JOIC
JERSEY OFFICE OF THE
INFORMATION COMMISSIONER

2025

JERSEY OFFICE OF THE INFORMATION COMMISSIONER

ANNUAL REPORT

Fulfilling the obligations of the Authority under Article 44 of the Data Protection Authority (Jersey) Law 2018 and the Information Commissioner under Article 43 of the Freedom of Information (Jersey) Law 2011.

JOIC
JERSEY OFFICE OF THE
INFORMATION COMMISSIONER

Contents

04 - 05	2025 AT A GLANCE
06 - 07	THE JERSEY DATA PROTECTION AUTHORITY
08 - 09	CHAIR REPORT
10 - 13	INFORMATION COMMISSIONER'S FOREWORD
14 - 20	GOVERNANCE, ACCOUNTABILITY AND TRANSPARENCY
21 - 23	PRINCIPAL RISKS
24 - 27	PERFORMANCE REPORT
28 - 40	ENFORCEMENT AND COMPLIANCE
41 - 47	MAKING PRIVACY INSTINCTIVE
48	ENVIRONMENTAL, SOCIAL AND GOVERNANCE
49 - 52	PEOPLE AND ORGANISATIONAL DEVELOPMENT
53 - 56	FINANCE REPORT
57 - 61	APPENDIX 1

2025 at a glance

Data Protection Registrations increased by

46%

From 2020 to 2025

Responded to

209

Self-Reported Data Breaches

Of the complaints **OPENED** in 2025

50% Were about requests for access to personal information

73% Of complaints investigated closed with a breach determination

Most common breach types were:

UNAUTHORISED ACCESS	**25%** of reported breaches
UNAUTHORISED DISCLOSURE	**70%** of reported breaches

80% Membership Increase for Let's Go DPO Network

LET'S GO DPO

2025 Young Privacy Ambassador Programme

1882 young people engaged with

99% Of individuals representing a controller/processor said k**nowledge of data protection** obligations **improved** following participation in a JOIC outreach session

97% Of young people providing feedback said knowledge of JOIC, protecting their personal information & understanding of individual rights improved

Worked with partners across international borders to:

- build greater resilience
- ensure our approach reflects highest standards of global expertise

It's All About You
Self Selecting Survey

Findings showed

34% Increase

in islanders' awareness of the **Data Protection (Jersey) Law 2018** since 2022

The Jersey Data Protection Authority

Our **Role**

The Jersey Data Protection Authority (the Authority) is an independent statutory body established to promote respect for the private lives of individuals through ensuring privacy of their personal data by:

- Implementing and ensuring compliance with the Data Protection (Jersey) Law 2018 (the **DPJL 2018**) and the Data Protection Authority (Jersey) Law 2018 (the **DPAJL 2018**).
- Influencing attitudes and behaviours towards privacy and processing of personal data, both locally and internationally.
- Providing advice and guidance to Island businesses and individuals and making recommendations to the Government of Jersey in response to changes in international data protection laws.

Our **Vision**

Our vision is to create an island culture whereby the protection of personal data and **privacy becomes instinctive**, with individuals and organisations taking a proactive approach to embed such protection throughout their daily activities and business planning. For example, as we would approach caution when crossing the road – to look carefully and consider traffic conditions before crossing. Or putting your seatbelt on before you drive. You do both, not because any law requires you to do so, but rather to keep yourself safe. Yet you most likely do not think about it. It has become instinctive over time.

Our **Purpose**

To provide those who interact with Jersey organisations and the Government of Jersey with the highest standard of personal data protection.

2022 – 2025 **Strategic Outcomes**

1. Achieving and maintaining the highest standard of data protection in Jersey.
2. Maximising technological and economic opportunities to enhance the Island's reputation as a safe place to host personal data and do business.
3. Protecting our future generations by putting children and young people first.

Many of the deliverables completed in 2024 - 2025 have been adopted as day-to-day activities which continue to enhance our mandate and the broader benefits to our community.

Our new strategic focus covers three broad priorities, whilst still serving Jersey and JOIC's purpose to 'provide those who interact with Jersey organisations and Government with the highest standard of personal data protection'. These priorities are considered core areas of concern in terms of privacy and risks to individuals.

The three new Strategic Priorities (2026 - 2028) of the JDPA are interconnected and mutually support one another:

Children's privacy

Helping to foster a safer digital environment to protect children's personal data by setting clear standards for organisations, promoting responsible design of digital services, and taking strong enforcement action where risks to children are identified.

Artificial intelligence

Promoting responsible local use, development and deployment of AI-driven technologies by setting out clear standards in terms of our expectation of compliance with data protection laws and principles, thereby safeguarding individuals' rights, fostering innovation, and establishing a trusted framework for ethical AI use. The JDPA will first focus on the use of AI in the context of Human Resources and Employment.

Cyber security

Helping to strengthen organisations' personal data security and cybersecurity protections through clear guidance to reduce the risk of data breaches, enhance resilience against cyber threats, and ensure the ongoing privacy and safety of individuals' personal data.

It is with great anticipation that we embark on the next phase of our evolution focusing on our three Strategic Priorities throughout 2026 – 2028.

Chair Report

ELIZABETH DENHAM CBE
Chair, Jersey Data Protection Authority

On behalf of the Authority, it is my pleasure to present to the Minister and members of the States Assembly our Annual Report for 2025. This fulfils our statutory obligation under Article 44 of the Data Protection Authority (Jersey) Law 2018.

2025 has been a landmark year for the Jersey Data Protection Authority. Building on the momentum of hosting the Global Privacy Assembly (GPA) Annual Conference in October 2024 - themed The Power of 'I' - we entered this year with renewed clarity of purpose and a strengthened sense of our place on the international data protection stage. The insights and connections forged at that conference, and the global conversations it sparked around individual agency, digital identity, and the rights of citizens in an increasingly complex technological world, have directly shaped our thinking and informed the development of our new three-year strategy, commencing 2026-2028.

That strategy sets out an ambitious but grounded vision for data protection in Jersey, with three clear priorities: children's privacy, artificial intelligence, and cyber security. These are not abstract concerns - they reflect the lived realities of Jersey's citizens, businesses, and public institutions, and mirror the most pressing challenges facing data protection authorities across the globe. The GPA community continues to grapple with each of these themes, and Jersey's voice in those discussions is increasingly valued and respected. Our new strategy ensures we remain not only aligned with global best practice but genuinely contributing to it.

Although Jersey is a small jurisdiction, local and international co-operation is key to its success and retention of adequacy with the EU. We must be independent, but we must also work with the Government and the States of Jersey, public bodies, sister regulators and law enforcement to ensure we are serving the interests of the community.

Our outreach work in 2025 has gone from strength to strength. We have been deliberate in our efforts to meet people where they are — both physically and in terms of their level of data protection knowledge and confidence. For businesses and entrepreneurs, we introduced weekly Data Protection Express Clinics for start-ups, offering accessible, practical guidance at the earliest stages of their business. For small and medium-sized enterprises, we ran both daytime and evening 'Confused to Confident' sessions, designed to demystify data protection obligations and empower business owners to act with confidence. Through our 'Let's Go DPO' sessions, participants received practical guidance and assistance to handle the challenging process of data breaches - giving organisations the expertise and resources needed to manage their responses efficiently and responsibly.

Beyond the meeting room and training suite, we have taken our message directly to the community through pop-up stands at local retail outlets and street walks to raise awareness among business owners. Data protection should not feel like something that happens behind closed doors - and this year we have worked hard to make it visible, relevant, and approachable for everyone.

This year also brought a change in the composition of our Authority. I am delighted to welcome Tom Noel as a new member of the Jersey Data Protection Authority. Tom brings valuable expertise and fresh perspective, and we look forward to benefiting from his contribution in the years ahead. At the same time, we say a warm and heartfelt farewell to Helen Hatton, whose service to the Authority has been characterised by wisdom, integrity, and a deep commitment to the public interest. Helen's counsel and her considerable professional standing have strengthened this Authority. On behalf of all members, I extend our profound gratitude to her.

The members of the Authority have played a key strategic and oversight role, but full credit for the achievements of 2025 go to Commissioner Paul Vane and his committed team. In a regulatory landscape that grows more complex by the day, their work matters.

Data protection is ultimately about trust. The technological opportunities before us - in artificial intelligence, in data-driven innovation, in the digital economy - will only be realised where people trust that their data will be used fairly, transparently, and with respect for their dignity and rights. The JOIC is well placed to ensure that Jersey remains a jurisdiction where that trust is earned and maintained. I look forward with confidence to the year ahead.

Elizabeth Denham *CBE*

> *Data protection is ultimately about trust... ensuring data is used fairly and transparently.*

Information Commissioner's Foreword

PAUL VANE BA(HONS) SOC POL CRIM (OPEN)
Information Commissioner

2025 was a year of purposeful action for my office. We focused on turning strategic intent into practical outcomes. We continued to engage widely with organisations to clarify expectations, promote fair processing, and encourage compliance and accountability, building further on the success of the Global Privacy Assembly conference held in Jersey in October 2024.

We continued to support schools with practical guidance sessions, helping raise awareness of online safety and the importance of privacy with students, and we amplified the importance of data protection with the small business community through our community outreach programme. Significantly, we started development of our 2026 to 2028 strategy, starting with a survey of all registered data controllers to identify general understandings of data protection obligations and areas in need of improvement or additional support.

We also invested in collaboration with industry bodies, public authorities, civil society, and our counterparts in other jurisdictions. The risks we face are global and interconnected, and so must be our responses. By sharing insights and aligning good practice, particularly around the complex arena of online harms, we help create a safer and more trustworthy digital environment for everyone in Jersey.

The last 12 months has marked a decisive moment in the evolution of data protection, both globally and here in Jersey. As technologies advance at pace, the potential for responsible innovation grows. But so too do the risks to individuals' rights and freedoms. Against this backdrop, my office has set a clear strategy focused on three areas where robust data protection has never been more vital: Artificial Intelligence in human resources; Children's privacy, with a particular emphasis on Educational Technologies (EdTech); and Cyber Security, with a specific focus on the quality of Data Protection Impact Assessments (DPIAs) and data breach reporting obligations.

AI in human resources is fast becoming an operational tool. It is no longer just experimental. Automated recruitment tools, performance analytics, and workforce management systems increasingly shape decisions that affect people's livelihoods and can have significant impacts on individual's privacy.

While these tools can enhance efficiency and support fairer outcomes, they can also embed bias, obscure accountability, and erode transparency if deployed without appropriate due diligence. Our strategy emphasises rigorous assessment of AI-driven human resources platforms, clear lines of accountability, and meaningful human oversight at every stage of the employment lifecycle. We are urging organisations to test for bias, document accountability and explainability, and ensure that employees and individuals understand when, how, and why automated tools are used to make or inform decisions about them.

Children's privacy remains a critical challenge facing most Data Protection Authorities. The rapid expansion of EdTech[1], accelerated by changing learning environments, has brought many educational benefits. Yet many platforms collect and take inferences from extensive behavioural data, often in ways that children, parents, and schools may not fully understand. Our strategy prioritises age-appropriate design, strict purpose limitation, and high standards of transparency from all education providers serving children in Jersey. We will continue to promote strong governance by schools and EdTech platform providers alike, including clear contractual controls and the minimisation of data collection to only that which is demonstrably necessary and in the best interests of the child.

Cyber security remains a core element to fostering public trust. Cyber, and in many cases data breaches are becoming more sophisticated and more frequent, and the consequences for individuals can be both immediate and severe. Our strategy underscores the critical role of Data Protection Impact Assessments in identifying and mitigating risk at the design stage, and it reinforces organisations' legal obligations to report personal data breaches promptly and comprehensively. Cyber security and data protection are intrinsically linked and can no longer be viewed as a purely technical function. It must be a board level priority, a legal obligation, and should be central to organisational integrity.

As we look ahead, our focus is clear. To safeguard individuals' rights while enabling innovation that serves people and society.

[1] 'Edtech' - short for educational technology, refers to the integration of technology into educational practices to enhance learning experiences. It encompasses tools and resources such as software, online platforms, and digital content aimed at improving teaching methods and student engagement https://www.unesco.org

These priorities sit within a wider context of increasing evidence of online harms stemming from the misuse of AI and digital platforms. Deepfakes and other synthetic media can be, and as we have seen in Jersey recently, already have been used to deceive, defraud, or harass at scale. Harmful or illegal content spreads rapidly with real world consequences for people. It can significantly impact reputations and wellbeing but can also affect the outcomes of elections and democratic discourse. In an Island the size of Jersey, these harms are amplified significantly. As a regulator, we recognise that these risks are not abstract. They are here, they are evolving, and they demand a proactive, collaborative response grounded in the law and in ethics.

