THE OFFICE OF THE
Data Protection Authority
BAILIWICK OF GUERNSEY

Annual Report

2025

FOR THE PERIOD

1 Jan 2025 – 31 Dec 2025

The Data Protection Principles

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

Contents

“

This Annual Report... tells stories and it sets out the numbers which show significantly improving productivity. It is a tool of accountability, but also provides transparent insight which will inform constructive engagement with our stakeholders.

”

Chairman's Foreword

An introduction from our Chairman

Richard Thomas CBE
Chairman
Guernsey Data Protection Authority

Guernsey's Data Protection Authority has come a long way in eight years. We can fairly claim to be effective, efficient and well-respected.

We have succeeded in squaring many circles. We are independent, but accountable. We are a regulator working within an exacting legal framework but have demonstrated the value of pragmatic informality with both enforcement activities and the handling of complaints. We deal with complex issues in a fast-changing technological world, but we simplify and avoid jargon as we help organisations get it right and help people to understand their rights. We are a small organisation in a small Bailiwick, but we can also be a laboratory for new approaches. And we have found ways to work with others to punch above our weight, domestically and internationally.

Above all, any Data Protection Authority must be judged by the outcomes it achieves across a wide range of responsibilities. This Annual Report is a record of the main outcomes achieved in 2025. It tells stories and it sets out the numbers which show significantly heavier workloads and improved productivity. It is a tool of accountability but also provides transparent insight which will inform constructive engagement with our stakeholders.

The future is also flagged. Towards the end of the year we developed a fresh three-year Strategic Plan. This spells out how we will continue to promote responsible use of personal information — preventing harm whilst supporting prosperity and innovation. Annual business plans and budgets provide the detail to make the best possible use of the resources available to us.

This is my last Foreword as Chairman of the Authority and I do not disguise my pride at what has been achieved. But it is people who really secure the outcomes. As our Commissioner, Brent Homan has brought fresh thinking and powerful leadership. He and his excellent team deserve full credit for all these results. I also thank my colleagues on the Board – not least Chris Docksey and Jane Wonnacott who stood down at the end of the year – for providing inspiration, wisdom, objectivity and support.

April 2026

> **We deal with complex issues in a fast-changing technological world, but we simplify and avoid jargon as we help organisations get it right and help people to understand their rights.**

Commissioner's Executive Summary

At the Office of Data Protection Authority (ODPA) we are committed to advancing data protection rights in the Bailiwick. And to that end, framed by our regulatory pillars of Balance, Trust and Partnership, 2025 has proven a banner year of firsts and exceptional results.

Brent R Homan
Data Protection Commissioner
(Bailiwick of Guernsey)

Balance

is about choosing the right tool for the right situation.

From an enforcement perspective that means embracing our philosophy of *Assertive, Agile Enforcement*, to achieve the best possible outcome for all parties, in the most expedient manner possible. This means that in most instances we resolve concerns outside the formal route. By virtue of this strategy, we have seen the length of investigations fall to historic lows despite a record number of complaints received. In fact, at the end of 2025, there were no ongoing investigations greater than a year in length.

Balance also means that we focus our formal enforcement efforts on matters of highest risk, including the administrative fine sanctions levied against Jacksons (£65,000) and the Medical Specialist Group (£100,000). In those matters, success is never measured by the quantum of fine itself, but whether the enforcement action results in greater protections for the Bailiwick, a commitment that both organisations have made.

Finally, notwithstanding efforts, some matters can't be resolved consensually. In those situations, the public rightfully expects us to defend their data rights in court. This is exactly what happened in our first ever contested Royal Court hearing where an appeal of our breach determination regarding a local law firm's handling of health records was dismissed, upholding the integrity of our investigative process. This brings us to our second regulatory pillar – **Trust.**

Trust

is about demonstrating integrity in all we do. And while it includes having the resolve to protect peoples' data rights through court actions, it is so much more.

Trust is also earned through accountability and transparency, and it is on that principled foundation that we have built our new Strategic Plan for 2026-29. The Strategic Plan makes clear our commitment to elevating data protection in the Bailiwick by educating and equipping society, supporting a modern, safe and progressive digital economy, and responding to non-compliance proportionally, through *Assertive, Agile Enforcement.* We are holding ourselves to account through this plan, with commitments including: (i) developing our outreach programme to encompass all sectors of the community, especially vulnerable groups; and (ii) resolving 90% of complaints and breaches within a year.

But delivering results in 2025 and charting an even more ambitious course for the next three years, cannot be achieved alone. It requires trusted partners, both in the Bailiwick and beyond, which brings us to our third regulatory pillar — **Partnership.**

> **The Strategic Plan makes clear our commitment to elevating data protection in the Bailiwick by educating and equipping society, supporting a modern, safe and progressive digital economy, and responding to non-compliance proportionally, through Assertive, Agile Enforcement.**

Partnership

greatly expands our capacity to protect and promote data rights in the Bailiwick and you will find the "Power of Partnership" throughout this report.

Domestically, our commitment to partnership has produced a series of "firsts". For the first time, we had a series of in-person engagements in Sark. We partnered with the school to deliver children's lessons and worked with government as it develops its data protection framework. And partnering with schools throughout the Bailiwick, we introduced the Parents' Online Safety Workshop. This series was launched in Alderney and then rolled out across Guernsey, equipping parents with practical strategies to protect their loved ones online.

On the regulatory partnership front, in January we launched the Guernsey Consumer Cooperation Forum ("GCCF") alongside the Channel Islands Financial Ombudsman and the Guernsey Competition Regulatory Authority. The GCCF will encourage the sharing of best practices and collaboration on common consumer priorities for the Bailiwick.

Internationally, the ODPA continued its global leadership in 2025. As secretariat and co-chair of the International Enforcement Working Group ("IEWG") we hosted a capacity building session at the Global Privacy Assembly's general meeting on effective enforcement collaboration, focussing on key global investigations against companies such as TikTok and 23andMe.

Towards addressing the global priority of protecting our children, our office was honoured to be a coordinator for the Global Privacy Sweep uniting 27 authorities from around the world to assess websites and apps that target children. In June, the ODPA hosted partners from the *British, Irish & Islands Data Protection Authorities* network to advance shared priorities including the promotion of children's rights and the critical importance of data protection for global financial hubs.

Finally, in December we launched our first ever joint investigation into a cyber incident involving a trade union, alongside partners in the UK, Jersey and the Isle of Man.

With that, I invite you to explore and enjoy the Annual Report, discovering how your Data Protection Authority strived to promote and protect your data rights in 2025.

Who we are

Our vision and regulatory pillars guide everything we do to ensure personal information is handled with care, integrity and accountability.

Our vision

A safe and prosperous community where people can trust that their personal information will be used responsibly.

Our purpose

We safeguard people's data rights by protecting them against harm and promoting the responsible use of personal information.

Our approach

We achieve this through:

- placing the promotion of data rights and the protection of individuals at the heart of everything we do
- education and outreach
- helping organisations get things right
- allowing innovation to thrive, safely
- taking proportionate, assertive and agile enforcement action against significant non-compliance

Our three pillars – Balance, Trust and Partnership

We strive to secure the best possible outcomes for people by strengthening and protecting their data rights. We work towards this by putting our regulatory principles of balance, trust and partnership into practice every day.

Balance

We choose the right tool for the right situation. We are fair, proportionate and evidence based. Through education, we help organisations build a culture of proactive compliance, but we will enforce the law assertively when necessary.

Trust

We earn trust by acting with integrity and living our core values:

Impartial and ethical: we are independent. We do what is right, not what is convenient, maintaining the highest standards of ethical conduct.

Cooperative and accountable: we engage authentically with stakeholders. We are transparent and seek constructive relationships to achieve effective outcomes and value for money.

Ambitious and progressive: we strive for excellence and lead in areas that require our expertise. We value privacy, innovation and continuous improvement in an ever-evolving environment.

Partnership

As a small regulator, we embrace the "Power of Partnership" to expand our capacity to take action and amplify the impact of our actions. Strong domestic and international relationships are vital to protecting the Bailiwick's personal data from misuse. Together, we ensure the Bailiwick remains a trusted and competitive jurisdiction.

Our three-year Strategic Plan

Our new Strategic Plan (2026-9) has been developed following extensive consultation both internally and externally through our Guidance Advisory Panel comprising key representatives from the public, private and third sectors in the Bailiwick.

The Strategic Plan sets out a progressive pathway to achieve our vision of a safe and prosperous community where people can trust that their personal information will be used responsibility. It clarifies our purpose, approach and regulatory pillars of balance, trust and partnership and refines our strategic priorities.

The Strategic Plan is also informed by our environmental scan. In today's digital era, rapid technological advances, from genetic profiling to generative AI, have reshaped the data protection landscape requiring an innovative, bold and agile approach to protecting and respecting people's data rights.

Through the Strategic Plan, the ODPA is reinforcing its commitment to building on its achievements, while setting out three core strategic objectives for the next three years:

1.
Educate society, equip individuals and influence culture

2.
A modern safe, digital society and economy

3.
Assertive Agile Enforcement

About the Authority

Authority members

Chairman
Richard Thomas CBE
Four-year term commencing May 2023.

Voting Member
John Curran
Four-year term commencing May 2023.

Voting Member
Sarah Willis
Four-year term commencing January 2026.

Voting Member
Simon Entwisle
Four-year term commencing May 2023.

Voting Member
Mark Lempriere
Four-year term commencing May 2022.

Voting Member
Steve Wood
Five-year term commencing January 2026.

