

Annual Report

2019

For the period 1 Jan 2019 – 31 Dec 2019



Contents

Foreword	2
Introduction	3
About the Authority	6
Organisational chart	7
Strategic plan and activities	8
Case studies	17
Key statistics	21
Members' Report and Audited Financial Statements	22

Foreword



Richard Thomas CBE

**Chair, The Data Protection Authority
(Bailiwick of Guernsey)**

Data Protection is actually People Protection. At the abstract level, it protects their fundamental rights and freedoms. In the real world, where personal information has now become incredibly valuable, it protects people's privacy and it protects them from a wide range of social and economic harms which threaten their well-being.

Data protection equally protects organisations. There cannot be any organisation – private, public or voluntary sector – that does not handle personal information. Getting data protection right for their customers, clients, suppliers, patients, citizens and voters is simply a matter of self-interest. Any organisation will hit problems if it does not treat this valuable commodity as carefully as its money and its other assets. This extends well beyond the security measures needed to prevent a data breach. Handling information well – for the right purposes, for the right time and in the right way – inspires confidence and respect. Handling it badly damages commercial and political reputations and can prove very costly.

For the Bailiwick of Guernsey there is a further reason why data protection matters. Very soon, in accordance with the General Data Protection Regulation (GDPR), the European Commission will decide whether the Bailiwick should retain its 'Adequacy' status. Loss of that status, which permits the free flows of personal information which underpin the global digital economy, would be devastating for the financial services industry and other parts of the Bailiwick's economy. Of course, the European Commission is scrutinising the 2017 Law to make sure that it closely mirrors GDPR's provisions. But it is also required to make sure that Guernsey has a genuinely independent supervisory authority that can demonstrate effective functioning.

Fortunately, I am proud that we have established The Office of the Data Protection Authority (ODPA) as a body that is manifestly independent and is very clear about its effectiveness. This Annual Report documents what has been achieved during 2019, our first full year. The *Strategic Plan* sets out our ambitions through to 2022, highlighting how we are, and will be, actively helping organisations deliver their obligations, empowering individuals to exercise their rights and taking enforcement action where necessary. We have been fortunate to benefit from financial and political support from the States of Guernsey. We have excellent new premises and much of the infrastructure that we need. The self-funding arrangements due for 2021 will enhance both independence and effectiveness.

Everything that has been achieved – and will be achieved – depends upon good people. We have the best. I am delighted that the Board has formally resolved to re-appoint Emma Martins as our Commissioner until the end of 2022. As this Report shows, she is an outstanding leader – not only in ensuring the successes, but also in navigating calmly through inevitable frustrations. It is a great tribute to Emma and her excellent team that the challenges which the Covid-19 crisis has presented in the first half of 2020 have been managed without significant disruption.

The Board and I are fully confident that data protection really does matter in the Bailiwick of Guernsey.

Introduction



Emma Martins

Data Protection Commissioner
(Bailiwick of Guernsey)

I am pleased to present this Annual Report for The Office of the Data Protection Authority (ODPA) for 2019 in accordance with the requirements of Schedule 6, paragraph 13 of *The Data Protection (Bailiwick of Guernsey) Law, 2017*.

It is important to take time to reflect and appreciate that the laws which any government decides to implement sit at the heart of what that jurisdiction values, where power lies (and where it does not) and what it stands for as a community. There is, I think, evidence of a global awakening of the extraordinary scale and impact of personal data processing in this digital era. We have seen how it goes to the very core of who and what we are as human beings. At its heart, data protection is about empowering and protecting individuals. It is also about ensuring that we are well positioned to benefit from being well-regulated in an economy increasingly fuelled by data. So, firstly, I would like to encourage us all to recognise how fortunate we are to live in a jurisdiction that has chosen to put a value on individual protections and rights in the context of data when so many places across the globe do not.

2019 marked the one-year anniversary of the General Data Protection Regulation (GDPR) and our own *Data Protection (Bailiwick of Guernsey) Law, 2017* which both came into force in May 2018. Despite some early challenges in pursuing investigations which were initiated under the previous legal regime, our law is now working well. This important milestone provided an opportunity for us to look at how one of the most significant developments in data protection history has started to bed into our personal and professional lives, both locally and across the globe.

Now working independently from government, we have put in place new governance frameworks to ensure that we continue to carry out our statutory duties with the highest standards of integrity and accountability. The new legislation provides us with greater powers than before and in turn we must ensure that we maintain the trust and confidence that our regulated community, as well as the community more widely, have in us to do our job without fear or favour.

One important area of governance is financial and in moving away from Government oversight, we have also put in place robust financial control frameworks and I am pleased to confirm the completion of our first full independent financial audit this year.

Looking ahead, we will be moving to become self-funded from 2021 to ensure that we are independent from Government. Whilst agreement on this model took longer than hoped, we are pleased to now have the clarity we need to press ahead with the preparations. We have always fiercely guarded the independence and integrity of our regulatory activity, but perception can often be as important as the reality. We recognise that to maintain the trust and confidence that I reference above, we must be seen to be independent as well as conducting ourselves independently from an operational perspective. The States of Guernsey processes some of the largest and most sensitive data sets across the Islands and our ability to conduct enquiries independently across all sectors is crucial.

We have always been extremely mindful that every penny spent by our office comes from industry and Government (and therefore the taxpayer). How we spend that money matters – it matters from a governance as well as a reputational perspective. Data protection regulators play an increasingly important part in all jurisdictions and in this data driven economy, good data protection regulatory oversight is a building block of a forward-looking economy that seeks to harness new and innovative opportunities. It is also clear that, as a democracy, Government recognises the need to provide individuals with rights as well as redress for when those rights are not respected. There is, therefore, an economic and social value in regulation.

“

It is better to prevent harm than punish for it.

Given the extent to which data fuels the economy, the scale of the regulatory task is enormous – there is unlikely to be any aspect of our lives which is not somehow affected or influenced by the processing of our personal data, whether we are aware of that or not. So what does it mean to be an effective regulator in this area of such depth and breadth? There is no easy answer but at the ODPA we have, during this year, taken the time to think carefully about our statutory duties and how best we can, with limited resource, deliver outcomes that are meaningful and sustainable.

We have concluded that, whilst enforcement is important and necessary, if we can work towards building a community that understands and is therefore able to deliver on its compliance duties, that will always be better from a resources perspective, because effective enforcement is necessarily resource hungry and importantly it will also be better from a ‘harms’ perspective. In trying to take the conversation back to the central tenet that this is about each of us as human beings and the harms that can result from mishandling of our data, we recognise the simple fact that it is better to prevent harm than punish for it.

This approach has now been built in to our *Strategic Plan (2019-2022)* from which all our activities now flow. Our focus is on the principle of enlightened compliance, and our priority is harm prevention.

We are clear that this will not be delivered if there is an adversarial relationship with our regulated community, but rather needs to be developed through shared values and objectives. If we frame all our conversations and approach around enforcement, there is a danger that this will encourage businesses to position their perception of risk around themselves and their business. In the context of our personal data, the risk is actually about the rights and freedoms of us as individuals; our families; our friends. If we strive to improve understanding and awareness of that fact, we are more likely to encourage collective and cohesive action to embed high standards of data protection into everything that we do.