Maintaining Jersey's EU adequacy status remains central to Jersey's economy. Adequacy is not just a 'nice-to-have'. Rather, it is an essential component of the infrastructure required for frictionless data flows with the EU, underpinning our finance industry, digital services, professional sectors, and public administration. It is critical to competitiveness, to investor confidence, and to the jobs and livelihoods that depend upon the exchange of personal data across borders. Preserving adequacy requires more than compliance with the letter of the law. It requires a robust legislative framework, an effective regulatory authority and a demonstrable culture of accountability and high standards across all sectors. Our strategy, which as always is anchored in risk, fairness, and transparency, supports that objective, and we will continue to work with the Government of Jersey, industry bodies and other strategic partners to ensure Jersey remains a trusted, modern data protection jurisdiction.

As we look ahead, our focus is clear. To safeguard individuals' rights while enabling innovation that serves people and society. My office will continue to provide clear guidance, responsive engagement, and proportionate but effective enforcement through an 'Advise, Assess and Act' approach, meeting organisations where they are, helping them improve, and stepping in firmly where harms are foreseeable and avoidable. We will listen to our stakeholders, and to the experts who can help us anticipate the next wave of technological change.

Finally, I want to express my profound thanks to my team at the JOIC. Their professionalism, empathy, and unwavering dedication to upholding the fundamental human right of data protection has made our progress in 2025 possible. They have supported individuals seeking redress, guided organisations through complexity, and upheld the high standards we demand with integrity and care. It is a privilege to work alongside them. Similarly, I must also thank the members of the JDPA, who have provided strong leadership, guidance and direction since the new Authority was established in 2024. Together, with our partners and the community we serve, we will continue to build a data enabled future grounded in trust, fairness, and accountability.

Paul Vane
Information Commissioner

Governance, Accountability and Transparency

The Authority has responsibility to:

Ensure that the JOIC remains accountable to the people of Jersey, in properly fulfilling its mandate and delivering quality services to its stakeholders.

- Ensure that the JOIC provides value for money and complies with appropriate policies and procedures with respect to human resources, financial and asset management, and procurement. This includes formal approval of any single item of expenditure in excess of 10 per cent of the operating budget for the JOIC.

The Authority also provides an advisory function to the JOIC. With a balance of expertise in data protection, governance, and local knowledge of the Jersey Government and industry, the Authority provides strategic guidance to the JOIC with respect to fulfilling its mandate effectively and efficiently.

Delegation of Powers

There are other powers and functions that the Authority may exercise under the DPAJL 2018, most notably:

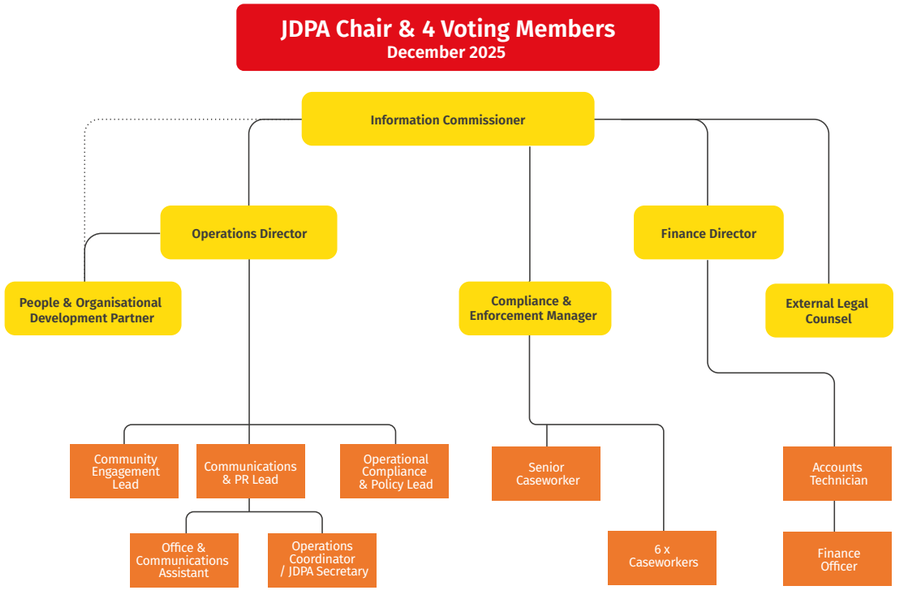
- Enforcing the Law.
- Promoting public awareness of data protection issues.
- Promoting awareness for controllers and processors of their obligations.
- Cooperating with other supervisory authorities.
- Monitoring relevant developments in data protection.
- Encouraging the production of codes.
- Maintaining confidential records of alleged contraventions.

The Authority has delegated all these other powers and functions to the Information Commissioner.

There are certain functions that the DPAJL 2018 stipulates that the Authority must perform itself, and which cannot be delegated to the Information Commissioner. The most important functions are that only the Authority can decide whether to issue administrative fines and/or public statements for contraventions of the law. While the JOIC will make the official finding in each case as to whether a contravention has occurred, it is the Authority that will determine whether a fine will be applicable and the value of that fine.

It is only in cases where because of their gravity or due to some other exceptional circumstances that the Authority will issue a public statement, where it is in the public interest to do so.

Authority Structure



Total current number Employees: 18 (17.8 FTE)

The Authority is currently comprised of a non-executive chair and four non-executive voting members.

The Authority meets at least four times per annum. The Authority operates sub-committees to ensure that relevant matters can be addressed fully, and recommendations are considered at the main Authority meetings.

2025 Authority Members

CHAIR OF THE AUTHORITY

Elizabeth Denham CBE

Elizabeth started her Chair appointment on 28 October 2024.

VOTING AUTHORITY MEMBER

Paul Routier MBE

VOTING AUTHORITY MEMBER

Stephen Bolinger

VOTING AUTHORITY MEMBER

Paul Breitbarth

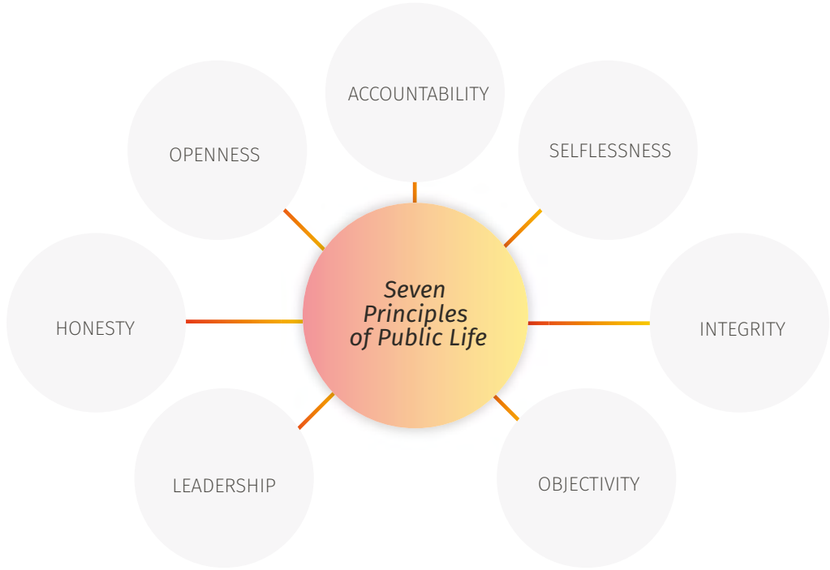
VOTING AUTHORITY MEMBER

Tom Noel

Further details regarding the Authority members' external appointments can be found at **www.jerseyoic.org/team**

Governance Report

The Authority is committed to ensuring a high standard of governance and all members are expected to conduct themselves in accordance with the Seven Principles of Public Life.



Authority Sub-Committees

Audit & Risk Committee (ARC)

The voting members who comprise the ARC are:

Helen Hatton (Chair) handed the role of ARC Chair to Tom Noel as of the 29 October 2025.

Paul Breitbarth.

Christine Walwyn (Co-opted accountant, Non-voting) Christine left as Co-opted member 15 November 2025.

ARC's terms of reference include its responsibility and accountability for

- Financial reporting including accounting policies, monitoring financial statements, reviewing and recommending annual audited financial statements to the Authority.
- Internal control & risk management including effectiveness of internal controls, the Authority's risk management strategy, framework and risk register.
- External audit with an emphasis on the appointment of external auditors, reviewing the audit scope, plan and audit findings to ensure follow up recommendations.
- Compliance and legal, to monitor compliance with legal and regulatory requirements.
- Whistleblowing and fraud, to review the adequacy of arrangements for employees and external parties. Plus, monitor reports of misconduct or fraud.
- ARC shall meet at least four times per annum and have at least 2 voting members with appropriate relevant financial experience to be appointed by the Authority.

The Remuneration & Human Resources Committee (R&HR) and Governance Committee were combined in July 2025.

The voting members who comprise the Governance R&HR Committee are:

Paul Routier MBE **(Chair)**

Stephen Bolinger

Elizabeth Denham CBE

The Governance, Remuneration and Human Resources Committee terms of reference include its responsibility and accountability for:

- Governance and Authority effectiveness, including the appointment of Authority members and the Information Commissioner, review governance documents and evaluate the Authority's decision-making and reporting structures.
- Being instrumental in the development of the Authority's remuneration strategy and policy for staff and senior executives, ensuring alignment with public service and industry standards, and transparency.
- Human resources and strategy including policies, procedures, organisational structure, metrics and complying with applicable laws.
- Succession planning and talent management.
- This Committee meets at least twice per annum.

The following table sets out the number of full Authority and Sub-Committee meetings held during 2025, and the number of meetings attended by each voting Authority member.

JDPA MEETINGS	Elizabeth Denham CBE	Helen Hatton	Paul Breitbarth	Paul Routier MBE	Stephen Bolinger	Tom Noel
19 February 2025 - Hybrid	✓	✓	✓	✓	✓	-
21 May 2025 - in person	✓	✓	✓	✓	✓	-
20 August 2025 - Virtual	✓	-	✓	✓	✓	-
12 November 2025 - in person	✓	-	✓	✓	✓	✓

AUDIT & RISK	Elizabeth Denham CBE	Helen Hatton	Paul Breitbarth	Paul Routier MBE	Stephen Bolinger	Tom Noel	Christine Walwyn
13 February 2025 - Hybrid	-	✓	✓	-	-	-	✓
28 March 2025 - Hybrid	-	✓	✓ *Via Video*	-	-	-	✓
30 April 2025 - Hybrid	-	✓	✓	-	-	-	✓
28 July 2025 - Hybrid	-	✓	✓	-	-	-	✓
29 October 2025 - Hybrid	-	-	✓	-	-	✓	-

GOVERNANCE	Elizabeth Denham CBE	Helen Hatton	Paul Breitbarth	Paul Routier MBE	Stephen Bolinger	Tom Noel	Christine Walwyn
17 April 2025 - Hybrid	✓	-	-	-	✓	-	-

The Remuneration and HR committee merged with the Governance committee in July 2025.

GOVERNANCE, REMUNERATION & HR	Elizabeth Denham CBE	Helen Hatton	Paul Breitbarth	Paul Routier MBE	Stephen Bolinger	Tom Noel	Christine Walwyn
29 July 2025 - Virtual	✓	-	-	✓	✓	-	-
5 November 2025 - Virtual	✓	-	-	✓	✓	-	-

2025 Authority Members' Remuneration

The Authority Voting Members received, in aggregate, £66,755 in remuneration in 2025. Further details regarding the Authority Voting Member remuneration can be found at page 55.

JDPA Performance Evaluation and Re-appointments

The Governance and R&HR Committee has established a comprehensive performance evaluation process for the Authority, consisting of the following components:

1. **Annual Peer Review** - Each voting member conducts a peer review, assessing the performance of every other member. The focus is on evaluating performance against the key attributes expected of a board member.
2. **Annual Self-Assessment of Skills and Diversity** - Individual voting members undertake an annual self-assessment, evaluating their competence across a broad spectrum of skills, knowledge, and experience essential for fulfilling the Authority's mandate.
3. **Independent External Review** - An independent external review of overall Authority effectiveness, to be conducted every three years.