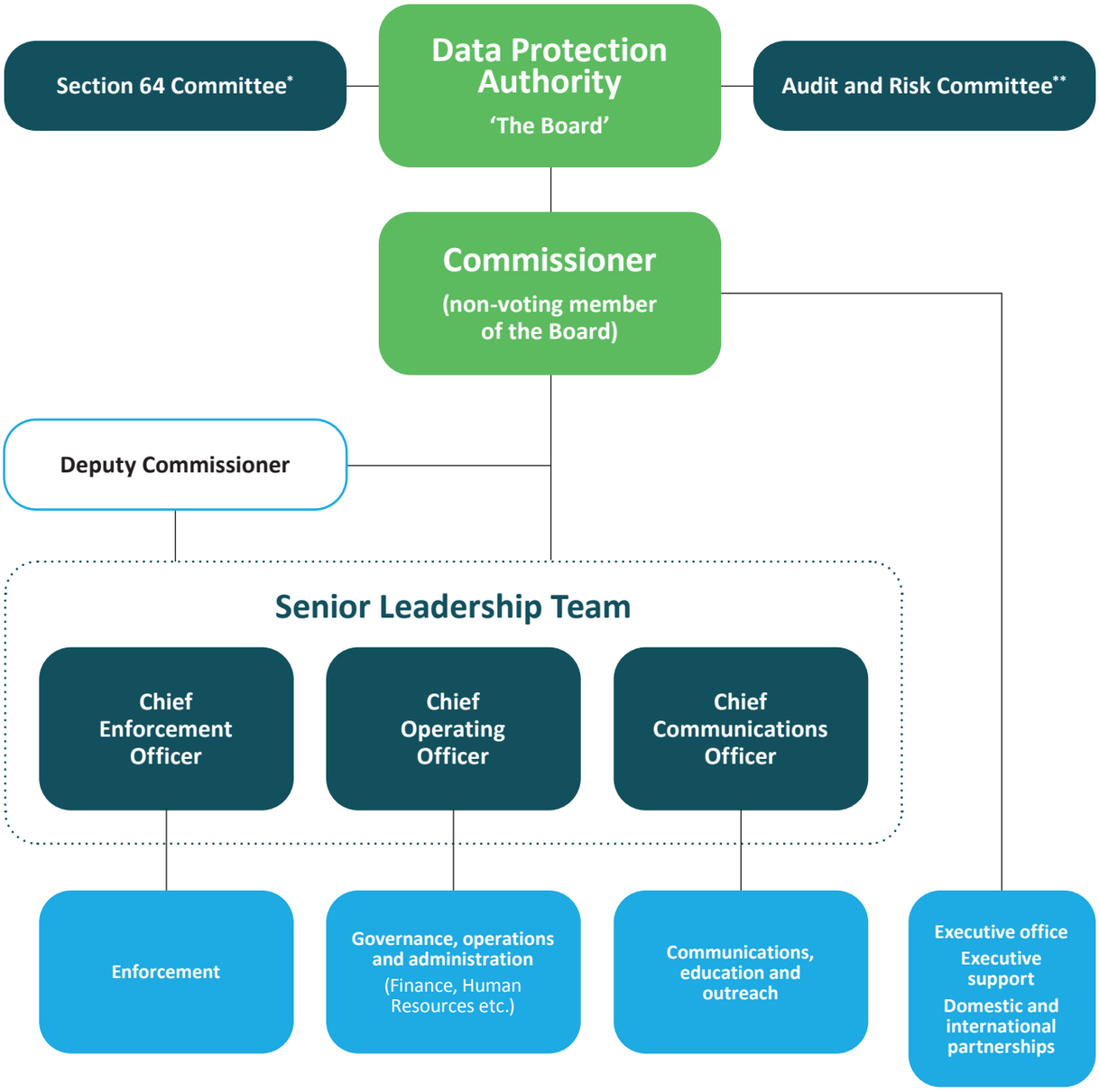
Voting Member
Nicola Wood MBE
Five-year term commencing May 2022.

Commissioner and non-voting Member
Brent R Homan
Five-year term commencing 1 January 2024.

Voting Member
Christopher Docksey
Four-year term commencing May 2022 (until January 2026).

Voting Member
Dr Jane Wonnacott
Four-year term commencing May 2022 (until January 2026).

Our organisation



*Section 64 Committee – the sub-committee of the Board responsible for the decision to publish public statements.

**Audit & Risk Committee – the sub-committee of the Board responsible for oversight of financial reporting, risk management and the application of corporate governance best practice.

2025 at a glance

Highlights of our work and impact during 2025.

1000+

children reached through 48 sessions across all Bailiwick schools

300+

children and families attended the annual ACE Invaders online safety event (co-organised by the ODPA)

New

online safety workshop launched for parents across the Bailiwick

18

thought leadership features published

13

podcasts produced

12

international privacy news reviews delivered

9

public statements issued, including two related to administrative fines

10

Bailiwick speaking and outreach events

12

international speaking engagements

90+

ODPA-related news articles published or broadcast

>21k

controllers and processors registered

1st

successfully defended Royal Court Appeal

Communications, education and outreach

A strategic approach to communication

Effective regulation depends on impactful communication. In 2025, we took a proactive, strategic approach to ensure that data protection rights and responsibilities are not only understood but lived. Through our actions we:

- translate law into accessible, practical guidance
- amplify enforcement outcomes to drive accountability
- create pathways for individuals and organisations to engage with their respective rights and responsibilities

Through targeted outreach, innovation and thought leadership, we empower our community to treat personal information responsibly, safeguard children and young people through education, and strengthen public trust.

By combining clarity, consistency and credibility across every channel, we uphold the integrity of the ODPA while driving a positive cultural shift towards responsible data use across the Bailiwick.

Empowering organisations and individuals to handle personal information responsibly is an overarching objective. We accomplish this by:

- driving compliance by improving awareness and understanding of data protection legislation and the Authority's enforcement actions
- safeguarding the data rights of children and young people through education and outreach
- supporting children and young people to exercise their data rights

Key communications activities

Website migration project

In November, we successfully migrated our website to a new, more user-friendly platform which has greatly increased our capacity to upload and refine content. We have also improved the user experience by making key content, such as public statements and guidance, easier to navigate.

We are in the process of examining how we can best monitor the performance of the website using our newly established analytics suite. This will help ensure that organisations and the public are getting the content they need in an efficient and intuitive fashion. This will also feed into our new Business Intelligence Strategy, working towards optimising resource and strategic decisions (see page 31).

As a data protection authority, we are mindful of the potential privacy considerations associated with the monitoring of website traffic. To that end, we are pleased to have found a solution which does not use analytics cookies and allows users to opt out of tracking.

Given this, the following figures reported do not represent the full volume of website visitors.

November website statistics

2,693 page views

646 unique visits

34% bounce rate

December website statistics

2,839 page views

754 unique visits

38% bounce rate

NB: Bounce rate refers to the frequency at which users arrive on the website and leave with their next click, so a lower figure here is better.

Data gathered since November 2025

Most visits by country
1. Guernsey
2. United Kingdom
3. Jersey
4. Ireland
5. United States

Most popular pages
Homepage
News
The Law
AFR appeal outcome
Search results

Device usage
1. 67% desktop
2. 31% mobile
3. 2% tablet

Public Statements

In 2025, we issued two administrative fines, the most serious sanction available to the ODPA under the local data protection legislation (see page 21 in the Enforcement section for a table of sanctions). The ODPA has had the ability to issue fines for seven years, fining four organisations in that time. Fines are an important tool in serious situations where there have been systemic failings, fundamental errors and/or significant harms to the public. They are one of several options available to us and we take a balanced and proportionate approach to every enforcement matter.

ODPA outreach programme

From speaking events and information workshops to podcasts and seminars, we focused on storytelling and shared experiences to encourage broader conversations around data protection and spark a wider interest in privacy-related matters.

Communications, education and outreach *continued*

ODPA Seeds: children inspiring cultural change

The ODPA is an accredited PSHE support agency for the States of Guernsey and delivers online safety/data protection sessions to hundreds of children across the island in Years 4, 8 and 10. All school sessions are delivered by our staff who are DBS checked and have completed the safeguarding children and young people training at Levels 1 and 2.

We also introduced a groundbreaking initiative in the mission to protect children — Parents' Workshops, offering practical tips and advice for parents whose children use popular social media and gaming apps. They were developed following an initiative by a visual content and outreach expert from the Office of the Privacy Commissioner for Bermuda (PrivCom) who spent a month with the Authority as part of a secondment programme.

In 2025, we launched a student intern programme to provide opportunities for the talented youth of Guernsey. Our first intern was particularly useful in helping us review and add to our content, ensuring that it remains relevant and accessible to young people.

We also held a successful children's online safety event in January. ACE Invaders was enjoyed by more than 300 children and their families. We rolled out a new format focused on exploring gaming safely, combined with educational activities. This approach proved popular, giving the event a new direction and appeal.

ODPA podcast programme

Our podcast programme continues to provide a platform for accessible and informed discussion on privacy, data protection and wider societal issues.

Two three-part series explore privacy as both a timeless human concern and a pressing contemporary challenge.

Privacy Across Time and Space featured insights from global privacy leaders: Alexander White, Queensland Privacy Commissioner; Alexandra Delaney Bhattacharya, Isle of Man Information Commissioner; and Shana Morgan, Global Head of AI at L3Harris Tech. This series explores: how 'data drove the Roman Empire'; indigenous data privacy and what Bollywood reveals about privacy in Indian culture.

The second series, *Data, Democracy and Freedom*, focuses on the impact of data use on democratic systems, civil liberties and freedom of expression. It features contributions from: Dr Colin Bennett, Professor Emeritus of Political Science at the University of Victoria; Travis LeBlanc, civil rights lawyer and former Chief of the US Federal Communications Commission Enforcement Bureau; and Susie Alegre, human rights lawyer and author.

This programme of podcasts was complemented by the annual Bijou Lecture. Inspired by the BBC's Reith Lectures, our flagship podcast features newly appointed Australian Privacy Commissioner Carly Kind discussing her vision as a new Commissioner for Australia, children's rights, how to make social media safer and the mass adoption of AI.

2025 Social media metrics

Social Media Channel	Followers/ subscribers	Total engagements
LinkedIn	7.6k	85k impressions 1.76k reactions 55 comments 64 reposts
Facebook (launched July)	36	29.5k views
SoundCloud (podcasts)	33	1.65k views
YouTube (vodcasts and videos)	90	1.8k views

Social media strategy update

Social media is one of the most effective ways we promote our activities, events and initiatives. We are continually reviewing and assessing how we use our various channels and strengthening our skills to better engage with our citizens and the local regulated community and to showcase our work and achievements within the Bailiwick and beyond.

Our presence continues to grow, with a steady increase in visitors and followers across both LinkedIn and Facebook. We have approached social media strategically with careful consideration. Facebook was introduced in July, with content specifically targeted at our regulated community, particularly sole traders and small businesses that are active on the platform.