Data and its protection is essentially a human issue and, as evidenced by the self-reported breach statistics we publish every two months, we continue to see that when things go wrong, it is often down to humans rather than technology and if we don’t frame our approach around this fact, we will miss opportunities and exacerbate risks.

As with any legal or regulatory requirements, there will always be a small minority who choose deliberately to do the wrong thing. But the vast majority of cases we see are down to ignorance, misunderstandings and genuine errors and there is much that we can all do to reduce these.

We want to build a regulatory regime that is effectively risk-based at heart but we also recognise the dynamic and multifaceted nature of the data environment we are now in. If we are to ensure our approach is relevant and meaningful, we must respond accordingly. There is no one-size-fits-all approach and the reality of having limited resources available to us means that the task is challenging and complex nor is it pre-determined. But we are clear that in striving for a collective and culturally attuned approach to the protection of personal data across our Bailiwick is how we will deliver the best outcomes. Law does not stand alone when we look at how people conduct themselves, there are many other factors influencing our behaviour. If we are to be genuinely effective in delivering good outcomes, we need to understand and actively engage with these other factors.

One such factor is ethics and the reason we are explicitly embedding a culture of ethics into everything we do, both internally and externally, is because we recognise that the scale and impact of personal data processing gets to the very heart of what it is to be human. Ethics runs deep in us as human beings and we are all capable of reflecting on our actions and the actions of others. Data protection legislation will always need to be seen through an ethical lens because it so often requires us to balance interests and make judgements. If we are to do that properly, we need to be well grounded in values, ethics and integrity.

Introduction *continued*

I want to encourage us all to see data protection as so much more than a legal, government, or even European construct; it is about each and every one of us. Approaching our regulatory duties with this knowledge, and asking our community to do the same will, I am sure, lead to better outcomes.

During this year I am proud to report that we have launched several initiatives to improve awareness and engagement, including fortnightly drop-in sessions for local businesses, a free events programme, study visits, and a podcast series and have started developing a schools programme.

In seeking to embed a culture of data protection into the Bailiwick, we want to leverage the opportunities that present themselves in this data driven economy without compromising on the highest standards of data protection. Data protection is not - and has never been - about inhibiting or railing against innovation, it is about ensuring that such progress is built on important protections and values. 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 interdependent. Our focus is, as it has always been, on ensuring we serve our community according to our values and strive for the Bailiwick to remain a jurisdiction which respects the protection of its citizens and continues to offer a high quality regulatory environment for existing and new businesses.

Lastly, I want to express my personal thanks to the whole ODPA team and board. Securing government agreement on our funding model has proved more challenging than we had anticipated which in turn has delayed some of our strategic activities. But it remains the case that we have made significant progress in all key areas. The achievements of this year are not down to one person, they are down to the team of people who continue to work with such professionalism and commitment to build on the work that was started in 2018. Although the scale of the task ahead of us can seem daunting for a small team, the energy and passion of our office staff and board members is humbling and inspiring. It is an enormous privilege to work alongside each and every one.

I hope that this report provides you with a flavour of the work that has been done, publicly as well as behind the scenes, to support the delivery of our statutory obligations and strategic objectives in supporting the citizens and businesses of our Bailiwick.

“

The achievements of this year are not down to one person, they are down to the team of people who continue to work with such professionalism and commitment.

”

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 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 takes action where they fall short.

The Office of the Data Protection Authority:



Empowers individuals and protects their rights



Promotes excellence in data protection

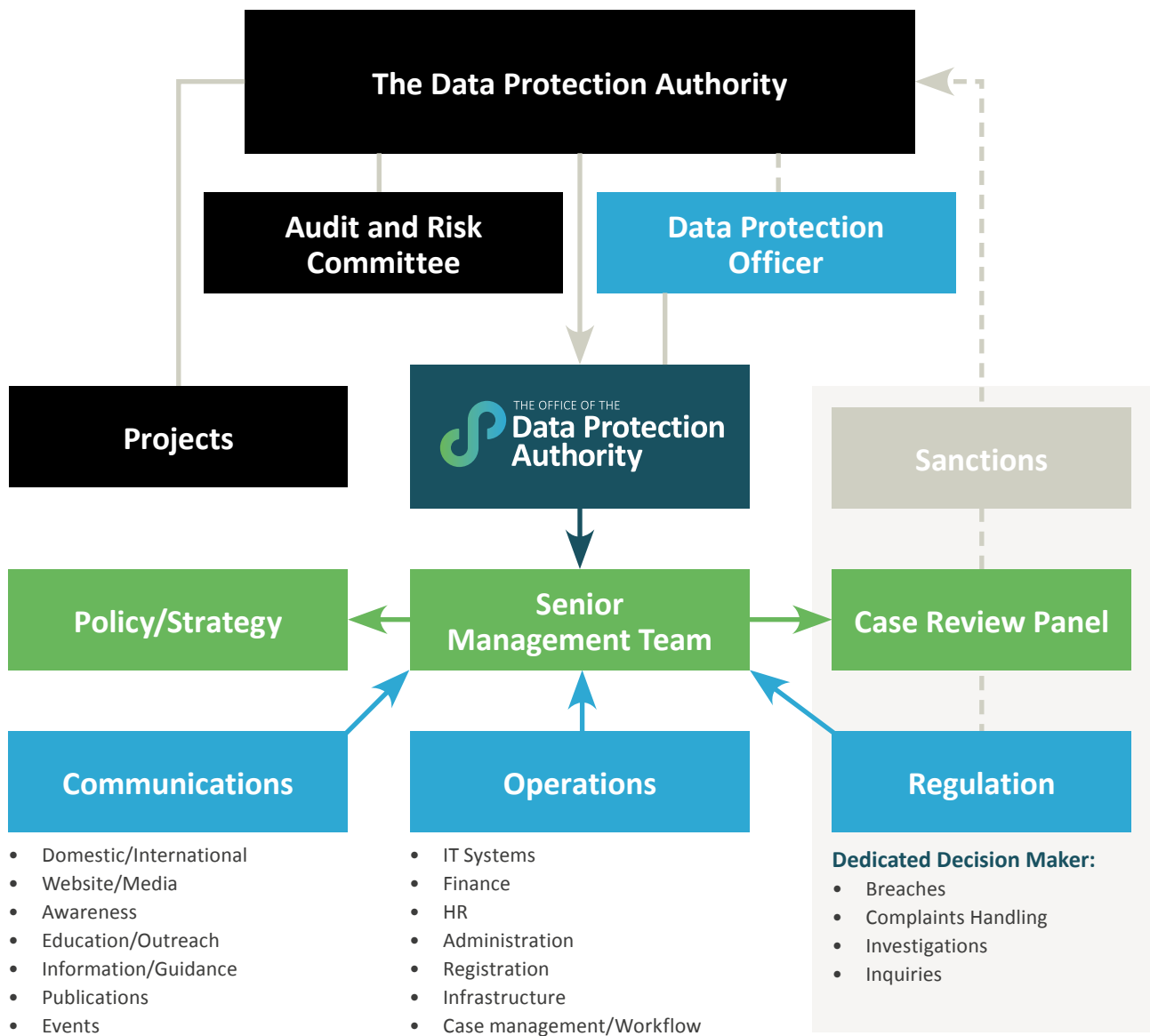


Supports the data economy to embrace innovation



**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

Strategic plan and activities

In 2019 the ODPA published its *Strategic Plan (2019-2022)* which sets out the ODPA's purpose and how it intends to deliver its regulatory objectives effectively and independently.

