

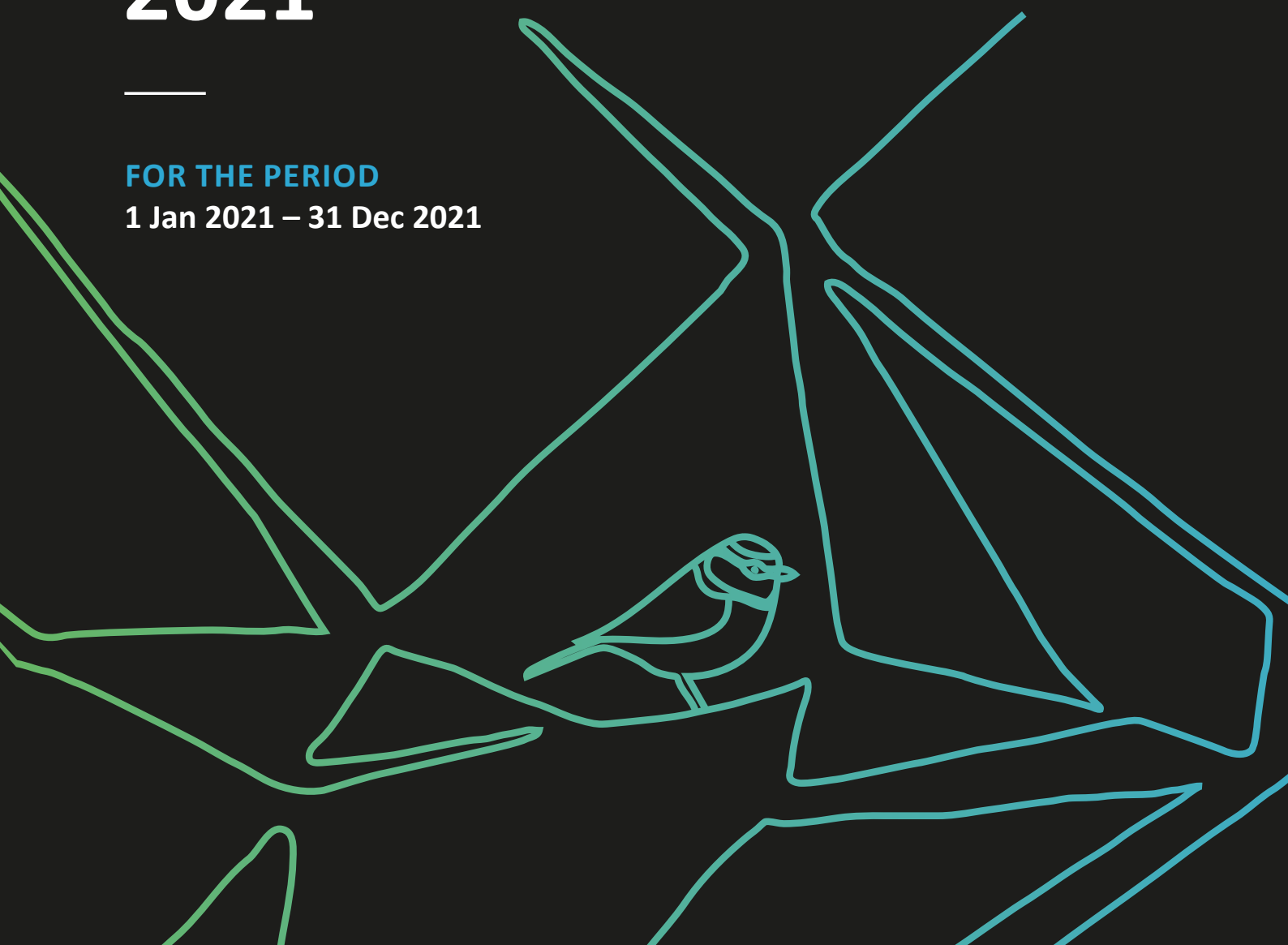
# Annual Report

**2021**

---

**FOR THE PERIOD**

**1 Jan 2021 – 31 Dec 2021**



# Contents

Foreword	2
Introduction	4
About the Authority	5
Organisational chart	6
Data protection in Plain English	7
Executive summary	8
Strategic plan and activities	10
Case studies	19
Key statistics	24
Casework annex	25
Members' report and audited financial statements	37



# Foreword

---



**Richard Thomas CBE**

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

April 2022

## Protecting people. Promoting prosperity.

**Protecting people. Promoting prosperity. These are the fundamental aims of data protection and they are the outcomes which the Guernsey Data Protection Authority seeks. This Annual Report documents the progress we have made over the past year.**

Personal data now lies at the very heart of the digital economy in ways which were unimaginable just 20 years ago. Handling that information well is vitally important for the trust which has to be built and maintained. The ODPA primarily exists to help organisations get it right and to help people safeguard their own interests and understand their rights. We are educators and promoters of good practice.

We also enforce the law and handle complaints. We have not needed to impose any fines this year. We hope that this indicates that public and private sectors are taking their responsibilities seriously, though we have had to issue a number of reprimands. These highlight examples of (relatively minor) non-compliance, but also signal how to avoid problems in the future. Complaints, some raising complex factual and legal issues, can take time to resolve, but we cannot provide redress and their primary value lies in providing raw intelligence.

We are fortunate to have the ability to innovate and build a distinctive reputation for the ODPA and, by extension, the Bailiwick. The prolonged pandemic restrictions have forced us to find and develop new ways of working. The social initiative which we launched in 2021, Project Bijou, has demonstrated new ways of getting a wide range of people to share their stories, to explore data protection issues and to engage others. It has brought home that doing data protection well is much more a behavioural and cultural challenge than a matter of

legal compliance. The Project enabled us to welcome virtually to the Bailiwick some very distinguished participants from around the world as well as many local contributors. Project Bijou continues into 2022 and already our work with the Youth Commission is promising exciting results.

The ODPA has established its foundations. The Fandango Project, to put in place necessary technology and a new website, was completed on schedule and under budget. This enabled the first round of registrations and fee collection to proceed remarkably smoothly in the first two months of the year. Although this took time, we were pleased to find an acceptable formula for repaying to the States of Guernsey the loans which had been needed to get us started. We finally find ourselves on a sound financial footing.

But it is people which make the ODPA. The members of the Authority have ultimate responsibility for strategy, oversight and ensuring that the *"object of [the] Law is being attained"*. I am proud of the way in which the Board has worked collegiately (and largely remotely) to fulfil its remit. Special recognition is owed to Jennifer Strachan, whose term of office ends in May 2022. As a founding member, Jennifer has been a real tower of strength and inspiration. She has especially urged us to understand and respond to the needs of the all-important small business community. And she has shown the real fortitude and determination which is essential for the establishment of any new organisation.

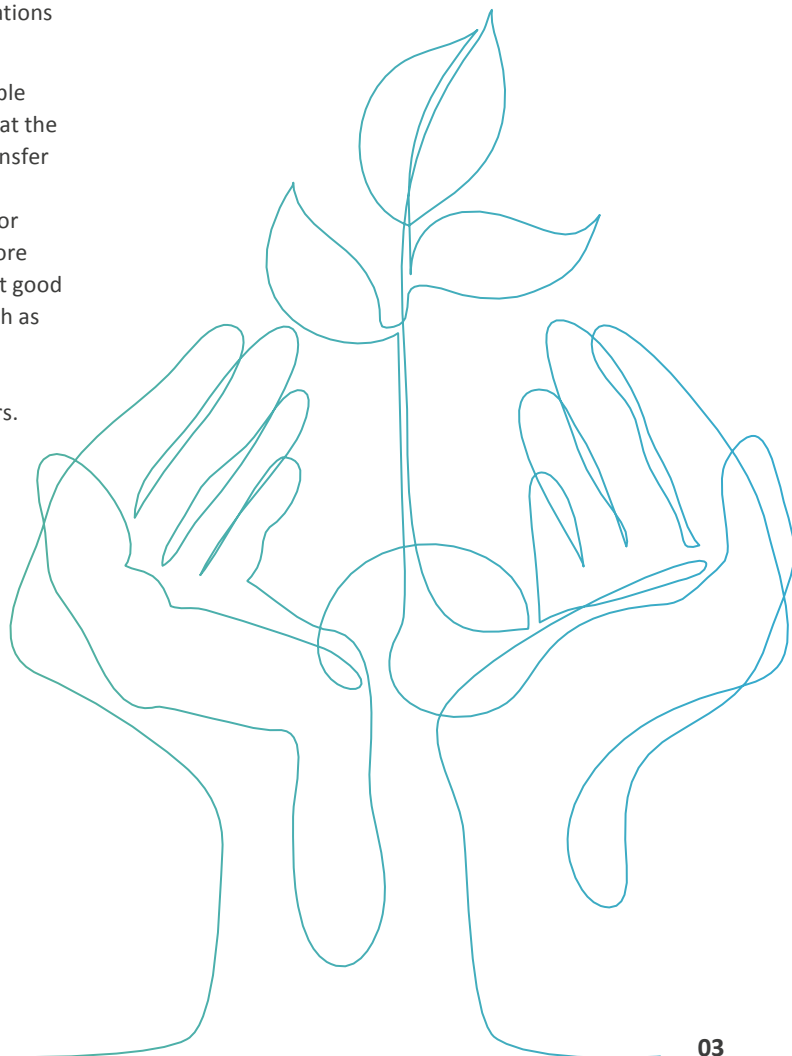
“

**We are fortunate to have the ability to innovate and build a distinctive reputation for the ODPa and by extension the Bailiwick.**

Whatever the contribution of the non-executive members, it is the Commissioner and her staff who do the real work and deserve the credit for success. Emma Martins has patiently and intelligently built a team which is manifestly well-motivated, committed and productive. This report, or a glance at our website, show the relationships they have developed and the tangible results that have been achieved. We are truly fortunate to be able to rely on Emma and such good people, not least as they have overcome the frustrations of the pandemic.

None of us rest on our laurels. It is a matter of considerable regret that the EU institutions have still not confirmed that the Bailiwick's arrangements remain “Adequate” for data transfer purposes. Nonetheless, our push to innovate and build a distinctive reputation will continue in 2022 and beyond for the benefit of the Bailiwick and its citizens. We will be more proactive. We will reach out more in the quest to support good practice. We will make better use of the information, such as self-reported breaches, which is readily available to us. We will do more to praise “saints” and reform “sinners”. We will explore creative ways to use our statutory powers. We will identify ways to tweak and improve the Law.

In the same way that organisations are accountable for how they handle personal information, we will continue to demonstrate our accountability for how we protect people and how we promote prosperity.



# Introduction

---



**Emma Martins**

**Data Protection Commissioner**  
(Bailiwick of Guernsey)

April 2022



**I am pleased to present this Annual Report for the Office of the Data Protection Authority for 2021 in accordance with the requirements of Schedule 6, para.13 of *The Data Protection (Bailiwick of Guernsey) Law, 2017 (the Law)*.**

I spoke in 2020's report about the extraordinary backdrop against which all of us had been working and living. The optimism that we had then that life would soon return to normal was sadly replaced with a growing sense that we were not yet at the end of the road. Indeed, 2021 brought further challenges across the globe and to us here in the Bailiwick. The experiences of 2020 did, however, mean we were well placed to respond quickly and effectively as events unfolded. Again, the entire ODPA team worked together with professionalism and good humour, and I would like to express my personal and heartfelt thanks to them all. These times have offered us all a great number of lessons, both in our personal and professional lives. To value and support those around you has been a key lesson and I am enormously proud of the way in which individually and collectively all staff have more than risen to the challenges presented. I am extremely grateful too for the invaluable leadership and support of our Chairman and Authority Members. We are fortunate as an office to work with such an exceptional team, and we hope that this is reflected in the energy and focus we all have in delivering on our regulatory duties with passion, focus and professionalism.