Communications highlights in numbers

2024-25 academic year

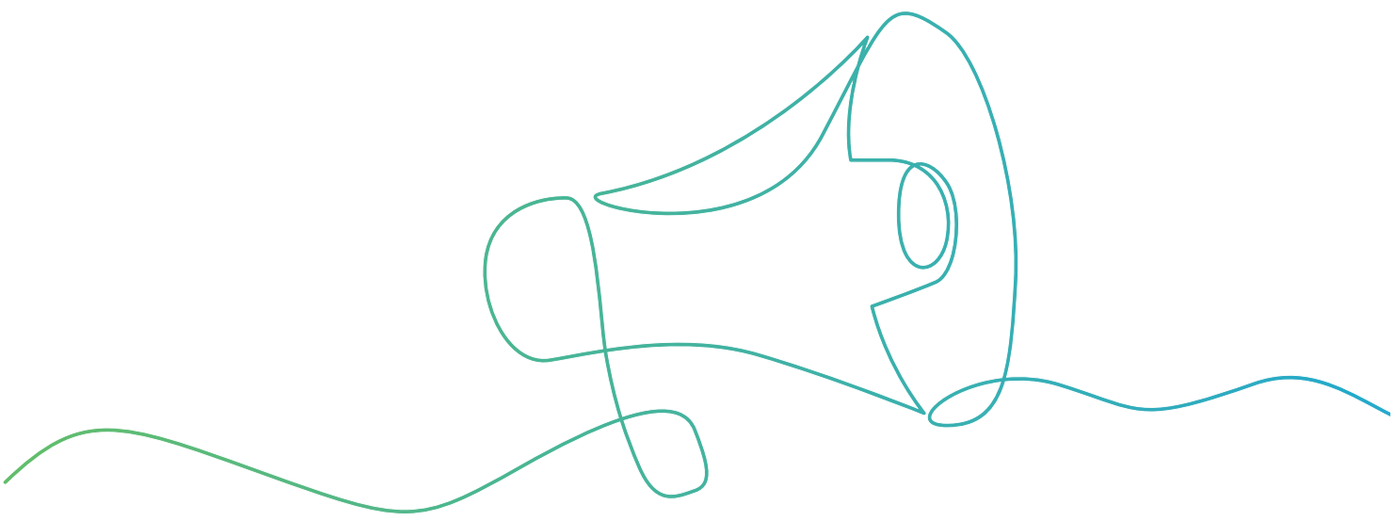
- 32 sessions delivered to secondary schools (nine through Youth Commission partnership in 2024 before bringing in-house for 2025)
- 484 Year 4 children reached across 10 primary schools in November 2024
- 11 in-house podcasts
- 2 guest podcasts
- 2 breakfast breach workshops

“

These interactive, informal workshops provide actionable advice on supporting our children in a digital era that holds both promise and peril. Protecting children’s rights is a priority for our office and we have developed a suite of tools to do just that, from conducting classroom sessions in schools to engaging with tech companies about safe practices.

”

Brent Homan, Data Protection Commissioner



Enforcement

Strengthening outcomes through assertive, agile and early resolution

Effective enforcement is not defined by the number of sanctions issued, but by the improvements achieved. In 2025, the Authority continued to embed its Assertive Agile Enforcement (AAE) model — a practical, outcome-focused approach that prioritises early resolution, constructive engagement and proportionate use of formal powers. It is an approach that promises swifter, better results, to the benefit of complainants, organisations and most importantly, the Bailiwick as a whole.

By addressing concerns swiftly where possible, encouraging meaningful commitments and reserving formal investigations for higher-risk or complex matters, we ensure regulatory action is timely and effective. When sanctions are required, they are applied with clarity and purpose — not as punishment for its own sake, but to secure corrective action, strengthen sector-wide standards and prevent future harm.

In an increasingly complex digital environment, this balanced and scalable approach enables us to protect individuals' rights, support organisations to improve, and maintain confidence in a fair and credible regulatory framework.

Assertive Agile Enforcement

The AAE model demonstrates that enforcement is not simply the act of identifying non-compliance, but the broader task of improving data protection standards in a way that is timely and proportionate. The approach brings together constructive engagement and formal powers where necessary.

A significant part of AAE begins long before any formal investigation is opened, allowing for matters to be addressed swiftly when the facts are straightforward. Many concerns can be resolved through discussion or targeted commitments, avoiding the cost and delay associated with more formal action. This ensures that investigative resources are reserved for situations where the risk of harm is higher or the matter is more complex.

Underlying this approach is the culture of compassionate compliance. Individuals often approach us when they are frustrated or feeling unsupported: responding with clarity and calm helps build confidence in the fairness of the process. Organisations also tend to be more cooperative when conversations are constructive and proportionate, which in turn leads to swifter and better outcomes.

There are situations where we can become aware of a data protection concern through intelligence rather than through a complaint or self-reported breach submission. These matters are often addressed through proactive engagements where we make clear to organisations the benefits of addressing the concern consensually without having to resort to a formal investigation. Incentive-wise, we have seen that avoiding a formal investigation can be an effective motivational factor to encourage positive engagement from organisations.

In the context of formal investigations, the AAE model emphasises the importance of beginning at the end, keeping in view the ultimate goal of concluding matters within a reasonable timeframe. We are mindful that an investigation that takes too long risks delivering a remedy that comes too late. By maintaining focus and taking opportunities for early resolution even within the formal process, we ensure that investigations remain proportionate.

Where a sanction is warranted, our main goal, including with administrative fines, is to ensure the organisation and wider sector learn from the outcome and make lasting data protection improvements.

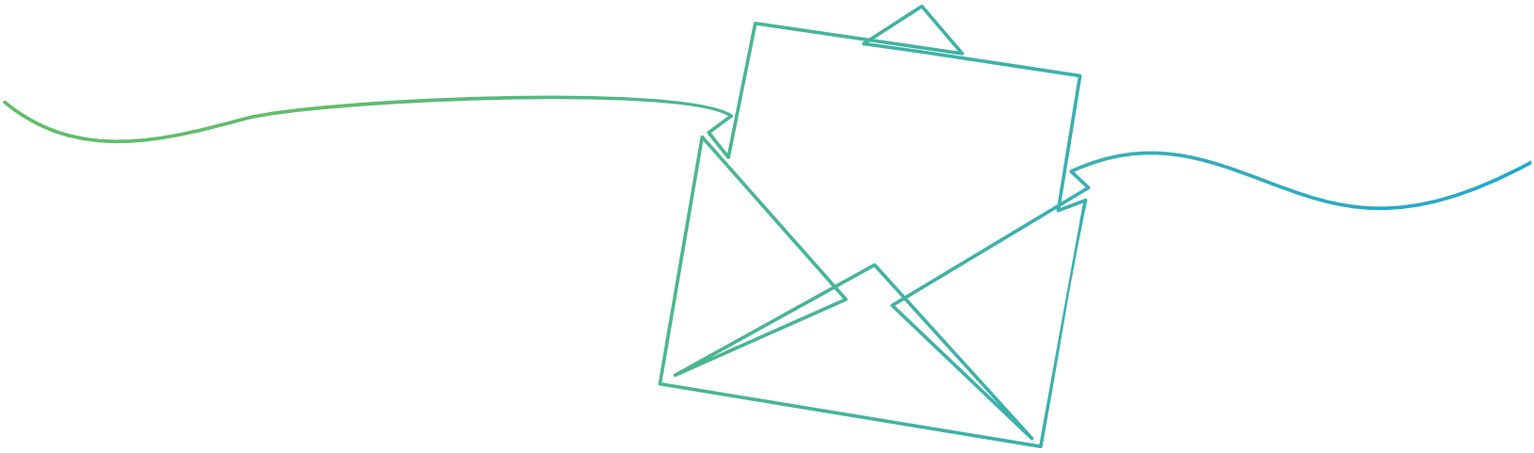
Together, these elements form a scalable set of tools ranging from informal advice to formal sanctions. The AAE model is shaped by the ongoing need to protect individuals' rights in an increasingly complex digital environment.

Enforcement framework

The Authority's enforcement framework is designed to support improvements in data protection practices by applying sanctions that are proportionate to the risks and harms identified. There are four sanctions available under the Law:

- Reprimand
- Warning
- Enforcement order
- Administrative fine

A **reprimand** represents a formal recognition that a contravention of the Law has occurred. A reprimand does not require further action but marks the contravention clearly and provides an important reference point should further concerns arise in the future.



A **warning** plays a different role. When we issue a warning, it signals that an activity is likely to contravene the Law if carried out or continued. This gives organisations a clear opportunity to avoid harm before it occurs.

The **enforcement order** is the sanction that most directly delivers remedial impact as it requires an organisation to take specified steps. They are used with serious contravention where changes are required to ensure compliance with the law. Examples of these steps include improving security measures, updating internal processes or strengthening accountability. Enforcement orders ensure that identified weaknesses are addressed. Enforcement orders are the most frequently issued sanction.

In matters where the risk or impact is particularly serious, an **administrative fine** may be issued. A financial penalty reinforces the expectation that organisations take their legal obligations seriously. Administrative fines are used in circumstances where other measures would not adequately reflect the gravity of the breach, or where deterrence is necessary. When an administrative fine is issued, it is often accompanied by an enforcement order to ensure corrective steps are taken.

Taken together, these sanctions form a balanced, flexible and proportionate enforcement model. Each has its purpose, but all serve the same aim of improving data protection practices and preventing future harm. Our approach places emphasis on corrective action that leads to meaningful and enduring data protection improvement rather than punishment for its own sake.

Phishing: a growing threat

Phishing has become one of the most disruptive cyber threats facing organisations and individuals. The aim is simple: to persuade someone to hand over information that can be used by cyber criminals for financial gain, identity theft, or other nefarious intentions. A message may look harmless enough, for example an invoice request or a note that appears to come from a colleague, but a single click on a link can lead straight to a malicious site designed to capture personal data or compromise an organisation.

Security measures, such as strong password generation and multi-factor authentication, have made it far more difficult for cybercriminals to force their way into accounts through technical means alone. Phishing allows them to bypass these protections entirely by targeting people through small lapses in attention.

Most phishing attempts arrive by email, through text messages, social media or even phone calls.

In recent years, we have seen a rise in both the volume and sophistication of phishing incidents, with several local organisations falling victim. In three cases during 2025, the failures were serious enough that the Authority issued sanctions, including an administrative fine to the Medical Specialist Group (“MSG”, see page 23). Each of these organisations failed to ensure a reasonable level of security proportionate to the sensitivity of the personal data processed.

These cases underscore that while phishing may start with a convincing message, its impact is shaped by the strength of organisational safeguards. The most reliable defence to the threat posed by phishing attacks is a workforce that understands how they operate and feels confident in recognising them. When employees are not equipped with that awareness, they unintentionally create an entry point that cybercriminals can quickly exploit.