The digital era brings with it opportunities and challenges and one such challenge is how to regulate effectively. The ODPA recognises that traditional models of regulation need to be reassessed in light of the new environment and whilst learning from the past, wants to ensure it is forward-looking, relevant and responsive.

In being clear about its purpose the ODPA seeks to build cooperation and trust with its regulated community.

The ODPA's key strategic objectives below set out how it seeks to predict and prevent harms to individuals from poor handling of their personal data and ensure that detection and enforcement activities are proportionate and effective.

Key strategic objectives:

- 1** To develop the ODPA's capabilities to deliver on its enhanced statutory duties.
- 2** To be a relevant, responsive and effective regulator.
- 3** To support organisations in delivering their obligations and empower individuals to exercise their rights.
- 4** To develop and maintain effective relationships.
- 5** To elevate discussions around the protection of personal data to engage the community and individuals in a relevant and positive way, recognising the personal, social and economic opportunities and threats that the data economy poses.

Please note, as mentioned in the Introduction, many of the ODPA's strategic activities were delayed during 2019.

This was due to staff time being diverted from these activities to negotiations with officers of the States of Guernsey around the specifics of the ODPA's proposed self-funding model. Further the delay in achieving that approval meant work could not commence on a number of key strands of the strategic activities.

Much thought and hard work has gone in to how to deliver tangible and positive outcomes for the Bailiwick and its citizens, below the Strategic Plan and its associated detailed activities in 2019 is presented:

Look out for our three key strategic projects:

Project Querelis,
The Fandango Project and
Project Bijou

1. To develop the ODPa's capabilities to deliver on its enhanced statutory duties

1.1. Develop and adopt an explicit risk control strategy to manage and prioritise workload by end 2019

Introduction of *Strategic Plan (2019-2022)* which sets out how the ODPa's approach to its regulatory duties and identified four pillars of activity – **Predict**, **Prevent**, **Detect** and **Enforce**.

The ODPa recognise the important role that each pillar plays as well as their interdependence. All ODPa work streams now flow from these areas and inform decisions around resource allocation and prioritisation.

The further planned detailed work in this area is now likely to be completed by Q1 2021 upon implementation of new administration systems. These new systems will allow the ODPa to collect, analyse and use information about the nature of enquiries and complaints which in turn will provide the opportunity to manage risks, assess performance and prioritise certain areas of activities.

1.2. Implement new internal policies and procedures to ensure consistent operational and administrative standards as well as appropriate governance by end 2019

Governance activity in 2019 encompassed four Board Meetings, establishing an Audit and Risk Committee, reviewing the Board's Code of Practice, and commencing governance arrangements around Section 64 activities (the section of the Law that covers the Authority's public statements).

In terms of internal processes and procedures around case-handling, the ODPa initiated Case Review Panels, and launched Phase 1 of **Project Querelis** (which focuses on complaint handling and workflow). **The Fandango Project**, a proposed internal ODPa project spent 2019 awaiting funding approval from The States of Guernsey. Once complete this project will build a fit-for-purpose technology stack (from public-facing website through to back-office systems) allowing the ODPa to work efficiently and effectively.

On staffing matters, the ODPa completed a major revision of the Staff Handbook, updated all staff Terms & Conditions, ran staff sessions covering the Code of Conduct, and the ODPa achieved the IASME Cyber Security Essentials standard.

In addition to these internal activities the ODPa also maintained support for office staff via outsourced IT, PR, HR, financial oversight, and legal advice. On the latter, to reduce costs, the ODPa is working to reduce its future use of external legal resource by growing its internal expertise.

1.3. Complete implementation of the structuring, resourcing and governance plan by end 2019

The ODPa completed its first phase of recruitment which had begun in 2018, and at end of 2019 the office employed 9 permanent staff. This resourcing was informed by the Strategic Plan, to ensure the ODPa had the right mix of skills in the right areas to enable effective delivery of its strategy.

Careful planning for the second phase of recruitment began in late 2019 as the ODPa looks to grow its staff to reduce its reliance, and spending, on outsourced support whilst continuing to be an effective and responsive regulatory office.

1.4. Project management and delivery of the new funding model by 1st quarter of 2020

As at end of 2019, the ODPa were awaiting a decision from the States of Guernsey on approval of its self-funding model, submitted in late 2018. Due to the delay in finalising that matter, this particular activity is likely to be completed in 2021.

1.5. Develop a Regulatory and Enforcement Action Policy that will set out our approach covering detection and enforcement by 1st quarter 2020

This work is ongoing and related to the activity described in 1.1 above. Completion of this work has been affected by the delays in the approval of the ODPA's self-funding model.

Project Querelis, which began in 2019, also supports this activity.

1.6. Play a key role in the Bailiwick's ongoing adequacy review by the European Commission

The Bailiwick is currently recognised as an **adequate** jurisdiction for the purposes of the General Data Protection Regulation (GDPR). In accordance with Article 45 of the GDPR, the European Commission began its assessment the Bailiwick's new legislative framework in April 2019. The Authority continues to work with the States of Guernsey to respond to the European Commission's enquiries and further communications are expected during 2020.

2. To be a relevant, responsive and effective regulator

2.1. Draft a paper setting out our overall approach to regulation and how we seek to reduce harms by 1st quarter 2020

The ODPA's senior leadership team are committed to building a regulatory office that is relevant and effective. It is recognised that in delivering on the regulatory duties of the office, it is important to openly and honestly assess how the objectives can be delivered. Development of this paper is ongoing and will be reviewed alongside the work being done on 1.1 (see above).

2.2. Develop effective mechanisms to resolve and learn from complaints

This activity is where **Project Querelis** sits. The project's initial phase began in 2019 and started shaping how the ODPA processes enquiries from members of the public and complaints made by members of the public against local regulated entities.

Querelis' aim is to ensure that the ODPA has robust and effective processes which enable it to meet its statutory requirements, and that there is consistent and accountable decision making around how enquiries, complaints, and casework completion are handled.

The ODPA also feeds any lessons learned from this area of its work into its communications activity as it is a rich source of real-world examples the whole regulated community can learn from, where appropriate.

2.3. Operate the deployment of resources and staff flexibly and responsively in light of identified compliance and enforcement objectives keeping this under continuous review

The ODPA has a small team of 10 people who were recruited due to their specific attitudes, experience, and talents. Staff are deployed appropriately according to operational and strategic priorities and workloads. This flexible approach, which was in place throughout 2019, gave the ODPA practical experience on which to make informed, and well-thought through decisions on where additional resources may be needed in future.