The pandemic has also served to remind us of the increasingly significant role data plays in all aspects of our lives. Public health responses to the crisis across the world, including the Bailiwick, relied on timely, accurate and complete data. It is important for us to ensure that conversations around data handling are balanced because data can do a lot of good when it is handled ethically. Data can also cause significant harm when it is mishandled – intentionally or otherwise. Ensuring a wider understanding of the fact that it is within our gift to determine how we use data also serves to encourage the regulated community to recognise the very real commercial and reputational opportunity that presents itself – which is that citizens and consumers are more aware and care more about their data. We want to do all we can to build trust and confidence around the data economy by supporting enlightened compliance by our regulated community.

We also know that we need to respond in the face of the actual and potential risks, and we will continue to do so robustly and fairly. It is our firm belief, based on direct experience, that the vast majority of local organisations want to look after the data in their care. They understand that their approach to the protection of people's data is inextricably linked to their reputation and we see it as our job to give them the tools to support the highest standards of data governance across all sectors.

One of the most challenging aspects of data protection regulation is its 'horizontal' rather than 'vertical' nature. By that I mean that its regulatory reach does not impact one particular sector, it impacts all sectors. The law applies equally to the small business as it does to the large but the risks they face and the way they are able to deliver on the compliance responsibilities will be hugely different. Our commitments, in our strategic plan, to support community-wide awareness and engagement reflects the realities of that challenge – that if we are to effect real and meaningful change in the way that data protection is perceived we need to engage in real and meaningful communications. Project Bijou, a social initiative launched during 2021 involving different people from within and outside the Bailiwick, is an example of how we are putting our words into action, and we have been delighted and humbled by the response. We continue to build and develop the project, including working with the Youth Commission to develop a children's outreach programme which we are very excited about. Supporting a generation of young people to grow up understanding their rights and engaging in conversations about the impact of data on our lives can create a virtuous circle - they become consumers who demand high standards of data handling and they also become the employers and employees who are responsible for that handling.

In all the work we do across our community to support the highest standards of the protection of our personal data, we will continue to build on the common ground and shared goals that are so important in this digital era. Committing to an ethical and sustainable data environment is increasingly important for the economy but first and foremost it is important for us as human beings. I hope that the information contained within this Report provides some insight into how we are translating those words into actions and, importantly, into outcomes.

# About the Authority

---

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

The Law creates the independent Data Protection Authority which is tasked with the development and implementation of the regulatory regime necessary to oversee the requirements of the Law. Comprising a Chairman 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 individuals. 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**



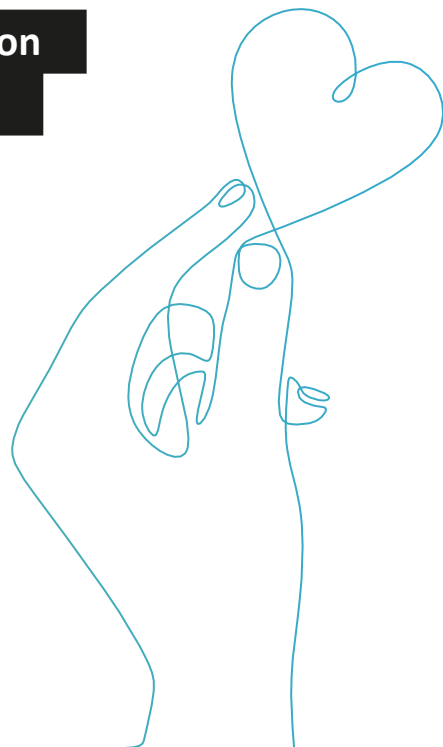
**Promotes excellence in data protection**



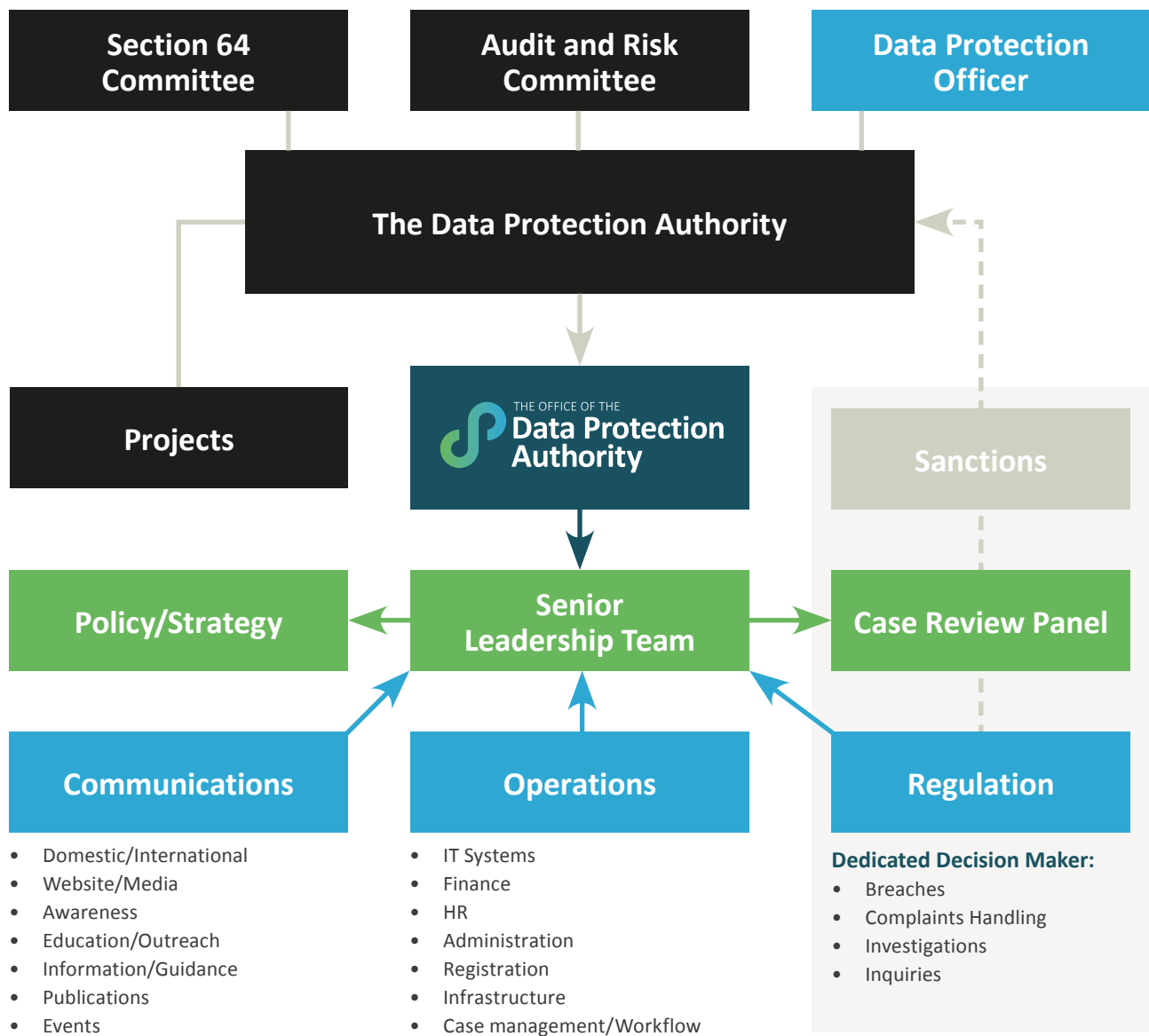
**Supports the data economy to embrace innovation**



**Regulates data protection legislation through an ethics-based approach**



# Organisational chart



## The Data Protection Authority

- Chairman – 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

# Data protection in Plain English

---

The Authority is committed to helping everyone engage positively and constructively with data protection rights and responsibilities. To do that, information and guidance is presented in a relevant and accessible way. Although it is sometimes necessary to use legal terminology, Plain English is used wherever possible.

Data protection is for all of us, not just for lawyers.

## Legal terms

## Plain English



'Complainant'

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



'Controller'

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



'Data subject'

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



'Data subject access request'

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



'Lawful processing condition'

Before a controller starts collecting or using people's data, they must identify and document a 'lawful processing condition' (or 'lawful basis') that can be relied on. Failing to do this makes the activity unlawful. 'Consent' is the most well-known example, but there are many others.



'Operative provision'

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



'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 that they have experienced a personal data breach.

More Plain English definitions of key terms can be found at: [odpa.gg/information-hub/glossary](https://odpa.gg/information-hub/glossary)

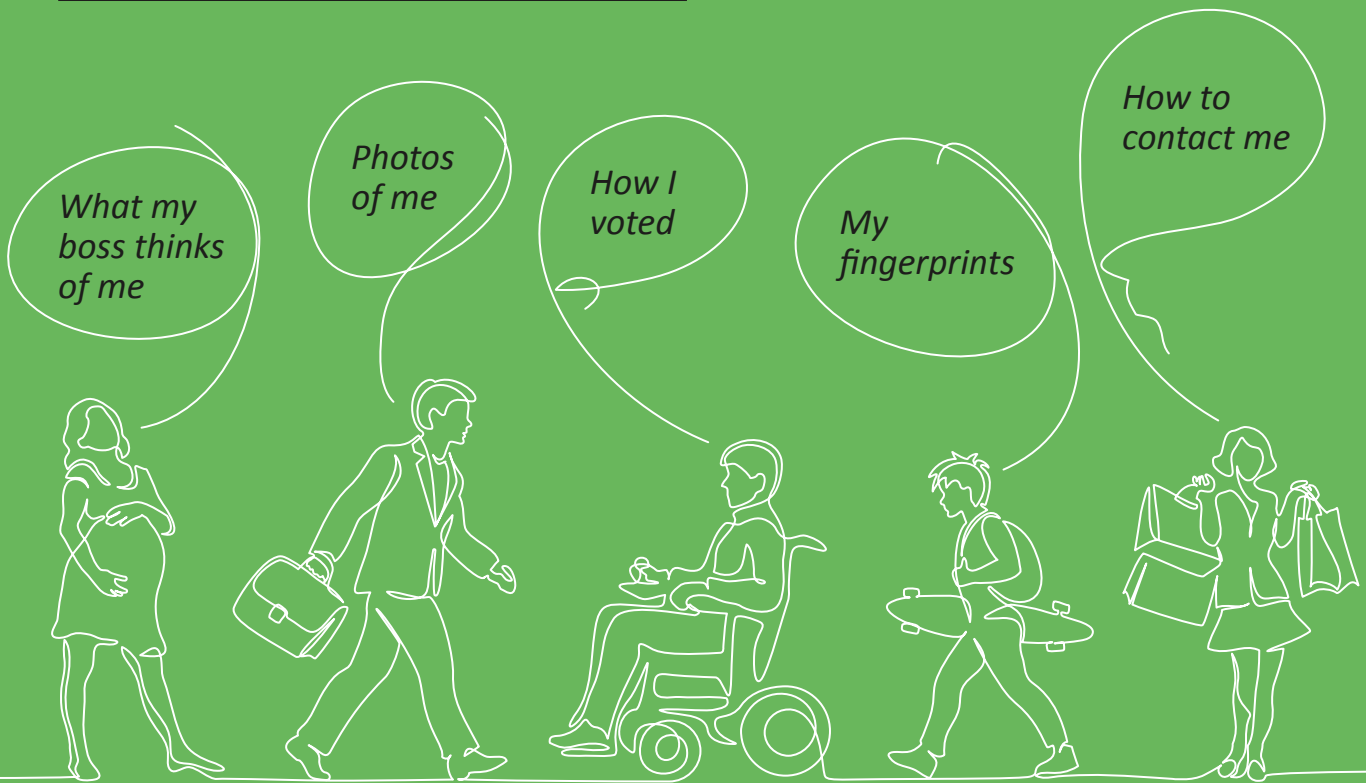


# Executive summary

---

**Data Protection = People Protection.**

**It's about protecting things like:**



That's all someone's personal data. Data protection is all about looking after this sort of information. **Data protection is people protection.** At its heart it is about taking care of information about living human beings so that their dignity and autonomy remains intact, and that the rights they have over their information are respected.

