



JERSEY OFFICE OF THE INFORMATION COMMISSIONER

# ANNUAL REPORT

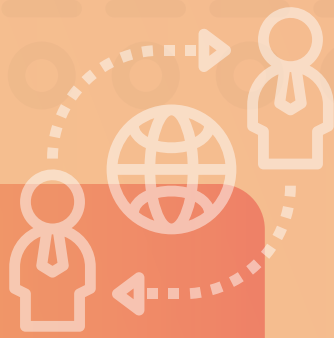
Fulfilling the obligations of the Authority under Article 44 of the Data Protection Authority (Jersey) Law 2018 and the Information Commissioner under Article 43 of the Freedom of Information (Jersey) Law 2011.

# THE CONTENTS

04 - 05	HIGHLIGHTS
06 - 09	THE JERSEY DATA PROTECTION AUTHORITY
10 - 11	CHAIR REPORT
12 - 15	INFORMATION COMMISSIONER'S FOREWORD
16 - 27	THE JERSEY DATA PROTECTION AUTHORITY
28 - 33	PRINCIPAL & EMERGING RISKS
34 - 37	PERFORMANCE REPORT
38 - 53	ENFORCEMENT AND COMPLIANCE
54 - 65	COMMUNICATIONS, ENGAGEMENT AND OUTREACH
66 - 71	46th GLOBAL PRIVACY ASSEMBLY
72 - 73	ENVIRONMENTAL, SOCIAL AND GOVERNANCE
74 - 77	PEOPLE AND ORGANISATIONAL DEVELOPMENT
78 - 83	FINANCE OVERVIEW
84 - 103	AUDITED FINANCIAL STATEMENTS



# 2024 HIGHLIGHTS



22

CASES **RESOLVED**  
**INFORMALLY** VIA  
AMICABLE RESOLUTION

JERSEY RETAINS  
EU COMMISSION  
**ADEQUACY STATUS**

COMPLETED  
**54**  
VIRTUAL  
COMPLIANCE  
AUDITS

DATA PROTECTION REGISTRATIONS  
INCREASED BY

**4.5%**

FROM 7,366 IN 2023 TO  
**7,697 IN 2024**

RESPONDED TO

**184**

SELF-REPORTED DATA BREACHES

ENGAGED WITH OVER A

**1/4**

OF JERSEY'S YOUNG  
PEOPLE

**99%**

OF DATA CONTROLLERS/PROCESSORS THAT  
ATTENDED A JOIC OUTREACH SESSION SAID THEIR  
**KNOWLEDGE OF DATA PROTECTION  
OBLIGATIONS IMPROVED FOLLOWING IT**

**86%**

OF YOUNG PEOPLE WE ENGAGED WITH SAID THEIR  
**KNOWLEDGE OF JOIC, PROTECTION  
OF THEIR PERSONAL DATA &  
UNDERSTANDING OF THEIR  
PERSONAL DATA RIGHTS IMPROVED  
AS A RESULT**

OF THE  
COMPLAINTS  
CLOSED IN 2024

<b>31%</b> were investigated and a breach determination made.	<b>4%</b> were investigated and resulted in a no breach determination
<b>47%</b> were not investigated, as per Part 4, Art. 20(2) of the DPJL 2018, sets out the basis upon which we investigate or reject the complaint	<b>17%</b> were withdrawn 

HOSTED

GLOBAL  
PRIVACY  
ASSEMBLY

28 | 10 | 24 —————> 01 | 11 | 24 —————> JERSEY, CHANNEL ISLANDS

**500** DELEGATES  
**70** COUNTRIES  
**80** SPEAKERS  
OVER 3 DAYS



# 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.

The Information Commissioner has separate responsibility for regulating the Freedom of Information (Jersey) Law 2011 (the FoI Law). This includes encouraging public authorities to follow good practice in their implementation of that law (including adherence to the relevant code of practice) and helping to promote transparency by supplying the public with information about the law and advice and guidance on how to exercise their rights.

## 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.

## OUR VALUES

Our values are hugely important to us, they create our identity and inform how we operate. We created our values to be more than words on a page, using them to guide decisions, select behaviours and drive continuous improvement in our service. Our values apply to us all, regardless of rank and flow through each area of our service, every day.

## OUR PURPOSE

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

### We are Fair.



We treat people equally, without favouritism or discrimination. We are impartial in our activities and free from bias or dishonesty. We are competent, reliable and respectful. Our decisions are open, honest and rationalised by a sound evidence base to promote integrity and trust.

### We are Collegial.



We share responsibility, including being honest and fair in our conduct towards others. We are willing to be judged on our performance. We work together to achieve our strategic outcomes. A collaborative approach allows us to work effectively together or individually. We communicate clearly, actively listen to others, take responsibility for mistakes and respect the diversity of our team. We demonstrate impartiality and accountability.

