- Voting Member – Mr John Curran
- Voting Member – Mr Christopher Docksey
- Voting Member – Mr Simon Entwisle
- Voting Member – Mr Mark Lempriere
- Voting Member – Mrs Jennifer Strachan
- Commissioner as *ex-officio* and non-voting Member – Mrs Emma Martins

The launch event on 25 May 2018 was preceded by a meeting of the Authority at which the following matters were addressed:

- Implementation project plan
- Budget for the Authority
- Resources and recruitment
- Office accommodation
- Corporate governance
- Code of practice for Authority members
- Disclosure of Interests
- Memorandum of Understanding with Committee *for* Home Affairs
- Funding project
- Appointment of auditors
- Resolution on frequency of future meetings

During the period of this report the Authority met a further two times (on 11 September 2018 and 6 December 2018).

Members are fully committed to ensuring the highest quality oversight and are ready to demonstrate that the Authority is acting with complete independence from the States of Guernsey in the delivery of their statutory roles.

Human Resources

Prior to the creation of the Authority, the Office of the Data Protection Commissioner was reliant upon government for staffing and the individuals working at the Office were civil servants.

Since 25 May 2018, staff have been employed directly by the Authority with day to day employment administration matters being handled internally. Additional administrative support for employment related matters is in place using a trusted external provider.

Financials and audit

Prior to the creation of the Authority, the Office of the Data Protection Commissioner was reliant upon government for all financial administration and budgeting, including audit.

Since 25 May 2018, the Authority has completely separated all banking arrangement, taken over control of its accounts and has appointed independent auditors.

New funding model

The ODPa submitted a detailed proposal of its funding model post-2019 to the States of Guernsey in November 2018. This proposal contained innovative features which would ensure that the bulk of funding is received from the regulated community with minimum administrative burden.

Appendix 2

Regulatory approach strategic activity details

Legislation

Parts II, III, IV, V, VI, VII, VIII and X of the Law set out the compliance duties of controllers and processors. These statutory requirements reflect the standards of the GDPR.

Strategic aims

Section 61 of the Law sets out the general functions of the Authority. These functions include administering and enforcing the Law as well as promoting awareness for individuals and the regulated community.

Prior to the Law coming into force on 25 May 2018, data protection legislation had been in place for the Bailiwick since 1986. The ODPa continues to build on the compliance foundations of the previous legislation and is drafting a four-year strategic plan that develops on the former but focuses on the enhanced compliance requirements.

These strategic aims will reflect careful consideration of the suite of regulatory duties and objectives the ODPa has and how they may be best approached with the available resources. Further, it will develop and incorporate its approach of 'predict – prevent – detect – enforce' when seeking to deliver meaningful regulatory outcomes. Each of these key regulatory areas, including how they interrelate as well as how the ODPa plans to approach them, will be further explored as the strategic plan develops and matures.

The strategic aims will set out how the ODPa aims to support organisations in delivering on their statutory obligations in a proactive and enlightened way. With the Bailiwick of Guernsey being a small jurisdiction already well accustomed to high standards of professional compliance in financial services regulation, the ODPa has unrivalled access and proximity to the regulated community which it will seek to leverage in delivering high quality data protection regulation.

Internal systems

A major review of the ODPa's casework system began in 2018 now that there are dedicated resources available to manage complaint-handling. The aim will be to ensure complaints are well-managed with objective and agreed criteria for handling, investigation and oversight which are consistently and fairly applied.

The IT infrastructure is being actively developed to enhance:

- Community engagement
- Information gathering and straight-through processing
- Workflow and case-management
- Performance monitoring and reporting
- Regulatory/statutory compliance
- Regulatory effectiveness and capacity

Further, procedures and systems are being put in place to ensure maximum use is made of the rich intelligence that complaints can provide and feed that into the awareness and compliance work programmes.

The ODPa is committed to exploring the opportunities that alternative dispute resolution may offer in case handling.