## Executive summary *continued*

The ODPa exists to:

- Empower individuals and protect their rights
- Promote excellence in data protection
- Support the data economy to embrace innovation
- Regulate data protection legislation through an ethics-based approach



The ODPa works to achieve the above through these **five strategic objectives**:

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

**2021 HIGHLIGHT:** financial independence achieved via the successful implementation of the self-funding model.

#### KEY STATISTICS:



**£1.5 million**  
income generated



**20,342**  
registered entities

### 2. To be a relevant, responsive and effective regulator

**2021 HIGHLIGHT:** proactive communication with public sector and industry.

#### KEY STATISTICS:



**180** personal  
data breaches  
reported



Lessons  
learned from  
these published  
every **2 months**



**35** complaints  
about local  
controllers  
assessed



**17** investigations  
and **1** inquiry  
conducted

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

**2021 HIGHLIGHT:** Increased frequency of free drop-in sessions, expansion of Schools Programme, continuous improvement of ODPa website.

#### KEY STATISTICS:



**33**  
organisations  
attended  
drop-ins



Over **230 children**  
involved in  
awareness-raising  
activities in schools



ODPa online  
registration process  
completed, on average,  
in **under 5 minutes**

### 4. To develop and maintain effective relationships

**2021 HIGHLIGHT:** proactive engagement with industry, government, and international institutions.

#### KEY STATISTICS:



ODPa staff invited to speak  
at **21 events**, locally and  
internationally.



### 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

**2021 HIGHLIGHT:** Project Bijou launched to engage organisations and individuals on a human-level.

#### KEY STATISTICS:



**32 contributors**  
presented content



Across **5 key themes** during  
week-long online launch event

# Strategic plan and activities

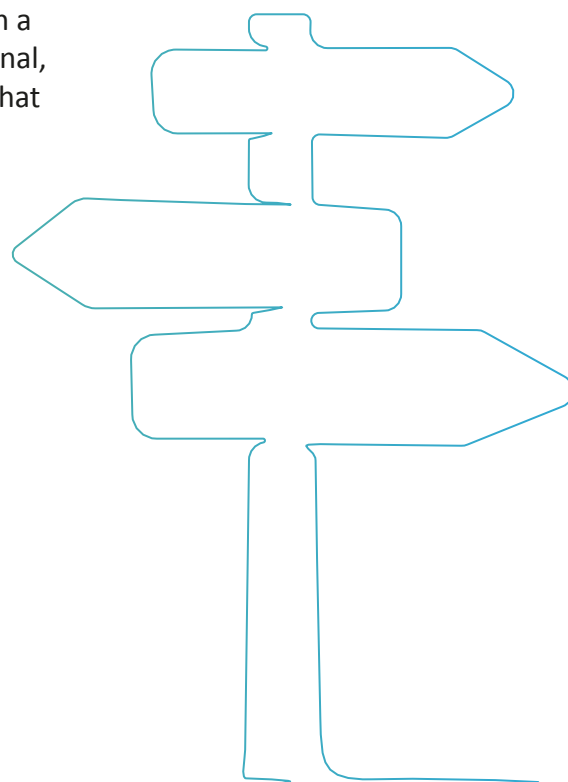
---

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

The ODPA's five 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.



Much thought and hard work goes into how to deliver tangible and positive outcomes for the Bailiwick and its citizens. Presented below is the Strategic Plan and progress against specific action points achieved during 2021:

## 1. To develop our capabilities to deliver on our enhanced statutory duties

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



Completed in 2020

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



Completed in 2020

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



Completed in 2021

During 2021 the second phase of recruitment concluded, with Case & Compliance Team and Communications Team both strengthened.

As at the end of 2021, the ODPA employed 12 employees on a mixture of full-time and part-time contracts.

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



Completed in 2021

The new fees regime was fully operational on 1 January 2021. Please see the 2020 Annual Report for details of why delivery of this was completed later than intended.

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



In progress throughout 2021

Work remains ongoing to develop strong foundations for this policy based on experience and observed trends.

It is linked to both **Project Eventus** (the audit programme) and **Project Querelis** as well as the completion of the phased recruitment programme detailed in 1.3 above.

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



In progress throughout 2021

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 of the Bailiwick's new legislative framework in April 2019. The ODPA has worked with States of Guernsey to provide timely and detailed responses to the Commission throughout the process of assessment.

In related work, the UK have started their own adequacy process which the ODPA are also feeding into via the States of Guernsey.

## 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



In progress throughout 2021

Work continued throughout 2021 to develop strong foundations so that the approach to this piece of work is evidence-based.

This work is linked to both **Project Eventus** (the audit programme) and **Project Querelis**, as well as the completion of the ODPA's phased recruitment programme.

### 2.2. Develop effective mechanisms to resolve and learn from complaints



In progress throughout 2021

This activity progressed throughout 2021 under **Project Querelis**.

There was good progress on the second phase of **The Fandango Project** (which was focused specifically on improvements to the ODPA's casework handling process).

Regular Case Review Panels took place throughout 2021 to ensure robust decision making, governance and sharing of experience gained and lessons learnt from casework.

### 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



Ongoing

During 2021, the ODPA's revised its organisational structure to better reflect how the teams work and where responsibilities are.

By the end of the year the Case & Compliance Team was fully staffed.

Within the Communications Team, changes to existing staff hours meant it became necessary to identify and appoint additional resource for start in January 2022.

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



Ongoing

Recognising that the public sector is responsible for significant and sensitive personal data, the ODPA proactively provides information and support where appropriate as well as taking action where there are concerns about processing within this sector.

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



Ongoing

During 2021, the ODPA, in conjunction with its Board, agreed to provide additional support to the designated ODPA Data Protection Officer (DPO) to enable succession planning and knowledge transfer. A longer-term aim is for the ODPA's DPO to then be redesignated to remove potential conflict issues (in accordance with the Law's requirements around the DPO role). This work will continue into 2022.

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



Ongoing

Relationships continued to develop during 2021 with the appointment of a Virtual IT Manager as well as existing relationships with finance, IT, infosec, HR, legal, PR and project support operating well, providing expertise not found in-house or not viable to employ directly.

Due to planned changes within the Communications Team starting in 2022, the ODPA will no longer need external PR support.

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



Ongoing

The ODPA's senior team maintains awareness of relevant national and international developments and continues to participate in European and International conferences of Data Protection Authorities. Despite the continued disruption caused to in-person conferences during 2021, ODPA staff did attend Global Privacy Alliance conference, the Common Thread Network meetings, the British, Irish and Islands Data Protection Authorities (BIIDPA) meeting, and the European Data Protection Authorities conference.

In addition, an ODPA staff member attended the Summer Academy dedicated to international transfers – which explored the legal developments and practical approaches globally.

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



Ongoing

Knowledge sharing sessions encouraging sharing of experience and discussion of points of law – structure of law, info law, lawful processing conditions, data subject rights, international transfers, structures within finance sector. Staff also attended advanced IT training, and personal development sessions such as developing effective habits.

Professional qualifications achieved by some staff to support their role and their personal development.

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



Ongoing

The ODPA made full use of Authority Members' wealth of experience to support and contribute to its operational and strategic activities.

In late 2021, the ODPA senior leadership team and all Authority Members held their first in-person meeting since early 2020. The meeting focused on strategy as well as planning for new Members who will be joining the Authority in May 2022.

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



Ongoing

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.

As the pandemic continued to disrupt everyone's personal and professional lives, the ODPA remained focussed on supporting all its staff through what was a very challenging period.

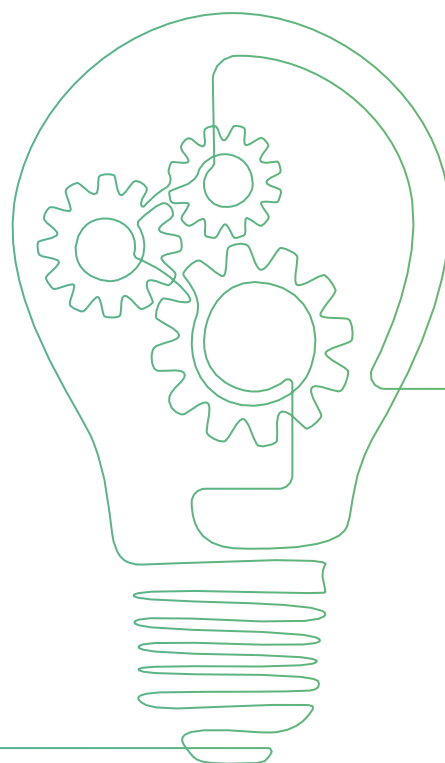
## 2.11. Be open to constructive exploration of innovative practices and activities within the regulated community



Ongoing

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.

The ODPA actively encourages early engagement in new and innovative practices involving personal data, and encourages organisations to understand that good data governance can support and enable digital and technological progress.



### 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**



Completed in 2020

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



Completed in 2020

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



Completed in 2020

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



Ongoing

Following the successful launch of the ODPA's events, drop-ins, and study visits in 2019, this work was continued during 2021.

During 2021 the ODPA delivered eight events (some online, some in-person), and a further five 'surgeries' were held in partnership with The Digital Greenhouse. Thirty-three free drop-in sessions and five study visits with local organisations were held.

Project Bijou, the ODPA's social initiative was launched via an online conference in May 2021, with 37 invited speakers providing content ranging from podcasts, to written pieces, to short videos.

Ten podcasts were produced during the year, over 680 people were subscribed to ODPA newsletters, and over 4,000 people followed the ODPA LinkedIn page.

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



Ongoing

With the launch of its new website in December 2020, the ODPA now has a fit-for-purpose platform for its communication outputs.

New guidance on international transfers was published during 2021. There was also an extensive improvement to the registration guidance area to support regulated community.

As stated in 3.4 above, Project Bijou was also launched to inspire engagement with data protection on a human level through the sharing of experiences and stories. The ODPA was encouraged by the positive response to the launch, which received attention from the UK, Europe, and the US.

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



Ongoing

During 2021, a key milestone for this objective was reached with the launch of Project Bijou in May 2021.

Its aim is to support and nurture positive cultural change around how people and organisations treat people's data and to engage people on a cultural level rather than simply on a legal/compliance one.

**3.7. Raise data protection awareness in school-age children**



Ongoing

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.

The ODPA Schools Programme (which launched in November 2020) was heavily impacted by restrictions placed on local schools, but still ~230 children were reached.

### 3.7 Continued

To increase the reach (and diversify the settings) where the ODPA can raise children's awareness a strategic partnership with the Bailiwick's Youth Commission was established in December 2021. During 2022, the plan is to do some knowledge transfer work between the ODPA and the Youth Commission and to ensure that the programme of activities for children are relevant and fun.

Post 2022 it is hoped that the Youth Commission will take the lead on delivering the programme with oversight from the ODPA.

### 3.8. Engage with and support the Bailiwick's data protection association (BGDPA)



Ongoing

The ODPA's Outreach Officer and the Chair of BGDPA stayed in regular contact throughout 2021 and the ODPA remains committed to encouraging the success of the association.