### We are Respectful.



We respect those we work and liaise with; this means that we actively listen to others and behave considerately towards others. We have self-respect and make responsible choices in what we say and do, to reach personal and organisational outcomes. We treat others in the way we want to be treated.

### We are Energetic.



We are enthusiastic and approach our activities with vigour and vitality.





# STRATEGIC OUTCOMES

## 01 Achieving and maintaining the highest standard of data protection in Jersey.



- a. Our purpose demands the highest standards of data protection for our citizens, and those who interact with Jersey, remembering that our Laws (like GDPR) have extra-territorial scope.
  - b. It is also important to remember that as a fundamental human right, data protection is intrinsically linked to well-being, mental health, reducing inequalities and improving living standards. All of these areas are key elements of the Island’s collective strategy in the coming years.
- committed to achieving and maintaining the highest standards of data protection. However, we cannot do this alone. We will continue to engage with all sectors of our community, such as charities, government, local businesses and youth groups (including both primary and secondary schools) to reach young people. Our deliverables in this area support our aim to be an exemplar and a source of leadership to our stakeholders. This in turn helps them to understand their role and their responsibilities, so that they too can deliver the highest standards of data protection.

This outcome covers all areas of our organisation and those who we are here to serve and support. From delivering proactive day to day guidance and resources, to forging ahead with our outreach and education programmes, to specific enforcement initiatives, such as targeted audits, we are

## 02 Maximising technological and economic opportunities to enhance the Island’s reputation as a safe place to host personal data and do business.



- a. Jersey is a unique jurisdiction where regulation (including in respect of personal data) is already entrenched in our society (particularly in the finance sector). It will be critical for our economy to ensure that Jersey remains at the leading edge; monitoring international legislative frameworks, trading corridors and innovation to ensure Jersey can act fast and seize opportunities that both grow and preserve our already strong reputation for data protection and privacy more widely.
  - b. Our strong relationships with relevant stakeholders in the digital sector and Government of Jersey have enabled us to participate in a major project on the feasibility of Data Stewardship services in Jersey. These and similar concepts can provide exciting opportunities for Jersey where the Island can be seen as a world leader. We are key stakeholders in those discussions.
- Proactively identifying relevant developments in the field of data protection, such as new and emerging technologies, economic or social change, our deliverables in this area start at grassroots level, with the aim of helping our stakeholders to ensure they have solid foundations, minimise risk and are alert to both future threats and opportunities. As a small but agile team, a key focus is on understanding the emerging landscape, working collegially with key change agents and providing thought leadership to facilitate positive change.
- This includes our ongoing responsibility to maintain an awareness of regulatory and legal changes which may impact on privacy and data protection in Jersey and to contribute to our ability to navigate new privacy frontiers.

## 03 Protecting our future generations by putting children and young people first.



- a. Given the exponential advances and uses of technology, it is critical, now more than ever, that we take steps to educate children on how online behaviours can affect their opportunities in later life and equip them with the tools to protect themselves against the many harms associated with growing-up in a digital environment, including educating on social media use, online gaming and the darker sides of the internet.
  - b. Equally, many of these young people will be our future digital innovators. It is incumbent upon us to help them embrace technological innovation in a safe way, and work with them to improve their own broader skills so as to ensure that Jersey remains not only a safe place to live, but also an exciting, attractive and progressive Island in which to do business.
  - c. Highlighting children is not at the exclusion of adult populations within our community. We respect all members of our community whilst recognising that some populations may be at higher risk and need greater protection. Our role as regulator is to ensure that we target our support accordingly and apply the Law in a fair and consistent manner, protecting those who need it most.
- In working towards this outcome, our deliverables build on our already strong relationships with the Island’s schools, through further development and wider roll-out of our education programme. Through specific targeted outreach campaigns, we will continue to raise children’s awareness of their data protection rights, whilst alerting them to the potential risks of their online and other activities.

# 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 2024. This fulfils our statutory obligation under Article 44 of the DPAJL 2018.

My term as Chair began in October 2024 on the retirement of the preeminent international data protection leader Jacob Kohnstamm, former Data Protection Commissioner of the Netherlands, who served as Authority Chair since the inception of the Authority in 2018.

During Jacob's tenure, he and his fellow Authority Members navigated the Jersey Office of the Information Commissioner (JOIC) through an unprecedented period of growth and change in terms of expertise, capacity and head count. He recruited highly respected Information Commissioners Dr. Jay Fedorak (2018-2021) and Paul Vane (2021 to present). Both of these leaders brought extensive practical experience, integrity and passion to their work.

As Chair, Jacob worked tirelessly with Government of Jersey, establishing a respectful relationship and establishing in law a fee model for private sector organisations which provides a large proportion of the funding for the JOIC to carry out its mandated

regulatory functions and supporting the private sector in compliance with the law. We are now in discussions with the Jersey Government to establish a Partnership Agreement which ensures that the public sector bodies also pay their fair share of the resources necessary for overseeing data protection in the public sector. I am hopeful that we will reach a long-term solution soon.