Complaint handling

The ODPA deals with complaints made by data subjects under section 67 of the Law as well as conducting inquiries under its own initiative (section 69). An investigation is concluded with a determination as to whether a breach of an operative provision has occurred, and if appropriate, the issuance of a sanction

The ODPA employs a core team of casework officers to progress such matters. However, the nature and complexity of some complaints makes it challenging for small regulatory offices such as the ODPA to retain capacity for specialised technological and/or legal inquiries. The ODPA has secured the services of trusted third party providers that can be engaged as required to provide forensic IT as well as legal support where investigations or inquiries require it.

Management of personal data breach reports

In line with GDPR standards, the Law requires controllers to report certain personal data breaches to the ODPA. The information contained within such reports is a rich source of intelligence, highlighting (often in almost real-time) harms and risks in the area of data processing. The ODPA has been clear from the outset of these reporting requirements that the regulated community must have trust and confidence in the office to handle the reports appropriately. Work continues to engage with industry to support this objective and the ODPA has been open and transparent with the public about the nature and volume of such breach reports via regular press release on breach statistics, these have been released to all local media (and published on odpa.gg) on a bi-monthly basis since June 2018.

Since the early days of the Law, the level of engagement in respect of personal data breach reports has been extremely positive. It is clear that the reporting of breaches is starting to be effectively built into the business processes of the local regulated community. Furthermore, the collated reporting is helping the ODPA to build an understanding of harms and increasingly identify potential systemic risks.

The ODPA will be developing communications and compliance work around the personal data breach report trends in order to improve awareness and reduce the likelihood of recurrence. Such information will also assist in informing the future targeting of compliance, inspection and enforcement resources, recognising the benefits of evidence-based activities.

The ODPA continues to work closely with the Cyber Security Lead for the States of Guernsey to ensure a consistent and constructive approach to all data security related matters and will, in the future, be exploring the sharing of statistical information where doing so may benefit industry or the jurisdiction as a whole.

Prior consultation

Section 46 of the Law requires the ODPA to be consulted in certain new legislative proposals where such draft legislation involves the processing of personal data. This important enhanced requirement of the Law reflects the significance and potential impact of the processing of personal data by government which by its nature carries with it special responsibilities in that it applies to everyone and is mandatory.

Individuals' rights

Part III of the Law sets out the statutory rights for individuals, some of which were in place in the previous legislative regime; some of which are new.

Individuals are able to pursue legal remedies to ensure compliance and enforce their legal rights. Such actions may be taken directly against controllers or raised with the regulator or the courts.

The ODPA has put in place procedures to ensure the investigation of complaints and conduct of inquiries is independent. There are permanent members of staff who are experienced investigators and the ODPA has secured the services of specialist legal and investigative support that can be called upon when investigations or inquiries require it.

The strategic aims of the ODPA will reflect careful consideration of its suite of regulatory duties and objectives and how they may be best achieved with the available resources. Further, it will develop its approach of 'predict – prevent – detect – enforce' when seeking to deliver meaningful regulatory outcomes.

In striving to support and encourage a raising of compliance in the community as a whole, the risks and harms to individuals can be minimised. The work programme to support controllers and processors is, therefore, neither strategically nor operationally separate from the focus on individuals and their rights.

The ODPA has included outreach work aimed at individuals in its communications strategy and where collaborative working will assist in these objectives, partnerships with suitable third parties are being explored.

The ODPA recognises that data harms are real and have the potential to impact individuals in significant and detrimental ways. Seeking to predict and prevent these harms is a priority whilst ensuring that the ODPA has the ability to respond to allegations of infringements in a timely and appropriate manner.

Redress mechanisms

Section 73 of the Law provides that all or any of the following sanctions may be imposed by the ODPA where it has determined that a breach has occurred or is likely to occur:

- A reprimand;
- A warning;
- An order (including an administrative fine).

The procedures which must be followed for the issuing of sanctions and the ordering of administrative fines (the latter is a reserved function of the Authority itself) are set out in detail in the Law.

The Law provides individuals with effective administrative and judicial remedy. Under section 79, a data subject can bring an action against a controller or processor for the breach of an operative provision. A court in which an action is brought may grant an order, relief or remedy (including damages) in respect of any distress, inconvenience or other adverse effect suffered by a data subject even if there is no physical or financial loss or damage.