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



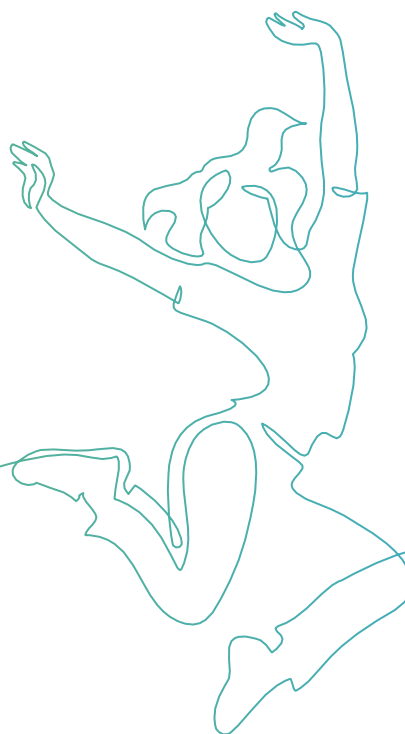
Ongoing

The ODPA Commissioner and Deputy Commissioner are regularly invited to speak at local industry events. Details of all 2021 speaking engagements are listed below.

1. Douzaines – General Q&A. 18 January 2021
2. Youth Commission – General Q&A. 20 January 2021
3. Chamber of Commerce Lunch and Learn. 2 February 2021
4. Defence and Security Circle. 10 March 2021
5. European Privacy and Security Summit. 17-18 March 2021
6. BPP Brexit Forum. 25 March 2021
7. PrivSec Global 'Why Do Cars Have Brakes? Questioning the Need for Regulation'. 22-24 June 2021
8. Jersey Data Protection Association: Three Crown Dependencies Three Years On. 21 June 2021
9. Data Protection in Healthcare (In-house session delivered at local healthcare organisation). 9 September 2021
10. GRC24 World Forum Data Protection Panel: Building an Effective Data Security Strategy. 8 September 2021
11. Chamber of Commerce Lunch & Learn. 12 August 2021
12. Guernsey International Legal Association. 16 September 2021
13. PrivSec Global. 22-23 September 2021
14. PrivSec Global (panel discussion on privacy culture). 22 September 2021
15. Meet the Experts (Digital Greenhouse). 21 October 2021
16. Meet the Experts (Digital Greenhouse). 11 November 2021
17. CMI Level 3: Data Protection / Information Law Session (College of Further Education). 17 November 2021
18. Guernsey Association of Pension Providers Members 'Lunch (General Update Plus Q&A). 26 November 2021
19. Chamber of Commerce: 'Humans: Your Biggest Risk, Your Biggest Opportunity'. 30 November 2021
20. PICCASO - Online Launch Event of Privacy Culture Initiative, (PICCASO stands for 'Privacy, InfoSec, Culture Change & Awareness Societal Organisation'. 9 December 2021
21. BPP Webinar: 'Managing AML Challenges in an Age of Data Protection and Privacy'. 14 December 2021

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.

The ODPA continued to be represented on the local Caldicott Committee during 2021 with the Deputy Commissioner attending. 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



Ongoing

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

The ODPA works to identify representative 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.

### 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



Ongoing

There were a number of occasions during 2021 where it was appropriate for the ODPA to proactively talk to its contacts within the States of Guernsey to ensure a constructive way forward.

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



Ongoing

The ODPA continuously reviews where there may be opportunities to consider where MoU relationships may be useful in the successful delivery of statutory duties.

Specifically, in November 2021, a new MoU was signed with the Channel Islands Financial Ombudsman (CIFO).

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



Ongoing

The ODPA continues to participate in European and International conferences for Data Protection Authorities (see 2.7 above for details) 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 EU's General Data Protection Regulation (GDPR) will emerge 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



Ongoing

Regular engagement between the ODPA and the European Commission continued throughout 2021 (as detailed in 1.6 above).

The ODPA also contributed to the submissions made by the States of Guernsey to the European Commission.

This important engagement with the European Commission will continue once the formal assessment of adequacy concludes.

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



Ongoing

ODPA staff attended, or spoke at, many events as detailed in section 3.9 above.

Also as detailed in section 2.7 above, senior ODPA staff represented the Bailiwick at the following online conferences and meetings:

1. The British, Irish and Islands Data Protection Authorities (BIIDPA). 24-25 June 2021
2. Global Privacy Assembly 2021. 18-21 October 2021
3. The Common Thread Network. Quarterly throughout 2021

## 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



**Completed in 2021**

The ODPA had hoped to launch Project Bijou via an in-person one-day conference locally following the disruption to in-person events throughout 2020 and 2021. It became clear that this was not going to be possible so it was decided that the Project would instead be launched via a week-long virtual event. The ODPA secured a diverse group of 32 contributors from various jurisdictions including: current and former privacy/data protection Commissioners, academics, lawyers, directors, data protection officers, ethicists, and even a midwife and a poet. The week was split into five themes, with the 32 contributors split across as follows:

1. The effects data harms have on people (5 contributors)
2. Why better engagement is needed (6 contributors)
3. The role culture plays in data and vice versa (7 contributors)
4. What drives behavioural change (8 contributors)
5. The benefits of looking after personal data (6 contributors)

Each day during the launch week beginning 25 May 2021, that day's theme was released at 8am and shared online so that people could consume the content at a time convenient to them. The launch week's content remains online for anyone to use in their own awareness-raising activities, and new contributors are planned for 2022.

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



**Ongoing**

The ODPA nurtures its relationship with local media, and is regularly contacted to provide comment on data-related news stories.

The ODPA works with local journalists and editors to provide factual information, build awareness of the Law, and demonstrate how data harms affect people. Throughout 2021, 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 86 news items, 12 broadcast media segments, and 3 magazine/editorial pieces.

The Commissioner also publishes 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



**Ongoing**

Where appropriate, and whenever possible, the ODPA provides 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.

During 2021, the ODPA published five Public Statements (as defined in section 64 of the Law) which were approved and issued by the Authority's Section 64 Committee regarding enforcement and related activities. All public statements are detailed in the 'Actions we've taken' area of the new ODPA website.

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



**Ongoing**

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, both businesses and individuals, to aspire to excellence in data protection. Much effort is put in to involve and engage all staff members in issues the ODPA is dealing with and to encourage a broader intellectual engagement with data related issues locally and internationally. Each member of staff understands the importance of their role in delivering on the four pillars of ODPA activities as well as the interdependence of all related activities.

During 2021 there was continued focus on supporting and developing staff professionally and personally, both in the office and ensuring their wellbeing during periods of remote working.

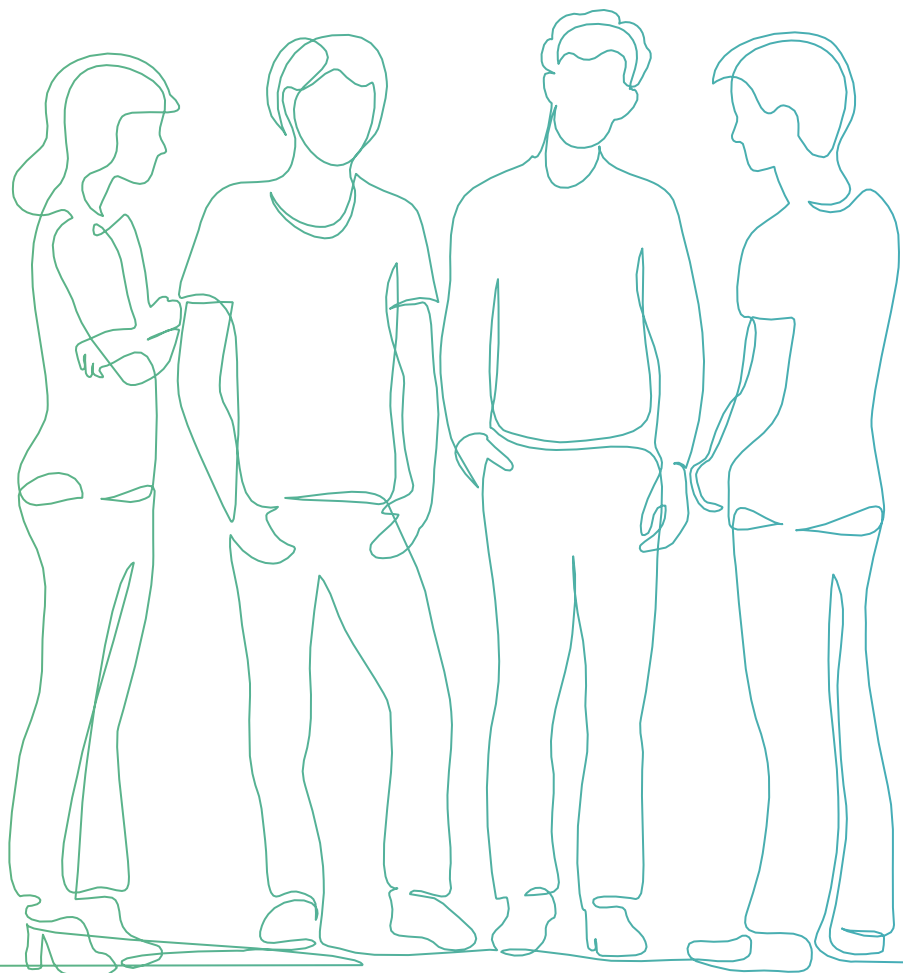
Development through formal training was also available and used by all ODPA staff.

## 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 2021 is detailed in 3.9 above, as a result of the ODPA's drop-in sessions, events, study visits, and invited speaking engagements, and 5.1 above on the launch of Project Bijou.

The ODPA also nurtured its ongoing connection with two key organisations: the Guernsey Chamber of Commerce, and Digital Greenhouse by offering their members free events and 'surgeries' aimed at supporting them in their compliance. As detailed in section 3.9, the ODPA also maintained its connection with the wider community through engagement with key groups including the health sector, law enforcement, and training providers.



# Case studies

---

The Authority has a statutory duty to promote awareness of data protection issues. Detailed following are anonymised and simplified case studies of real complaints people have submitted to the Authority about how local organisations have handled their data, together with what can be learned from them.



## Case study #1

---

### Background

An employee was responsible for the administration of a public social media account for the company they worked for and used their personal login to access the page.

The employee then left the company.

Following the employee's departure, a manager of the company logged in to their now former employee's computer to administer the company's social media account. However, this login also enabled them to access the former employee's personal social media account. Details of the personal social media account unrelated to the employee's previous employment with the company were copied and subsequently used by the employer.

### Learning points

- Be clear about roles and responsibilities for staff and ensure they are reflected accurately and clearly in all policies and procedures.
- It is important for us all, as employees and employers, to have clear boundaries between our personal and professional lives.
- If access to accounts/data/social media is required for work-related purposes, create separate accounts and passwords.
- Be aware of the potential impact on the privacy/confidentiality of all staff when undertaking any activities that relate to them and their data.



## Case study #2

---

### Background

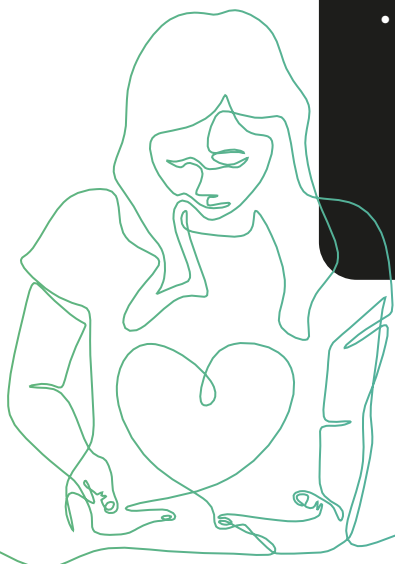
A patient asked their legal representative to make a 'data subject access request' (DSAR) to their GP on their behalf. The DSAR asked for **all** the patient's medical data (general) within a **particular date range** (specific).

Notwithstanding the apparent lack of clarity regarding the data being requested, the GP's practice did not seek any further information or clarification from the legal representative and went on to send the patient's complete medical history to the patient's legal representative by email.