JDPA Performance Evaluation

The Authority did not undertake the annual internal effectiveness review or self-assessment in 2025. The Authority concluded that due to the changes in Members it was prudent to wait for the new team to settle into their roles. The diversity and skills of the Authority were taken into account as a key part of the recruitment process undertaken in 2025.

Diversity of the Authority

At the end of 2025, the Authority comprised of four men and one woman, spanning a wide age range and representing four nationalities, including two Jersey based members. Together they bring strong professional diversity across data protection, law, IT, business administration, finance, economics, and education. For a small board/Authority, diversity is robust, with opportunities to improve gender balance as future vacancies occur.

Principal Risks

The delivery of the Authority's mandate and strategic outcomes are subject to a number of risks and uncertainties that could, either individually or in combination, impact the operational performance of our team.

We identify and manage these and other risks through our risk management framework which is based on the Authority's low appetite for risk.

Risks are overseen by the Audit and Risk Committee (ARC), who monitor risk movements and mitigating actions. We continue to monitor political and legislative developments and assess the opportunities and threats to enable us to regulate effectively. Risks are identified and scored against likelihood and consequence parameters to generate a risk matrix that is regularly monitored and used to guide the Authority's strategic thinking and actions. The Chair of the ARC is initiating a wholesale review of our approach to adopt an even more proactive approach to risk management in 2026.

The Authority currently measures risk as per the table to the right.

Low risk	Implement practicable short-medium term control measures.
Medium risk	Attention needed.
High risk	Corrective action needed; action is short term as appropriate.
Very high risk	Immediate corrective action required and continue monitoring.

The following tables detail the risk categories and then identifies the principal risks and mitigating actions.

Type of Risk	Definition
1. Legal and Regulatory	Risks associated with non-compliance in terms of general regulatory requirements, sector specific regulations and legislative frameworks.
2. Operational	Risks which could impact the Authority's ability to deliver its mandate and strategic outcomes. Operational risks arise from day-to-day activities including ineffective policies, poor financial control, failed processes or poor leadership.
3. Governance	Risks which arise from the potential negative consequences arising from poor leadership, weak internal controls, and ineffective decision-making.
4. Strategic	External issues over which we have no control but can affect the effectiveness and delivery of the Authorities strategic outcomes, mandate and its reputation.
5. Political	Political risks are potential, non-market events arising from government actions, instability. Including global risks such as changes in legislation (such as GDPR, wars, recession, etc.)

Risk Score

Summary of Principal Risks

Risk Description	How we manage the risk	Movement of the Risk
Political Uncertainty around Ministerial relations as a result of unpredictable oversight demands.	→ We continually seek to maintain open and fair dialogue. → We always seek clarification and record decisions/ requests. → We strive to work constructively with Sustainable Economic Development GoJ policy leads.	↑
Political The impact of protracted fee model ongoing since late 2020.	→ By maintaining momentum of constructive fee model discussions with GoJ.	↑
Operational Proposed online harms content removal law. A law which aims to make it easier for people in Jersey to get illegal/harmful content removed from global social media, websites and search engines. There is uncertainty as to impact on the Authority in terms of enforcement and advice provision. Combined with the potential reputational impact if not seen as able/willing to enforce.	→ By liaising with other key stakeholders to monitor the landscape. → By responding in full to the consultation, highlighting our concerns. → By maintaining open dialogue with the Government of Jersey and other Stakeholders.	↑
Operational Revenue. Economic uncertainty impacts on the number of entities trading in Jersey and registering with the Authority. Registration income is dependent on turnover and headcount of entities. Therefore, our registered entities may remain the same in number but represents less in revenue. Interpretation of administered entities within the Data Protection (Registration and Charges) (Jersey) Regulations 2018.	By monitoring → The number of entities deregistering and why, as the economy changes, as this impacts on revenue. → The Authority's operational costs and revenues closely. → The number of entities, liaising with relevant Jersey bodies – Statistics Jersey, Jersey Financial Services Commission and Jersey Business to help with data analysis. → And managing Stakeholder relationships to gauge industry movements. Eg Chamber of Commerce & IOD. By formally requesting changes to the Data Protection (Registration and Charges) (Jersey) Regulations 2018 to amend criteria for being classed as administered entity submitted to Government of Jersey for consideration in June 2021. Discussions remain on-going.	↑

Please see Appendix 1 on page 57 for the full summary of Principal Risks.

Performance Report

Our Island's vision[2] is based around ten shared responsibility community, environmental and economic Island Outcomes which drive Jersey's quality of life. We, as a community, must work together to help achieve the population level outcomes.

The Authority's activities contribute to the shared effort to create change at a population level. The Authority's performance accountability measures tell us whether a service or programme is contributing to the bigger picture by making a difference to the people it serves.

[2] https://www.gov.je/SiteCollectionDocuments/Government%20and%20administration/FUTURE%20JERSEY_SPREADS%2012072017.pdf

The Authority monitors three key questions :

How much did we do?	How well did we do it?
Is anybody better off?	

The whole emphasis of the Outcomes Based Accountability methodology is to drive a relentless focus on the last question.

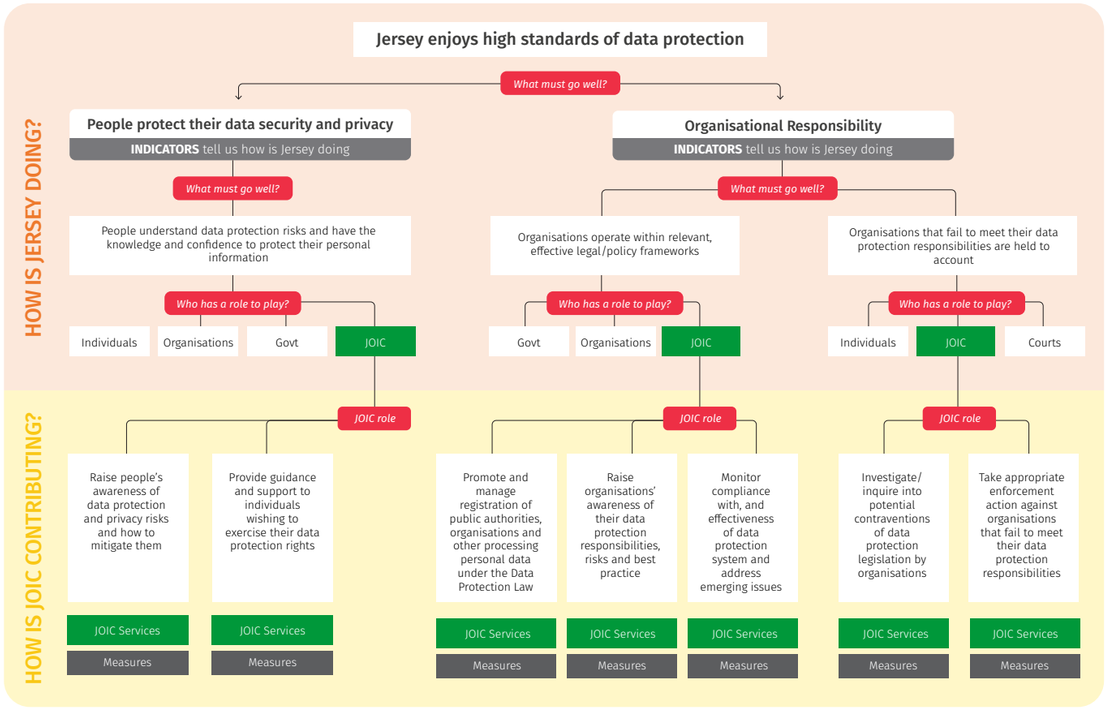
Success is not measured by how busy we are, or in isolation how well we deliver services. The key is whether those services actually make a difference for our customers.

We are not only concerned with the number of cases closed, audits undertaken, or campaigns run; we also strive to shift attitudes and behaviours towards our vision of a culture where '**privacy is instinctive**' and islanders are empowered to assert their rights. Our measurement model seeks to find evidence of progress in these more nuanced areas and determine 'is anyone better off?' as a result of our efforts.

We have chosen 'Outcomes Based Accountability' (OBA) as it supports evidence-based decision making, our role as a regulator and change agent. OBA improves clarity of reporting, strengthens scrutiny and prevents confusion between effort and impact.

This below chart shows the big picture: how all parts of the framework fit together - from the outcome we want to achieve to the shared responsibilities and our regulatory services.

The Framework



The framework shows how our daily work helps protect people, respond to emerging risks, and make a real difference for our community.

- Shows the big picture - connects our daily work to making Jersey safer
- Connects our work - shows how our regulatory services work together under AAA.
- Adapt to emerging risks - enables Strategic Priorities to re-focus effort where it matters most.
- Demonstrate impact - shows how we contribute to higher data protection standards.

The Authority's adoption of an 'Outcomes Based Regulation' approach, means that enforcement is not all about fines; it is a graduated series of responses to engender a change in behaviour which better protects the integrity of both data subjects and data controllers generating compliance and, importantly, trust. Enforcement outcomes are lessons learned to be shared. Our Regulatory Action and Enforcement Policy details, our approach to proportionate enforcement.

Throughout 2025 we have expanded performance measures across more of our services, helping us to measure where we are making a difference and adjusting our resources and approach to ensure that we change the trend and deliver a better impact.

Our vision is to create an Island culture whereby **privacy becomes instinctive** with individuals and organisations taking a proactive approach to privacy and data protection by it being embedded throughout their daily activities and business planning. In striving to achieve this we pride ourselves on making every touch point with a complainant, an enquirer, an organisation reporting a breach or a registration enquiry, an informative and positive experience aimed at fostering a constructive and educational relationship. We also facilitate learning and information exchange, helping us to understand the challenges faced by industry and the frustrations faced by complainants.

That said, we do not shy away from exercising our enforcement powers where warranted, or where the organisation at fault has demonstrated wilful neglect or a repeated pattern of behaviour.

The following sections highlight our enforcement activities, case data, breach data, outreach and engagement activities and most importantly the impacts and effectiveness.

Enforcement by the Authority

As per Part 4 of the Data Protection Authority (Jersey) Law 2018 (DPAJL 2018).

Complaints and Inquiries

Part 4, of the DPAJL 2018 sets out 'Enforcement by the Authority' detailing how we approach Complaints and Inquiries.

Authority Sanctions and Powers

The **Authority's Regulatory Action and Enforcement Policy,** introduced in 2020, is based on five key principles of enforcement, which supports the outcomes-based approach:

1. Proportionality
2. Targeted
3. Accountability
4. Consistency
5. Transparency

This policy seeks to promote the best protection for personal data without compromising the ability of businesses to operate and innovate in the digital age. It helps to engender trust and build public confidence in how Jersey's public authorities manage personal data.

Authority Sanctions

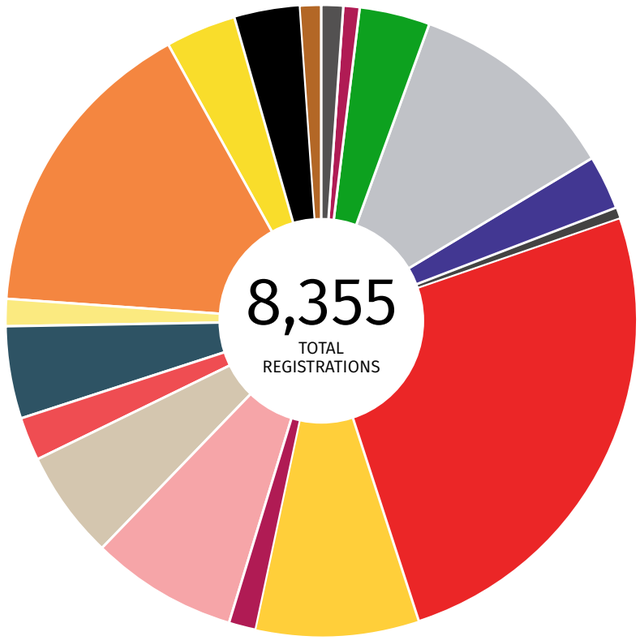
The Authority has several tools in its enforcement suite, namely:

- Words of Advice
- Reprimand
- Warning
- Order
- Public Statement
- Administrative Fine

This policy seeks to promote the best protection for personal data without compromising the ability of businesses to operate and innovate in the digital age. It helps to engender trust and build public confidence in how Jersey's public authorities manage personal data.