Section 85 of the Law allows for the ODPA to bring similar proceedings before the court in respect of any breach or anticipated breach by a controller or processor.

Section 87 of the Law provides for the offence of unlawful obtaining or disclosure of personal data to which a custodial sentence is attached.

Appendix 3

Raising awareness strategic activity details

Legislation

Part XI (section 61) of the Law set out the Authority's duty to: 'promote public awareness of risks, rules, safeguards, and rights in relation to processing, especially in relation to children'; and 'to promote the awareness of controllers and processors of their duties under this Law'.

Communications strategy

The ODPA has developed and published a comprehensive communications strategy that will reinforce the strategic plan. This strategy aims to support the approach of constructive engagement with the regulated community to help them embrace and deliver on their obligations, as well as with citizens to help them to understand their rights and how to exercise them.

The communications strategy's objectives are:

- To promote public awareness of risks, rules, safeguards and rights in relation to processing of personal information, especially in relation to children.
- To promote Guernsey's position as a jurisdiction with excellent and innovative data protection standards which retains its 'adequacy' recognition from the EU
- To promote awareness of the legal duties placed on organisations who are controlling or processing personal information.
- To protect the ODPA / Data Protection Authority's reputation by communicating in-line with its mission, vision and values.

The main communication channels are:

- the odpa.gg website;
- newsletter;
- PR;
- public statements;
- annual report;
- official guidance;
- events (the ODPA's, and others);
- social media.

The communications activities seek to put more emphasis on the human being at the heart of data protection legislation with less emphasis on box-ticking, dis-engaged, compliance. The ODPA motto, as featured in the communications strategy, is 'Excellence through Ethics'. This motto reflects the foundation of the ODPA's approach, striving to weave the thread of ethics into all communications activities.

The ODPA focused on sharing this message of the importance of ethical data use, through key channels (e.g. published blog pieces on data ethics and history of privacy; Business Life article in Sept/Oct 2018 issue on data ethics; Data Protection Leader article in November 2018 issue; Emma Martins interviewed for Thought Leaders in Privacy video series recorded in October 2018).

Plain English

The ODPA provides clear and accessible information for individuals seeking to exercise their rights directly with controllers and works explicitly to seek to empower individuals in respect of managing their own data and questioning the practices and approach of controllers.

The ODPA aims to be accessible to individuals seeking information or advice. The offices have been specially designed to ensure maximum privacy for members of the public who wish to discuss their concerns, explore the possibility of making a formal complaint or otherwise discuss data-related matters.

In line with the overarching communications strategy the ODPA is wholeheartedly committed to using plain English in all communication, to ensure that it does not lose people due to using legal or business jargon. Because of this, it plans to continue publishing plain English guidance documents for controllers/processors and for members of the public to ensure that the legislation is as accessible as possible. The ODPA is also planning to develop its website - odpa.gg - to improve the amount, accessibility and quality of information available.

Local media

As with any jurisdiction, local media coverage of data protection and related matters is important in promoting awareness in the community as well as encouraging relevant and searching questions of government, the ODPA as regulator, and industry in respect of data protection and related issues.

The ODPA recognises the important and positive part local media coverage can play in raising awareness and encouraging engagement and debate.

In line with the communications strategy, the ODPA ensures it contributes where it is considered appropriate to do so and where there are opportunities to advance those discussions and raise awareness.

In recognition of the public interest around data breaches, from June 2018 the ODPA committed to publishing information on a regular basis about the number of data breaches reported. It included the key message of enlightened self-interest in each press release (issued: 25 June, 27 August, 25 October, 20 December).

Events

A key channel identified in the communications strategy of the ODPA is events. Work on developing the events programme began in 2018 with a view to putting together a proposed plan for members of the public and the regulated community to comment on early in 2019.