The patient was unhappy that their entire medical record had been sent to, and seen by, their legal representative as they had only intended for them to convey their request and wanted the data to be sent directly to them. The patient was also concerned that the GP practice would send such a large volume of highly sensitive information (special category data) via unencrypted email. The GP's practice accepted that its own internal policies did not permit them to send medical data via email, but that it assumed because the request came in via email that it must be responded to the same way.

### Learning points

- Ensure you are aware of and plan for receiving requests from individuals for their personal data (DSARs).
- If you want to submit a DSAR, ensure that your request is clear on exactly what data you want and how you want to receive it.
- If you receive a DSAR and are not clear about any aspect of it, contact the requesting individual without delay to ensure clarity.
- If there is a third party acting for the requesting individual, ensure you have the appropriate consent and that you are clear about the instructions.
- If you are responding to a DSAR, talk to the person making the request and ensure you are providing their data back to them in a way that they are comfortable with and in a way that adheres to your own policies. All personal data must be stored and sent with care, and when you are dealing with special category data (e.g. medical information, criminal data, biometrics etc) you must use additional safeguards.



## Case study #3

---

### Background

A member of the public (the complainant) attended a meeting at an organisation. The meeting consisted of three people; the meeting facilitator, another attendee and the complainant. The three people discussed matters of a private and sensitive nature. The meeting facilitator provided no details about how they may collect, record, or use the personal information discussed at the meeting.

The discussion focused on the two attendees. Many months after the meeting, the complainant wanted detail of the discussion as they were concerned about data security and confidentiality. They made a data subject access request (DSAR) to the organisation for meeting notes and other processing details.

The organisation responded by saying that it would not provide any data, citing that it owed a duty of confidentiality to the other attendee.

A complaint was made to the Office of the Data Protection Authority (ODPA) and the organisation sought consent from the other attendee and provided details around the way in which the complainant's data was used, stored, and protected.

### Learning points

Had both attendees been given detailed information about how the organisation handled personal data, including the rights they had under the law, it is unlikely that a complaint would have been made in the first place. Individuals must be informed at the outset and prior to an organisation processing their data, how their information will be collected, what will happen to it and how it will be used. This then gives the individual the choice whether they wish to proceed or not.

In addition, reference to third parties in data being requested does not automatically mean that the data cannot be provided.



## Case study #4

---

### Background

An entrepreneur approached the ODPA about a software system he was in the initial stage of developing which involved the use of data about people.

The ODPA helped him understand his compliance obligations, including identifying appropriate conditions for lawful processing and developing a data processing notice. Working with the ODPA from the outset enabled the controller to better consider the data protection requirements, making compliance easier and improving his product as a result.

### Learning points

Considering the importance of protecting data at the outset enabled the company to develop its processes to ensure that data protection standards were built in from the beginning. This is a good approach to compliance and a more efficient use of resources.

It also enabled the controller to establish data protection by design and take reasonable steps for compliance. Taking this approach helps to build trust and confidence, it also reduces the likelihood of problems in the future.

Data governance cannot be an afterthought, it must be embedded into all aspects of an organisation's journey.

The ODPA holds fortnightly drop-ins so that organisations can discuss issues like this. Details of these, and a wealth of other resources and information are available at [odpa.gg](https://odpa.gg).





# Key statistics

For the period 1 Jan 2021 – 31 Dec 2021

20,342	Number of <b>local organisations</b> who fulfilled their legal obligation to register with the ODPA
£1,299,137	The ODPA's <b>expenditure</b>
£1,433,000	The ODPA's <b>operating budget</b>
£1,545,300	The ODPA's <b>registration fee<sup>1</sup></b> income
£100,000	<b>Loan repayment</b> paid to the States of Guernsey for ODPA initial set-up and associated costs
35	Number of data protection <b>complaints</b> received
180	Number of <b>breaches</b> reported
17	Number of <b>investigations conducted</b> by the Authority
1	Number of <b>inquiries</b> conducted by the Authority
10	Number of <b>investigations and inquiries resulting in a determination</b> that an operative provision has been or is likely to be breached
11	Number of <b>sanctions</b> imposed by the Authority under section 73. 7 controllers issued with: 8 reprimands, 1 warning, 2 orders
33	Number of representatives from organisations who attended ODPA fortnightly <b>drop-in sessions</b>
7	Number of <b>free public/industry events</b> held at ODPA premises
161	Number of <b>people registered to attend</b> ODPA public/industry events
21	Number of <b>invited speaking engagements</b> taken by the Commissioner and Deputy Commissioner
230	Number of children/young people attending <b>ODPA Schools Programme sessions</b>

# Casework annex

2021

---



For those readers who have a particular, more technical, interest in data protection issues this section gives a detailed breakdown and commentary of 2021 casework to ensure that any trends and issues are highlighted and learnt from.

The ODPA's casework comes from three routes:

1. members of the public lodging a formal **complaint against a controller**<sup>1</sup>,
2. controllers **reporting breaches**, and
3. **intelligence-based inquiries** launched by the ODPA itself to investigate a specific issue.

---

<sup>1</sup> A 'controller' is any organisation/business that decides how people's data is used.

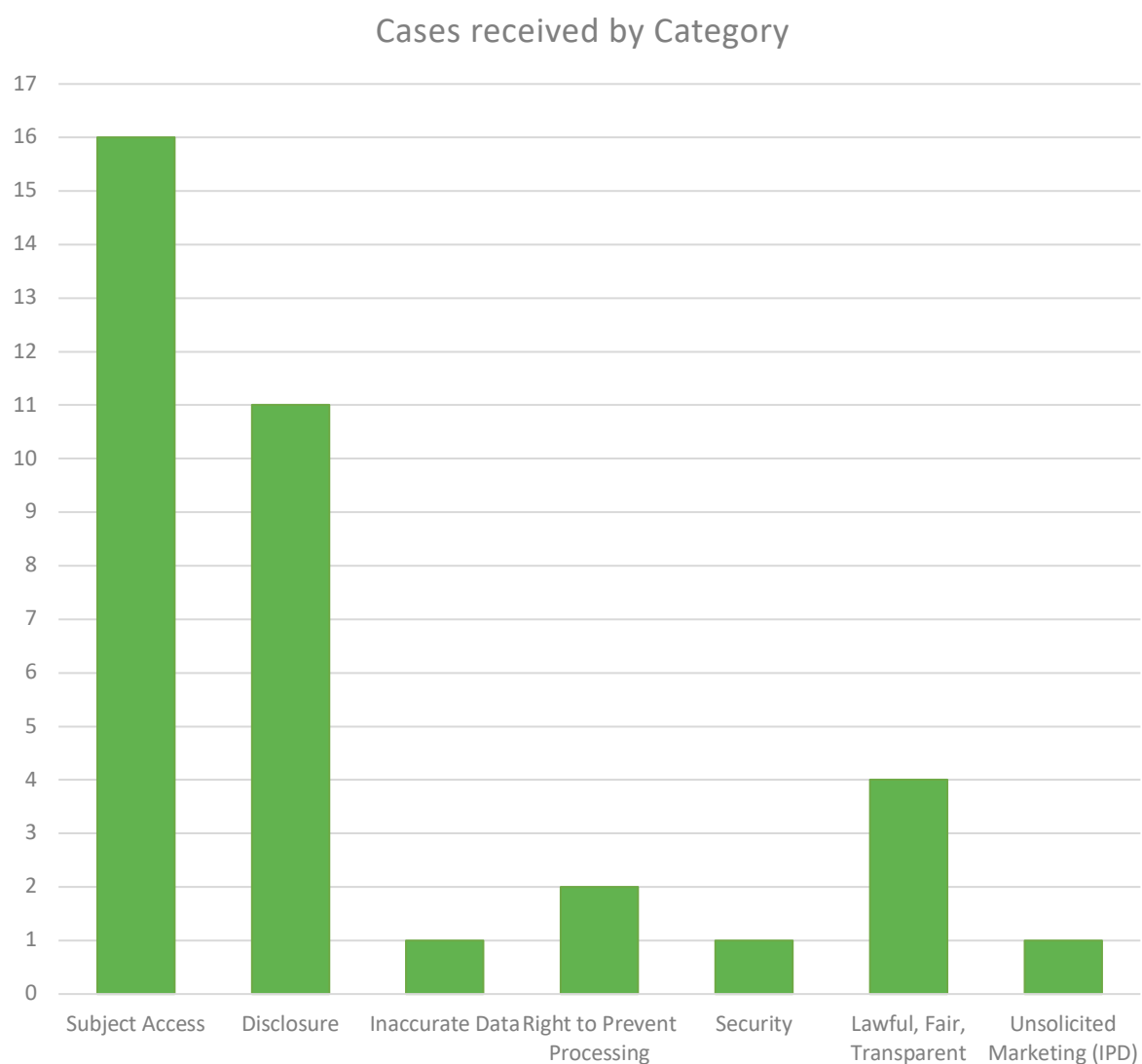
## Investigations and Inquiries

**Table 1: Overall casework activity during 2021**

This table details the number of investigations and inquiries opened and closed under sections 68 and 69 of *The Data Protection (Bailiwick of Guernsey) Law, 2017*.

Quarter	New cases received	Cases closed
Q1	11	13
Q2	10	20
Q3	7	19
Q4	8	3
Year total	36	55

**Figure 1: Cases received by category**



**Figure 2: Cases received by sector**

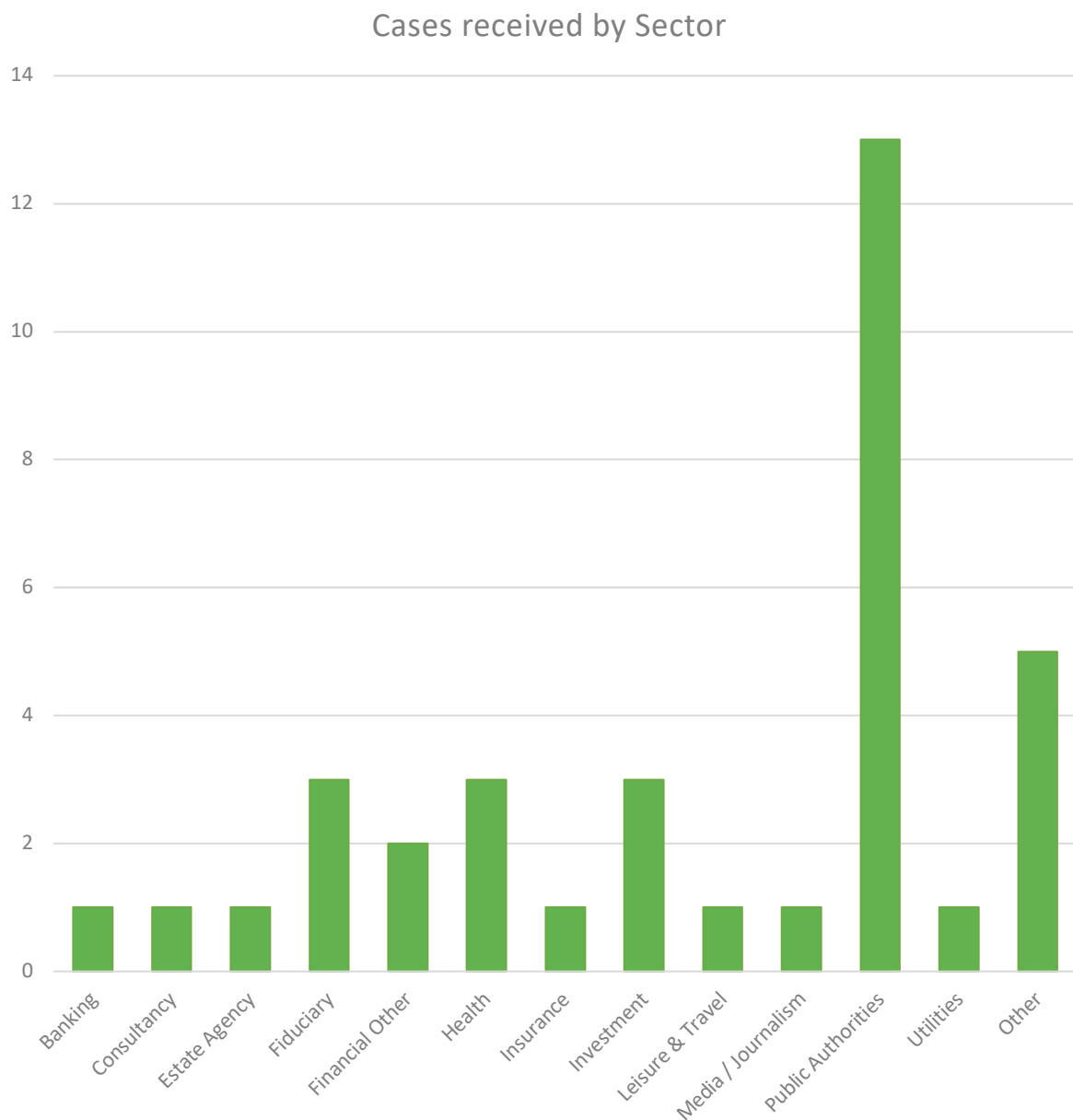


Figure 2 confirms what is an established trend: that the largest volume of casework received by sector casework relates to the activities of public authorities. This is no surprise given that public authorities can often process the most personal data and there is often little (if any) choice given to people about how their data will be used.