Enforcement and Compliance

Data protection is not new; it is part of good business practice and governance. Data protection holds organisations entrusted with personal data accountable, setting standards for how that information is used and as a last resort to provide a framework for enforcement where rules are breached.



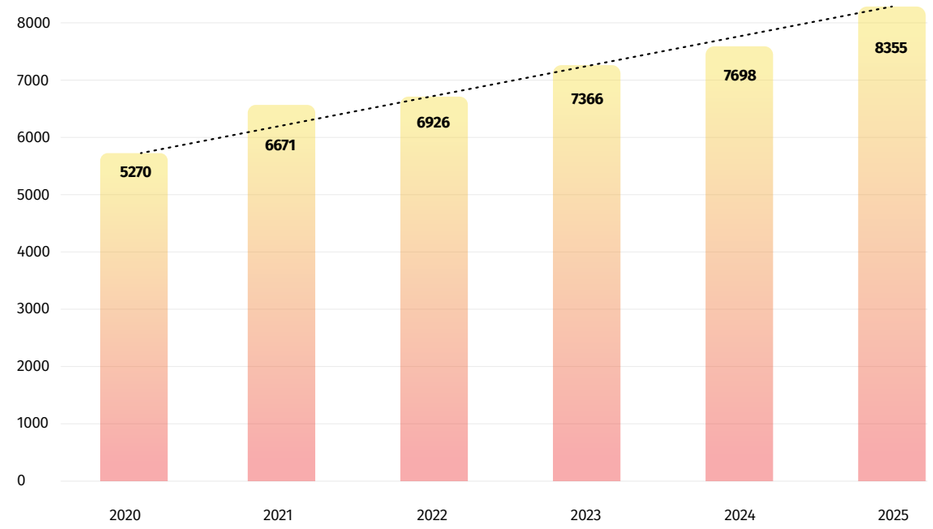
101	Agriculture & Fishing	471	Manufacturing, Wholesale & Retail
66	Animal Husbandry & Welfare	180	Media, Communication & Advertising
304	Charities	383	Professional Bodies/Professional Associations /Professional Consultancy
910	Construction, Trades & Services	121	Public Authority/Sector, Appointed Regulators & Statutory Bodies
238	Education & Childcare	1326	Real Estate & Property Management
45	Faith, Worship & Religion	302	Social Clubs & Associations
2106	Financial & Professional Services	269	Technology & Telecommunications
691	Health & Wellbeing	89	Utilities & Delivery Services
127	Legal Services		
626	Leisure & Fitness/Hospitality /Tourism/Travel/Entertainment		

Data Protection Registrations

The Data Protection Authority (Jersey) Law 2018 requires organisations established in Jersey who are processing personal data to register with the Authority. The principal purpose of registration is transparency and openness. Any failure to do so is a criminal offence.

The chart on the right highlights the overall number of registrations in 2025 and the industry sectors they represent.

Annual Data Protection Registrations



The Data Protection Registration Fee model became effective in January 2020 and is based on the principles of fairness, affordability, and risk. Fees have remained unchanged since the introduction in 2020, despite inflation and economic changes.

The bar graph shows the number of active registrations at the close of each calendar year.

Analysis of the registration data and comparison with data held by Statistics Jersey in early 2023 helped to highlight the sectors we were under-represented in terms of registrations and by inference awareness of data protection obligations.

An Authority project group established key tasks and activities to raise awareness amongst the following sectors, particularly amongst the smaller businesses, with fewer than 10 employees, as the Jersey economic landscape comprises over 89% small businesses.

- Construction, Trade & Services
- Education and Childcare
- Health & Wellbeing
- Leisure & Fitness/Hospitality/Tourism/Travel/ Entertainment
- Manufacturing, Wholesale & Retail

We collaborate with Customer and Local Services and Jersey Business to ensure all new start-ups are signposted to their data protection responsibilities.

The Construction Council, Landlords Association, the Chamber of Commerce, the Institute of Directors Jersey, the Law Society, Jersey Care Commission and the Jersey Financial Services Commission are all working with us to raise awareness.

We have hosted radio campaigns, special events, pop-up events and social media to raise awareness.

The chart above shows the trend and improvement in engagement and awareness of data protection obligations.

Since 2020
Registrations have risen

46%

The additional registration activities and interventions include a proactive approach including spot checking the registration details submitted and where appropriate we engage directly with the entity to validate the fee band submissions, chase every non-renewal each year and we now operate a tell us in confidence avenue on our website. Data subjects actively advise us if entities they want to use for services are not registered and we follow up.

We retain a high level of collaborative work with professional bodies, trade associations, outreach and leverage our communication channels to continuously raise awareness regarding all data protection obligations.

Excelling in Regulation

Strategic Outcome: **Achieving and maintaining the highest standard of data protection in Jersey**

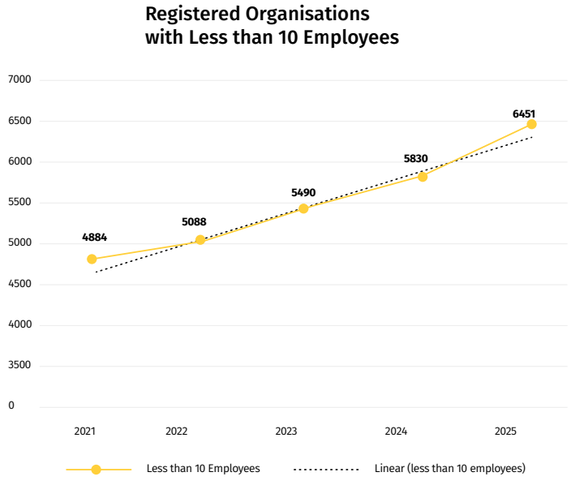
Our 'Excelling in Regulation' cornerstone is about maintaining strong data protection standards by leading by example in compliance and enforcement.

Number of registered organisations with less than 10 employees

AMBITION:
Increasing

TREND:
Increasing

TARGET:
89% of all registrations



The Jersey economy is made up of over 89% businesses with less than 10 employees. Our research highlighted that, in particular, we were light in the number of registrations from the following categories of businesses:

- health & wellbeing
- trades & construction
- retail

Campaigns focusing on these sectors and the broader businesses with less than 10 employees have raised data protection awareness and in turn registrations. This campaign will remain for 2026.

Registered organisations with less than 10 employees currently make up 76% of all our registrations, an increase from 75% in 2024.

The target is for 89% of all registrations to be for organisations with fewer than 10 employees (growing in line with increased overall registrations).

The data is collected when organisations register with us.

Compliance and Enforcement Case Data

The chart above/below highlights the number of complaints and self-reported data breaches per sector opened per sector in 2025.

	REGISTRATIONS		AMICABLE RESOLUTIONs		COMPLAINTS		SRDBS	
	Count	%	Count	%	Count	%	Count	%
TOTAL	8355	100	15	100	135	100	209	100
Agriculture and Fishing	101	1%	0	0%	0	0%	2	1%
Animal Husbandry and Welfare	66	1%	0	0%	0	0%	1	0%
Charities	304	4%	0	0%	2	1%	25	12%
Construction, Trades and Services	910	11%	1	7%	3	2%	4	2%
Education and Childcare	238	3%	2	13%	4	3%	14	7%
Faith, Worship and Religion	45	1%	0	0%	0	0%	10	5%
Financial and Professional Services	2106	25%	3	20%	27	20%	53	25%
Health and Wellbeing	691	8%	0	0%	8	6%	29	14%
Legal Services	127	2%	0	0%	5	4%	8	4%
Leisure and Fitness/Hospitality/ Tourism/Travel/Entertainment	626	7%	0	0%	7	5%	6	3%
Manufacturing, Wholesale and Retail	471	6%	0	0%	4	3%	2	1%
Media, Communication and Advertising	180	2%	1	7%	9	7%	1	0%
Professional Bodies/Professional Associations/Professional Consultancy	383	5%	0	0%	2	1%	3	1%
Public Authority/Sector, Appointed Regulators and Statutory Bodies	121	1%	5	33%	44	33%	27	13%
Real Estate and Property Management	1326	16%	0	0%	4	3%	4	2%
Social Clubs and Associations	302	4%	0	0%	0	0%	3	1%
Technology and Tele-Communications	269	3%	0	0%	1	1%	2	1%
Utilities and Delivery Services	89	1%	0	0%	6	4%	15	7%
No organisation type (domestic CCTV for complaints or not completed correctly)	0	0%	3	20%	9	7%	0	0%

The large employer and data users namely Public Authorities attract the highest number of complaints and based on proportionality this is not unreasonable, representing 34% of our complaints.

Since the introduction of the DPJL 2018, the number of complaints has fluctuated year on year, with the self-reported data breaches averaging 210 per annum.

	Complaints and Inquiries	Amicable Resolutions	Self-Reported Data Breaches
2018	184	-	141
2019	145	-	256
2020	140	-	229
2021	90	-	232
2022	58	**25**	188
2023	81	**15**	215
2024	86	**22**	184
2025	135	**15**	209

Amicable Resolution

Amicable Resolution is a process which seeks to resolve matters between the individual (the complainant) and the data controller without undertaking a formal complaint route.

Throughout 2025 Amicable Resolution remained a positive option with 25% of matters being successfully completed.

If the Amicable Resolution process is successful JOIC will consider matters concluded and no formal investigation will be undertaken. The Amicable Resolution process is designed to take place over 12 weeks although it may be extended with the agreement of both parties.

If, however, the Amicable Resolution process is not successful (either in whole or in part), we will ask you whether the individual wishes to convert matters into a formal complaint. It means that if we decide that it is appropriate to carry out a full formal investigation this will be done in accordance with the procedure and time frames set out in the Law.

Complaints

If an individual believes their personal data has been processed in a way contrary to the DP(J)L 2018 they can submit a formal complaint.

Complaints received in 2025 related to a blend of topics but predominantly focused on:

- The right of access request (50%)
- Unauthorised disclosure of personal data (21%)
- Unfulfilled rectification/erasure requests (12%)
- Concerns about personal data security (8%)

2025 follows a similar pattern to the previous 3 years.

25% **Amicable Resolution cases** resolved successfully

50% of all complaints were regarding **The Right of Access**

21% of all complaints were regarding **Unauthorised disclosure**

Complaints Opened Per Year By Type	2022	2023	2024	2025	Total
I asked for access to/copies of my personal information and I've not received it/they have withheld it from me	16	30	27	67	140
Direct marketing	1	2	1	-	4
I asked for my information to be rectified/erased/sent to another controller and my request has been refused	5	7	9	16	37
I don't think my personal data is being/has been kept safe	5	5	12	11	33
My information has been shared and it shouldn't have been	18	21	22	29	90
Other	4	1	3	3	11
Someone has collected my personal data, but I didn't give it to them	2	3	5	7	17
TOTAL	51	67	79	133	332

50% of all the complaints we received in 2025 were about the right of access to information being withheld or only partially completed. The complaints we investigate are often as a result of dissatisfaction due to the wholesomeness of the information received due to over-redacting, failing to respond to requests or declining to share certain aspects of information expected by the applicant.

21% of the 2025 complaints received were about perceived oversharing of personal information. The complaints received regarding sharing personal data are mostly due to employers over-sharing information, the blind copy function not being used when sending group emails, information being shared without a basis between controllers and ex- employees using personal data without authorisation.

12% (16) complaints received were about requests covering the rectification, the erasure or transfer of personal information

Following structured investigations throughout 2025, the Authority issued a blend of Orders, Reprimands and Words of Advice. We monitor the implementation of the Orders to ensure the Data Controller/Processor responds appropriately to the correct standard and within a defined time frame. Depending on the complexity of the Orders, the implementation process can take several months.

Of the complaints closed in 2025

- 27% were investigated and a breach determination made.
- 57% were not investigated, as per Part 4, Art. 20(2) of the DPAJL 2018 sets out the basis upon which we investigate or reject the complaint.
- 6% were withdrawn
- 10% were investigated and resulted in a no breach determination.

The complaints we have investigated have resulted in a range of sanctions being issued, including Reprimands and Orders, some of which were issued within Public Statements.

27% led to breach findings

10% led to NO breach findings

Public Statements and Fines

The Authority issued six **public statements in 2025** for contraventions of the DPJL 2018. Of the six:

- Two attracted fines
- Two were extremely serious contraventions
- Two stated that 'the nature of the breach would have warranted initiating the relevant process to assess the imposition of an administrative fine'

FINE Star-Delta Electrical Services

The Authority issued a fine to Star-Delta Electrical Services (Star-Delta) in the sum of £4,000.