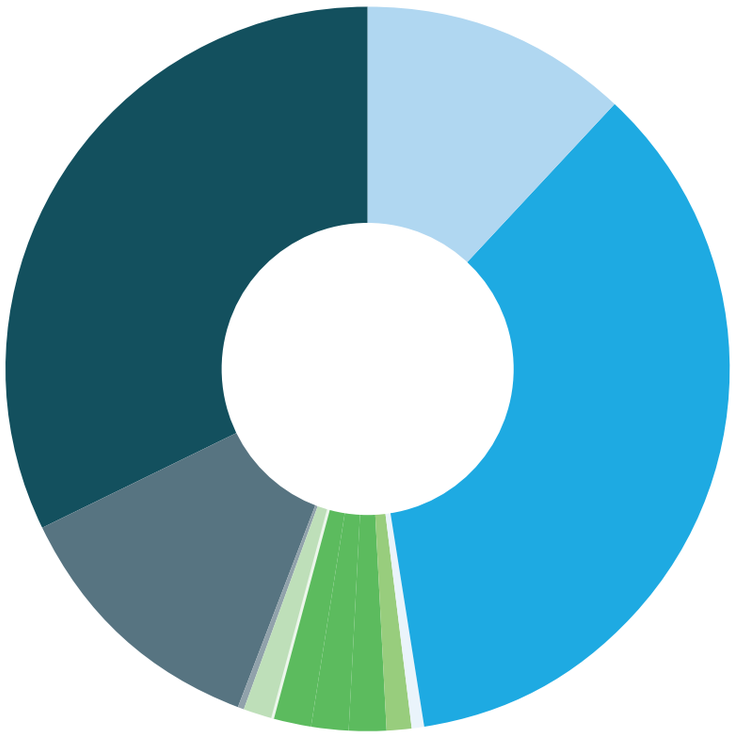
To support organisations and individuals in recognising and resisting these threats, we produced the ‘Protect against phishing’ guidance. This guidance strengthens everyday awareness and reduces the likelihood that organisations will be successfully targeted. The guidance sits within the ODPA’s wider effort to help the Bailiwick understand and arm itself against evolving cyber risks.

Enforcement *continued*

Number of complaints and self-reported breaches (2025)

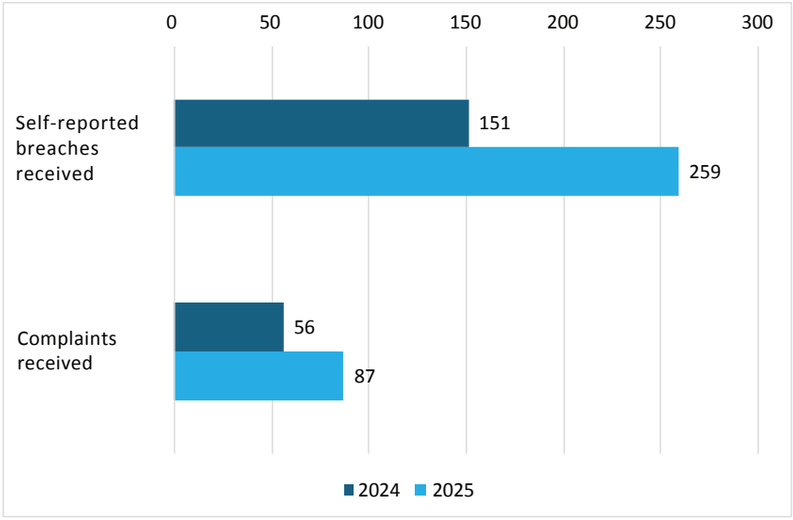
The table below provides an overview of complaint handling and breach management activity during 2025. It summarises, among other things, the number of complaints received, the volume of self-reported personal data breaches and the number of breaches closed. Together, these figures offer an insight into organisational compliance and the effectiveness of case management processes over the year. The following are notable trends:

Key statistics	Number:
Complaints received	87
Self-reported breaches:	259
Investigations opened	5
Inquiries opened	8
Breach determinations	13
Sanctions	12
Controllers sanctioned	11
Reprimands	1
Warnings	0
Orders	9
Administrative fines	2
Cases closed (complaints/inquiries)	88
Breaches closed	233



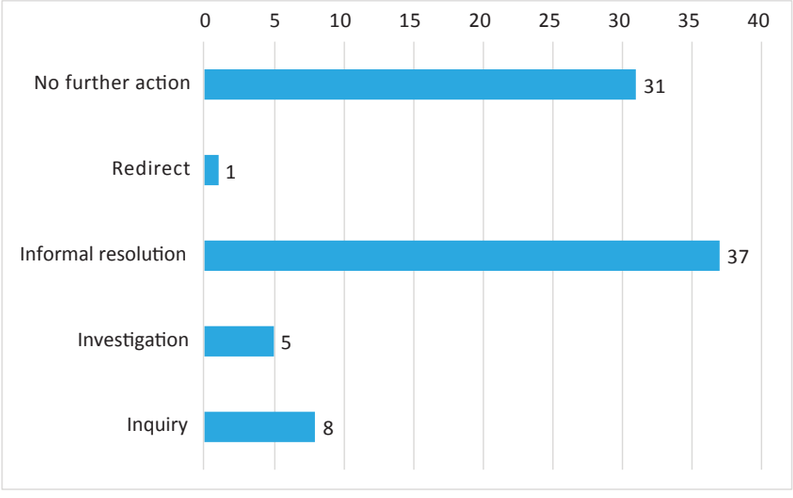
Number of complaints and self-reported breaches (2024 & 2025)

This chart compares the volume of complaints received with the number of self-reported personal data breaches in 2024 and 2025. It shows a significant increase year on year, with complaints rising by 55% and self-reported breaches increasing by 72%. This growth may reflect heightened public awareness of individuals' rights to raise concerns, alongside improved organisational understanding of the requirement to notify the ODPA of personal data breaches within 72 hours.



2025 complaint outcomes

This chart summarises the outcomes of complaints assessed in 2025. Informal resolution was the most common outcome, reflecting the ODPA's commitment to the Assertive Agile Enforcement model outlined above. Such resolutions typically involve organisations providing previously withheld personal data, rectifying inaccuracies, or the ODPA issuing letters of concern or advisory feedback.

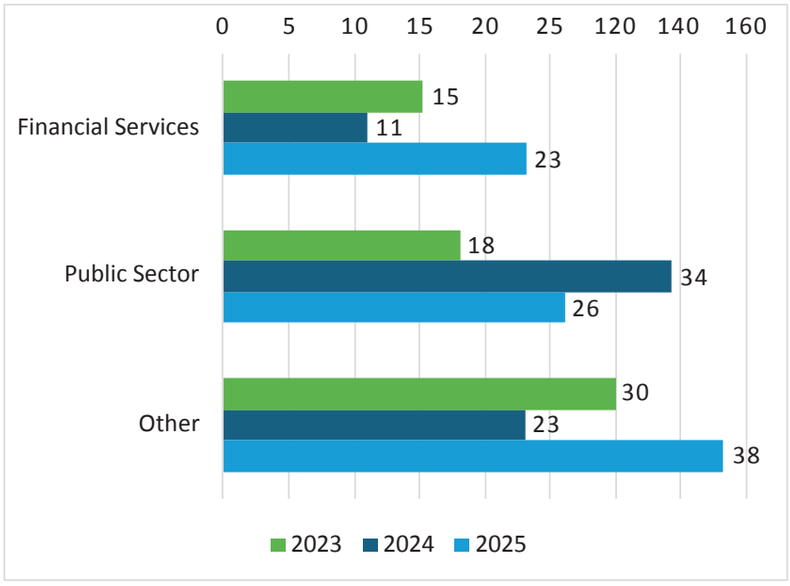


Cases where no further action is taken commonly include complaints relating to matters outside our jurisdiction such as domestic CCTV or cases where initial enquiries confirm that the processing is lawful.

Enforcement *continued*

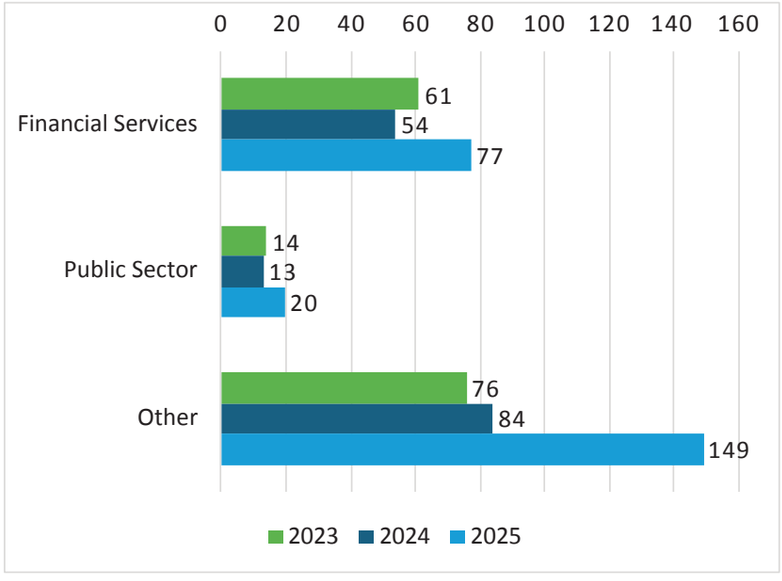
Complaints by sector

The 2025 statistics show an overall rise in complaints, despite a reduction in Public Sector complaints, with the Financial Services sector standing out with a doubling in complaints from 2024.



Self-reported breaches by sector

This chart compares the sectors that reported personal data breaches in 2023, 2024, and 2025, highlighting which sectors most frequently self-reported incidents and how this has changed over time.

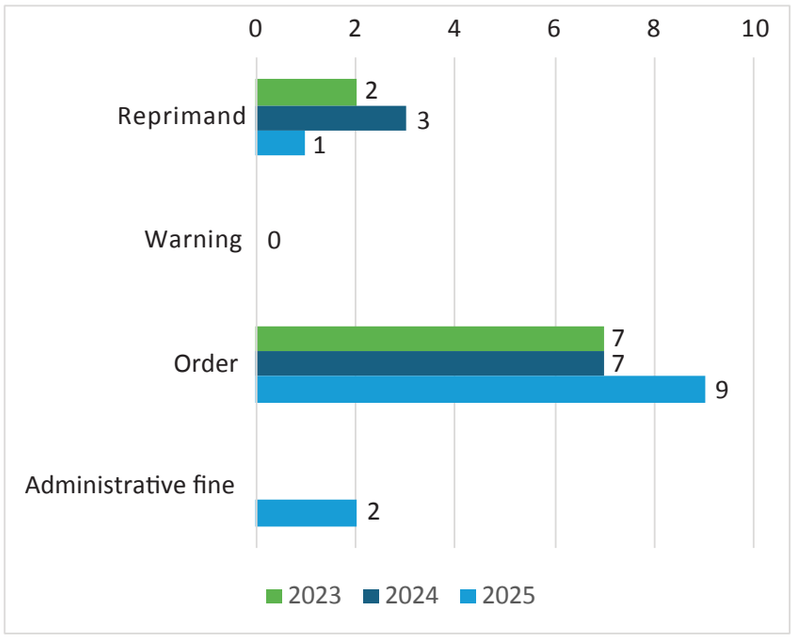


In 2025, there was a clear increase in self-reported breaches across several sectors. The 'Other' category recorded the highest number of reports, with notable rises also seen in the Financial Services.