**Figure 3: Cases assessments**

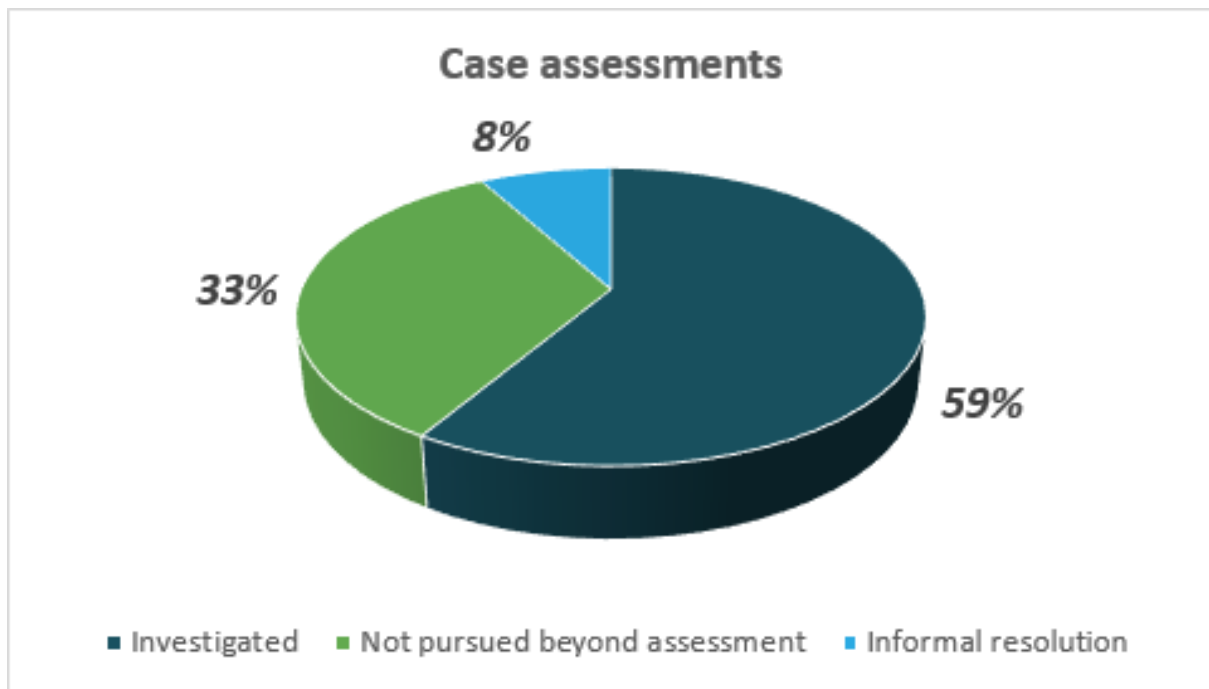


Figure 3 outlines what the outcome of initial case assessments were during 2021. When a complaint is received, it is assessed to see if there is an opportunity to informally resolve it. This means getting an outcome the complainant wants without launching a formal investigation. An example of informal resolution is a call to a controller, asking that they respond to a data subject access request that once completed, means the complainant has achieved their desired outcome. Where informal resolution is not possible, the complaint will be assessed to ensure there has been sufficient information provided to commence an investigation and that there is no reason why an investigation would not be appropriate. This means that not all complaints proceed to formal investigation.

**Figure 4: Age of active cases**

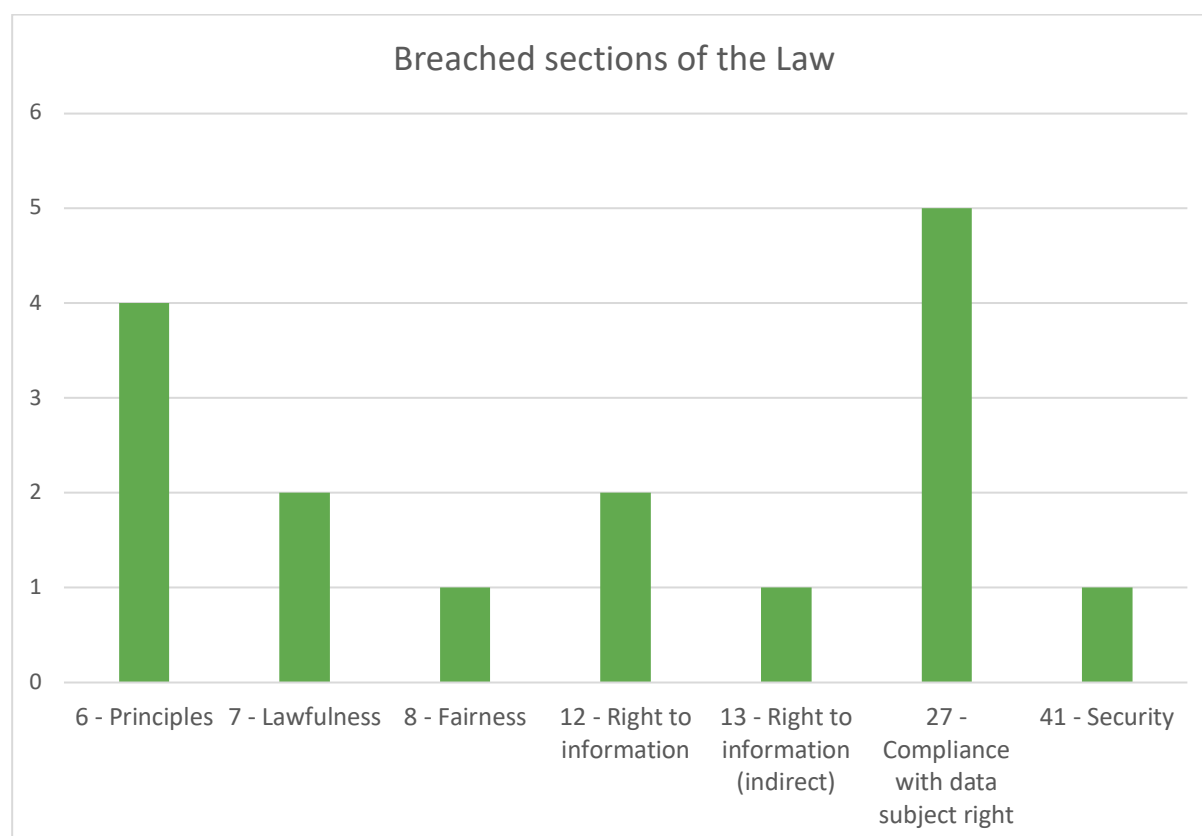


Figure 4 gives a breakdown of how long a case has been open. There are statutory timescales that must be adhered to in all casework, so things can take much longer than might initially be envisaged by both the complainant and the controller. Where possible, and appropriate, the ODPa seeks to expedite issues using informal resolution. Once an investigation or inquiry is opened, the ODPa must follow the timescales set in the local law meaning that even when the investigation phase of a complaint has concluded there would still be several months before the case is considered closed. This delay in cases being concluded was exacerbated in 2021 due to resourcing issues coupled with the complexity of certain cases. In addition, where an order<sup>2</sup> has been issued in a case these are not formally closed until the controller complies with the order; so this also delays case closure.

---

<sup>2</sup> An order is a type of enforcement activity that instructs the controller to take certain action.

**Figure 5: Breached sections of Law**



### Compliance with a data subject right

The largest volume, by type, of breach determinations made during 2021 related to section 27 of the Law 'compliance with data subject right'. Here are the most common issues found during 2021 around data subject rights requests and how controllers can avoid them:

Issue	Solution
Not telling the person that you are applying an <b>extension to the designated period</b> (1 month), and not having a valid reason for doing so.	<p>Make sure you are ready to respond rapidly to anyone who may submit a rights request to you. Have a process, and test it regularly.</p> <p>Remember that you can <b>only</b> extend the time you take to respond to someone if you can <b>demonstrate that the request itself</b> is complex or if there are lots of requests from the same person and in any case you must tell the person that you are going to take longer to respond and the reasons why.</p>
Not responding to the person's request <b>within the designated timescale</b> (1 month).	<p>As above: make sure you keep to the timescale detailed in the Law, be ready to respond rapidly to anyone who may submit a rights request to you: have a process, and test it regularly.</p>



Not telling the person that they have a <b>right to complain</b> to the Authority.	Remember that if you do not comply with the person's request you have a statutory obligation to let them know that they have a right to submit a formal complaint to the Authority about your failure to comply and/or to appeal to the Court to pursue civil action against you.
--	---

After 'data subject rights' the next most common breach determinations issued were in relation to the lawfulness of processing and a person's right to know what happens with their information. Together with fairness of processing, these sections of the Law underpin the first of the seven data protection principles contained in Section 6(2) of the Law and are common issues. How to deal with them are covered below.

### Lawful, fair and transparent

The first data protection principle states that controllers must process personal data "*lawfully, fairly and in a transparent manner in relation to the data subject*".

This means you must:

1. have a **valid legal reason** for processing personal data.
2. obtain it **without deceiving the person** whose data it is, and
3. **make it clear** exactly how you are going to use their data.

Much of the ODPA's casework in 2021 related to controllers failing to adhere to this principle. Based on 2021's casework the ODPA offers the following learning points:

Issue	Solution
Not having a valid legal basis for what you are doing with people's information (lawfulness)	Make sure you understand what you are doing with people's data and why you are doing it. Then take steps to identify and document a lawful condition for processing from Schedule 2 of the Law.
Deceiving or misleading people about how their data is being used (fairness)	Always be clear with people about the purpose you are processing their data for.  Make sure that you take extra care with any non-routine activity, as this type of activity can often be unexpected (and could be perceived as being unfair) and may not be reflected in your existing notices that people are familiar with.
Information given to people about how their data is used is insufficient, inaccurate, and unclear (transparency, right to information)	Please refer to Schedule 3 of the Law for details of what you are legally required to provide to people whose data you are using, known as a data processing notice.

**Figure 6: Sanctions issued**



**‘Reprimand / Warning / Order / Administrative fine’**

These are the formal enforcement actions available to the Authority, and can be issued separately or in combinations at the conclusion of a case. On some occasions where a very low-level breach of the Law has been found, and no harm has occurred, no sanction would be issued.

- **Reprimand**

In most cases in 2021 where a breach of the Law had occurred, controllers were issued a formal reprimand. A reprimand gives a clear signal that a controller has breached the Law and recognition of the reprimand in a public statement can result reputational damage for controllers who receive one.