In deciding whether it was appropriate to issue an administrative fine, the Authority gave weight to the following:

a. Star-Delta pursued the Client and their partner on social media, manipulating images of the Client and their partner, such as attaching images of their faces to the bodies of rats, animating their photographs. This was a deliberate campaign initiated by Star-Delta to 'name and shame' the Client and their partner, rather than pursuing them through the Petty Debts Court in the usual way.

b. This was a targeted and deliberate attack. Star Delta initially refused to remove the posts.

c. The Client provided an impact statement outlining the very real distress that had been caused to them and their partner.

The Authority concluded that the sum of £4,000 was appropriate and reasonable in the circumstances. In addition to the fine, the Authority also issued a formal reprimand and made a number of orders pursuant to Art.25(3) of the DPAJL 2018. The orders included the completion of registration, not re-publishing the offending posts and not publishing any new/additional posts about the Client and or their partner on any social media platforms owned/operated by Star-Delta.

The lessons learned from the two fine cases focus on:

- Personal information obtained for a legitimate business purpose must not be repurposed in an unlawful way.
- Inappropriate sharing of personal information.
- Personal information should only be used for the purpose for which it was given.
- Vindictive or threatening behaviour by Controllers to their clients/staff (data subjects) are viewed as a significant aggravating factor and the Authority will have no hesitation in issuing an administrative fine in similar circumstances.
- If an organisation repeats inappropriate behaviour the Authority will likely increase the severity of its sanction.

FINE JRSY Laser Limited

The Authority issued a fine to JRSY Laser Limited (JRSY Laser) in the sum of £500.

In deciding whether it was appropriate to issue an administrative fine, the Authority gave weight to the following:

a. The Authority had already given a specific warning that vindictive behaviour and threats to release personal data would not be tolerated and that if any similar future behaviour occurred it would likely result in the issuing of an administrative fine. The Director shared personal data with staff members where there was no lawful basis to do so.

b. The Authority considered a significant aggravating factor in this case was that the Director made a threat towards an individual, which they had been warned previously they must not do.

c. JRSY Laser neither understood nor appreciated the responsibilities they had with regards to staff personal data. The Director initially offered to remove the Employee's information from their systems as more of a gesture rather than a genuine acceptance of inappropriately sharing the information.

d. The victim impact statement explained they had suffered from emotional distress, anxiety and low self-esteem, which had impacted on their confidence to carry out their work. They also reported feeling threatened, embarrassed and hurt by the content of the email shared with the JRSY Laser staff because it was very negative about the Employee's character.

Two Public Statements highlighted that **'the nature of the breach would have warranted initiating the relevant process to assess the imposition of an administrative fine'**

The Office of the Financial Services Ombudsman and the Jersey Financial Services Commission were both issued Public Statements. Both cases may have warranted fines, had the data controllers not been public authorities and therefore not subject to fines under the current framework.

Two Public Statements with **extremely serious contraventions**

The Parish of Grouville and the Department for Children, Young People, Education and Skills were also both issued with Public Statements in 2025. The Authority considered that both entities failed to take proportionate and reasonable steps to prevent the relevant contraventions.

All the public statements are published in detail on our **website**.

The lessons learned in the contraventions detailed above include advising data controllers to ensure that they have in place appropriate measures to respond to individual rights, plus have appropriate systems, policies and adequately trained staff to respond to data protection mandated obligations.

Importantly, also noted was a requirement for data protection to be built in by design and default; so as to adopt a 'privacy first' approach.

Other Complaint Outcomes

Other complaints which resulted in breach determinations being made led to the Authority issuing a range of Orders in 2025, to many other data controllers and processors, the details and names of which cannot be made public. These enforcement Orders covered key topics, such as;

- Ordering a controller to appropriately fulfil a rectification matter and then undertake relevant training in this topic.
- Being ordered to undertake a wholesale review of data protection policies and procedures, including updating privacy policies to truly reflect processing activities and develop and implement an acceptable use policy.
- Requiring Data Protection Officers to be upskilled and adequately trained.
- Ordering significant improvements in achieving and fulfilling proportionate technical and organisational measures in terms of security and fulfilling individual rights requests timescales.
- Ordering a controller to provide staff members with appropriate, relevant and role specific data protection training. Requiring the controller to report back to the Authority within a stipulated timeframe.

The Authority applies the Outcomes Based Accountability philosophy of 'who is better off' in relation to our enforcement activities. We aim to change behaviours and issue proportionate effective enforcement to avoid reoccurrence of contraventions.

The chart below highlights that of those entities that received enforcement action, five of them 'reoffended' in 2025. Although this exceeded our annual target of 'no more than four', we are working with the data controllers to improve their data protection practices.

Excelling in Regulation

Strategic Outcome: **Achieving and maintaining the highest standard of data protection in Jersey**

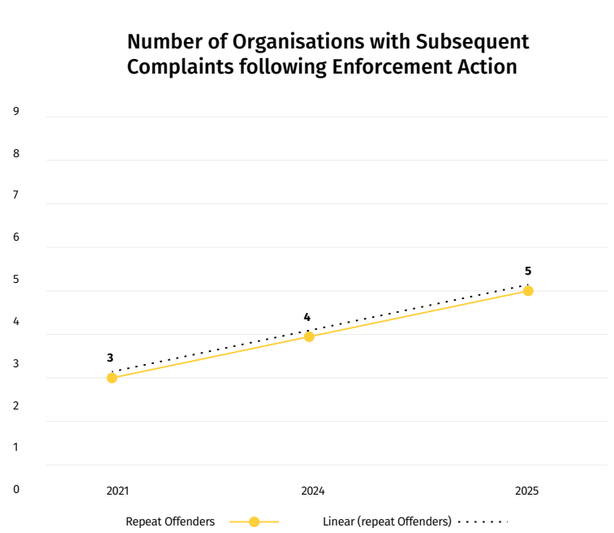
Our 'Excelling in Regulation' cornerstone is about maintaining strong data protection standards by leading by example in compliance and enforcement.

Number of organisations with a subsequent complaint in the same year, after enforcement action.

AMBITION:
Decreasing

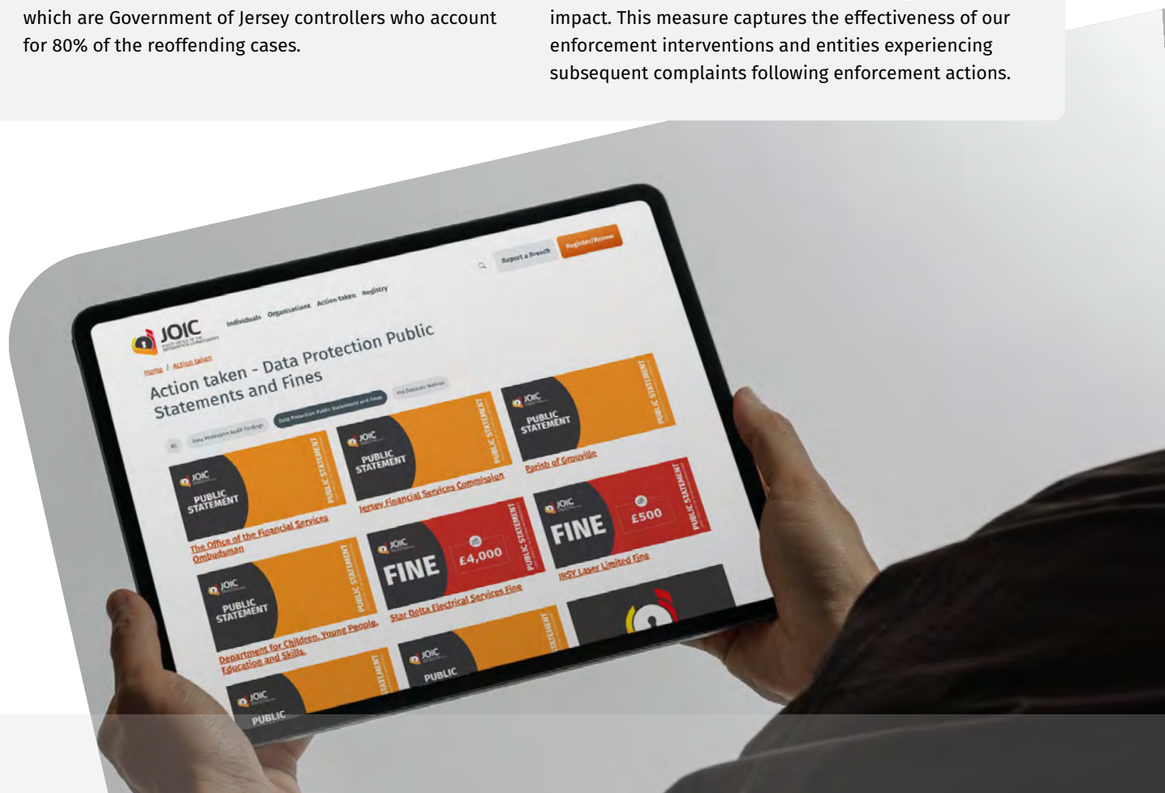
TREND:
Increasing

TARGET:
Not greater than 4



The trend for 2025 has resulted in an increase by 1 repeat offender since 2024, which exceeds our target. We will therefore focus C&E activities on the reoffenders, 60% of which are Government of Jersey controllers who account for 80% of the reoffending cases.

Our focus is on outcomes-based regulation and accountability (OBA), as well as evaluating "what needs to go well" and whether our work is making the correct impact. This measure captures the effectiveness of our enforcement interventions and entities experiencing subsequent complaints following enforcement actions.



Personal Data Breach Reporting

Under the DPJL 2018 'in the case of a personal data breach, the controller must, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach in writing to the Authority' (Article 20).

A Personal data breach is something that happens when someone's personal data (including more sensitive, special category data) is accidentally or unlawfully lost, stolen, disclosed or accessed. This can include sending an email to the wrong person that includes someone's personal data, leaving a notebook on the bus, or a hacker gaining access to computer systems and files it should not have been able to access or preventing access to an organisation's systems. Such breaches can lead to various risks such as identity theft, fraud, harm, distress or financial loss. Organisations must act quickly to protect affected individuals and take preventative measures to contain the incident and prevent the same issue happening in the future.

Self-Reported Data Breaches Opened per Year, by Organisation Type

Organisation Sector	2020	2021	2022	2023	2024	2025
Agriculture & Fishing	3	3	1			2
Animal Husbandry & Welfare	1			2	2	1
Charities	16	18	23	20	15	25
Construction, Trades & Services	2	6	3	2	9	4
Education & Childcare	19	8	9	18	6	14
Faith, Worship & Religion	2	1		1		10
Financial & Professional Services	84	79	61	81	54	53
Health & Wellbeing	11	23	29	16	31	29
Legal Services	10	4	4	14	9	8
Leisure & Fitness/Hospitality/Tourism/Travel/ Entertainment	2	8	6	7	7	6
Manufacturing, Wholesale & Retail	12	10	8	8	3	2
Media, Communication & Advertising	1			2		1
Organisation Type Not Applicable	1	1			1	
Professional Bodies/Associations/Consultancy	6	2	2	4	6	3
Public Authority/Sector/Regulators	54	50	26	23	25	27
Real Estate & Property Management	4	4	2	4	5	4
Social Clubs & Associations	2			3		3
Technology & Telecommunications	4	5	7	2	2	2
Utilities & Delivery Services	3	6	5	4	9	15
Total	237	228	186	211	184	209

The chart above identifies organisational sectors who complied with the breach reporting requirements and submitted details to the Authority in 2025.

Faith, worship and religion saw 10 reports in 2025 which was unusual – this was in relation to a phishing attack on the churches, this was low level and the data controllers had instigated effective mitigations by the time they had reported the breach.

Sectors with notable breach reporting levels are highlighted below. Most of the breaches occurred due to human error and cyber incidents. When reviewing the breaches, we assess the gravity and nature of the breach, prior to launching any Inquiries. The breaches were all deemed low level and did not generate any formal Inquiries, except one from the Professional Bodies sector. That breach has now been turned into a joint Inquiry with other Data Protection Authorities – including the UK Information Commissioner and the Crown Dependencies Data Protection Authorities.

The sectors below reported the most breaches in 2025. The Authority will be carefully monitoring those entities with repeat breaches.