2.4. Prioritise oversight and engagement with the public sector for all processing but specifically in the delivery of Future Digital Services

Communications with States of Guernsey remain ongoing in this area. The ODPA recognises the huge importance of processing within the public sector. Therefore it is essential that open and timely discussion between the States of Guernsey and the ODPA is maintained as the States progress through their digital transformation programme. The ODPA notes the potential for power imbalance that can exist between the citizen and the State, and the potential harms that can arise for individuals as a result of this, seeking to encourage openness and accountability in all related areas of activity.

2.5. Lead by example in our commitment to data protection and the ethical approach to data governance in everything that we do

The ODPA continues to work hard to embed the highest standards of legal and ethical data handling practices into all external and internal activities, as clearly the standards expected of the regulated community also apply to the ODPA. For example: the ODPA's Privacy Notice is regularly reviewed and updated as its activities evolve, and careful decisions were made about what third party services were selected for the ODPA's social media presence and its event ticketing provider.

2.6. Ensure availability of appropriate legal, technical and communications support through the development of trusted partnerships

Whilst the Bailiwick has had data protection legislation for many years, it was difficult to be specific about the operational requirements of the new office once the new legislation was implemented. For those areas of ODPA activity where there was uncertainty about the level of demand, a decision was made to provide support through the use of professional contracted partnerships. These areas are legal, human resources, IT, PR, finance, and technical support.

Putting these trusted partnerships in place allowed the ODPA to understand from experience exactly what the nature of demands are in the new regime, further allowing more accurate analysis of the effective allocation and expenditure of resources in future. These contracts are kept under constant review to ensure best value and to inform decision-making.

2.7. Keep international data protection and associated developments under continuous review

The ODPA's senior team ensures awareness of relevant national and international developments and continues to participate in European and International conferences of Data Protection Authorities. For 2019 this included attendance at: EU regulator conference in Georgia (Spring 2019); the ICDPPC in Tirana (October 2019); the Open Data Institute (ODI) Summit (November 2019).

The ODPA also took part, for the first time, in a Global Privacy Enforcement Network (GPEN) 'Privacy Sweep' of local healthcare providers in September/October 2019. All ODPA staff also joined the International Association of Privacy Professionals (IAPP) in 2019.

2.8. Provide support to employees for continuous learning around developments in data protection, privacy and associated issues

All ODPA staff have been on structured courses with a view to achieving formal qualifications. Where appropriate, staff also maintain contact with regulatory staff in other jurisdictions to share best practice.

To ensure technical knowledge is shared effectively across the ODPA team, staff take part in regular 'knowledge sharing' sessions where certain issues/subjects are explored in depth either through sessions delivered by senior staff, or via external bodies (e.g. webinars).

During 2019 all ODPA staff were involved in the development and delivery of its events programme, which was an opportunity for new starters to increase their knowledge and awareness of the Law. More informally, the ODPA staff room includes a well-stocked library where staff are encouraged to take time each week to focus on reading the Law, and educating themselves on the wider issues that surround it.

2.9. Utilise the skills and experience of The Data Protection Authority Members to improve the knowledge of ODPA staff

During 2019 the ODPA was very grateful to Authority Member Christopher Docksey for delivering two knowledge sharing sessions on the Law's accountability principle, and relevant European Court of Human Rights and Court of Justice of the European Union legal cases.

2.10. Ensure all ODPA staff are supported and valued allowing them to contribute to the overall aims and success of the organisation

The individuals who make up the ODPA team and the Authority Members themselves remain the most valuable asset, and they are treated as such. All staff are valued for the unique talents they each have and the important part they each play in ensuring the ODPA remains an effective regulator.

The ODPA's work culture is supportive, inclusive, and encourages each team member to be themselves. Because there was a lot of change, growth, and mounting pressure on the ODPA's small team in 2019 they chose to focus heavily on staff well-being and team development. This focus supported staff to remain effective as a team, building on the existing genuine commitment staff have not only to the ODPA's mission, but to each other.

2.11. Be open to constructive exploration of innovative practices and activities within the regulated community

This specific activity was added to the Strategic Plan in December 2019 in response to conversations between the ODPA and industry. It reflects the ODPA's huge appetite for supporting innovation in the local economy, by working constructively with local organisations who may need support whilst exploring new ways of doing things that involve people's data.

3. To support organisations in delivering their obligations and empower individuals to exercise their rights

3.1. Complete the website and CRM project to improve the user experience as well as the internal administrative processes by 1st quarter 2020

This activity was ongoing at end of 2019 due to the ODPA's self-funding model awaiting States of Guernsey approval. Despite this delay ODPA staff began preparations for the project to understand, map and streamline internal processes in readiness.

3.2. Explore the targeting of regulatory support and response to different sectors by end 2020

In 2019 the ODPA piloted specific sector support activities to Healthcare providers, as this sector is accustomed to regulation and presents a high-risk to individuals due to its routine processing of special category data. This support took the form of the GPEN Privacy Sweep which took place in September/October 2019, and two free events on 'Data Protection in Healthcare'.

The other sector the ODPA targeted was start-up/micro/small businesses, many of whom may be less accustomed to regulation in this area and may not have the resources available to support their own compliance. In recognition of the specific challenges faced by these types of local businesses, the ODPA rolled out a suite of free, accessible and convenient resources they can make use of (fortnightly drop-ins, free events programme, podcast series, and focus on plain English).

These activities around Healthcare and small businesses allowed the ODPA to test the efficacy of its approach across a range of scenarios, and inform its future approach.

3.3. Explore alternative dispute resolution mechanisms for complaint handling by 2nd quarter 2020

The ODPA acknowledge that this is a very difficult area which continues to be explored. As defined in the ODPA's Strategic Plan, this activity falls in the 'Prevent' category – in this case, preventing the circumstances arising that would lead someone to suffer harm and to lodge a formal complaint against a local organisation due to the way they might be handling personal data.

A key aspect of this activity is about empowering individuals who are disputing a local organisation's use of their personal data. To this end the ODPA made some subtle improvements to its website so that the 'Your Rights' area was geared more towards arming individuals with plain English descriptions of their ten rights under the Law, together with simple step-by-step advice on how they can exercise their rights.

Giving individuals the knowledge, power, and support to exercise their rights in this way is an effective tool in preventing those individuals being harmed due to their data being misused.

3.4. Deliver on our Communications Strategy, keeping it under continuous review and exploring effective communication tools and methods for all audiences

The ODPA launched a number of initiatives as part of its Communications Strategy during 2019.

To enable businesses of all sizes to access the ODPA's technical expertise and support, in March 2019 a calendar of free fortnightly drop-in sessions began. Alongside the drop-ins, the ODPA also began offering 'study visits' from March 2019. Two such visits were completed during the year.

This was followed in July 2019 by the launch of regular free events, which was itself shaped by a public consultation exercise during the earlier part of the year.

The ODPA podcast series started in March 2019, a total of eight episodes published during the year.

The ODPA monthly newsletter subscriber list grew to 403 during the year, and its LinkedIn page had 1,183 followers by the end of the year.