- **Warning**

A warning can be issued when a controller's proposed activity is considered likely to result in the Law being breached. This provides a clear indicator to the controller to review their plans and to make changes to ensure a breach does not occur.

- **Order**

An order instructs the controller to bring specific activities into compliance with the Law.

- **Administrative fine**

Administrative fine orders are used when significant harm has been caused by the controller's activity, or where there have been significant failings. No administrative fines were issued for cases closed during 2021.

## Self-reported breaches

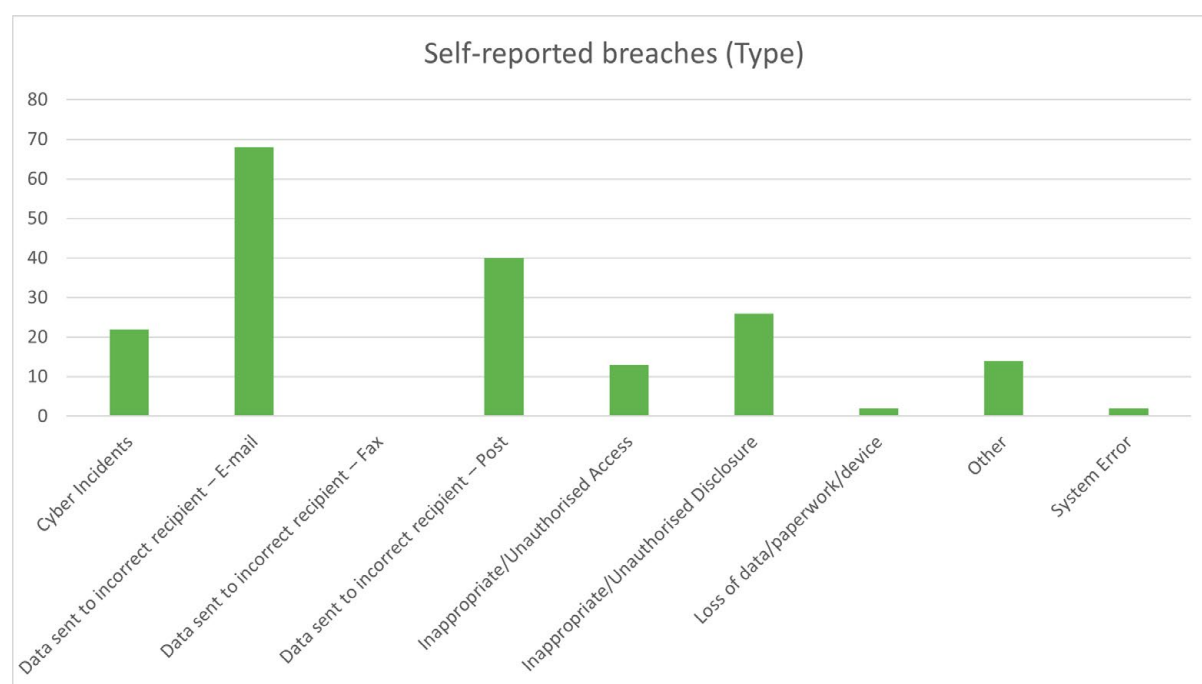
In addition to handling and investigating the complaints detailed above, the ODPA also reviews all breaches that are reported in by local controllers.

There is a statutory duty for controllers to give written notice of a personal data breach to the Authority. This is an important compliance duty, ensuring appropriate and timely action is taken where personal data has been compromised. It also provides valuable insight to trends across the regulated community enabling the ODPA to provide relevant guidance and support.

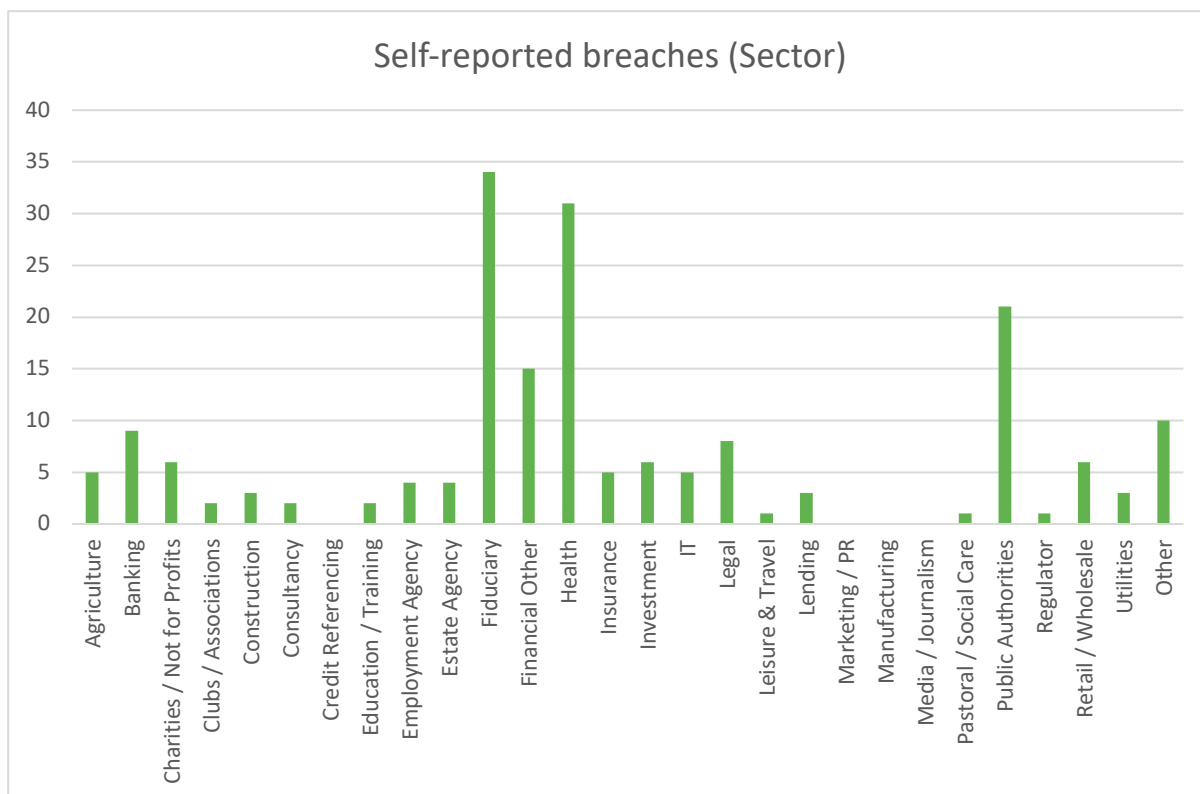
Statistics and commentary are published regularly and have highlighted the role that human error plays in data breaches, enabling communications to be targeted accordingly. They have also shown those sectors which report the highest number of breaches. It is unsurprising that controllers in the public, health and fiduciary sectors, who handle very significant volumes of personal data, experience higher levels of incidents.

The ODPA seeks to encourage a culture of open and constructive discussion and learning from these incidents and recognises that ensuring accurate and up to date information is available to the local regulated community plays an important part.

Below are two graphs summarising the self-reported breaches received during 2021, sorted by the type<sup>3</sup> of breach, and by sector.



<sup>3</sup> Note: in January 2022 the ODPA are introducing an updated breach classification process which will take better account of the reason the breach occurred, and what its outcome was.



## Other casework under ancillary legislation:

As of the end of 2021, the ODPAs were dealing with 1 case under *The European Communities (Implementation of Privacy Directive) (Guernsey) Ordinance, 2004* ('IPD'). IPD legislation relates to electronic communication including direct marketing, whether that be via e-mail, SMS or other methods. This case is included in the figures given above as the matter is dealt with in accordance with the enforcement provisions of the Law.

## Other relevant casework activities:

### 1. Section 69 Inquiries

There was 1 inquiry being carried out under section 69 of the Law at the end of 2021.

An inquiry is an investigation that is opened on the Authority's discretion. It is not necessary for there to have been a complaint about a controller or processor's activities in order for an inquiry to be commenced, rather an inquiry can be launched where intelligence or previous regulatory activity indicates a pattern of suspected non-compliance or a severe incident of suspected non-compliance.

## **2. Powers exercised under Schedule 7 of the Law**

The ODPA issued 2 information notices during 2021.

An information notice is a tool available to the Authority. It empowers the Authority to compel the production of information from any controller/processor where it is required in connection with the Authority's functions or powers. These notices must usually be complied with within 28 days, however, the Authority can reduce the period for compliance where the circumstances warrant such a reduction.

# Members' report and audited financial statements

Year Ended 31 December 2021

---

## 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

# **The Data Protection Authority**

## **Contents**

---

	Page
<b>Members' Report</b>	1 - 2
<b>Independent Auditor's Report</b>	3 - 5
<b>Income and Expenditure Account</b>	6
<b>Statement of Other Comprehensive Income</b>	7
<b>Balance Sheet</b>	8
<b>Statement of Changes in Reserves</b>	9
<b>Notes to the Financial Statements</b>	10 - 16
<b>Detailed Income and Expenditure Account (unaudited)</b>	17

# **The Data Protection Authority**

## **Members' Report For the Year Ended 31 December 2021**

---

The members present their report and the financial statements for the year ended 31 December 2021.

### **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 and 7.

### **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 2021

---

### Independent auditor

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

### Going concern

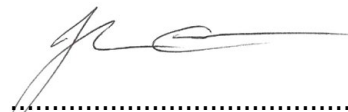
At 31 December 2021 The Data Protection Authority had net liabilities of £559,155. Despite the net liability position the financial statements have been prepared under the going concern assumption.

Cash flow forecasts have been prepared and approved by the Members of the ODPA covering a period extending beyond twelve months from the date of approval of these financial statements. After reviewing these cash flow forecasts the members of the ODPA have reasonable confidence that the ODPA will be in a position to meet its liabilities as they fall due for at least twelve months from the date of approval of the financial statements. As such the financial statements continue to be prepared on the going concern basis.

This report was approved by the members on 26 April 2022 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 2021 which comprise the Income and Expenditure Account, the Statement of Other Comprehensive Income, the Balance Sheet, the Statement of Changes in Reserves and the 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 FRS 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 2021 and of its surplus for the year then ended;
- are in accordance with United Kingdom Generally Accepted Accounting Practice.

#### **Basis for opinion**

We conducted our audit in accordance with International Standards on Auditing (ISAs) 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 International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants (including International Independence Standards) (IESBA Code), together with the ethical requirements that are relevant to our audit of the financial statements in Guernsey, and we have fulfilled our other ethical responsibilities in accordance with these requirements and the IESBA Code. We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

#### **Other information**

The members are responsible for the other information. The other information comprises the information included in the Members' report 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.

## **The Data Protection Authority**

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

---

#### **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 United Kingdom Generally Accepted Accounting Practice, 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 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.

As part of an audit in accordance with ISAs, we exercise professional judgment and maintain professional scepticism throughout the audit. We also:

- Identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for our opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control.
- Obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Authority's internal control.
- Evaluate the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by management.
- Conclude on the appropriateness of management's use of the going concern basis of accounting and, based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the Authority's ability to continue as a going concern. If we conclude that a material uncertainty exists, we are required to draw attention in our auditor's report to the related disclosures in the financial statements or, if such disclosures are inadequate, to modify our opinion. Our conclusions are based on the audit evidence obtained up to the date of our auditor's report. However, future events or conditions may cause the Authority to cease to continue as a going concern.
- Evaluate the overall presentation, structure and content of the financial statements, including the disclosures, and whether the financial statements represent the underlying transactions and events in a manner that achieves fair presentation.

We communicate with those charged with governance regarding, among other matters, the planned scope and timing of the audit and significant audit findings, including any significant deficiencies in internal control that we identify during our audit.