At the end of 2024, we felt the loss of the most senior authority member, Gailina Liew, who served from 2018 to 2024 and brought extensive local and international thought leadership in board governance. I will miss her wise counsel, and her ability to enculturate me to the Jersey environment. But with a balance of local and international experts serving on the authority, Paul Routier MBE, Helen Hatton, Stephen Bolinger and Paul Breitbarth, we are in good shape to face the challenges of advanced technology and an unsettled geopolitical environment.

The focus of our attention for 2024 was our hosting of the Global Privacy Assembly Annual Conference in October. For our Authority, and for the Island of Jersey, it was a huge honour of momentous proportions. The Office has grown in stature, recognised for its work on an international stage and participating in privacy discussion on a global

Throughout 2024, we engaged with 26% of the total population of Jersey's under 18s. 86% of the young people we engaged with said their 'knowledge of JOIC, protection of their personal data and understanding of their personal data rights improved as a result of participating in one of our outreach sessions'. The work outlined in this report



**The focus of our attention for 2024 was our hosting of the GPA Conference. It was a huge honour of momentous proportions. The Office has grown in stature, recognised for its work on an international stage.**

scale. Few jurisdictions get the opportunity to host this prestigious conference, attracting data protection authorities and private sector companies across the world. It was with pride and home-grown Jersey flavour that we hosted a hugely successful conference, attracting 500 participants and providing a platform and unique, engaging agenda for professionals from all corners of the globe. We discussed the challenges of new and disruptive technologies and how they can be harnessed to improve society, business and government while protecting the agency and dignity of individuals and groups. AI governance and modern technologies will be one of our strategic priorities for 2025.

The number of data protection complaints and enquiries remain constant (average 85) since the introduction of the Data Protection (Jersey) Law 2018 along with self-reported data protection breaches which average 217 annually.

demonstrates a modern, independent Regulatory Authority that has the confidence to take on the data protection issues of the day and ensure that its work is relevant to Jersey businesses, government, and citizens. This will be a particular focus in 2025.

The JOIC is well placed to ensure that data is managed, protected, and respected to unlock technological innovation that will be key to Jersey's economy. Data protection is about trust: the opportunities that are before us today will only be realised where people trust their data will be used fairly and transparently. In my first Annual Report as Chair of the JDPA, I will conclude with a simple note of thanks to the Minister and Assistant Minister for Sustainable Economic Development, Commissioner Paul Vane and his team. It is a privilege to collaborate with this outstanding team and colleagues and I look forward to the year ahead.

**Elizabeth Denham CBE**  
Chair, Jersey Data Protection Authority



# INFORMATION COMMISSIONER'S FOREWORD

**Paul Vane**  
INFORMATION COMMISSIONER

Data protection is the cornerstone of public trust in our economy. As technology advances and data-driven innovation expands, individuals must have confidence that their personal data is handled responsibly, securely, and transparently. At the JOIC, our role is to uphold the highest standards of data protection, ensuring that organisations remain accountable, enforcement is effective, and above all, people's rights are safeguarded.



Jersey is well situated as a safe place to do business with both the EU Adequacy decision and the UK Government's confirmation in late 2023 that Jersey has the necessary data protection and privacy standards needed to safeguard UK personal data, enabling the transfer of personal data without the need for further safeguards or specific authorisation is welcomed and reassuring to the business community. The local data protection laws and in particular the Authority's mandate and regulatory activities are essential pillars to these adequacy decisions which permit businesses to transfer personal data and thrive for the Jersey economy.

Over the past year, we have continued to strengthen our regulatory approach, working closely with businesses, policymakers and the public to promote compliance and best practices through our ethos of outcome-based regulation. The evolving landscape of data protection laws across the globe reflects the growing importance of privacy in modern society, and we remain committed to ensuring that these laws are not only adhered to but also understood and embedded into organisational culture.

## ACCOUNTABILITY AND ENFORCEMENT

Accountability is fundamental to a fair and trustworthy data ecosystem. Organisations must take proactive steps to ensure they meet their obligations - protecting data by design, being transparent with individuals, and fostering a culture of compliance by adopting the mindset of doing the right thing. We continue to support businesses in achieving these goals through clear guidance, robust frameworks and ongoing engagement, helping them navigate their regulatory requirements while maintaining high ethical standards.

Regulation must be backed by meaningful enforcement. In 2024, we have taken decisive action where necessary and proportionate, ensuring that non-compliance carries real consequences whilst at the same time ensuring the best possible outcome for the individual affected. At the same time, our focus is on prevention - helping organisations understand their responsibilities before issues arise, promoting self-regulation, and encouraging the adoption of privacy-first practices.