3.5. Provide clear, meaningful and inspiring communications, guidance and engagement

The ODPA continued its focus on plain English in all its communications materials, and used simple infographics where possible.

In early 2019 it produced a leaflet aimed at the general public called 'Why you should care about data protection'. In March 2019 it published a general guidance document to help local organisations through the end of the law's transition period which ended on 25 May 2019. Official guidance on the new right of Data Portability which came into effect on 25 May 2019 was also published at the same time.

3.5 Continued

The majority of the ODPa's engagement activities in 2019 were achieved via its events programme. A proposed programme of events was put out for public/industry consultation in April 2019. Following this consultation, 7 event subjects were developed and delivered. All events (listed below) were free, and all sold-out within hours of being announced. Two event subjects attracted very long waiting lists so a second session was run for each of those.

1. 28 Jan 2019: Data Protection Day.
2. 10 Apr 2019: Data Protection Forum: public/industry consultation session.
3. 10 Jul 2019: The Seven Data Protection Principles.
4. 4 Sep 2019: Data Protection in the Workplace
5. 18 Sep 2019: Doing the right thing with personal data – data ethics in practice
6. 2 Oct 2019: How to respond to 'subject access requests'
7. 16 Oct 2019: The human at the heart – individuals' rights under data protection legislation
8. 27 Nov 2019: Data breaches – human error vs. technology (two sessions held on same day due to demand)
9. 11 Dec 2019: Data protection in Healthcare (two sessions held on same day due to demand)

All the above events were delivered by either the commissioner or the deputy commissioner in the ODPa's 'Aristotle Suite' – a flexible space that can be used as a single large boardroom / event space, or two meeting rooms.

3.6. Encourage industry compliance through enlightened self-interest and cultural change

The ODPa has been focusing on this issue for some time, to move data protection compliance away from a one-off box-ticking exercise and more towards an ongoing human-centric activity built on cultural engagement and influence.

In June 2019 this focus manifested itself into a culture change project which seeks to encourage everyone in the Bailiwick to share knowledge, ideas and stories about why data matters as a way of building understanding, engagement, and compliance within the field of data protection. **Project Bijou**, as it is known, is due for launch in 2020.

3.7. Raise data protection awareness in school-age children

This activity forms part of the ODPa's commitment and statutory obligation to promote public awareness of data protection risks, rules, rights and safeguards, particularly in relation to children. Building children's awareness in this area has several benefits including: they will be less likely to fall victim to harms that may arise from misuse of their personal data; they may share their new awareness with adults in their lives, so the message is spread wider; when these engaged and informed young people enter the workforce their awareness, attitudes, and actions could serve to strengthen overall compliance.

To achieve these benefits, formal preparation of the ODPa's schools programme began in April 2019. Age-appropriate resources from primary school through to post-16 were developed and tested with focus groups in local schools.

This proactive engagement with local schools led to the ODPa being invited to the Guernsey College of Further Education's 'Freshers Fair' in September 2019, as well as being invited to speak to year 13 students at The Grammar School.

In February 2019 the ODPa again sponsored and exhibited at 'Digital ACE', a public event attended by ~2,000 people, mainly families with young children.

Throughout 2019, the deputy commissioner continued to sit on the Bailiwick's Online Safety Committee which meets bi-monthly. Other members of this multi-disciplinary committee include teachers, telecoms providers, law enforcement representatives, and representatives of safeguarding agencies. A sub-group of the Online Safety Committee is responsible for the organisation of the Digital ACE event and the deputy commissioner played a part in this.

3.8. Engage with and support the Bailiwick's data protection association

In January 2019 the ODPa held an event primarily aimed at members of this association to mark Data Protection Day. The Authority Chair, Richard Thomas, also in January spoke at an event organised by the association.

Throughout the year the ODPa allowed the association free use of its boardroom. In late 2019 the ODPa's outreach officer made contact with the association's chair to ensure continuation of regular, formal support for the association and its members.

3.9. Engage with and support representative organisations to improve industry and public awareness and understanding

The ODPa commissioner and deputy commissioner are regularly invited to speak at local industry events. In 2019, the ODPa also accepted invitations to speak at local schools and at industry events in the UK and Ireland. Details of all these speaking engagements are listed following.

3.9 Continued

In addition to providing speakers, the ODPA also made regular contact with many local industry associations and groups to ensure that key messages were reaching their audiences.

1. Appleby seminar: 'Crisis? What crisis?' (16 Jan 2019)
2. Mourant (internal update for staff) (16 Jan 2019)
3. NED Forum (13 Feb 2019)
4. Lion's Club (12 Mar 2019)
5. Chamber of Commerce - April lunch (15 Apr 2019)
6. Mourant - 'Guernsey In-house Network' launch event (14 May 2019)
7. IoD Breakfast - year on from law change / transition (17 May 2019)
8. Data Protection World Forum - 'GDPR a year on: A regulator's view' (3 Jun 2019, London)
9. Carey Olsen: Data Protection in the financial services industry (4 Jun 2019)
10. Guernsey Community Foundation (staff awareness session) (17 Jun 2019)
11. Safer (staff awareness session) (25 Jun 2019)
12. Barclays AI Frenzy – Digital Greenhouse (28 Jun 2019)
13. GTA - 2019 Compliance CPD Series (4 Jul 2019)
14. GCFE: Freshers' Day (13 Sep 2019)
15. PrivSec (23-24 Sep 2019, Dublin)
16. Guernsey Community Foundation: charity leaders event (10 Oct 2019)
17. BPP CI: The data protection horizon - 2020 and beyond (17 Oct 2019)
18. GIFA Academy: overview of law and why it matters (23 Oct 2019)
19. Executive Leaders Network: Data Protection & Privacy Conference (14 Nov 2019, Reading)
20. GCFE talk to BTEC business students: data protection, Freedom of Information and Computer Misuse (15 Nov 2019)
21. Data protection for start ups: why it is never too soon to think about your data (22 Nov 2019) (BGDPA Panel Session for Global Entrepreneurship Week)
22. Data Governance, Europe (27-28 Nov 2019, London)
23. Talk to Grammar School year 13 students re: facial recognition (2 Dec 2019)

The ODPA continued to be represented on the local Caldicott Committee during 2019 with the deputy commissioner attending the quarterly meetings. The Caldicott Committee comprises representatives of local healthcare organisations and is a forum to discuss the governance of clinical information.

4. To develop and maintain effective relationships

4.1. Work with industry, key bodies, representatives, associations and professionals, recognising the important role they play in shaping the regulatory environment for regulatees whilst being constantly vigilant to protect against regulatory capture

In the context of personal data, the regulatory environment is horizontal across the whole community and the ODPA recognises the need to engage with representative bodies to assist in communicating information and guidance to as wide an audience as possible.

Communication from the regulated community to the regulator are as important as communication from the regulator to the regulated community.

The ODPA works to identify all such bodies in the Bailiwick and proactively communicate where that is appropriate. This communication helps the ODPA understand the needs of specific groups within the regulated community and how best to create and present relevant information to them about their statutory duties.