The aim of the events programme is to effect positive cultural change by:

- being accessible to local organisations and citizens of all ages
- improving compliance by building awareness of topical issues in data protection
- encouraging innovation and excellence in data protection practices
- exploring official guidance with the regulated community
- gathering feedback from local industry and individuals

Schools programme

The ODPA began work towards developing an education programme for school-age children, to be delivered in partnership with local schools. This is an important activity, as there are two-fold benefits to building children's awareness: firstly, a well-informed young person is more likely not to fall victim to harms that may arise from misuse of their personal data; and secondly, a well-informed young person may share their new awareness with adults in their lives, so the message is spread wider. Furthermore, these engaged and informed individuals will enter the workforce in years to come and could serve to strengthen compliance through their own actions and behaviour.

The ODPA is now able to offer student visits, either as work experience or in support of their academic courses. The aim is to support and encourage interest in the area of data and data protection as a career option as well as to encourage awareness and consideration of the younger generation's perspective of data-related matters by the ODPA in its own work.

Appendix 4

Relationships strategic activity details

Engagement with local regulated community

The ODPA benefits from many years of building positive and respected relationships with the regulated community. With a significant percentage of data processing being undertaken by the financial services industry, the ODPA takes advantage of the numerous professional and industry bodies that represent key areas within this sector. Working with these bodies enables access to these groups in support of the communications strategy.

The ODPA is developing tools and templates that provide a framework to support and facilitate the accountability requirements, recognising the enhanced obligations for controllers and processors specifically in respect of the necessity to demonstrate compliance to the ODPA.

The ODPA is working with industry representative groups to ensure, as far as is practicable, those tools and templates are tailored to and responsive of the different sectors and environments of the regulated community.

Where such representative groups exist for other sectors, such as small businesses and third sector, the ODPA proactively seeks early engagement and support. Such groups can also act as useful conduits for updates and guidance issued by the ODPA.

Guernsey has a newly constituted Association of Data Protection Officers (ADPO) which seeks to support and develop data protection professionals in the jurisdiction. The ODPA is pleased to support the work of the ADPO, recognising the key role played by data protection officers in delivering high standards of compliance for controllers and processors.

The ODPA continues to work with the local training agency in supporting the delivery of data protection professional development.

The ODPA's new offices were specially designed to ensure maximum privacy for representatives of controllers and processors who attend for meetings. In addition, there is a dedicated boardroom which is used for Authority meetings as well as being a space which can be used for small public and consultation events.

Engagement with other regulators

The ODPA continues to benefit from its links with regulators further afield by sharing knowledge and learning from different approaches through informal and formal channels.

Informally, an ODPA staff member visited both the UK Information Commissioner's Office (ICO) and the European Data Protection Supervisor to learn from their respective communications teams. Two staff members visited the Irish Data Protection Commission's senior management team to share knowledge around regulation and operational process.

In June 2018 two ODPA staff members represented the Bailiwick at the annual British, Irish and Islands' Data Protection Authorities (BIIDPA) forum in the Isle of Man. This gathering of regulators takes a slightly different format to other events and is invaluable for the cooperation and development of all involved.

The Deputy Commissioner represented the Bailiwick at the closed session of the International Conference of Data Protection & Privacy Commissioners (ICDPPC) in October 2018. The Commissioner and an additional ODPA staff member attended the open sessions of this event. This large-scale week-long event in Brussels made international news due to a keynote speaker, Apple CEO Tim Cook, calling for comprehensive federal privacy laws in the US.

Consultation exercises with citizens and regulated community

The ODPA recognises that having a genuine understanding and appreciation of the experiences and views of the regulated community matters if it is to be a relevant and responsive regulator. Ensuring regular communication with controllers, processors and citizens plays an important part. The first of a series of consultation exercises relating to the ODPA's event programme is planned for 2019. The ODPA will continue to ensure meaningful and regular communications with industry, utilising public consultation exercises where appropriate.

Collaborative working

Data protection increasingly involves other regulatory arenas. To ensure consistency as well as efficient use of limited and/or specialist resources, the ODPA is working towards agreeing Memorandums of Understanding (MoUs) with key third parties who work in the regulatory space where such collaborative working assists in delivering on the strategic and operational objectives of the office.

A MoU was signed with the States of Guernsey in 2018 and a MoU is being sought with the Guernsey Financial Services Commission. Whilst the ODPA has officers capable of conducting criminal investigations, a MoU is being drawn up with Guernsey Police to ensure appropriate resources and support for criminal investigations.