Sanctions issued

The 2025 sanctions chart highlights a shift in how regulatory outcomes were applied. Orders increased to nine, as they continue to be the most frequently used sanction. An order requires an organisation to bring specific practices or processes into compliance with the Law — in simple terms, it is a formal instruction to fix or amend something that has gone wrong.

Two administrative fines were issued in 2025 for Jacksons and the Medical Specialist Group (see dedicated sections below). In both cases, the circumstances met the statutory threshold and an administrative fine was considered necessary to reinforce future compliance.



Compared with 2023 and 2024, the 2025 pattern demonstrates a broader use of the full range of sanctions and an increased emphasis on more structured corrective measures. This evolution reflects our commitment to proportionality and aligns with our strategy of Assertive Agile Enforcement.

Note: Not every contravention results in a sanction being issued.

Assertive Agile Enforcement in action

ODPA in the Royal Court

Appeal against a breach determination: AFR Advocates

In December 2025, the Royal Court of Guernsey dismissed an appeal brought by three partners in a law firm trading as AFR Advocates ("AFR") against a breach determination issued by the Authority. The appeal arose from an investigation into an incident in 2022 and marked the first occasion on which a controller exercised its right of appeal under section 84 of the Law.

The incident concerned the hand delivery of a bundle of legal documents to the home address of an individual involved in private litigation. The bundle, which exceeded 200 pages, contained sensitive personal data, including health information classified as special category data. It was left on the individual's doorstep in an ordinary ring binder, not enclosed in an envelope and in view of the public road. The individual was not present at the time and raised concerns that their personal data had been exposed to unnecessary risk.

Following a complaint, the Authority concluded that AFR had failed to safeguard the integrity and confidentiality of the personal data and had not taken reasonable steps to ensure its security during delivery. A breach determination and reprimand were issued. The Royal Court upheld the Authority's findings in full, reinforcing that data protection obligations apply equally to the physical handling of information and that practices must reflect the sensitivity of the data involved. The judgment provided important clarity on the application of the Law.

Administrative fine cases

Failure to secure systems: Medical Specialist Group LLP

In late 2021, the Medical Specialist Group LLP (MSG) identified that its email server had been compromised after suspicious activity indicated unauthorised access. An internal investigation revealed that cyber criminals had gained access several months earlier by exploiting known vulnerabilities that had not been addressed. As a result, emails containing sensitive patient health data were accessed and later used in phishing campaigns targeting patients.

The Authority's inquiry found that the organisation had failed to take reasonable steps to ensure the security of personal data. In particular, routine security updates had not been applied to the email server for an extended period, including updates that directly addressed the vulnerabilities exploited.

Weaknesses were also identified in the use of threat detection software, contributing to a delay of more than three months between the initial compromise and its detection and reporting.

Further shortcomings were identified in the handling of the breach, including a failure to properly establish root causes and recognise deficiencies in security monitoring. Given the scale of the incident and the sensitivity of the data affected, the Authority determined that the threshold for a financial penalty had been met. An administrative fine of £100,000 was imposed, with part of the amount (£25,000) deferred (and potentially waived) subject to completion of remedial actions under an action plan. This sanction was accepted without appeal. This case highlights the importance of cyber security, particularly where organisations process special category data.

Unlawful alteration of marketing preferences: Jacksons

In January 2023, an inquiry was initiated into Jacksons, a Channel Islands car dealership, after intelligence indicated that customers had received marketing communications contrary to their stated preferences. The investigation revealed that customer records had been amended to change marketing preferences from "No" to "Yes" without the knowledge or consent of the individuals concerned.

An internal review confirmed that 430 customer records had been altered unlawfully over the course of approximately one year, primarily within Jacksons' Motormall operations. The practice originated from a directive issued by a senior employee and was carried out by sales staff. This senior employee is no longer with the company and the Authority found no evidence to suggest that there was awareness of the practice by the Jacksons' data protection officer or its board of directors. The Authority concluded that the amendments represented a deliberate interference with individuals' data rights.

The Authority found breaches of the principles relating to lawfulness, fairness and transparency and accuracy. Given the intentional nature of the conduct, an administrative fine of £65,000 was imposed alongside an enforcement order requiring that Jacksons take certain steps to comply with the Law. The sanctions were accepted without appeal. The enforcement order was confirmed to have been complied with by the Authority in December 2025.

This case serves as a clear reminder that respecting individuals' marketing preferences is a core obligation under the law and that consent records must be accurate and protected from inappropriate interference.

Case summaries — alternative enforcement outcomes

Case study #1:

When AI gets it wrong

A concern was raised with the Authority by an individual whose name had been incorrectly associated with the criminal history of another person. The issue arose through an AI-generated summary produced by a search engine's automated results feature. When the individual's name was entered, the system generated a summary that blended their identity with that of a person convicted of a serious offence. Although entirely inaccurate, the presentation of the information gave the impression of legitimacy and caused the person involved significant distress.

Further review showed that the AI system had combined publicly available information based solely on a shared last name. Because the summary appeared prominently and was phrased as a definitive statement, correcting the inaccuracy required significant effort. The situation highlighted how generative AI, when applied to personal data can create harm when users assume outputs are reliable.

This case illustrates why AI-generated content must be verified and not treated as infallible. These systems can produce material that sounds authoritative while containing inaccuracies, especially where personal data is involved. Without verification, these errors can undermine reputations and cause distress.

AI is a powerful and useful tool that should inform judgement, not replace it.

As AI-driven features become more common, both individuals and organisations should adopt a discerning approach to outputs, recognising that speed and fluency do not equate to accuracy, particularly where personal data is involved.

The outcome

In response to this complaint the Authority engaged with both the platform in question and supported the complainant in contacting a Data Protection Authority counterpart with relevant jurisdiction. The information was rectified thereafter.

Case study #2:

Sharing of safeguarding information

A concern was recently raised with the Authority involving the sharing of safeguarding information between several agencies responsible for supporting individuals at risk.

The person who contacted the Authority questioned whether some of the disclosures made were lawful and expressed disagreement with the assessment that a safeguarding risk existed. The Authority initiated enquiries with the organisation to understand the basis on which the information had been shared and whether the disclosures complied with the requirements of the Law.

Following these enquiries, it was established that the organisation had assessed the disclosure of specific information as necessary considering the safeguarding risk posed to the parties involved. Once such an assessment is made, the Law provides several conditions that permit organisations to share safeguarding information lawfully. These provisions recognise that, in safeguarding situations, timely information sharing is essential to ensure that risk is properly managed and imminent harm avoided.

The Authority recognises that individuals may disagree with the risk assessment leading to the disclosure. However, the existence of that disagreement does not in itself prevent the lawful sharing of information where the conditions under the Law are met. Safeguarding decisions often involve complex judgments, and the Law is designed to ensure that necessary information can be shared to protect those at risk.

The outcome

The Authority recognises that individuals may disagree with the risk assessment leading to the disclosure. However, the existence of that disagreement does not in itself prevent the lawful sharing of information where the conditions under the Law are met. Safeguarding decisions often involve complex judgments and the Law is designed to ensure that necessary information can be shared to protect those at risk.

Case study #3:

Inaccurate medical information

A self-reported breach was submitted to the Authority involving a medical setting where a patient was provided with care based on another patient's test results. The incident came to light when the patient attended an appointment and ascertained that the diagnosis and treatment plan they had received were derived from another individual's results. Although it was later confirmed that the error had not caused physical harm, the breach had the potential to do so.

Enquiries made by the Authority confirmed that the error arose from inaccurate handling of medical data during the diagnostic process. The results were attributed to the wrong patient in the organisation's system, leading clinicians to rely on information that did not apply to the individual concerned.

The organisation acknowledged that additional verification steps should have been taken and proactively identified practical steps to reduce the chance of future recurrence. Given the cooperation and proactive commitment to improvements by the organisation, no further formal action was required by the Authority.

This case underscores the heightened responsibility placed on organisations when processing medical information. Accuracy is not simply a matter of administrative correctness; it is fundamental to safe and effective care. The potential consequences of errors are amplified in clinical environments where decisions directly influence treatment and patient outcomes.

The outcome

The Authority emphasised that lessons must be drawn from incidents of this nature. Robust checks, clear procedures and a culture of careful data handling are essential safeguards. Even where harm does not materialise, the risk created highlights why the accuracy of personal data processing remains a core obligation under the Law.

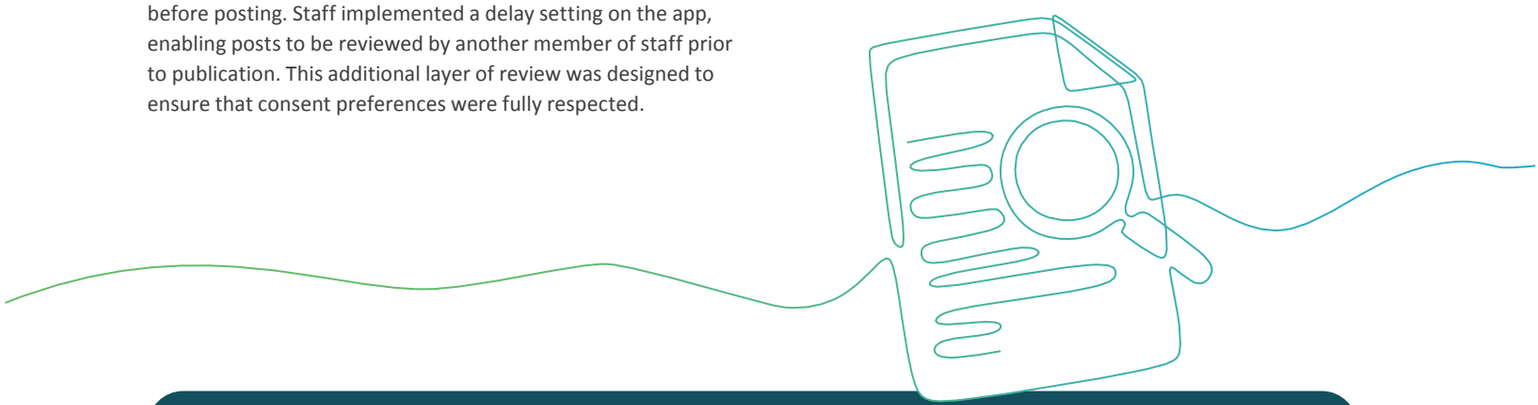
Case study #4:

Consent for school photography

A concern was raised with the Authority regarding a school's routine use of a classroom communication app to share updates with parents. Despite the parents not consenting for photographs of their child to be shared, the child appeared in several images posted to the platform. The parents were particularly worried that these photos could be further shared on other social media sites beyond the school's control.