From all the cases investigated and closed in 2024, the Authority were requested to consider issuing administrative fines to two data controllers. The

“  
**The evolving landscape of data protection laws across the globe reflects the growing importance of privacy in modern society, and we remain committed to ensuring that these laws are not only adhered to but also understood and embedded into organisational culture.**

Authority noted that in both cases the aggravating factors warranted the issuing of a fine as set out in the Regulatory Action and Enforcement Policy.<sup>1</sup>

Our Law currently prevents us from publishing specific details of reprimands and orders we have issued, but that does not take away from our belief that strong enforcement builds public trust and confidence, demonstrating that data protection is not optional but a fundamental right.

<sup>1</sup> <https://jerseyoic.org/media/l5sfz1s0/joic-regulatory-action-and-enforcement-policy.pdf>

# PROTECTING PEOPLE AND DELIVERING VALUE

Above all, our mission is to protect people. I have often said that we are ‘people protectors’ and not just a data protection regulator. Individuals deserve control over their personal data, clarity on how it is used, and the assurance that their rights will be upheld. We continue to advocate for greater transparency, fairness, and security in data privacy practices, ensuring that privacy is a core principle instilled from the outset rather than an afterthought.

At the same time, we are committed to delivering excellent value for money in everything we do. We operate efficiently, prioritising resources in our small team to where they have the greatest impact - whether through targeted investigations, guidance that prevents costly non-compliance, or collaborative initiatives that strengthen industry-wide standards. By adopting innovative regulatory approaches, leveraging technology, and continuously improving our processes, we ensure that every pound spent translates into stronger data protection and privacy outcomes for individuals, businesses, and our society as a whole.

## INTERNATIONAL COLLABORATION

In January 2024 the EU Commission published the Adequacy Review report of the functioning of the adequacy decisions. The report contained ‘the Commission on the first review of the adequacy decisions that were adopted on the basis of Article 25(6) of Directive 95/46/EC1 (Data Protection Directive)’.

We were delighted to read that the ‘Commission determined that eleven countries or territories ensure an adequate level of protection for personal data transferred from the European Union’ which included Jersey.

The EU Commission made particular reference in the report to

*‘the developments in the Jersey legal framework since the adoption of the adequacy decision, including legislative amendments, case law and activities of oversight bodies, which have contributed to an increased level of data protection. In particular, Jersey has significantly*

*modernised its data protection framework by adopting the Data Protection (Jersey) Law 2018 and the Data Protection Authority (Jersey) Law 2018 which entered into force in 2018 and align the Jersey regime closely with the GDPR.*

*In the area of government access to personal data, public authorities in Jersey are subject to clear, precise and accessible rules under which such authorities can access and subsequently use for public interest objectives, in particular for criminal law enforcement and national security purposes, data transferred from the EU. These limitations and safeguards follow from the overarching legal framework and international commitments, notably the ECHR and Convention 108, as well as from Jersey data protection rules, including the specific provisions for the processing of personal data in the law enforcement context set out in the Data Protection (Jersey) Law 2018, as modified by Schedule 1 to that Law. In addition, Jersey law imposes a number of specific limitations on the access to and use of personal data for criminal law enforcement and national security purposes, and it provides oversight and redress mechanisms in this area.*

*Based on the overall findings set out in the SWD, the Commission concludes that Jersey continues to provide an adequate level of protection for personal data transferred from the EU.’*

We are delighted to be participating in a series of high-level roundtable discussions which the European Commission is undertaking with all countries who provide an adequate level of protection for personal data.

The EU Commissioner identified that the adequate countries form one of the world’s broadest networks for safe and free data flows and that in today’s world, cross-border data flows are an integral part of our economy and daily lives. To this end he set in motion a series of discussions commencing in March 2024.

The EU Commissioner identified that the shared commitments have already led to significant benefits for individuals, businesses, and our economies. The priority is to build on these achievements and further strengthen our cooperation in promoting trusted flows. ‘With the development of Artificial Intelligence and global challenges arising from new technologies, our collaboration at bilateral and international level is more crucial than ever. I would like to increase our engagement in these matters, by discussing how we can maximise the benefits of our

partnership on data flows, and explore new avenues for joint actions, including through enforcement cooperation.’

Jersey has actively participated at each roundtable discussion which have focussed on data flows, tools to promote and facilitate compliance by small and medium-sized companies and sharing information on activities of data brokers across borders.

The roundtable discussions are thought provoking and are generating broader understanding between adequate countries, shared learning and collaboration.

It would be remiss of me not to mention our international activities, and in particular the success of last year’s Global Privacy Assembly which we had the honour of hosting in Jersey. Amongst some key outcomes identified, simplifying the complex global regulatory environment and encouraging more effective collaboration were key themes discussed. Also highlighted was the need to do more involving young people as well as how to address the real harms associated with failures of basic data privacy. The message was clear. Privacy is a fundamental human right and needs to be accessible for all humanity. Too many people are denied the opportunity to be treated fairly and equally, just because of their culture, geography, disability or gender.