Appendix 5

Members' Report and Audited Financial Statements

Period Ended 31 December 2018

The Data Protection Authority

Authority Information

Members	Richard Thomas CBE (Chairman) Simon Entwisle John Curran Christopher Docksey Mark Lempriere Jennifer Strachan
Registered office	St Martin's House Le Bordage St Peter Port Guernsey GY1 1BR
Auditor	Grant Thornton Limited Lefebvre House Lefebvre Street St Peter Port Guernsey GY1 3TF
Accountants	BDO Limited Place du Pre St Peter Port Guernsey GY1 3LL

The Data Protection Authority

Contents

	Page
Members' Report	1 - 2
Independent Auditor's Report	3 - 4
Statement of Comprehensive Income	5
Balance Sheet	6
Notes to the Financial Statements	7 - 10
Detailed Statement of Comprehensive Income (unaudited)	11

The Data Protection Authority

Members' Report For the Period from 25 May to 31 December 2018

The members present their report and the financial statements for the period ended 31 December 2018.

Members' responsibilities statement

The members are responsible for preparing the Members' Report and the financial statements in accordance with the requirements of The Data Protection (Bailiwick of Guernsey) Law, 2017 ("the Law") and generally accepted accounting practice.

The members are responsible for keeping proper financial accounts and adequate accounting records that are sufficient to show and explain the Authority's transactions to enable them to ensure that the financial statements comply with the Law and associated legislation. They are also responsible for safeguarding the assets of the Authority and hence for taking reasonable steps for the prevention and detection of fraud and other irregularities.

Principal activity

The Data Protection Authority is the independent regulatory authority for the purposes of the Data Protection (Bailiwick of Guernsey) Law, 2017 and associated legislation.

Results

The deficit for the period is set out in detail on page 5.

Members

The members who served during the period were:

Richard Thomas CBE
Simon Entwisle
John Curran
Christopher Docksey
Mark Lempriere
Jennifer Strachan

Establishment

These are the first financial statements of the Authority which commenced activities on 25 May 2018.

Disclosure of information to auditors

Each of the persons who are members at the time when this Members' Report is approved has confirmed that:

- so far as the member is aware, there is no relevant audit information of which the Authority's auditors are unaware, and
- the member has taken all the steps that ought to have been taken as a member in order to be aware of any relevant audit information and to establish that the Authority's auditors are aware of that information.

The Data Protection Authority

**Members' Report (continued)
For the Period from 25 May to 31 December 2018**

Independent auditor

The auditor, Grant Thornton Limited, has expressed a willingness to continue in office.


Post balance sheet events

There have been no significant events affecting the Authority since the period end.

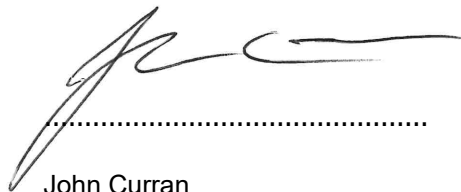
Going concern

The Authority is in a net liability position at the balance sheet date and therefore will require funding to support the future working capital and operational requirements. The members are satisfied that the Authority will be able to meet its liabilities as and when they fall due as a result of the legal obligation of the States of Guernsey to provide sufficient funding and assurances received in relation to funding for the year commencing 1 January 2020. Accordingly, the members have prepared these financial statements on a going concern basis.

This report was approved by the members and signed on their behalf:



Richard Thomas CBE



John Curran

Date: 2nd October 2019

Independent auditor's report To the members of The Data Protection Authority

Opinion

We have audited the financial statements of The Data Protection Authority (the 'Authority') for the period ended 31 December 2018 which comprise the Statement of Comprehensive Income, the Balance Sheet and notes to the financial statements, including a summary of significant accounting policies. The financial reporting framework that has been applied in their preparation is applicable law and United Kingdom Accounting Standards, including Financial Reporting Standard 102 'The Financial Reporting Standard applicable in the United Kingdom and the Republic of Ireland' ('FRS 102'), Section 1A 'Small Entities'.