The ODPA also seeks their assistance and support in disseminating guidance and updates that may be useful to them by presenting at their events or contributing to publication. They are also encouraged to get involved with the ODPA rolling events programme, including 'drop-ins'. In working with any external body or representative, the ODPA conducts itself with the highest ethical and legal standards to prevent actual, or perceived, regulatory capture.

4.2. Ensure open and constructive engagement with the States of Guernsey in discussions around legislative and policy areas involving the processing of personal data

The ODPA continues to communicate regularly with key officers of the States of Guernsey to develop open and constructive relationships which enable timely discussions around proposed legislative and policy changes which involve personal data. Where prior consultation is required under section 46, the ODPA endeavours to engage and respond promptly and comprehensively.

4.3. Explore the use of Memorandums of Understanding with other bodies to ensure a consistent and coherent regulatory and enforcement environment for regulatees

Following on from the creation of an Memorandum of Understanding (MoU) with the Committee for Home Affairs in 2018, governing the relationship between the two entities, the ODPA sought to build relationships with other regulators and formalise those in MoUs.

Given business activities are reliant on a variety of personal data, there are overlaps between the ODPA's functions and other local regulators and MoUs between these organisations will assist in underpinning a robust regulatory regime locally.

The global nature of the data economy means that there will be occasions when the data processing activities the ODPA is looking at will stretch beyond the Bailiwick's borders. To assist this, and build upon the international obligations laid down in the Law, work has commenced to draw up MoUs with data protection regulators in other jurisdictions, so that the regulatory mechanism more closely reflects the international nature of data use.

4.4. Continue to work with other regulators across the EU and beyond in strategic and operational matters

The ODPA is an active member of BIIDPA – a collective of British, Irish and Islands' Data Protection Authorities of the UK, Ireland, Cyprus, Jersey, Isle of Man, Malta, Guernsey, Gibraltar and Bermuda.

A member of the ODPA casework team visited the UK's ICO in April 2019, and Authority Member Christopher Docksey addressed the plenary session of the ICDPPC conference in October 2019. He spoke on the accountability principle, and referenced the ODPA's work.

The ODPA continue to participate in the European and International conferences for Data Protection Authorities which provide a forum for the exchange of ideas and learning experiences. It is anticipated that the expectations regarding cooperation and consistency as set out in the GDPR will develop for all Data Protection Authorities in the next few years.

4.5. Continue to work with the European Commission during and beyond formal assessment of adequacy

The GDPR's 'adequacy' requirements will likely require ongoing assessment and review to ensure that approved jurisdictions continue to provide robust and independent regulatory oversight. It is expected that such reviews will take the form of regular updates to the European Commission, as well as responding to questions from them.

In 2019 the ODPA provided a substantial contribution to the States of Guernsey's submission to the European Commission, and will continue to provide support to the States of Guernsey and engage directly with the European Commission where that is appropriate.

4.6. Where most effective, seek representation and attendance at key industry and regulator events

The commissioner and other senior ODPA staff attended the following regulatory events:

1. European Spring Conference (Tbilisi, 8-10 May 2019)
2. BIIDPA (Jersey, 26-28 June 2019)
3. ICDPPC (Tirana, 20-24 October 2019)

See also related activities detailed in 3.9 above.

5. To elevate discussions around the protection of personal data to engage the community and individuals in a relevant and positive way, recognising the personal, social and economic opportunities and threats that the data economy poses

5.1. Explore the feasibility of holding a conference to encourage learning and discussion for the wider community by end 2019

Following the success of the 2019 free events programme, the ODPA is satisfied that there is considerable demand for a conference. Planning has commenced on the scope, topic, and aim of the conference. The plan is to launch **Project Bijou** at this conference.

5.2. Regularly publish comment and thought pieces on data related matters

The ODPA is fortunate to have a positive relationship with local journalists, and as such it is regularly approached to comment on data-related news stories.

The ODPA works with local journalists and editors to provide factual information, building awareness of the Law, and how data harms affect people. Throughout 2019 the ODPA continued supplying local media with bi-monthly statistics and supporting commentary around self-reported data breaches. This proactive media engagement, together with other activities resulted in 64 news articles, 13 broadcast media segments, and five magazine/editorial pieces during 2019.

The commissioner also published regular blogs and letters, either via the ODPA's website or directly in magazines/newspapers.

5.3. Provide relevant comment to the media where this advances our aims and encourages broader discussion and awareness

Where appropriate, and whenever possible, the ODPA will provide commentary to local media either proactively (e.g. via the bi-monthly breach statistics press releases) or reactively in response to a journalist making contact on a specific issue.

Related to this activity is the establishment, in 2019, of the Authority's Section 64 Committee. This comprises three Authority Members who together approve any 'Public Statements' (as defined in section 64 of the Law) regarding the ODPA's enforcement and related activities. This Committee has been formed as the issuing of public statements is a reserved function of the Authority, and cannot be delegated.

5.4. Provide a supportive and stimulating environment for staff to allow them to be exemplars of their professions

The aim is for each employee to work for the ODPA because it is rewarding for them as individuals and they are empowered to support the wider Bailiwick community to aspire to excellence in data protection engagement by businesses and individuals alike. In 2019 much effort was put in to involve and engage all staff members in issues the ODPA was involved in and to encourage a broader intellectual engagement with data-related issues locally and internationally.

5.5. Connect with industry and community representative organisations to encourage their engagement in supporting the data rights and obligations of those they represent

Much of this activity in 2019 is detailed in 3.9 above, as a result of the ODPA's fortnightly drop-in sessions, events, study visits, and invited speaking engagements.

The contact with a variety of organisations and industry bodies throughout the year meant that the ODPA was able to identify sectors with specific needs and tailor the delivery of support to address those needs. An example was the specific 'Data Protection in Healthcare' event, run as two sessions in December 2019, that enabled a particular focus on the particular areas of risk that processing in a healthcare environment brings with it.

The ODPA recognises that you cannot connect people with their rights as individuals, or their obligations as part of an organisation, if they see the Law as merely a prompt for a once-a-year box ticking paper exercise. Instead the ODPA seeks to elevate and embed data protection as a human-centric ongoing activity that evolves, that is never 'done' and underpins good governance practices with trust and confidence. One of the mechanisms for embedding this outlook is via **Project Bijou**'s planned activities.

Case studies

The Authority has a statutory duty to promote awareness of data protection issues. Detailed below are three anonymous case studies of individual's complaints investigated by the ODPa, and what the wider regulated community can learn from them.

The case studies include some use of the following legal terms:

Legal terms

Plain English



'Complainant'

The **person** who lodged the complaint with the ODPa about how their personal data was being (or had been) used.



'Data subject'

The **person** that the data in question relates to.



'Controller'

The **organisation/business** that decided how personal data was to be used, and in the context below who the complaint was about.



'Self-reported breach'

This is the act of **completing the ODPa's breach report form** in order to fulfil a controller's legal obligation to let the ODPa know their organisation/business has experienced a personal data breach.



'Subject access request'

This is when a person **uses their legal right** to ask an organisation/business what data is held about them and to seek access to that data.