The success of the week also highlighted the strength and quality of our local service industry, many of whom were involved in providing an exceptional experience for the 500 or more visiting delegates. Jersey is blessed with some incredible talent, and I was delighted to see an Island business community coming together to show off the best of Jersey. Equally pleasing was seeing full hotels and restaurants, a busy transport network, increased retail spending and hearing our visitors’ feedback and desire to return to Jersey, all of which will have provided a significant injection to the local economy at a normally quiet period in the year. I must extend my heartfelt thanks to all those involved, including my JOIC team and our event organisers who all ensured the delivery of an exceptional event and helped cement the longer-term prosperity of our Island.

## THE FUTURE

Looking ahead, we will continue to evolve alongside the ever-changing digital landscape, ensuring that data protection remains at the heart of a fair, competitive, and trusted digital economy. By working together - regulators, businesses, and individuals—we can create a future where privacy and innovation go hand in hand, building a digital environment that works for everyone.

In the early part of 2025, we will be setting our strategy for the next three years and taking on board the outcomes and actions from the GPA Conference in October. Jersey has an opportunity to be a leader in many respects, our geographical size proving time and time again that we can operate on a global stage and be noticed.

Finally, I would like to extend a warm welcome to our new Chair, Elizabeth Denham CBE, who brings with her a wealth of knowledge, experience, expertise and wisdom to our Authority. I am very much looking forward to working closely with Elizabeth and our Authority Members to further the excellent work of my JOIC team, in whom I remain immensely proud and grateful for their tireless efforts.

**Paul Vane**  
Information Commissioner







# THE JERSEY DATA PROTECTION AUTHORITY

The Authority is a statutory body which oversees the protection of personal data. The Authority consists of the Chair, and as per Article 3 of the DPAJL 2018 ‘no fewer than 3 and no more than 8 other voting members’ and the Information Commissioner as an ex officio and non-voting member.

The Chair and voting members are appointed by the Minister. The Information Commissioner is the Chief Executive and:

- a** is responsible for managing the other employees of the Authority.
- b** is in charge of the day-to-day operations of the Authority.
- c** has the functions conferred or imposed on him or her by the Law and any other enactment.

The Information Commissioner, on behalf of the Authority, undertakes the functions of the Authority under the DPAJL 2018 and the DPJL 2018 other than the issuing of a public statement under Article 14 and the making of an order to pay an administrative fine under Article 26 of the DPAJL 2018, or any other function specified by the Authority by written notice to the Information Commissioner.

The Authority is established to undertake a variety of key activities which includes promoting public awareness of risks and rights in relation to processing, especially in relation to children and to raise awareness for controllers and processors of their obligations under the data protection laws. It is also incumbent upon the Authority to report to Government on the operation of the data protection laws and to advise the Minister and the States of Jersey on any amendments that the Authority considers should be made to the laws.

All of the Authority’s functions must be performed independently and free from direct or indirect external influence.

The Authority’s activities regularly involve collaboration with local and international partners, sharing expertise in data protection, regulation and financial services. The Authority has established positive working relationships with local Government, public authorities, private sector stakeholders and international partners characterised by collaboration and respect. The Authority is strongly purpose-driven, thus both the strategic outcomes and business planning processes are more than just words on a page. The Authority and in turn data protection are pivotal in helping to engender trust and confidence in the Jersey economy. By safeguarding personal and sensitive information, we contribute to the foundation of trust upon which Jersey’s economy thrives.



**JOIC**  
**JERSEY OFFICE OF THE  
INFORMATION COMMISSIONER**



# Governance, Accountability and Transparency

## THE DATA PROTECTION AUTHORITY

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 of 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. Similarly, 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