In our opinion, the financial statements:

- give a true and fair view of the state of the Authority's affairs as at 31 December 2018 and of its deficit for the period then ended;
- are in accordance with United Kingdom Accounting Standards, including FRS 102 Section 1A 'Small Entities'; and

Basis for opinion

We conducted our audit in accordance with International Standards on Auditing (UK) (ISAs (UK)) and applicable law. Our responsibilities under those standards are further described in the 'Auditor's responsibilities for the audit of the financial statements' section of our report. We are independent of the Authority in accordance with the ethical requirements that are relevant to our audit of the financial statements in Guernsey, including the FRC's Ethical Standard, and we have fulfilled our other ethical responsibilities in accordance with these requirements. We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Who we are reporting to

This report is made solely to the Authority's members, as a body, in accordance with Paragraph 12 of Schedule 6 of The Data Protection (Bailiwick of Guernsey) Law, 2017. Our audit work has been undertaken so that we might state to the Authority's members those matters we are required to state to them in an auditor's report and for no other purpose. To the fullest extent permitted by law, we do not accept or assume responsibility to anyone other than the Authority and the Authority's members as a body, for our audit work, for this report, or for the opinions we have formed.

Conclusions relating to going concern

We have nothing to report in respect of the following matters in relation to which the ISAs (UK) require us to report to you where:

- the members' use of the going concern basis of accounting in the preparation of the financial statements is not appropriate; or
- the members have not disclosed in the financial statements any identified material uncertainties that may cast significant doubt about the Authority's ability to continue to adopt the going concern basis of accounting for a period of at least twelve months from the date when the financial statements are authorised for issue.

Other information

The members are responsible for the other information. The other information comprises the information included in the Members' Report set out on pages 1 to 2, other than the financial statements and our auditor's report thereon. Our opinion on the financial statements does not cover the other information and, except to the extent otherwise explicitly stated in our report, we do not express any form of assurance conclusion thereon. In connection with our audit of the financial statements, our responsibility is to read the other information and, in doing so, consider whether the other information is materially inconsistent with the financial statements or our knowledge obtained in the audit or otherwise appears to be materially misstated. If we identify such material inconsistencies or apparent material misstatements, we are required to determine whether there is a material misstatement in the financial statements or a material misstatement of the other information. If, based on the work we have performed, we conclude that there is a material misstatement of this other information, we are required to report that fact.

We have nothing to report in this regard.

Responsibilities of members for the financial statements

As explained more fully in the members' responsibilities statement set out on page 1, the members are responsible for the preparation of the financial statements which give a true and fair view in accordance with UK GAAP, and for such internal control as the members determine is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error.

In preparing the financial statements, the members are responsible for assessing the Authority's ability to continue as a going concern, disclosing, as applicable, matters related to going concern and using the going concern basis of accounting unless the members either intend to liquidate the Authority or to cease operations, or have no realistic alternative but to do so.

Auditor's responsibilities for the audit of the financial statements

Our objectives are to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes our opinion. Reasonable assurance is a high level of assurance, but is not a guarantee that an audit conducted in accordance with ISAs (UK) will always detect a material misstatement when it exists. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of these financial statements.

A further description of our responsibilities for the audit of the financial statements is located on the Financial Reporting Council's website at: www.frc.org.uk/auditorsresponsibilities. This description forms part of our auditor's report.



Grant Thornton Limited
Chartered Accountants
St Peter Port
Guernsey

02 October 2019

The Data Protection Authority

Statement of Comprehensive Income
For the Period from 25 May to 31 December 2018

	2018 £
Income	415,059
Administrative expenses	(554,129)
Deficit for the period	<u><u>(139,070)</u></u>

There is no difference between the deficit for the financial period stated above and total comprehensive income.

The results above derive from continuing activities.

There was no other comprehensive income for 2018.

The notes on pages 7 to 10 form part of these financial statements.