We also provide those charged with governance with a statement that we have complied with relevant ethical requirements regarding independence, and to communicate with them all relationships and other matters that may reasonably be thought to bear on our independence, and where applicable, related safeguards.

## **The Data Protection Authority**

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

---

#### **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.



**Grant Thornton Limited**  
Chartered Accountants  
St Peter Port  
Guernsey

Date: 28 April 2022

# The Data Protection Authority

## Income and expenditure account For the Year Ended 31 December 2021

		£	2020 £
Income		<b>1,545,300</b>	155,550
Administrative expenses		<b>(1,303,425)</b>	(1,243,045)
<b>Operating surplus/(deficit)</b>		<b>241,875</b>	(1,087,495)
Loan waived	7	<b>243,788</b>	-
Effective interest		<b>(41,243)</b>	(35,237)
<b>Surplus/(deficit) for the financial year</b>		<b>444,420</b>	(1,122,732)

The results above derive from continuing activities.

The notes on pages 10 to 16 form part of these financial statements.

The Data Protection Authority

Statement of Other Comprehensive Income  
For the Year Ended 31 December 2021

	£	2020 £
Surplus/(deficit) for the financial year	444,420	(1,122,732)
<b>Other comprehensive income</b>		
Loan amortisation	(14,140)	219,639
<b>Total comprehensive income/(deficit) for the year</b>	<b>430,280</b>	<b>(903,093)</b>

The notes on pages 10 to 16 form part of these financial statements.

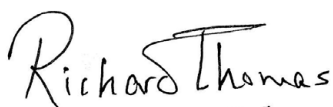
The Data Protection Authority

Balance Sheet  
As at 31 December 2021

	Note	£	2020 £
<b>Fixed assets</b>			
Intangible assets	5	147,498	148,873
Tangible fixed assets	6	70,548	98,225
		<u>218,046</u>	<u>247,098</u>
<b>Current assets</b>			
Prepayments		108,808	48,439
Cash at bank		171,596	105,771
		<u>280,404</u>	<u>154,210</u>
<b>Current liabilities</b>			
Creditors: amounts falling due within one year	7	(249,558)	(441,085)
<b>Net current assets/(liabilities)</b>		<u>30,846</u>	<u>(286,875)</u>
<b>Total assets less current liabilities</b>		<u>248,892</u>	<u>(39,777)</u>
Creditors: amounts falling due after more than one year	8	(808,047)	(949,658)
<b>Net liabilities</b>		<u>(559,155)</u>	<u>(989,435)</u>
<b>Reserves</b>			
Deficit		(559,155)	(989,435)
<b>Total reserves</b>		<u>(559,155)</u>	<u>(989,435)</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:



Richard Thomas CBE (Chairman)

26 April 2022



John Curran

26 April 2022

The Data Protection Authority

Statement of Changes in Reserves  
For the Year Ended 31 December 2021

	Other comprehensive income £	Income and expenditure account £	Total reserves £
<b>At 1 January 2020</b>	-	(86,342)	(86,342)
Deficit for the financial year	-	(1,122,732)	(1,122,732)
Loan amortisation	219,639	-	219,639
<b>At 1 January 2021</b>	<b>219,639</b>	<b>(1,209,074)</b>	<b>(989,435)</b>
Surplus for the year	-	444,420	444,420
Loan amortisation	(14,140)	-	(14,140)
<b>At 31 December 2021</b>	<b>205,499</b>	<b>(764,654)</b>	<b>(559,155)</b>

The notes on pages 10 to 16 form part of these financial statements.



**Notes to the Financial Statements  
For the Year Ended 31 December 2021**

---

**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 presentation currency of these financial statements is sterling with all amounts rounded to the nearest whole pound.

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. These judgments are set out in more detail in note 2.

The following principal accounting policies have been applied:

**1.2 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.

**1.3 Intangible assets**

Intangible assets are initially recognised at cost. After recognition, under the cost model, intangible assets are measured at cost less any accumulated amortisation and any accumulated impairment losses.

All intangible assets are considered to have a finite useful life. If a reliable estimate of the useful life cannot be made, the useful life shall not exceed ten years.

Website development costs are amortised over their useful economic life which is estimated as four years.

**1.4 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	- Over the remaining period of the lease
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 2021**

---

#### **1. Accounting policies (continued)**

##### **1.5 Debtors**

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

##### **1.6 Cash at bank**

Cash at bank is represented by current bank accounts and deposits with financial institutions repayable without penalty on notice of not more than 24 hours.

##### **1.7 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.

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 Income and expenditure account.

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. If there is a decrease in the impairment loss arising from an event occurring after the impairment was recognised, the impairment is reversed. The reversal is such that the current amount does not exceed what the carrying amount would have been, had the impairment not previously been recognised. The impairment reversal is recognised in the statement of comprehensive income.

##### **1.8 Operating leases**

Rentals paid under operating leases are charged to the Income and expenditure account on a straight line basis over the lease term.

##### **1.9 Administrative expenses**

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

**Notes to the Financial Statements  
For the Year Ended 31 December 2021**

---

**1. Accounting policies (continued)**

**1.10 Finance costs**

Finance costs are charged to the Income and expenditure account over the term of the debt using the effective interest method so that the amount charged is at a constant rate on the carrying amount. Issue costs are initially recognised as a reduction in the proceeds of the associated capital instrument.

**2. Significant judgments in applying accounting policies and key sources of estimation uncertainty**

In the application of the entity's accounting policies, which are set out in note 1, the members have made judgements, estimates and assumptions about the carrying amounts of assets and liabilities that are not readily apparent from other sources. The estimates and associated assumptions are based on historical experience and other factors that are considered to be relevant. The resulting accounting estimates will, by definition, seldom equal the related actual results.

The estimates and assumptions that have a significant risk of causing a material adjustment to the carrying amounts of assets and liabilities within the next financial year are addressed below:

**Notional interest rate**

The loan from the States of Guernsey has been advanced on an interest free basis. In line with the requirements of FRS 102 the liability is measured at the present value of the future payments discounted at a market rate of interest for a similar debt instrument. The members have therefore had to consider what the appropriate market rate of interest would be. The members consider that if they had borrowed the funds from a bank then a market rate of interest would be 4% above base. This rate has been used to calculate the notional interest charge on the loan which is included in the income and expenditure account of £41,243 for year ended 31 December 2021 (2020: £35,237).

As the loan has been provided on an interest free basis, any change to this notional rate will impact on the amortisation period, but does not have any impact on the total repayment amount.

**3. Employees**

The average monthly number of employees during the year was 11 (2020: 10).

**4. 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 2021

---

5. Intangible assets

	Website construction £
<b>Cost</b>	
At 1 January 2021	150,289
Additions during the year	38,081
At 31 December 2021	<u>188,370</u>
<b>Amortisation</b>	
At 1 January 2021	1,416
Charge for the year	39,456
At 31 December 2021	<u>40,872</u>
<b>Net book value</b>	
At 31 December 2021	<u><u>147,498</u></u>
At 31 December 2020	<u><u>148,873</u></u>

The Data Protection Authority

Notes to the Financial Statements  
For the Year Ended 31 December 2021

6. Tangible fixed assets

	Leasehold improvements £	Furniture and fittings £	Office equipment £	Total £
<b>Cost</b>				
At 1 January 2021	65,731	1,762	97,929	165,422
Additions	-	-	10,523	10,523
Disposals	(15,030)	-	-	(15,030)
At 31 December 2021	50,701	1,762	108,452	160,915
<b>Depreciation</b>				
At 1 January 2021	24,415	662	42,120	67,197
Charge for the year	10,959	352	20,003	31,314
Disposals	(8,144)	-	-	(8,144)
At 31 December 2021	27,230	1,014	62,123	90,367
<b>Net book value</b>				
At 31 December 2021	23,471	748	46,329	70,548
At 31 December 2020	41,316	1,100	55,809	98,225

7. Creditors

	2020 £	2020 £
Trade creditors	8,575	42,994
Deferred rent	20,012	28,017
Sundry creditors and accruals	17,287	19,596
Amounts payable to the States of Guernsey (note 9)	203,684	106,690
Amount payable to the States of Guernsey - transitional loan	-	243,788
	249,558	441,085

The amount due to the States of Guernsey in relation to the transitional loan was interest free and unsecured. The transitional loan was advanced in 2018 to help fund the creation of The Data Protection Authority. During 2021 the States of Guernsey agreed to waive the amount due and therefore this is accounted for as other income of £243,788 within these financial statements.

# The Data Protection Authority

## Notes to the Financial Statements For the Year Ended 31 December 2021

### 8. Creditors: Amounts falling due after more than one year

	£	2020 £
Amount payable to The States of Guernsey (note 9)	<b>808,047</b>	949,658

In accordance with the loan agreement dated 15 November 2021 between The Data Protection Authority and The States of Guernsey the loan is interest free and unsecured. Annual loan repayments will equate to the annual operating surplus of The Data Protection Authority with £100,000 due on 30 June in the year and the balance (being not less than £50,000) due by 31 March in the following year. It is the intention of both parties that the loan will be repaid by 31 March 2027. However this is on the understanding that levies payable to The Data Protection Authority will be sufficiently increased to enable significantly increased loan repayments during 2025 and 2026.

As the loan has been advanced on an interest free basis then in accordance with the requirements of FRS102 it has been accounted for as a financing transaction. Financing transactions are measured at the present value of the future payments discounted at a market rate of interest. The members consider that the market rate of interest for this loan would be 4% over the Bank of England base rate. The present value of the future loan repayments are disclosed in note 9.

### 9. Amounts payable to the States of Guernsey

Analysis of the maturity of loans is given below:

	£	2020 £
Amounts falling due within one year	<b>203,684</b>	106,690
Amounts falling due between 1 and 2 years	<b>117,626</b>	111,064
Amounts falling due between 2 and 5 years	<b>690,421</b>	838,594
	<b>1,011,731</b>	1,056,348

### 10. Commitments under operating leases

At 31 December 2021 the Authority had future minimum lease payments under non-cancellable operating leases as follows:

	£	2020 £
Within one year	<b>82,471</b>	76,848
Within one to two years	<b>82,471</b>	76,848
Within two to five years	<b>41,235</b>	115,272
<b>Total</b>	<b>206,177</b>	268,968

**The Data Protection Authority**

**Notes to the Financial Statements  
For the Year Ended 31 December 2021**

---

**11. Controlling party**

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

The Data Protection Authority

**Detailed Statement of Income and expenditure account (unaudited)  
For the Year Ended 31 December 2021**

	£	2020 £
Income	<b>1,545,300</b>	155,550
Administrative expenses	<b>(1,303,425)</b>	(1,243,045)
Loan waived	<b>243,788</b>	-
Effective interest	<b>(41,243)</b>	(35,237)
<b>Surplus/(deficit) for the year</b>	<b>444,420</b>	(1,122,732)
<b>Income</b>		
Annual notification fees	<b>1,545,300</b>	155,550
<b>Administrative expenses</b>		
Salaries and other staff costs	<b>726,919</b>	659,481
Members fees	<b>22,022</b>	15,225
Project costs	<b>33,308</b>	83,903
Rent, rates and premises expenses	<b>106,383</b>	100,974
Legal and professional fees	<b>138,118</b>	218,250
Communication costs	<b>37,907</b>	19,983
Travel	<b>12,421</b>	8,652
IT costs	<b>110,460</b>	69,136
Office and sundry expenses	<b>25,771</b>	25,165
Insurances	<b>12,460</b>	10,679
Amortisation	<b>39,456</b>	1,416
Depreciation	<b>31,314</b>	30,181
Loss on disposal of tangible asset	<b>6,886</b>	-
	<b>1,303,425</b>	1,243,045
Transitional loan written off	<b>243,788</b>	-



# Excellence Through Ethics.