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

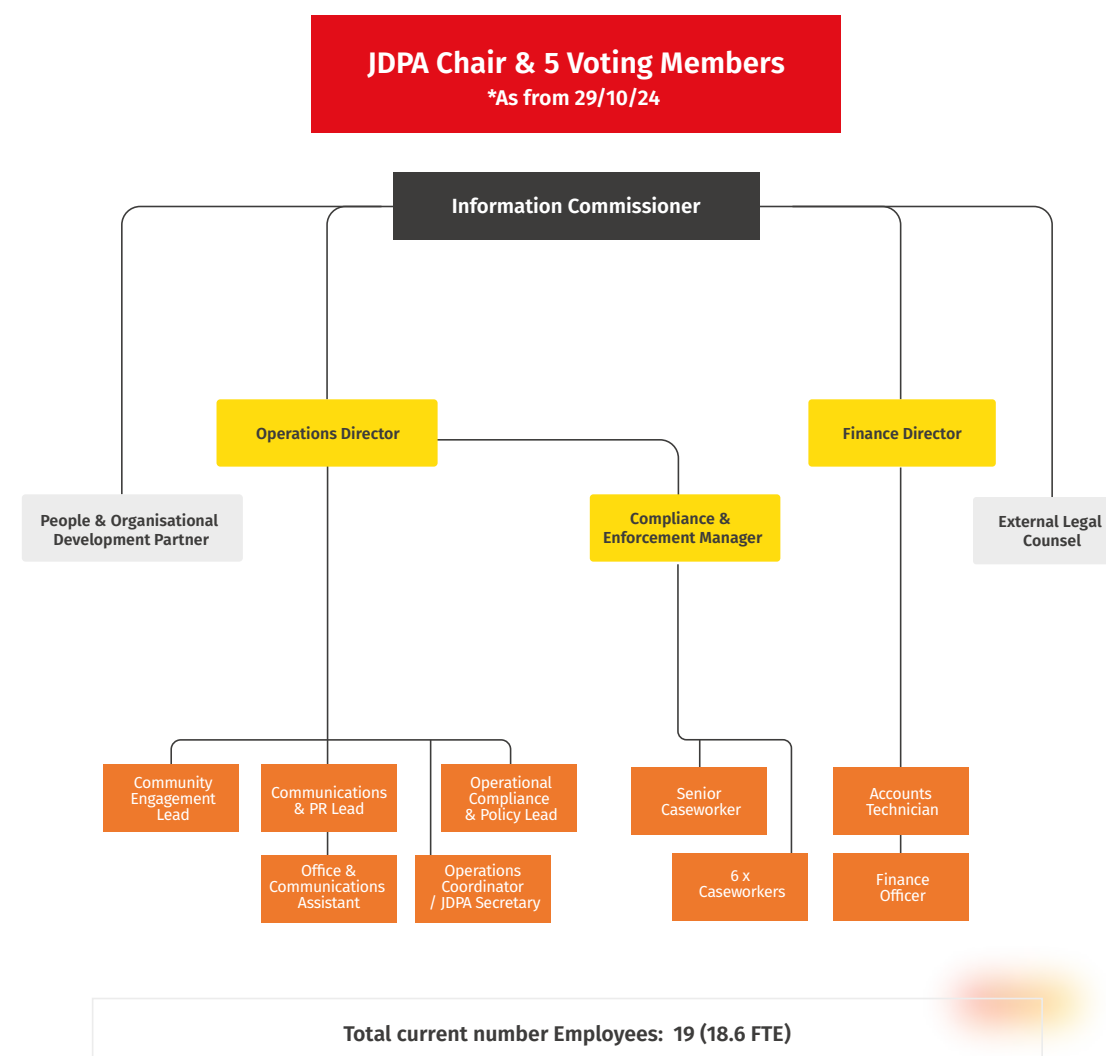
As members are appointed by the Minister, the Chair wrote to the Minister in June 2022 to request he consider appointing Members for a four-year term of office. Given that Article 3(5) of the DPAJL 2018 also sets out the duration of the term of office of appointed Authority Members:

- 5 Each voting member is appointed for a term of 5 years or such shorter period as the Minister thinks fit in a particular case and is eligible for reappointment up to a maximum period of service of 9 years.

Since the Authority's inception, the Minister appointed Authority Members on a three-year term. To allow for maximum contribution and stability, a four-year term was deemed as more suitable, allowing sufficient time to deliver the best value, without risking a lack of diversity in thinking.

The Minister approved this request on 13 November 2023 in R.169 presented to the States Assembly.<sup>2</sup>

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 taken back to the main Authority meetings.



<sup>2</sup> <https://statesassembly.je/publications/assembly-reports/2023/r-169-2023>



# Authority Members



CHAIR OF THE AUTHORITY (28 OCTOBER 2024 - PRESENT)

**Elizabeth Denham** CBE

TENURE

Elizabeth joined the Authority as of 1 May 2023 for a first term that is due to expire on 30 April 2027. Elizabeth applied for the position of Chair and following an open recruitment process, the Minister appointed Elizabeth as Chair. Elizabeth started her Chair appointment on 28 October 2024.



CHAIR OF THE AUTHORITY (MAY 2018 - 28 OCTOBER 2024)

**Jacob Kohnstamm**

TENURE

Jacob has been Chair of the Authority since May 2018. Jacob’s term of office was extended by the Minister, for six-months, as his replacement was recruited. The handover took place at the 46th Global Privacy Assembly conference on 28 October 2024.



VOTING AUTHORITY MEMBER

**Helen Hatton**

TENURE

Helen joined the Authority on 1 August 2019 for a period of three years and was reappointed for a second term which is due to expire on 31 July 2025.



VOTING AUTHORITY MEMBER

**Paul Routier** MBE

TENURE

Paul joined the Authority on 1 August 2019 for a period of three years and was reappointed for a second term which is due to expire on 31 July 2025.



VOTING AUTHORITY MEMBER

**Stephen Bolinger**

TENURE

Stephen joined the Authority on 1 May 2023 for a first term that is due to expire on 30 April 2027.



VOTING AUTHORITY MEMBER

**Paul Breitbarth**

TENURE

Paul joined the Authority as of 1 May 2023 for a first term that is due to expire on 30 April 2027.