'Operative provision'

This means **any part of the Law** that a controller must comply with.

Case study #1

Background

An email, intended for the complainant, was sent by an employee of the company ("the controller"). This email contained sensitive financial information as well as references to the complainant's health. The information was included in the body of the e-mail (i.e. not sent as an attachment) and the email was not encrypted.

The controller sent the email to an incorrect recipient having missed out a letter in the email address. The incorrect recipient of the e-mail happened to be an acquaintance of the complainant, further exacerbating the situation. The complainant was made aware of the error when the acquaintance forwarded them the email. This incident caused considerable distress to the complainant.

The complainant contacted the controller regarding the error and as a result, the controller self-reported the breach to the ODPA. An e-mail was sent by the controller to the unintended third-party recipient requesting the email be deleted but no response was received.

The complainant was left feeling exposed in light of the personal and sensitive information that had been shared with someone they would never have chosen to share such information with.

Learning points

This incident demonstrates how seemingly minor errors can cause significant distress. Whilst mistakes are inevitable in any workplace, processes can be put in place to minimise the harm these mistakes cause, such as encrypting personal data or other appropriate measures. Staff must also be trained regularly and reminded to consider the impact of the personal data they handle falling into the wrong hands.

Case study #2

Background

The complainant was approached by a recruitment agency of whom they had previously been a client. The recruitment agency alerted the complainant to a vacancy that appeared to match the complainant's skill set.

The complainant agreed to meet the recruitment agency to discuss the vacancy further. During this meeting, the complainant informed the agency that they did not wish for their details to be shared with the recruiting company at that time but would read over the job description and consider their options.

In the meantime, whilst carrying out duties in their current job role which included liaising with external companies, the complainant was alerted by a company that the recruitment agency had shared a version of the complainant's CV with them.

When the complainant approached the recruitment agency with their concerns, they were assured that the CV details were anonymised, and they could not have been identified from the correspondence. The complainant had suspicions that this was not the case owing to the fact the recipient of their CV had clearly been able to identify them from the information received. It was at this point the complainant felt they needed to make a formal complaint to the ODPA.

Upon the ODPA conducting an investigation, it transpired that the recruitment agency had included the complainant's name in the subject heading of the email, thus negating any anonymisation of details within the CV itself.

When approached by the ODPA, the recruitment agency stated that they had the complainant's consent to share the CV. However, when asked to provide evidence of that consent, they were only able to point to a meeting note that implied consent had been given by the complainant for the sharing of their personal data.

The ODPA found that the recruitment agency had been unable to demonstrate that they had specific, informed and freely given consent from the complainant that would have allowed them to share their personal information in an unredacted or otherwise not anonymised format.

Learning points

There are three lessons to learn from this incident. Firstly, anonymisation is a valuable tool that allows data to be shared, whilst preserving privacy, but the preservation of privacy must be stringently ensured. Secondly, The Data Protection (Bailiwick of Guernsey) Law, 2017 is unequivocal in stating that it is a controller's responsibility to 'clearly demonstrate that the data subject has given the consent', this must be 'presented in a manner which is clearly distinguishable from other matters'. Thirdly, organisations must keep in the forefront of their minds the very real harm their actions can cause to people's careers, reputations, and personal lives due to their data being mis-used.

Case study #3

Background

The complainant made a Subject Access Request to a healthcare provider to obtain information relating to the provision of medical care. Acknowledgement of that request was promptly received.

After a period of over one month, no further communication from the healthcare provider had been forthcoming. The complainant contacted the healthcare provider seeking an update on their Subject Access Request to which the healthcare provider responded claiming that they would have to apply an extension period of two months, provided for by section 27(4) of the Law, to the Subject Access Request. No reasoning was given to justify the need for the extension period.

A further two months passed where the complainant received no further communication from the healthcare provider. Following e-mail correspondence with the healthcare provider, it became clear that the healthcare provider were applying another extension to the Subject Access Request for which they notified the data subject in writing. This time however, the healthcare provider cited the range and complexity of the systems the personal data was stored on as the reason for the extension.

The complainant made a complaint to the ODPA.

A subsequent investigation by the ODPA found that the healthcare provider breached an operative provision of the Law – namely section 27(4) relating to compliance with the ‘designated period’.

The Data Protection (Bailiwick of Guernsey) Law, 2017 is clear that in order for a controller to appropriately apply an extension to a Subject Access Request under section 27(4), the ‘complexity’ of the request must be taken into account as opposed to the complexity of the controller’s systems on which the personal data is held. Furthermore, in instances where an extension is valid, this can only be applied once and the request must be fulfilled by the end of the initial extension period.

Learning point

A key learning point that arises from this situation is that controllers must consider the request itself, rather than internal factors when determining the appropriateness of applying an extension to a Subject Access Request.

Key statistics

For the period 1 Jan 2019 – 31 Dec 2019

2,395

Number of **additional local organisations** who fulfilled their legal obligation to register with the ODPA

£1,164,773

The ODPA's **operating budget**

67

Number of data protection **complaints** received

50

Number of **investigations** conducted by the Authority

4

Number of **inquiries** conducted by the Authority

8

Number of **investigations and inquiries resulting in a determination** that an operative provision has been or is likely to be breached

6

Number of **sanctions** imposed by the Authority under section 73
Note: all six sanctions imposed were formal reprimands

54

Number of representatives from organisations who attended ODPA fortnightly **drop-in sessions**

11

Number of **free public/industry events** held at ODPA premises

325

Number of **people registered to attend** ODPA public/industry events

23

Number of **invited speaking engagements** taken by the commissioner and deputy commissioner

Members' Report and Audited Financial

Period Ended 31 December 2019

The Data Protection Authority

Authority Information

Members

Richard Thomas CBE (Chairman)
John Curran
Christopher Docksey
Simon Entwisle
Mark Lempriere
Jennifer Strachan
Emma Martins (Non-voting member)

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
Rue du Pre
St Peter Port
Guernsey
GY1 3LL

The Data Protection Authority

Contents

	Page
Members' Report	1 - 2
Independent Auditor's Report	3 - 5
Statement of Comprehensive Income	6
Balance Sheet	7
Notes to the Financial Statements	8 - 11
Detailed Statement of Comprehensive Income (unaudited)	12

The Data Protection Authority

Members' Report For the Year Ended 31 December 2019

The members present their report and the financial statements for the year ended 31 December 2019 (comparative period from 31 May 2018 to 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 surplus for the year is set out in detail on page 6.

Members

The members who served during the year were:

Richard Thomas CBE
Simon Entwisle
John Curran
Christopher Docksey
Mark Lempriere
Jennifer Strachan
Emma Martins (Non-voting member)

Disclosure of information to auditor

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 auditor is 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 auditor is aware of that information.

The Data Protection Authority

Members' Report (continued) For the Year Ended 31 December 2019

Independent auditor

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

Post Balance Sheet event

COVID-19 is a developing situation and as of 21 May 2020, the assessment of this situation will need continued attention and will evolve over time. Having considered future cash flow forecasts, the Members, continue to believe that it is appropriate to prepare the financial statements on a going concern basis. This is because the Data Protection (Bailiwick of Guernsey) Law 2017 requires the States of Guernsey to provide funds sufficient to enable the Authority to properly and effectually discharge its functions.