Following contact from the Authority, the school undertook a detailed review of its practices and implemented a series of measures to prevent recurrence. These included ensuring that a child's image could be more easily cropped or discarded before posting. Staff implemented a delay setting on the app, enabling posts to be reviewed by another member of staff prior to publication. This additional layer of review was designed to ensure that consent preferences were fully respected.

The school also committed to providing bespoke data protection training for staff, distributing additional guidance on good practice and adjusting classroom routines so that children could be photographed individually to avoid appearing in the background of wider shots.



The outcome

Given the cooperation and commitment to improvements by the school, no further formal action was required by the Authority. The Authority was encouraged by the breadth of the remedial measures identified. This case highlights the importance of seeking, recording and honouring consent accurately, particularly when processing children's personal data.

Domestic and international partnerships

Achieving superior results for the Bailiwick by working together

In 2025, the Authority further advanced its domestic and international partnerships to expand its capacity to take action and amplify the impacts of those actions.

Domestic partnerships

Partnership begins at home, and 2025 saw us broaden our presence across the Bailiwick as we visited both Alderney and Sark, holding stakeholder drop-in sessions to offer advice to the regulated community and delivering workshops in local schools bringing data protection and online safety directly to children, teachers and parents. In Sark, we also worked closely with the government to advance their data governance frameworks, supporting the island as it develops the regulatory foundations appropriate to its own unique needs.

Following on from its launch in 2024, the Guidance Advisory Panel met twice in 2025. Comprising representatives from the public, private and third sectors, the panel reviewed several pieces of guidance, providing valuable feedback enabling our guidance to meet the needs of the regulated community.

Our children's education programme represents a dynamic partnership with Guernsey's schools. This year saw an expansion and modernisation of our school programme, ensuring our children can benefit from everything that the digital era has to offer while being equipped with the necessary tools and knowledge to avoid online risks and harms.

An innovative addition to our strategy to promote and protect children's rights has been the launch of Parents' Workshops. By partnering with Bailiwick schools, the objective of the workshops is to arm those "front-line" parents and care-givers with practical, actionable guidance and tips in areas ranging from the most popular games and platforms with kids today, to how to have conversations with your children about online safety.

Our domestic partnerships also included private sector alliances. Through the Authority's participation in the Digital Greenhouse's Meet the Experts programme, we were able to offer guidance to local startups at precisely the point in their journeys when enduring data protection habits are most easily established.

Finally, together with the Channel Islands Financial Ombudsman ("CIFO") and the Guernsey Competition and Regulatory Authority ("GCRA"), we launched the Guernsey Consumer Cooperation Forum (the "GCCF"). Consumer issues adversely impacting individuals often span the remits of more than one regulator and in recognition of this the GCCF will work together on matters of shared priority to benefit local citizens. This will include joint outreach events and the sharing of compliance approaches amongst the authorities.

"This year saw an expansion and modernisation of our school programme, ensuring our children can benefit from everything that the digital era has to offer while being equipped with the necessary tools and knowledge to avoid online risks and harms."

International partnerships

Whether it is protecting children, promoting data protection in cross-border financial sectors or embracing the power of AI while mitigating its risks, many global data protection issues have a profound domestic relevance and impact. And there is no more efficient way to tackle those issues than through international cooperation.

Throughout the year, the ODPA advanced its leadership role on the international stage.

> **“Consequently, we have contributed to global policy discussions and forged collaborative alliances that have enhanced our ability to respond to emerging data protection challenges.”**

The Global Privacy Assembly (“the GPA”) represents the most important data protection network in the world and within the GPA the ODPA is the secretariat and a co-chair of the International Enforcement Cooperation Working Group (IEWG). As part of our IEWG activities we led a capacity-building session at the GPA’s annual meeting. Attended by over 80 members, the session revealed the practical realities of high-profile enforcement activity and coordination, exploring leading cases including Canada and the UK’s joint investigation of 23andMe and the Irish authorities’ investigations of TikTok and Instagram.

In 2025, the ODPA also stepped into the role of a co-coordinator of the Global Privacy Enforcement Network’s Global Privacy Sweep, focusing this Sweep on children's privacy. As a co-coordinator, the ODPA helped design the Sweep's methodology, managed the coordination across participating jurisdictions and ensured the integrity of the findings. With 27 participating authorities and 876 services examined in total, the Sweep assessed the data protection practices of websites and apps that were either popular with, or targeted at, children. The full findings of the Sweep were published early in 2026.

In June, we hosted the British, Irish & Islands Data Protection Authorities (BIIDPA), welcoming some of our closest international counterparts for an annual working session on shared regulatory challenges and priorities. The agenda covered enforcement cooperation, protecting children’s data rights, legislative developments across the Crown Dependencies and British Overseas Territories, data protection in financial services, artificial intelligence and areas where a more joined-up regional approach delivers genuine value.

Finally, in December we launched a joint investigation alongside the Data Protection authorities of Jersey, the Isle of Man and the UK into the cyber incident that compromised data of the trade union Prospect Custodian Trustees Ltd (Prospect) in June 2025. Prospect has more than 160,000 members and approximately 3,000 Bailiwick residents have been affected by the personal data breach. The investigation marks the first joint action between the jurisdictions’ authorities and reflects the regulators’ commitment to collaborate on protecting people’s data rights across all four jurisdictions. By pooling resources and expertise, the investigation is structured to deliver a focused, efficient and expedient inquiry.

Governance, operations and administration

Disciplined financial stewardship for a sustainable future

Throughout 2025, we strengthened our approach to financial management and delivered a disciplined, transparent and accountable operation. Despite operating within a zero-to-zero annual budget, we concluded the year with a series of notable achievements while also laying the groundwork for greater long-term financial resilience.

One of the year's most significant governance successes was exceeding our income target by 0.5%. This reflects the stability of our fee-paying community and the effectiveness of our internal income management processes. We also issued administrative fine sanctions totalling £165,000. £140,000 of that sum was paid by year-end (£65,000 from Jacksons and £75,000 from the Medical Specialist Group (MSG). A further £25,000 would be payable if MSG fails to complete specified remedial measures under an action plan and transferred to the States of Guernsey, in line with our statutory obligations and commitment to financial transparency.

Our progress in reducing the outstanding start-up loan from the States of Guernsey represented another key achievement. A £100,000 contribution brought the remaining balance to £698,850 by year end, demonstrating responsible and disciplined fiscal stewardship of public funds. Alongside this, we effectively managed our budget, supported by increasingly robust forecasting tools and practices.

Operational expenditure, including staff costs, travel, and legal services, was controlled carefully. Notwithstanding the significant costs of a court appeal, we remained firmly within budget.

We extend our appreciation to our business partners for their collaboration and support throughout the year, and we acknowledge the fee-paying community whose contributions make our work possible. Their continued engagement and trust are critical to the broader regulatory ecosystem.

Looking ahead, we also recognise several ongoing challenges. Our zero-to-zero budget continues to limit flexibility, particularly in responding to unforeseen demands or investing in new capabilities. As the organisation evolves, it is prudent to consider establishing a modest capital reserve to strengthen our resilience against unforeseen costs and enable more strategic, long-term planning.

The fee model also continues to present constraints. The obligation to restrict annual fee increases to no more than RPIX is an important safeguard for fee payers, but it places pressure on our cost base and can result in fractional fee adjustments that can appear unusual. It remains vital to remind the business community of the core principles and shared responsibilities of the Levy Collection Agent fee model whereby one organisation collects fees on behalf of other regulated entities.

The year ahead will also bring important strategic projects. In 2026, we will enhance our SharePoint environment, improve our regulatory systems built on Microsoft Dynamics, and begin formal adoption of AI tools within our workplace to improve efficiency, capability, and regulatory outcomes. These initiatives represent not only operational enhancements but a wider commitment to innovation — both within the Authority and across the community we serve. We aim to demonstrate how thoughtfully applied innovation can strengthen governance, improve service delivery, and support a more efficient and future ready regulatory framework.

Together, these achievements and forward-looking priorities highlight a year of careful financial stewardship and a clear focus on building a stronger, more capable organisation.

Environmental, Social and Governance (ESG) in action

We believe responsible regulation extends beyond our statutory duties. In 2025, we strengthened our commitment to operating as an environmentally sustainable, socially responsible and well-governed organisation by moving ESG from intention into action.

We embedded clearer governance frameworks to enhance accountability and transparency, invested in staff wellbeing and community partnerships to build a resilient and engaged team. We improved how we measure and manage our environmental impact, particularly in relation to travel. By taking a structured, proportionate and data-led approach, we are ensuring that ESG principles are not peripheral initiatives but integrated into how the Authority operates and makes decisions.

Through continuous improvement and practical delivery, we are building an organisation that reflects the standards of responsibility, integrity and trust that we promote across the Bailiwick.

In 2025, ESG activity focused on embedding good governance, strengthening staff wellbeing and community engagement, and improving how we measure and reduce our environmental impact.

Environmental

- The methodology for calculating carbon emissions was improved in 2025 to provide a more accurate picture of travel impact
- Domestic (UK) and international engagements were the main driver of emissions in the first half of the year
- Emissions lessened in the second half of 2025 as travel patterns changed, including reduced travel by air and using lower emission modes (boat, rail, car) where available

Social

- Lunch & Learn sessions covered mental health awareness, menopause and the responsible use of AI
- Carbon literacy training and climate awareness workshops were delivered
- Staff participated in local fundraising (Skipton Sleepout for the Homeless, Saffery Walk) and volunteering initiatives (field clearing at GROW Guernsey, beach cleanups), supported by a formal volunteering day entitlement

Investing in Guernsey talent

A significant part of our ethos represents investing and giving back to the community that we serve. Towards that aim, the ODPA introduced a Guernsey student internship, to provide an island-based employment opportunity for our talented youth.