VOTING AUTHORITY MEMBER

**Gailina Liew**

TENURE

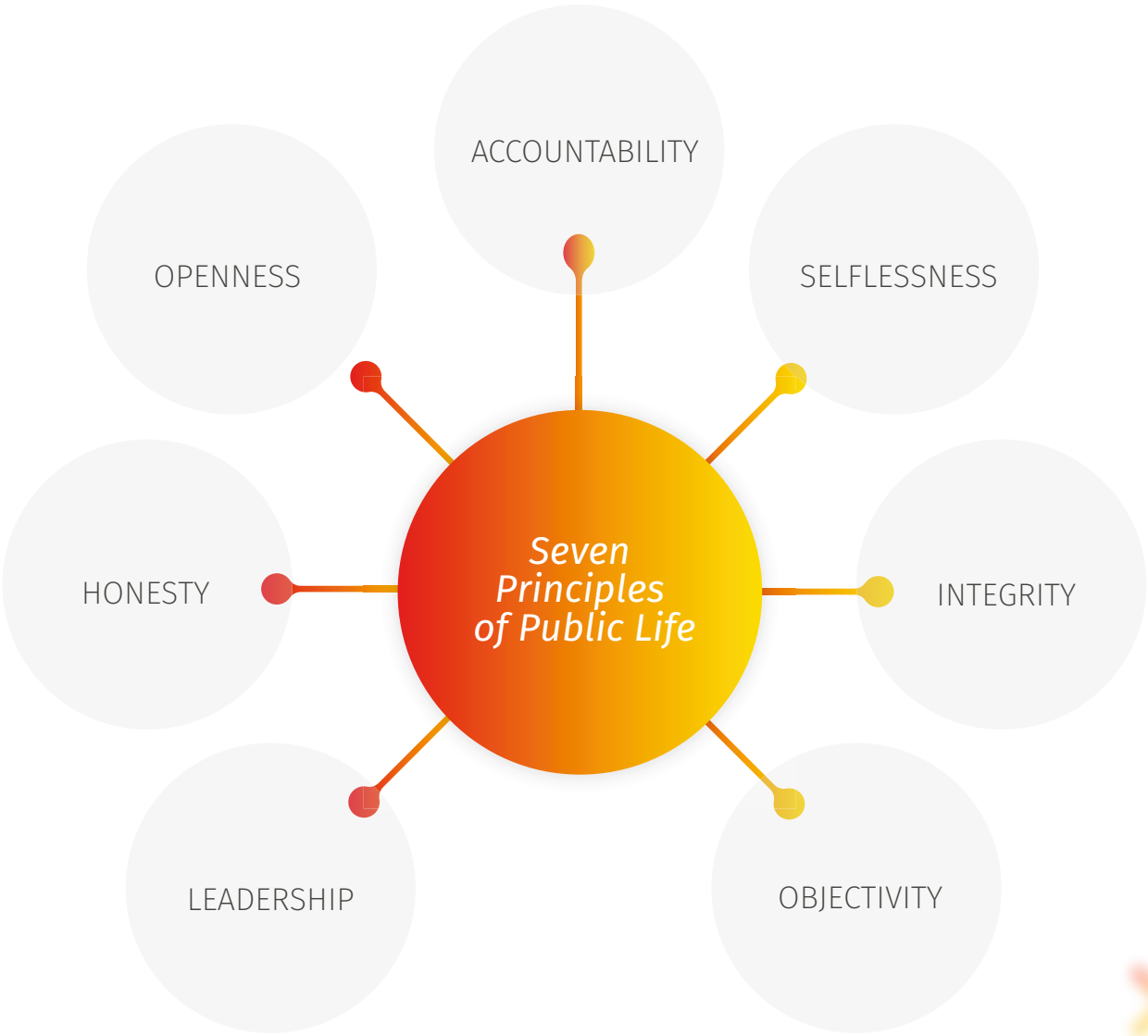
Gailina joined the Authority in October 2018 for a period of three years and was reappointed for a second term which expired on 28 October 2024.

Further details regarding the Authority members external appointments can be found at <https://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)
- Paul Breitbarth joined ARC on the 12 July 2023 meeting date.
- Christine Walwyn (Co-opted accountant, Non-voting)

The ARC’s mandate is to advise and make recommendations to the Authority. The purpose of the ARC is to:

- Assist the Authority in its oversight of the integrity of its financial reporting, including supporting the Authority in meeting its responsibilities regarding financial statements and the financial reporting systems and internal controls.
- Monitor, on behalf of the Authority, the effectiveness and objectivity of external auditors.
- Provide input to the Authority in its assessment of risks and determination of risk appetite as part of the overall setting of strategy.
- Assist the Authority in its oversight of its risk management framework.

## GOVERNANCE COMMITTEE

The voting members who comprise the Governance Committee are:

- Gailina Liew (Chair)
- Jacob Kohnstamm
- Elizabeth Denham CBE joined at Governance Committee meeting on 29 June 2023.
- Stephen Bolinger joined the Governance Committee at the meeting on 16 October 2024.