The Data Protection Authority

Balance Sheet
As at 31 December 2018

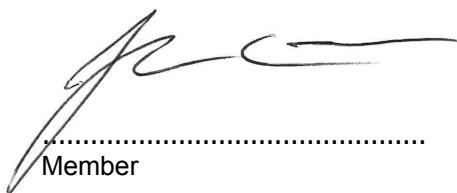
	Note	2018 £
Fixed assets		
Tangible assets	4	134,533
Current assets		
Debtors and prepayments	5	96,956
Cash at bank and in hand		376,446
Current liabilities		<u>473,402</u>
Creditors: amounts falling due within one year		(747,005)
Net current liabilities		<u>(273,603)</u>
Net liabilities		<u><u>(139,070)</u></u>
Reserves		
Deficit		(139,070)
Total reserves		<u><u>(139,070)</u></u>

The financial statements have been prepared in accordance with the provisions of FRS 102 Section 102 1A - small entities.

The financial statements were approved and authorised for issue by the members and were signed on the members' behalf by:



.....
Member



.....
Member

Date: 2nd October 201

The notes on pages 7 to 10 form part of these financial statements.

The Data Protection Authority

Notes to the Financial Statements For the Period from 25 May to 31 December 2018

1. Accounting policies

1.1 Basis of preparation of financial statements

The financial statements have been prepared under the historical cost convention and in accordance with Section 1A of Financial Reporting Standard 102, the Financial Reporting Standard applicable in the UK and the Republic of Ireland.

The preparation of financial statements in compliance with FRS 102 requires the use of certain critical accounting estimates. It also requires management to exercise judgment in applying the Authority's accounting policies.

The following principal accounting policies have been applied:

1.2 Going concern

The Authority is in a net liability position at the balance sheet date and therefore will require funding to support the future working capital and operational requirements. The members are satisfied that the Authority will be able to meet its liabilities as and when they fall due as a result of the legal obligation of the States of Guernsey to provide sufficient funding and assurances received in relation to funding for the year commencing 1 January 2020. Accordingly, the members have prepared these financial statements on a going concern basis.

1.3 Income

Annual notification fees are recognised to the extent that it is probable that the economic benefits will flow to the Authority and the income can be reliably measured. Income from annual notification fees is measured at the fair value of the consideration received or receivable.

1.4 Government grant and other income

Grants received are of a revenue nature and are recognised in the statement of comprehensive income in the same period as they relate. Any grant amounts not expended are returned to the Budget Reserve and not retained by the Authority. Amounts not expended reduce the grant income and are accrued for in these financial statements as 'Amounts payable to the States of Guernsey'.

The grant received is reflected in the statement of comprehensive income in order to match the expenditure incurred in relation to data protection law matters during 2018 and those incurred in setting up and operating the Authority.

In addition to the grant above, the States of Guernsey settled expenses on behalf of the Authority in the sum of £31,776. This amount has also been reflected in income to match the expenditure incurred.

1.5 Tangible fixed assets

Tangible fixed assets under the cost model are stated at historical cost less accumulated depreciation and any accumulated impairment losses. Historical cost includes expenditure that is directly attributable to bringing the asset to the location and condition necessary for it to be capable of operating in the manner intended by management.

The Data Protection Authority

Notes to the Financial Statements For the Period from 25 May to 31 December 2018

1. Accounting policies (continued)

1.5 Tangible fixed assets (continued)

Depreciation is charged so as to allocate the cost of assets less their residual value over their estimated useful lives.

The estimated useful lives range as follows:

Leasehold improvements	- 6 years
Furniture and fittings	- 20% straight line
Office equipment	- 20% straight line

1.6 Debtors

Short term debtors are measured at transaction price, less any impairment.

1.7 Cash at bank and in hand

Cash at bank and in hand is represented by cash in hand, current bank accounts and deposits with financial institutions repayable without penalty on notice of not more than three months.

1.8 Financial instruments

The Authority only enters into basic financial instruments transactions that result in the recognition of financial assets and liabilities like trade and other debtors and creditors, loans from banks and other third parties, loans to related parties and investments in non-puttable ordinary shares.