Governance

Policies and procedures identified in the ESG gap analysis continued to be reviewed, updated and approved throughout the year.

ESG governance moved from planning into active delivery, with clearer oversight through senior management and the Audit & Risk Committee.

Looking ahead

In 2026, the focus will be on completing governance documentation, further reducing travel emissions, and continuing to support staff wellbeing and community engagement in a sustainable and proportionate way.

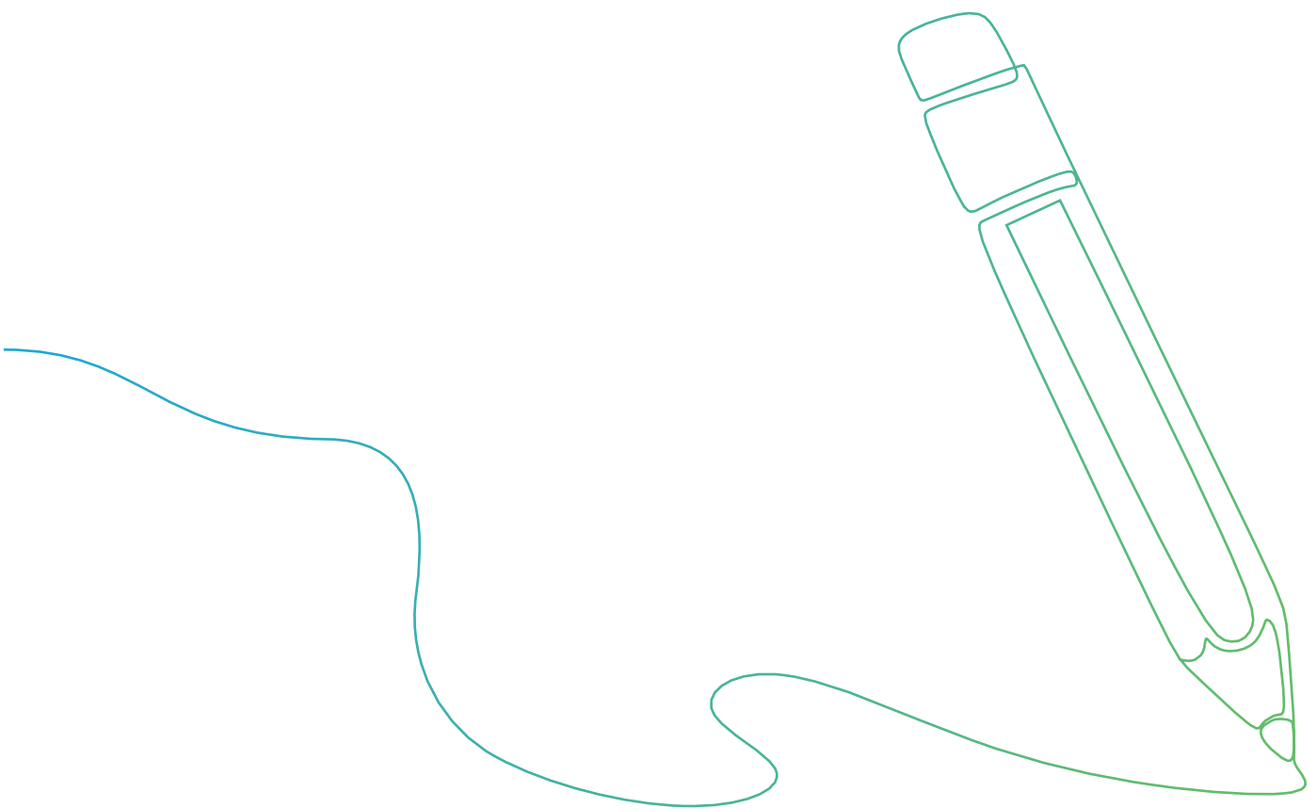
Business Intelligence

Leveraging environmental scanning and analyses to better serve the Bailiwick

During the year, the Authority has developed a dedicated Business Intelligence function to enhance its ability to deliver effective, independent and accountable regulation for the Bailiwick and its citizens. By bringing information together more consistently, Business Intelligence supports an elevated understanding of trends, pressures and outcomes. This helps ensure that decisions are informed by evidence and aligned with the strategic aim of protecting people and promoting the responsible use of personal information.

As this work develops, the ODPA is progressing towards the creation of a Business Intelligence dashboard that will provide a clearer, more accessible view of the Authority's activities across education, engagement and enforcement. Embracing a Business Intelligence philosophy will help ensure that limited public resources are directed to areas of greatest risk and public impact, supporting transparency, value for money and continuous improvement in a rapidly changing digital environment.

Financial Statements



The Data Protection Authority

Members' Report and Audited Financial Statements

Year Ended 31 December 2025

The Data Protection Authority

Authority Information

Members	Richard Thomas CBE (Chairman) John Curran Christopher Docksey Simon Entwisle Mark Lempriere Nicola Wood MBE Jane Wonnacott Brent Homan (Non-voting member)
Registered office	Block A Lefebvre Court Lefebvre Street St Peter Port Guernsey GY1 2JP
Independent Auditor	Grant Thornton Limited St James Place St James Street St Peter Port Guernsey GY1 2NZ

The Data Protection Authority

Contents

The Data Protection Authority

Members' Report
For the Year Ended 31 December 2025

The members present their report and the audited financial statements for The Data Protection Authority ("the Authority") for the year ended 31 December 2025.

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 including Financial Reporting Standard 102 'The Financial Reporting Standard applicable in the UK and Republic of Ireland', Section 1A 'Small Entities' (FRS 102 Section 1A).

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

Principal activity

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

Results

The deficit (2024 : surplus) for the year is set out in detail on page 6.

Members

The members who served during the year were:

Richard Thomas CBE
John Curran
Christopher Docksey - term ended 1 February 2026
Simon Entwisle
Mark Lempriere
Nicola Wood MBE
Jane Wonnacott - term ended 1 February 2026
Brent Homan (Non-voting member)

On 28 January 2026 the States of Deliberation appointed Steve Wood and Sarah Willis as voting members. The term commencement date was 1 January 2026.

Disclosure of information to independent auditor

Each of the persons who are members at the time when the 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 independent 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 independent auditor is aware of that information

Members' Report (continued)
For the Year Ended 31 December 2025

Independent auditor

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

Going concern

The members confirm their assumption that the ODPA is a going concern, and that no material uncertainty exists in this report. The assumption is based on the relationship which the ODPA has with the States of Guernsey which is established in law.

This report was approved by the members on 30 April 2026 and signed on its behalf by:

....

Richard Thomas CBE (Chairman) John Curran

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 2025 which comprise the Income and Expenditure Account, the Balance Sheet, the Statement of Changes in Reserves and notes to the financial statements, including a summary of significant accounting policies.

In our opinion, the accompanying financial statements:

- give a true and fair view of the financial position of the Authority as at 31 December 2025, and of its financial performance for the year then ended;
- are in accordance with United Kingdom Generally Accepted Accounting Practice including Financial Reporting Standard 102 'The Financial Reporting Standard applicable in the UK and Republic of Ireland', Section 1A 'Small Entities' (FRS 102 Section 1A).

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 Member’s Report but does not include the financial statements and our auditor’s report thereon.

Our opinion on the financial statements does not cover the other information and 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, 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

The members are responsible for the preparation of the financial statements which give a true and fair view in accordance with FRS 102 Section 1A, are prepared in accordance with The Data Protection (Bailiwick of Guernsey) Law, 2017 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.

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

Grant Thornton Limited
Chartered Accountants
St Peter Port, Guernsey

Date: 30 April 2026

Income and Expenditure Account
For the Year Ended 31 December 2025

	Note	2025 £	As restated 2024 £
Income		**1,975,970**	1,762,303
Administrative expenses		**(1,857,426)**	(1,838,170)
Operating surplus/(deficit)		**118,544**	(75,867)
Interest income		**9,091**	-
Effective interest		**(39,051)**	(57,363)
Operating surplus/(deficit) before loan amortisation		**88,584**	(133,230)
Loan amortisation		**(122,583)**	203,958
Total comprehensive (loss)/income for the financial year		**(33,999)**	70,728

The results above derive from continuing activities.

The notes on pages 9 to 15 form part of these financial statements.

There are no other comprehensive income or loss for the year ended 31 December 2025 (2024 : nil).

The Data Protection Authority

Balance Sheet
As at 31 December 2025

	Note		2025 £		2024 £
Fixed assets					
Intangible assets	5		**23,110**		7,058
Tangible fixed assets	6		**107,486**		114,033
			130,596		121,091
Current assets					
Prepayments and sundry debtors		**97,712**		58,685	
Cash at bank		**22,548**		287,231	
		120,260		345,916	
Creditors: amounts falling due within one year	7	**(170,796)**		(397,266)	
Net current liabilities			**(50,536)**		(51,350)
Total assets less current liabilities			**80,060**		69,741
Creditors: amounts falling due after more than one year	8		**(483,178)**		(438,860)
Net liabilities			**(403,118)**		(369,119)
Reserves					
Deficit			**(403,118)**		(369,119)
Total reserves			**(403,118)**		(369,119)

The notes on pages 9 to 15 form part of these financial statements.

The financial statements on pages 6 - 15 were approved and authorised for issue by the members and were signed on the members' behalf by:

.....
Richard Thomas CBE (Chairman)
Date: 30 April 2026

.....
John Curran
Date: 30 April 2026

Statement of Changes in Reserves
For the Year Ended 31 December 2025

	Notional loan amortisation reserve	Income and expenditure account	Total reserves
	£	£	£
At 1 January 2024	**346,086**	**(785,933)**	**(439,847)**
Deficit for the financial year	**-**	**(133,230)**	**(133,230)**
Loan amortisation	**203,958**	**-**	**203,958**
At 1 January 2025	**550,044**	**(919,163)**	**(369,119)**
Surplus for the financial year	**-**	**88,584**	**88,584**
Loan amortisation	**(122,583)**	**-**	**(122,583)**
At 31 December 2025	**427,461**	**(830,579)**	**(403,118)**

The notes on pages 9 to 15 form part of these financial statements.

The Data Protection Authority

Notes to the Financial Statements
For the Year Ended 31 December 2025

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 ("FRS 102"), the Financial Reporting Standard applicable in the UK and Republic of Ireland.

The functional and 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 financial statements have been prepared on a going concern basis.

The following principal accounting policies have been applied consistently during the year:

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 on an accrual basis.

Deferred income represents amounts received for registration fees in respect of future periods.