The rapid development and fluidity of the COVID-19 virus makes it difficult to predict the ultimate impact at this stage. The Members do not underestimate the seriousness of the issue and the inevitable effect it will have on both the Guernsey and global economy and many businesses across the world. The Members expect the COVID-19 pandemic may reduce future annual registration fees below those currently forecast, although at this stage the full financial effect cannot be estimated.

Going concern

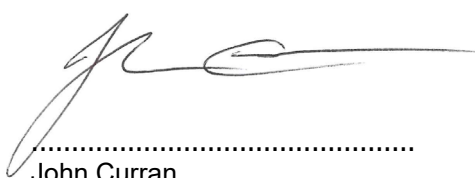
The Authority is in a net liability position at the Balance Sheet date and therefore will require funding to support the future working capital and operational requirements. The members are satisfied that the Authority will be able to meet its liabilities as and when they fall due as a result of the 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.

The Members are closely monitoring the latest developments arising from COVID-19. The members have considered the possible future impact on the level of income arising from annual notification fees and remain confident that the going concern basis remains appropriate in preparing these financial statements.

This report was approved by the members on 21 May 2020 and signed on its behalf.



Richard Thomas CBE (Chairman)



John Curran

The Data Protection Authority

Independent Auditor's Report to the Members of The Office of the Data Protection Authority

Opinion

We have audited the financial statements of The Data Protection Authority (the 'Authority') for the year ended 31 December 2019 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 2019 and of its surplus for the year 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.

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.

Independent Auditor's Report to the Members of The Office of the Data Protection Authority (continued)

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.

Use of our report

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.

The Data Protection Authority

Independent Auditor's Report to the Members of The Office of the Data Protection Authority (continued)



Grant Thornton Limited
Chartered Accountants
St Peter Port
Guernsey

22 MAY 2020

The Data Protection Authority

Statement of Comprehensive Income For the Year Ended 31 December 2019

	2019 £	2018 £
Income	1,217,501	415,059
Administrative expenses	(1,164,773)	(554,129)
Surplus/(deficit) for the year/period	52,728	(139,070)

There is no difference between the surplus for financial year ended 31 December 2019 or deficit for the financial period ended 31 December 2018 stated above and total comprehensive income.

The results above derive from continuing activities.

There was no other comprehensive income for 2019 (2018: £nil).

The notes on pages 8 to 11 form part of these financial statements.

The Data Protection Authority

Balance Sheet As at 31 December 2019

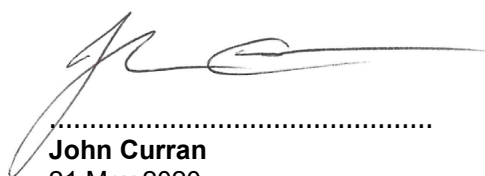
	Note	2019 £	2018 £
Fixed assets			
Tangible assets	4	123,722	134,533
Current assets			
Debtors and prepayments	5	12,856	96,956
Cash at bank and in hand		162,506	376,446
		<u>175,362</u>	<u>473,402</u>
Current liabilities			
Creditors: amounts falling due within one year	6	(385,426)	(747,005)
Net current liabilities		<u>(210,064)</u>	<u>(273,603)</u>
Net liabilities		<u>(86,342)</u>	<u>(139,070)</u>
Reserves			
Deficit		<u>(86,342)</u>	<u>(139,070)</u>
Total reserves		<u>(86,342)</u>	<u>(139,070)</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 by:



Richard Thomas CBE (Chairman)
21 May 2020



John Curran
21 May 2020

The Data Protection Authority

Notes to the Financial Statements For the Year Ended 31 December 2019

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.

The Members are also closely monitoring the latest developments relating to COVID-19. The Members have assessed the impact on the level of income arising from annual notification fees and remain confident that the going concern basis remains appropriate in preparing these financial statements.

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. Income from annual notification fees is recognised upon receipt.

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.

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.

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

The Data Protection Authority

Notes to the Financial Statements For the Year Ended 31 December 2019

1. Accounting policies (continued)

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.

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 year was 10 (period ended 31 December 2018: 7).

3. Taxation

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

The Data Protection Authority

Notes to the Financial Statements
For the Year Ended 31 December 2019

4. Tangible fixed assets

	Leasehold improvements £	Fixtures and fittings £	Office equipment £	Total £
Cost				
At 1 January 2019	65,731	1,262	76,009	143,002
Additions	-	500	17,236	17,736
At 31 December 2019	65,731	1,762	93,245	160,738
Depreciation				
At 1 January 2019	2,497	12	5,960	8,469
Charge for the year	10,959	298	17,290	28,547
At 31 December 2019	13,456	310	23,250	37,016
Net book value				
At 31 December 2019	52,275	1,452	69,995	123,722
At 31 December 2018	63,234	1,250	70,049	134,533

5. Debtors and prepayments

	2019 £	2018 £
Amount receivable from the States of Guernsey	-	76,865
Prepayments	12,856	20,091
	12,856	96,956

The Data Protection Authority

Notes to the Financial Statements For the Year Ended 31 December 2019

6. Creditors

	2019 £	2018 £
Trade creditors	17,325	66,162
Deferred rent	36,022	34,422
Amount payable to the States of Guernsey	243,788	631,055
Accruals	88,291	15,366
	<u>385,426</u>	<u>747,005</u>

The amount payable to the States of Guernsey is interest free, unsecured and has a future payment date that is still to be agreed.

7. Commitments under operating leases

At 31 December 2019 the Authority had future minimum lease payments under non-cancellable operating leases as follows:

	2019 £	2018 £
Within one year	76,848	67,242
Within one to two years	76,848	76,848
Within two to five years	192,120	268,969
Total	<u>345,816</u>	<u>413,059</u>

8. Post balance sheet events

COVID-19 is a developing situation and as of the date of approval of these financial statements, the assessment of this situation will need continued attention and will evolve over time. From the view of the Members, COVID-19 is considered to be a non-adjusting subsequent event and as a result, no adjustment is made in these financial statements. The Members will be closely monitoring developments relating to COVID19 and the possible future impact on the Authority.

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 Year Ended 31 December 2019

	2019 £	2018 £
Income	1,217,501	415,059
Administrative expenses	(1,164,773)	(554,129)
Surplus/(deficit) for the year/period	52,728	(139,070)
Income		
Annual notification fees	214,100	90,515
States of Guernsey grant	998,000	292,768
Other income	5,401	31,776
	1,217,501	415,059
Administrative expenses		
Salaries and other staff costs	655,957	279,641
Members fees	26,833	21,875
Rent, rates and premises expenses	101,691	49,686
Legal and professional fees	168,637	51,163
Advertising and communications costs	29,219	20,298
Travel and entertaining	57,755	36,721
IT costs	63,189	69,547
Depreciation	28,547	8,469
Office and sundry expenses	25,005	13,150
Insurances	7,940	3,579
	1,164,773	554,129

Excellence Through Ethics.