- **Health & wellbeing 14%** - following the publicity around the JRSY Laser fine in 2025 awareness was raised in this sector and breaches were reported throughout the year.
- **Charities 12%** - this sector saw a variety of charities reporting breaches as a result of human error combined with a level of over reporting.
- **Utilities 7%** - one utility operator had several breaches, JOIC reviewed the breaches but insufficient to launch an inquiry.
- **Education & Childcare 7%** - the breaches in this sector included sharing a child's image without consent and a staff member accessing information.
- **Financial & Professional Services 25%** - this sector is very proficient in reporting all levels of breaches and tend to over report.
- **Public Authorities 13%** - as part of our 2026 – 2028 strategic priorities we will be reviewing the level of breach reporting in this sector.

Sector Breaches

Financial sector
25%

Health sector
14%

Public authorities
13%

Self-Reported Data Breaches Opened per Year, by Breach Type

Breach Type	2020	2021	2022	2023	2024	2025	Total
Alteration	2	3	1	0	1	0	7
Destruction	1	1	1	1	1	0	5
Lack of Availability/Access	4	1	6	5	2	2	20
Loss	16	11	5	7	2	7	48
Unauthorised Access	49	45	30	53	62	54	293
Unauthorised Disclosure	156	165	143	145	116	146	871
Unknown/Other	9	2	0	0	0	0	11
Total	237	228	186	211	184	209	1255

Specific breach detail

146
unauthorised disclosure breaches

146 self-reported data breaches were due to unauthorised disclosure (emails sent and received in error/information being sent and received by the wrong recipient). In all cases, the breaches were mitigated and actioned to a satisfactory standard by the Controller themselves but in some instances the Authority worked with the Controller to ensure appropriate steps were taken and data protection compliance was met by providing substantive advice and guidance.
No Self-Reported Data Breaches relating to unauthorised disclosure were of the severity or risk to the individuals involved to be turned into a formal Inquiry in 2025.

54 self-reported data breaches involved a number of different issues including ransomware, phishing attacks, lost data, and other processes leading to breaches. In most cases, the breaches were appropriately mitigated, presenting no risk to the data subject. However one ransomware breach was turned into a joint Inquiry/Investigation (with another 3 jurisdictions) due to the nature and severity of the breach.

54
breaches from varied causes

Most reported breaches do not warrant the conducting of a formal regulatory response and/or the imposition of a formal sanction. However, the Authority may impose an Administrative Fine in a case of deliberate, wilful, negligent, repeated or particularly harmful non-compliance. It is important to note that failing to report a breach, where required, could result in a severe penalty.

Making Privacy Instinctive

In 2025, our Communications and Outreach efforts were driven by our vision to make privacy instinctive for Islanders, aligned with our three strategic priorities. We worked towards these via dynamic, targeted education and awareness campaigns delivered with impact through interactive events and workshops, practical guidance sessions, community activities and media initiatives that brought privacy to life across our community.

Raising awareness and standards among organisations

Our interactive events programme for data controllers and processors featured a blend of workshops and guidance sessions for organisations of all sizes.

Our programme is focused on:

- Helping participants gain a clear understanding of our role, obligations under the Data Protection (Jersey) Law 2018 and how we can support those with data protection responsibilities.
- Increasing knowledge of data protection and promoting good data protection practices.
- Providing relevant information in an engaging manner.
- Providing practical, actionable insights, to help participants confidently perform their role.

Support for ‘Fewer than 10’

In 2025, we launched **Data Protection Express**, weekly drop in clinics for sole traders, small businesses and start ups, offering support with data protection obligations and simple steps to strengthen privacy practices. Participants benefit from clear, practical advice about local data protection law and the opportunity to ask questions about their responsibilities.

To further support smaller organisations and informed by focus group insight, we also delivered **Data Protection Essentials webinars** covering key principles of local data protection law, including individual rights. We also met small business owners across the Island and hosted information stands to raise awareness of data protection obligations and our guidance available.

Our **Let’s Go DPO** network continued to grow in 2025, with members valuing direct engagement with the regulator alongside peer learning. Workshops covered data breaches, data sharing best practice and subject access request support. Membership increased from 181 to 326 and we will continue expanding the network in 2026 to support our strategy.

Our **Board Support sessions** continued to help board members, directors and non executive directors understand data protection risks, responsibilities and accountability. Participants consistently value the chance to work with experts in a safe environment and stress test their organisation’s practices to identify risks early.

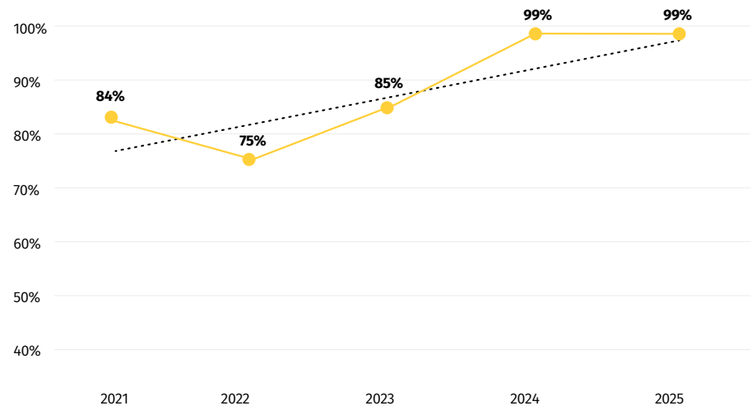
Our **wider events programme** focused on collaboration to maximise reach. We delivered guidance workshops for organisations including Association of Jersey Charities, Digital Jersey and Jersey Entrepreneurs Group. Our leadership team regularly appeared as guest speakers at industry seminars.

Data Protection Week 2025 activities ranged from an interactive school assembly to awareness sessions for individuals and industry. Our Breakfast with the Commissioner seminars provided updates about our strategy, activity, enforcement action and philosophy.

To mark International Data Protection Day, we partnered with Guernsey’s Office of the Data Protection Authority on a joint podcast with both Information Commissioners exploring the shared challenges and opportunities of regulating small jurisdictions.

The table below shows the percentage of data controllers and processors whose understanding of data protection obligations improved after attending a JOIC outreach session. The strong results for 2025, along with steady progress over the past five years, are encouraging.

Percentage of Individuals Representing a Controller/Processor Whose Knowledge Improved



Engaged with
1882
young people

97%
of young people providing feedback said knowledge improved

Protecting Children's Privacy

We continue to prioritise education for Jersey's young people and our vision to create an Island of young privacy ambassadors gained momentum in 2025. Throughout the year we engaged with 1882 young people across ten secondary schools and further education establishments.

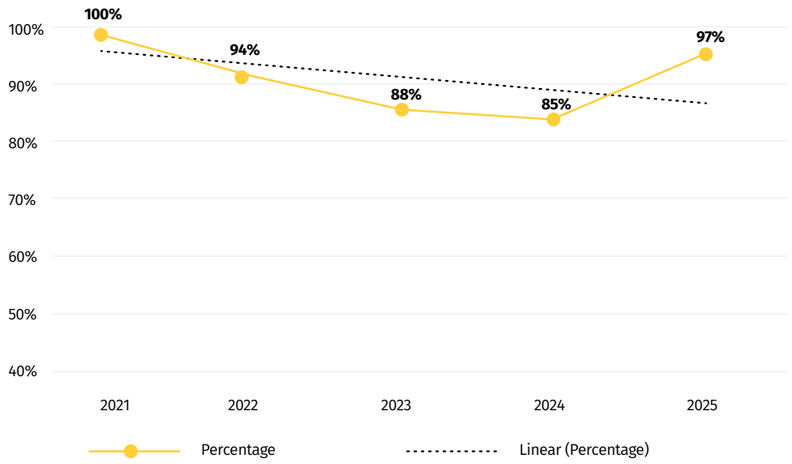
The learning outcomes of our young persons' programme are:

- To raise awareness of our role, obligations under the Data Protection (Jersey) Law 2018 and how we can support young people in protecting their personal information and privacy rights.
- To raise young people's awareness of their privacy rights to increase knowledge of key privacy issues and promote good privacy behaviours.
- To provide relevant information in an engaging manner.
- To provide practical, actionable insights to help young people confidently protect their personal information.

Our sessions brought the importance of protecting personal information and the risks involved in sharing both in person and online into sharp focus via interactive activities.

The table below highlights 97% of young people providing feedback said their knowledge of the Jersey Office of the Information Commissioner, protecting their personal information and understanding individual rights improved as a result of participating in a JOIC outreach session in 2025. It is pleasing to note feedback consistently remains above 86%.

Percentage of Young People with improved knowledge



Our Courtroom Challenge continued throughout the year, giving sixth form students experience of a mock data protection trial to bring privacy law to life. We also ran energetic, practical workshops for Year 10 and further education students starting work placements.

We welcomed the chance to partner with the Office of the Children's Commissioner for Jersey, gaining valuable insight into how young Islanders manage and safeguard their personal information in today's fast moving, digital world.

Connecting with Community

The learning outcomes of our programme for individuals, are:

- To raise awareness of our role, obligations under the Data Protection (Jersey) Law 2018 and how we can support individuals in protecting their personal information and privacy rights.
- To raise individuals' awareness of their privacy rights.
- To increase knowledge of data protection issues and promote good data protection practices.
- To provide relevant information in an engaging manner.
- To provide practical, actionable insights to help individuals confidently protect their personal information.

We continued to bring data protection into the heart of Jersey's community with targeted activities including pop up information stands at key locations, which were timed to align with international data protection and privacy-related awareness days.

We were honoured to join Jersey Consumer Council's 30th anniversary event to raise awareness of our office and Islanders' individual rights, as well as attend Jersey Children's Day, where we shared our key messages with more than 100 children and adults through meaningful conversations.

Local Radio & TV

Amplifying our Messages

We amplified our key messages via a mix of media engagement, online and traditional advertising and our quarterly Stay in Touch newsletter to enhance visibility and reinforce our position. Updates included Public Statements and accompanying lessons learned, findings for data controllers regarding our rolling audit programme, community outreach activities and international collaboration. **Subscriptions to our quarterly newsletter increased by 132% since the start of 2025,** demonstrating growing interest in our work and activities.

The Information Commissioner and Operations Director regularly raised awareness via interviews with flagship local media channels.

Surveys and Insights

In late 2025, we partnered with the Isle of Man Information Commissioner to run a **Data Protection in Practice – Insights Survey**. The project explored how organisations are applying key principles of their data protection laws, to help us identify improvements, shape guidance and strengthen data protection culture in our respective jurisdictions.

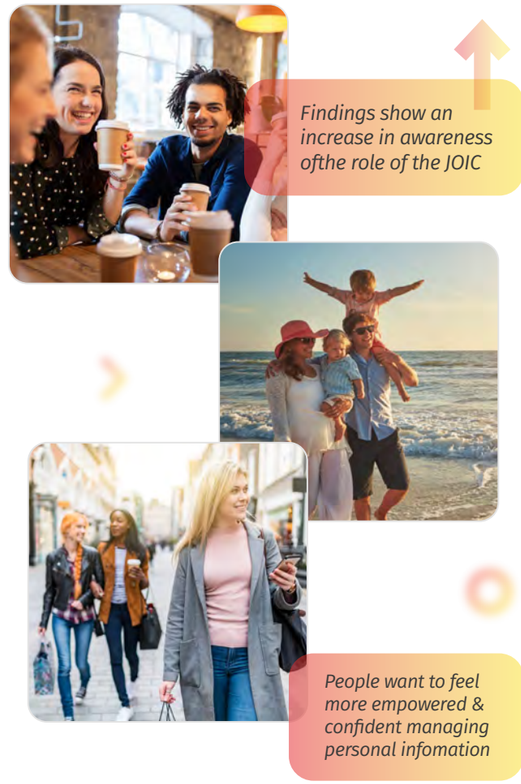
The survey focused on seven areas: training, Data Protection Officer roles, data subject access requests, data protection impact assessments, data sharing, AI deployment and breach management. It was carried out in line with the Market Research Society Code of Conduct. Regard was also paid to the Code of Practice for Tier 1 Statistics (the guidelines for public authority statistics producers in Jersey). Findings will be published in early 2026.

We run our annual It's All About You self-selecting survey to understand Islanders' views about data protection and privacy.