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.

Notes to the Financial Statements
For the Year Ended 31 December 2025

1. Accounting policies (continued)

1.4 Tangible fixed assets (continued)

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

The estimated useful lives range as follows:

Leasehold improvements	- Over the remaining period of the lease
Furniture and fittings	- 20% straight line
Office equipment	- 20% straight line

The assets' residual values, useful lives and depreciation methods are reviewed, and adjusted prospectively if appropriate, or if there is an indication of a significant change since the last reporting date.

Gains and losses on disposals are determined by comparing the proceeds with the carrying amount and are recognised in profit or loss.

1.5 Debtors

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

1.6 Financial instruments

The Authority only enters into basic financial instruments transactions that result in the recognition of financial assets and liabilities like trade and sundry debtors and creditors and loans from 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 Income and Expenditure Account.

The Data Protection Authority

Notes to the Financial Statements
For the Year Ended 31 December 2025

1. Accounting policies (continued)

1.7 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.

1.8 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.

1.10 Effective interest on financial instruments

Where a financial instrument represents a financing transaction and is received at below market rate or interest free, it is initially recognised at the present value of the future cash flows, discounted using a market rate of interest for a similar instrument.

Following initial recognition, the financial assets and financial liabilities are subsequently measured at amortised cost using the effective interest method. Interest income or expense is recognised in income and expenditure account over the term of the instrument using the effective interest rate. The amount recognised represents a notional interest charge or credit and reflects the unwinding of any discount or premium applied on initial recognition. Loan amortisation reflects changes between actual and revised estimated cash flows, with the resulting impact on the present value of the loan recognised in the income and expenditure account using the original effective interest rate.

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 judgments, 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 (notes 8,9) 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 £39,051 for year ended 31 December 2025 (2024: £57,363).

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.

Notes to the Financial Statements
For the Year Ended 31 December 2025

3. Employees

The average monthly number of employees, including directors, during the year was 14 (2024: 12).

The Authority makes pension contributions to its employees independent pension plans. The Authority pays fixed contributions into a separate entity and has no further payment obligations.

4. Taxation

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

5. Intangible assets

	Website development £
Cost	
At 1 January 2025	**188,371**
Additions	**26,349**
At 31 December 2025	**214,720**
Amortisation	
At 1 January 2025	**181,313**
Charge for the year	**10,297**
At 31 December 2025	**191,610**
Net book value	
At 31 December 2025	**23,110**
At 31 December 2024	7,058

The Data Protection Authority

Notes to the Financial Statements
For the Year Ended 31 December 2025

6. Tangible fixed assets

	Leasehold improvements £	Furniture and fittings £	Office equipment £	Total £
Cost				
At 1 January 2025	**102,143**	**9,763**	**75,806**	**187,712**
Additions	**-**	**-**	**10,895**	**10,895**
At 31 December 2025	**102,143**	**9,763**	**86,701**	**198,607**
Depreciation				
At 1 January 2025	**4,942**	**1,652**	**67,086**	**73,680**
Charge for the year	**10,231**	**1,701**	**5,509**	**17,441**
At 31 December 2025	**15,173**	**3,353**	**72,595**	**91,121**
Net book value				
At 31 December 2025	**86,970**	**6,410**	**14,106**	**107,486**
At 31 December 2024	97,202	8,111	8,720	114,033

7. Creditors: amounts falling due within one year

	2025 £	2024 £
Trade creditors	**21,986**	24,007
Deferred rent	**61,951**	49,111
Sundry creditors and accruals	**25,179**	29,784
Deferred income	**-**	250,000
Amounts payable to the States of Guernsey (note 9)	**61,680**	44,364
	170,796	397,266

Notes to the Financial Statements
For the Year Ended 31 December 2025

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

	2025 £	2024 £
Amount payable to the States of Guernsey (note 9)	**483,178**	438,860

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. Under the terms of the loan, annual loan repayments equal the annual surplus of The Data Protection Authority with £100,000 due on 30 June in the year and any balance due by 31 March in the following year.

The loan agreement states that the loan is to be repaid in full by no later than 31 March 2027, which may be extended by mutual agreement between the Parties. The current expectation of the members, based on cash flow forecasts is that the loan repayment date will need to be extended to 2032.

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

	2025 £	2024 £
Amounts falling due within one year	**61,680**	44,364
Amounts falling due between 1 and 2 years	**66,461**	48,240
Amounts falling due between 2 and 5 years	**231,901**	171,378
Amounts falling due after more than 5 years	**184,816**	219,242
	544,858	483,224

The Data Protection Authority

Notes to the Financial Statements
For the Year Ended 31 December 2025

10. Commitments under operating leases

At 31 December 2025 the Authority had future minimum lease payments due under non-cancellable operating leases for each of the following periods:

	2025 £	2024 £
Not later than 1 year	**81,100**	81,100
Later than 1 year and not later than 5 years	**324,400**	324,400
Later than 5 years	**250,058**	331,158
	655,558	736,658

11. Controlling party

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

12. Other comprehensive income - prior period adjustment

Amounts payable to the States of Guernsey were initially recognised at the present value of expected future repayments, discounted using a market rate of interest. The resulting discount on initial recognition, together with subsequent movements arising from the unwinding of the discount and revisions to estimated cash flows, was recognised within Other Comprehensive Income (OCI).

On reassessment of the presentation requirements under Section 11 of FRS 102, it was concluded that movements arising on the loan are more appropriately presented through the Income and Expenditure Account rather than Other Comprehensive Income. The comparative information has therefore been restated to reflect this presentation. As a result, the unwinding of the discount amounting to £203,958 as at 31 December 2024, previously presented within the Statement of Other Comprehensive Income, has been restated within the loan amortisation line item included in the Income and Expenditure Account.

This restatement relates solely to the presentation of amounts previously recognised and does not affect the measurement of the loan, the related loan amortisation, nor total reserves. As a result of the restatement, the Statement of Other comprehensive Income has been removed.

13. Post balance sheet events

Following the financial year-end, two new members were appointed to the Authority to replace two retiring members. These changes do not affect the financial position of the Authority at the reporting date.

There have been no other significant events affecting the Authority since the financial year-end which would require adjustment to or disclosure in these financial statements.

Detailed Statement of Income and expenditure account (unaudited)
For the Year Ended 31 December 2025

	2025 £	2024 £
Income	**1,975,970**	1,762,303
Administrative expenses	**(1,857,426)**	(1,838,170)
Interest income	**9,091**	-
Effective interest	**(39,051)**	(57,363)
Loan amortisation	**(122,583)**	203,958
Total comprehensive (loss)/income for the financial year	**(33,999)**	70,728
Income		
Annual notification fees	**1,975,970**	1,762,303
Administrative expenses		
Salaries and other staff costs	**1,104,862**	982,725
Recruitment and relocation fees	**11,930**	17,646
Members fees	**63,706**	54,950
Project costs	**10,713**	20,405
Rent, rates and premises expenses	**114,744**	150,580
Office move expenses	**-**	75,340
Legal and professional	**279,308**	245,148
Communication costs	**33,591**	17,229
Travel	**50,375**	47,488
IT costs	**114,008**	119,259
Office and sundry expenses	**29,742**	27,659
Insurances	**16,709**	15,816
Amortisation	**10,297**	45,755
Depreciation	**17,441**	15,270
Loss on disposal of tangible assets	**-**	2,900
	1,857,426	1,838,170
Interest income		
Bank interest income	**9,091**	-

Key terms and definitions

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 everyone, not just for lawyers.

Legal terms	Plain English
'Assertive Agile Enforcement (AAE)'	A practical, outcome-focused approach that prioritises early resolution, constructive engagement and proportionate use of formal powers.
'Complainant'	An **individual** who lodged a complaint with the ODPA about how their personal data was being (or had been) used.
'Complaint'	Individuals can lodge **a complaint** under section 67 of the Law if they believe their personal data has not been handled in a way that complies with the Law.
'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 **individual** that the data in question relates to.
'Data subject access request'	This is when an individual **uses their legal right** to ask a controller what data is held about them and to seek access to that data.
'Informal resolutions'	Such resolutions typically involve organisations providing previously withheld personal data, rectifying inaccuracies or the ODPA issuing letters of concern or advisory feedback.
'Inquiry'	These are conducted under section 69 of the Law where the ODPA believes there **is a need to determine the compliance of processing.** Inquiries do not require a complaint to have been made to initiate.
'Investigation'	These are conducted under section **68 following the assessment of an individual's complaint** submitted under section 67 of the Law.
'Law'	The Data Protection (Bailiwick of Guernsey) Law, 2017.

Legal terms	Plain English
'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.
'Levy Collection Agent (LCA)'	These are organisations registered with and/or regulated by the Guernsey Financial Services Commission (GFSC) who are authorised to declare, and pay the levies for, other controllers or processors.
'Personal data'	Any information about or related to an identified (or identifiable) **living human being.** Personal data (or personal information) can include factual information about people as well as opinions expressed about people. It can also include anonymised data that could identify people if it was combined with other information.
'Personal data breach'	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. There will likely be a breach whenever **any personal data** is accidentally lost, corrupted or disclosed or if someone accesses it or passes it on without proper authorisation to do so.
Processor	Any entity that is given the task of processing personal data by a controller. Processors do not determine the nature or the means of the processing, they just do what the controller tells them to do.
'Self-reported breach'	This is the act of **completing the ODPA's breach report form** in order to fulfil a controllers legal obligation to let the ODPA know that they have experienced a personal data breach.
'The Data Protection Authority'	The body created by the Law as the data protection regulator for the Bailiwick of Guernsey. It comprises seven voting members and the Commissioner as an ex officio, non voting member. Also known as 'the Authority', all of its functions, except for three reserved functions, have been delegated to the Commissioner and staff.

Your Rights

1.
Right to information for personal data collected from subject
(section 12 and 13)

2.
Right of access
(section 15)

3.
Right to object to processing for direct marketing purposes
(section 17)

4.
Right to object to processing on grounds of public interest
(section 18)

5.
Right to object to processing for historical or scientific purposes
(section 19)

6.
Right to rectification
(section 20)

7.
Right to erasure
(section 21)

8.
Right to restriction of processing
(section 22)

9.
Right not to be subject to decisions based on automated processing
(section 24)

10.
Right to data portability
(section 14)

For more information on your rights, visit: **www.odpa.gg/individuals/individuals-rights**

THE OFFICE OF THE
Data Protection Authority
BAILIWICK OF GUERNSEY

+44 (0) 1481 742074 | enquiries@odpa.gg | odpa.gg