Debt instruments (other than those wholly repayable or receivable within one year), including loans and other accounts receivable and payable, are initially measured at the present value of the future cash flows and subsequently at amortised cost using the effective interest method. Debt instruments that are payable or receivable within one year, typically trade debtors and creditors, are measured, initially and subsequently, at the undiscounted amount of the cash or other consideration expected to be paid or received. However, if the arrangements of a short-term instrument constitute a financing transaction, like the payment of a trade debt deferred beyond normal business terms or financed at a rate of interest that is not a market rate or in case of an out-right short-term loan not at market rate, the financial asset or liability is measured, initially, at the present value of the future cash flow discounted at a market rate of interest for a similar debt instrument and subsequently at amortised cost.

Financial assets that are measured at cost and amortised cost are assessed at the end of each reporting period for objective evidence of impairment. If objective evidence of impairment is found, an impairment loss is recognised in the Statement of Comprehensive Income.

For financial assets measured at cost less impairment, the impairment loss is measured as the difference between an asset's carrying amount and best estimate of the recoverable amount, which is an approximation of the amount that the Authority would receive for the asset if it were to be sold at the Balance Sheet date.

1.9 Operating leases

Rentals paid under operating leases are charged to the Statement of Comprehensive Income on a straight line basis over the lease term.

The Data Protection Authority

Notes to the Financial Statements
For the Period from 25 May to 31 December 2018

1. Accounting policies (continued)

1.10 Administrative expenses

Administrative expenses are measured at transaction price and accounted for on an accruals basis.

2. Employees

The average monthly number of employees during the period was 12.

3. Taxation

The Authority is exempt from the provisions of the Income Tax (Guernsey) Law, 1975 as amended.

4. Tangible fixed assets

	Leasehold improvements £	Furniture and fittings £	Office equipment £	Total £
Cost				
Additions during the period and at 31 December 2018	65,731	1,262	76,009	143,002
Depreciation				
Charge for the period	2,497	12	5,960	8,469
Net book value				
At 31 December 2018	<u>63,234</u>	<u>1,250</u>	<u>70,049</u>	<u>134,533</u>

5. Debtors and prepayments

	2018 £
Amount receivable from the States of Guernsey	76,865
Prepayments and accrued income	20,091
	<u>96,956</u>

The Data Protection Authority

Notes to the Financial Statements For the Period from 25 May to 31 December 2018

6. Creditors

	2018 £
Trade creditors	66,162
Deferred rent	34,422
Amount payable to the States of Guernsey	631,055
Accruals	15,366
	<u>747,005</u>

On 26th April 2019 and 2nd July 2019 the Authority repaid £47,912 and £334,055 respectively, to the States of Guernsey. £297,000 of the balance payable at 31 December was in relation to a transition loan. For the purposes of these financial statements, the loan is considered to be interest free, unsecured and has no fixed date of repayment.

7. Commitments under operating leases

At 31 December 2018 the Authority had future minimum lease payments under non-cancellable operating leases as follows:

	2018 £
Within one year	67,242
Within two to five years	345,817
Total	<u><u>413,059</u></u>

8. Related party transactions

During the period, £292,768 was received from the States of Guernsey in the form of a grant and a further £31,776 was received to cover specific expenditure. An additional amount of £631,055 is payable to the States of Guernsey as at the Balance Sheet date. This balance comprises two amounts lent to the Authority in relation to the set-up and transition period totalling £238,232 and £297,000 respectively and £95,823 in relation to a grant under spend.

9. Controlling party

The members are of the opinion that there is no ultimate controlling party.

The Data Protection Authority

Detailed Statement of Comprehensive Income (unaudited) For the Period from 25 May 2018 to 31 December 2018

	Period from 25 May to 31 December 2018 £
Income	415,059
Administrative expenses	(554,129)
Deficit for the period	(139,070)
Income	
Annual notification fees	90,515
States of Guernsey grant	292,768
Other income	31,776
	415,059
Administrative expenses	
Salaries and other staff costs	279,641
Members fees	21,875
Rent, rates and premises expenses	49,686
Legal and professional fees	51,163
Advertising and communications costs	20,298
Travel and entertaining	36,721
IT costs	69,547
Depreciation	8,469
Office and sundry expenses	13,150
Insurance	3,579
	554,129

Excellence Through Ethics.