Findings show that from 2022 to 2025, awareness of the Data Protection (Jersey) Law 2018 rose by 34%. In 2025, 90% of respondents said they were aware of risks to their personal information and concerned about them sometimes, often or every day. Credit and debit card details remained the top concern for over 96% of respondents each year, followed by passport, biometric, ID and health data. The 2025 results sent a clear message to organisations they must handle personal information lawfully and be fully accountable for how they process it.

The Government of Jersey's annual Opinions and Lifestyle Survey explores Islanders' experiences to help shape public services and in 2025, the survey included questions from our office. Findings showed a quarter of respondents were either not aware or had only some awareness of risks to their personal information. Meanwhile, 45% of respondents had only some confidence or weren't at all confident managing risks to their personal information.

The above insights highlight emerging risks and help us target enforcement and outreach where it has the greatest impact, ensuring our approach remains intelligence led and grounded in real world behaviour.



International Collaboration

International collaboration remains essential to strengthening global data protection standards. By working closely with partners worldwide, we build resilience and ensure our approach reflects global expertise.

In September, the Information Commissioner represented Jersey at the **47th Global Privacy Assembly,** also attending as a member of the Executive Committee. The Assembly brings together more than 130 authorities to lead global work on privacy.

The Commissioner spoke on a panel discussing the privacy and data protection challenges of targeted advertising in the age of AI and delivered two speeches in the Closed Session, including a report on the 46th Assembly held in Jersey in 2024. The event offered valuable insight into global AI challenges and their relevance to Jersey.

In June we attended the annual **British, Irish and Islands Data Protection Authorities** meeting, which promotes supervisory consistency across neighbouring jurisdictions. Delegates shared strategies on children's privacy, international cooperation, responsible innovation, the importance of data protection in supporting healthy and progressive global financial sector jurisdictions, as well as modern enforcement approaches. These exchanges help authorities adopt successful practices that benefit their communities.

In November, we took part in the **Global Privacy Enforcement Network's** international sweep that focused on Children's Privacy. More than 30 authorities examined whether websites and apps are transparent, use age assurance measures and limit the collection of children's data. The sweep aimed to increase awareness of privacy rights and responsibilities, encourage compliance with privacy legislation, identify concerns that may be addressed through targeted education or enforcement and enhance cooperation between global data protection and privacy authorities. Findings will be published in early 2026.

Environmental, Social and Governance

We are mindful of how our actions impact the natural world and proud to have retained Eco Active status from the Government of Jersey's Eco Active business network.

During 2025, we further strengthened our commitment to Eco Active with attendance at Eco Active led events including training courses exploring waste management and the true value of reducing, reusing, and recycling, particularly exploring the impact of AI and digital technology on the planet. During the year, our staff also attended a guided tour around the Island's Energy Recovery Centre.

Our team is committed to:

- Enhancing energy awareness in the workplace
- Taking a proactive approach to office recycling
- Improving energy efficiency and eco awareness among staff
- Preventing waste and reducing the risk of pollution and other negative environmental impacts

We conduct regular reviews of our office to identify opportunities for energy savings and during 2025, our in-house Eco Active champion increased awareness among staff, of the benefits of environmentally friendly forms of travel to work.

We have taken the following actions:

1. Conduct regular reviews to identify where energy can be saved.
2. Have energy saving lighting across our workplace and switch off computers, monitors, and communal equipment at the end of each day.
3. Use 100% recyclable printer paper and recycle printer toners.
4. Reuse and recycle technical equipment wherever possible.

People and Organisational Development

Strengthening organisational resilience during a year of change

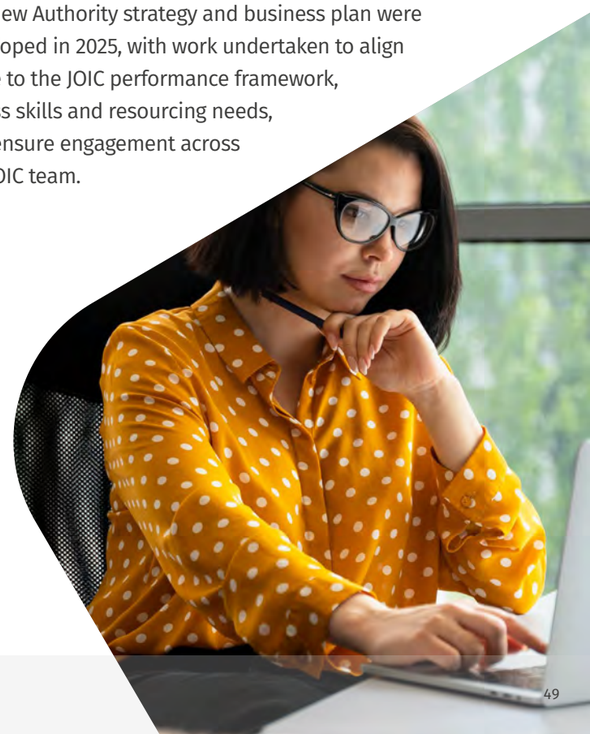
In 2025, the JOIC and the Authority focused on building organisational resilience and ensuring continuity during a period of change and development. Key priorities included strengthening capacity through targeted recruitment, securing several senior appointments, and stabilising the workforce to support future delivery.

During the year we reviewed core HR processes and procedures, restructured administrative tasks and laid the groundwork for the introduction of an HR system to improve efficiency and cost-effectiveness.

Employee engagement, learning, and wellbeing remained central to our approach, with new themes introduced to support development and maintain a positive culture.

While 2025 brought some pressures for JOIC's people and organisational development programme, progress continued despite these constraints. Budget limitations during the year meant that some recruitment and development activity moved more slowly than planned. In addition, the extended consultation process with government regarding senior reappointments required significant time and attention, which inevitably affected capacity for other areas of delivery.

The new Authority strategy and business plan were developed in 2025, with work undertaken to align these to the JOIC performance framework, assess skills and resourcing needs, and ensure engagement across the JOIC team.



Workforce stability and diversity maintained despite budget constraints

The Authority

One longstanding Authority voting member retired in 2025 and was replaced by a new voting member who assumed oversight of JOIC's finance and governance from September 2025.

Excluding the most recent appointment, the average tenure for Authority members as of 31 December 2025 is approximately three and a half years, providing a strong level of continuity and organisational knowledge.

At the end of 2025, the Authority comprised of four men and one woman, spanning a wide age range and representing four nationalities, including two Jersey based members. Together they bring strong professional diversity across data protection, law, IT, business administration, finance, economics, and education. For a small board, diversity is robust, with opportunities to improve gender balance as future vacancies occur.

JOIC Team

At the end of 2025, the JOIC comprised of 18 employees (17.8 FTE) permanent employees. This was 0.8 FTE lower than the previous year. Two people left and one post was not replaced, due to funding issues. There were no promotions in 2025.

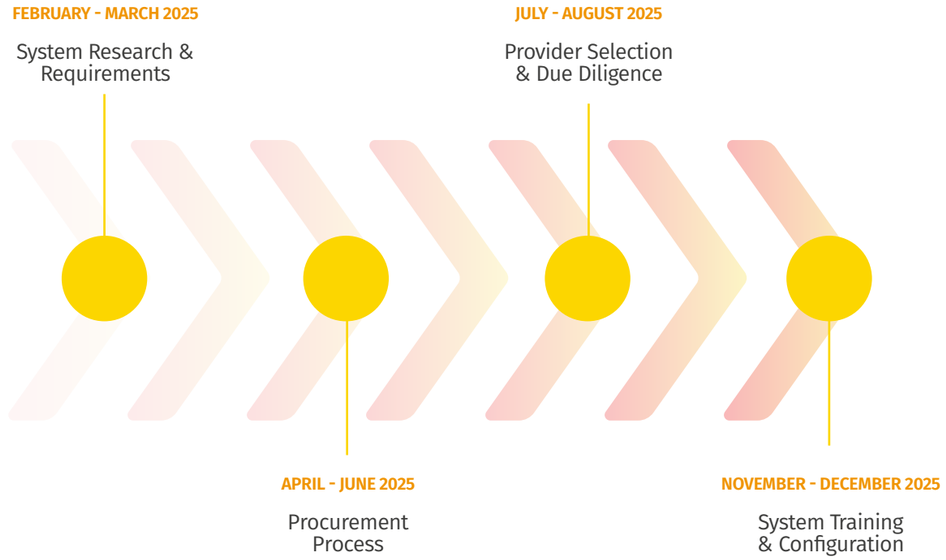
In total approximately 90% of the JOIC team were female and 10% male in 2025, a similar figure to the previous year. The JOIC senior leadership team comprised of four permanent employees, three female and one male, supported by two external consultants.

JDPA and JOIC	2024	2025
JOIC	18.6 FTE	17.8 FTE
JDPA	7	5

Significant progress toward modernising HR through system implementation

The JOIC does not currently operate a dedicated HR system, although certain processes, such as absence and leave management, are automated. With the combined JOIC and Authority full-time equivalent headcount at approximately 24, the need for a comprehensive HR system to improve efficiency and employee experience, as well as to save time and reduce costs, became evident.

During 2025, a project team undertook research and defined the organisation's requirements for an HR system. A procurement process was subsequently conducted, and a provider was selected in Quarter 3 2025. The new HR system will be implemented in phases from Quarter 1 2026 and include system modules such as employee information, absence management, training, performance, recruitment and employee engagement.



Administrative efficiencies achieved ahead of HR system rollout

In line with JOIC's commitment to efficiency and in preparation for the new HR system, we reviewed a range of People and Organisational Development tasks in 2025 to identify those that could be streamlined, automated within the system, or delegated to the administration team. Some efficiencies were gained in 2025, particularly across routine areas of administration and we expect to see further improvements as the HR system is introduced, particularly around the larger people processes such as recruitment, employee development, and absence management.

Strong commitment to learning and wellbeing despite pressures

The JOIC Learning and Wellbeing Programme offers a range of short, impactful sessions designed to support both personal and professional development. In 2025, fifteen sessions were delivered to the JOIC team, covering topics such as Safeguarding, Customer Service, Discrimination legislation, Cyber Security, and Workstation Wellbeing. The programme also included sessions focused on JOIC's benefits including pay and reward, private medical insurance, and pensions.

Reduced budgets combined with increased workloads limited opportunities for professional qualifications in 2025. Several team members progressed towards professional qualifications, spanning Freedom of Information, Data Protection and Accounting, maintaining essential skills and expertise within our workforce.

Aligning strategy and people for the future

During 2025, the leadership team continued to progress existing strategic plans while supporting the Information Commissioner in shaping the 2026 – 2028 strategy. From a People and OD perspective, this involved reviewing the strategy through several lenses including performance management, employee skills, and communication and engagement, ensuring a strong foundation for future delivery.

Building strength with long term talent and succession planning

Building on progress in recent years, the leadership team continued to identify potential successors and prioritise development and career progression opportunities for motivated and capable employees, in 2025. Although development can take time and resources remain limited, this work continues to be an essential discipline, ensuring that investment is focused where it can deliver the greatest benefit for both individuals and the organisation.

Finance Report

The Authority took a careful and measured approach to financial management throughout 2025. Early in the year, income remained steady while spending was kept under close control, ensuring resources were focused on key priorities and delivered good value. The first quarter ended with an underspend of £56k, mainly due to stronger than expected registration income, reflecting the positive impact of continued efforts to increase engagement with business registrations, including targeted outreach to sectors where uptake has historically been lower.

This positive trend continued through the middle of the year. By the end of Quarter 2, 96% of the annual income budget had already been achieved, putting the organisation in a strong position to meet its full year targets. Expenditure remained aligned with the business plan, and ongoing cost control supported financial stability.

In Quarter 3, the position improved further, with additional unplanned income from the registration project alongside underspends in areas such as staffing, consultancy, and operational costs. While generating a surplus was not the primary aim, this outcome provided valuable financial resilience during a period of rising costs.

Overall, the year ended on a positive note, despite the original budget including a planned deficit, total income reached £2,575,092, exceeding the budget by £68,479. Expenditure was also lower than expected, with staff and non-staff costs both coming in under budget, resulting in an overall underspend of £197,013. After taking account of year-end adjustments, the final reported surplus was £82,583. This reflects a balanced and responsible approach to financial management, while ensuring the organisation remains stable and well prepared for the future.

Financial Summary 2025

Budget Area	Budget to Q4	Actual to Q4	Variance
Income	£2,506,613	£2,575,092	+£68,479
Staff	£1,672,389	£1,623,078	+£49,311
Non-Staff	£867,628	£788,405	+£79,223
Total budget Variance to Q4			+£197,013

Income

	Budget for the full year 2025	Actual for the full year 2025	Variance
Interest	£6,000	£10,140	+£4,140
Fees	£2,347,613	£2,410,050	+£62,437

Government Funding

The Jersey Data Protection Authority took receipt of two grant payments during 2025.

The first was received for Freedom of Information. The Grant is paid to the Information Commissioner as part of an FoI partnership agreement, with the JDPA being the grant receiving authority which enables the grant to be received and utilised to fulfil the FoI statutory obligations.

The second grant was received to support Data Protection activities in the year.

	Freedom of Information	Data Protection
Grant paid in 2025	£70,000	£83,000

Registration Fee Income

Fee income of £2,410,050 has been received to the end of the year which represents 102.7% of the full year set budget (2024: £2,325,260. 100.8% of the full year budget).

The below table shows a comparison of fees in each registration fee band at year end for 2024 and 2025

	Current year 2025	Prior year 2024	% +/-
Full time equivalent fee	£601,130	£554,060	+8.50%
Past year revenues	£111,000	£95,750	+15.93%
Subject to proceeds of crime	£114,650	£115,250	-0.52%
Administered Services	£1,519,450	£1,510,650	+0.58%
Special Category Data	£63,820	£49,550	+28.80%

This increase mainly reflects the ongoing registration project fee work which was undertaken throughout 2025. Targeted efforts to raise awareness among SMEs about the need to register have led to an increase in new registrations.

The project also involved additional proactive checks of submitted registrations which identified missing or incorrect information, resulting in additional fee income being generated.

Remuneration and Staff

The below table shows the Authority Remuneration and time commitments for the members during 2025.

The rates are subject to an external review with the last review occurring during 2024, the findings were submitted to the Minister who approved the following:

Role	Time Commitment	Day Rate	Annual Remuneration
Authority Chair	18 days p.a	£1,016.50	£18,297
* Committee Chair and Voting member	15 days p.a	£802.50	£12,037.50
Voting Member	12 days p.a	£802.50	£9,630

There are no other payments made to the Authority members. Authority members are independent contractors and do not constitute an employee for the purposes of the Employment (Jersey) Law 2003 or other local legislation.

* Staff costs include the Commissioner's salary.

Total Staff costs for the year were underspent at year end.

Budget 2025	Actual 2025	Variance
£1,672,389	£1,623,078	£49,311

There were 19 roles recorded in the 2025 budget with 18 of these in post at year end. Recruitment was delayed through the year to utilise the staff savings while the vacant role was reviewed.

Commissioner Salary 2024	Commissioner Salary 2025	% increase on 2024
£163,309	£168,038	3%

**The figures above include employer social security and pension contributions. The grade offered to the Information Commissioner is a 10.3 on the JOIC pay scale.*

Non-Staff Costs

Non staff expenditure was carefully managed throughout the year, resulting in an overall underspend against budget. This was achieved without reducing delivery, with services and key activities maintained while ensuring spending was targeted where it added the most value. Cost control measures, including contract renegotiations and a disciplined approach to committing expenditure only when necessary, contributed to lower costs across areas such as consultancy, IT, travel, and operational activities.

Additional factors included lower than expected demand for specialist support and unplanned maintenance. Budgets were also flexibly reallocated to support strategic priorities during the year.

Budget 2025	Actual 2025	Variance
£867,628	£788,405	£79,223

Overall, this reflects a balanced and considered approach to financial management, maintaining service delivery while avoiding unnecessary spend and strengthening the organisation's financial position for the future.

Full audited accounts can be viewed on our **website.**

APPENDIX 1

PRINCIPAL RISKS

Risk Description	How we manage the risk	Movement of the Risk
Operational Freedom of Information (FOI) Law Change in scope. Likely expansion to capture additional scheduled public authorities (including the JDPA and Information Commissioner). Likely to generate an increase in formal FOI requests and appeals.	→ The Information Commissioner responded and contributed to the FOI consultation and workshops. → The Information Commissioner highlighted concerns and operational impacts in the 2025 FOI annual report. → The Information Commissioner's FOI team carefully monitors impacts and trends of appeals.	↔
Strategic Greater accessibility & availability of technology in all areas, impacts on ability to keep abreast of developing changes in personal data processing. Impact on detriment to the individual and reputation of JOIC.	→ With ongoing horizon scanning. → Collaboration and effective stakeholder management. → By developing relevant internal policy and external guidance. → By implementing an effective communications and outreach plan.	↔
Political Insufficient and/or unpredictable Government funding for Government data protection activities. Any changes or absence of fee/grant monies from Government impacts on our ability to plan effectively and could impact on our ability to deliver our regulatory mandate.	→ With continual reviews of activity data to see if we are achieving our performance measures – assessing any shortfall to see if it is resource or funding related. → By protecting our independence as a key priority. → By maintaining the ongoing proactive discussions which commenced in late 2020 to effect a change in the annual grant/fee Government contribution for data protection. → Through prudent budgeting and spending. → By monitoring and analysing registration data and revenues.	↑
Political The Value for Money Review undertaken at the request of the Government of Jersey to help inform them as to any financial commitments/grant/fee monies to the Authority. There is a reputational risk associated with a review of this nature. Report stated that '*Overall, JOIC are delivering value for money, however, there are opportunities to improve this. Within the resources available, JOIC is delivering on its core functions under data protection legislation, including protecting the individuals rights in respect of personal data, providing education and awareness, administering and enforcing data protection laws, investigating complaints and potential data breaches and obtaining international co-operation on data protection matters.*'	→ By carefully managing Government of Jersey expectations as to interpretation, relevance and implementation of the VFM report recommendations. → By embracing the opportunity of the evaluation. → By providing timely and relevant information to Government of Jersey and auditors. → By facilitating the opportunity for the auditors to understand our work and mandate. → By using the outcomes-based accountability framework to explain Authority purpose and approach to performance measurement. → By reviewing the results and the prioritisation of the recommendations.	↔

Risk Description	How we manage the risk	Movement of the Risk
Political Political unrest and wars in Ukraine and Israel-Gaza. Risks → Cyber implications. → Economic costs. Political instability and unpredictable landscapes.	→ By liaising with stakeholders. → By horizon scanning.	↔
Operational Asset management, software and hardware security	→ By achieving proportionate and relevant accredited security standards. → With routine testing, maintenance, asset replacement and training in terms of equipment, systems and processes.	↔
Operational Annual recurring uncertainty of Government of Jersey (GoJ) grant monies and impact on our operational activities. Any changes or absence of fee/grant monies from Government impacts on our ability to plan effectively and could impact on our ability to deliver our regulatory mandate.	→ Through prudent budgeting and spending. → By monitoring and analysing registration data and revenues. → By maintaining proactive liaison with Government of Jersey to progress fee discussions in order for GoJ to contribute financially to the provision of data protection regulation in Jersey.	↔
Operational Talent Management, Retention and Succession Planning. Maintaining a capable and knowledgeable team. It is essential that the statutory functions of the Jersey Data Protection Authority are fulfilled to the highest standard to maintain credibility and trust.	→ By embedding succession planning throughout the organisation. → By building skills and knowledge through personal and professional development. → By aligning our Organisational Development strategy with our mandate and strategic outcomes. → By striving for diversity and inclusion throughout our activities. By aligning our training and development with our succession planning and performance management.	↑
Operational Training and Development. It is essential the JOIC maintains sufficient and progressive knowledge to avoid poor quality advice/regulation. Financial uncertainty limits budget and resources for training and development.	→ We have a constantly evolving learning and development programme. → By ensuring personal training plans are in place, manage expectations. → By ensuring job descriptions are up to date and understood. → By implementing a Competency framework to establish the core (general) competencies needed to succeed in each role. → By aligning with talent and succession management, performance management (OBA) and career opportunities.	↑

Risk Description	How we manage the risk	Movement of the Risk
Legal and Regulatory Perception – industry, public and Government perception that our effectiveness, as a regulator, is based solely on our fining and public statement actions.	→ By publishing quarterly newsletters – explaining enforcement. → By increasing prominence on website of decisions taken. → By continuing JOIC's focus is on outcomes-based regulation. → By enforcing with appropriate and proportional enforcement sanctions as per our **Regulatory Action and Enforcement Policy.** → By maintaining a consistent and compliant investigation, inquiry, and audit processes. → By adopting Outcomes Based Accountability (OBA) measures to report on enforcement activity. → By adopting outcomes-based regulation.	↓
Strategic Developing relevant management information on data protection trends. The absence of relevant and timely information impacts on service performance, informed decision making and relevant strategic outcomes.	→ By continuously monitoring and interpreting our operational data to understand local trends and lessons learned. And by creating baselines for most vital areas to track. → With ongoing horizon scanning. → With collaboration and effective stakeholder management. → By measuring the impacts of resources in relation to Business Plan and Statutory Obligations. → By considering the most effective options for gathering information and tracking progress/improvement.	↔
Strategic The potential impacts of some Ministerial decisions and Data Protection implications therein. Data protection risks not evaluated and potential impact on Jersey's reputation.	→ By maintaining effective stakeholder management with GoJ/policy leads.	↔
Strategic Changes in key GoJ relationships, especially in either or both of the Policy Principal and Senior Policy roles. Such changes impact on relationship management and relevant knowledge.	→ We maintain constructive communications with key personnel. → By clarifying and recording decisions/requests.	↔
Strategic The impacts of the new U.S. Administration on privacy frameworks and relevant bodies.	→ By horizon scanning. → Through collaboration at the international level.	↔
Operational Any changes to legislation around AML and Combating Financing of Terrorism could reduce number of companies administered in Jersey could reduce our revenue income.	→ Monitor with help from the JDPA and JSFC.	↔

Risk Description	How we manage the risk	Movement of the Risk
Legal & Regulatory Internal compliance – failing to comply with the Data Protection Authority (Jersey) Law 2018 in terms of case management, process and reasonableness of decisions made.	→ We understand our compliance obligations and what this looks like on a practical level. → By monitoring how we implement and sustain our obligations. → By having effective and ongoing training, staff feedback, internal audits and reviews. → By deploying technology to help us achieve statutory deadlines.	↓
Legal & Regulatory JOIC Internal Compliance how we operate and how we are looking after the team, due diligence etc. with regard to: → Employment (Jersey) Law 2003. → Discrimination (Jersey) Law 2013 → Data Protection (Jersey) Law 2018. → Freedom of Information (Jersey) Law 2011. → Data Protection Authority (Jersey) Law 2018. → Health and Safety at Work (Jersey) Law 1989.	Ongoing. → Ensure we understand our compliance obligations and what this looks like on a practical level. → By monitoring how we implement and sustain our obligations. By implementing effective and ongoing: → Induction → Training → Recruitment → Review of processes → Staff feedback → Internal Audits	↔
Governance Poor Stakeholder relations – impacting on inclusion in projects and Island decisions	→ By managing stakeholder communications and working relationships by listening and measuring feedback. → By managing stakeholder communications and mapping plan and listen and measure feedback.	↔
Operational Cyber threat and Information Security. The Authority recognises that it is a target for cyber threats.	→ By ensuring that critical applications are only accessible through secure portals requiring layered authentication. → By employing industry best practices as a fundamental part of our cyber security policies, processes, software and hardware. → By ensuring we maintain ongoing Cyber awareness training within our team.	↔
Legal & Regulatory Appeal of JDPA/JOIC investigatory decisions to the Royal Court. Risk of public scrutiny of JDPA/JOIC processes and procedures and potential reputational credibility. Plus, cost implications.	→ By ensuring we maintain a stringent case management process. → In timely engagement of legal support in appropriate cases. → With regular and ongoing training. → With timely and transparent communication. → By focusing on our regulatory functions.	↔
Governance Authority Talent Management and Retention.	→ We ensure that we have in place timely JDPA succession planning and an Authority recruitment plan for 2026/7. → JDPA effectiveness reviews to be ongoing. → By maintaining data protection expertise within the Authority. → By maintaining local members to provide for an understanding of unique local landscape in which JDPA operates.	↔

JOIC®

JERSEY OFFICE OF THE
INFORMATION COMMISSIONER

+44 (0) 1534 716 530

2nd Floor, 5 Castle Street,
St. Helier, Jersey, JE2 3BT

www.jerseyoic.org