The membership of this Committee is currently under review as the JDPA heads into 2025.

The Governance Committee’s mandate is to advise and make recommendations to the Authority. The purpose of the Governance Committee is to:

- Keep the Authority’s corporate governance arrangements under review and make appropriate recommendations to ensure that the Authority’s arrangements are, where appropriate, consistent with best practice corporate governance standards.
- Review the balance, structure and composition of the Authority and its committees. Its role also encompasses the selection and appointment of the Authority’s senior executive officers and voting members of the Authority and giving full consideration to succession planning and the skills and expertise required to lead and manage the Authority in the future.
- Evaluate the performance of Authority members on a regular basis as described more fully later in this report.



# REMUNERATION & HUMAN RESOURCES COMMITTEE (R&HR)

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

- Paul Routier MBE (Chair)
- Jacob Kohnstamm
- Stephen Bolinger joined R&HR on 3 November 2023 meeting date.

The R&HR Committee is mandated to advise and make recommendations to the Authority, with the purpose of:

- Assisting the Authority in ensuring that the Authority and Executive retain an appropriate structure, size and balance of skills to support the organisation’s strategic outcomes and values.
  - Assisting the Authority in meeting its responsibilities regarding the determination, implementation and oversight of remuneration arrangements to enable the recruitment, motivation and retention of employees generally.
  - Overseeing arrangements for appointments
- (including recruitment processes) and succession planning.
- Assisting the Authority by reviewing and making recommendations in respect of the remuneration policies and framework for all staff.

Each Sub-Committee Chair reports back to the Authority, making recommendations for consideration.

The following table sets out the number of full Authority and Sub-Committee meetings held during 2024, and the number of meetings attended by each voting Authority member.

## JDPA MEETINGS

	Elizabeth Denham CBE	Jacob Kohnstamm	Helen Hatton	Gailina Liew	Paul Breitbarth	Paul Routier MBE	Stephen Bolinger	Christine Walwyn
1 March 2024	✓ <i>Via Video</i>	✓	✓	✓	✓	✓	✓	X
27 March 2024 <i>Virtual Meeting</i>	✓	✓	✓	✓	✓	✓	✓	X
29 May 2024	✓	✓	✓	✓	✓	✓	✓	X
21 August 2024 <i>Hybrid Meeting</i>	✓ <i>Via Video</i>	✓	✓ <i>Via Video</i>	✓	✓ <i>Via Video</i>	✓	✓ <i>Via Video</i>	X
28 October 2024	✓	✓	✓	✓	✓	✓	✓	X
22 November 2024	✓	X	✓ <i>Via Video</i>	<i>As an invited Guest only</i>	✓	✓	✓	X

## AUDIT & RISK

	Elizabeth Denham CBE	Jacob Kohnstamm	Helen Hatton	Gailina Liew	Paul Breitbarth	Paul Routier MBE	Stephen Bolinger	Christine Walwyn
14 February 2024 <i>Virtual Meeting</i>	X	X	✓	X	✓ <i>Via Video</i>	X	X	✓
27 March 2024	X	X	✓	X	✓ <i>Via Video</i>	X	X	✓
25 April 2024	X	X	✓	X	✓ <i>Via Video</i>	X	X	✓
29 July 2024	X	X	✓ <i>Via Video</i>	X	✓ <i>Via Video</i>	X	X	✓ <i>Via Video</i>
23 October 2024	X	X	X	X	✓ <i>Via Video</i>	X	X	✓

## GOVERNANCE

	Elizabeth Denham CBE	Jacob Kohnstamm	Helen Hatton	Gailina Liew	Paul Breitbarth	Paul Routier MBE	Stephen Bolinger	Christine Walwyn
23 April 2024	✓ <i>Via Video</i>	✓ <i>Via Video</i>	X	✓ <i>Via Video</i>	X	X	X	X
16 October 2024	✓	✓	X	✓	X	X	✓	X

## REMUNERATION & HR

	Elizabeth Denham CBE	Jacob Kohnstamm	Helen Hatton	Gailina Liew	Paul Breitbarth	Paul Routier MBE	Stephen Bolinger	Christine Walwyn
2 August 2024	X	✓ <i>Via Video</i>	X	X	X	✓ <i>Via Video</i>	✓ <i>Via Video</i>	X
25 October 2024	X	✓ <i>Via Video</i>	X	X	X	✓ <i>Via Video</i>	✓ <i>Via Video</i>	X

# 2024 AUTHORITY MEMBERS’ REMUNERATION

The Authority Voting Members received, in aggregate, £84,582.06 in remuneration in 2024. Further details regarding the Authority Voting Member remuneration can be found on page 83.

# JDPA PERFORMANCE EVALUATION AND RE-APPOINTMENTS

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

## 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.

## ANNUAL SELF-ASSESSMENT OF SKILLS

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.

## INDEPENDENT EXTERNAL REVIEW

An independent external review of overall Authority effectiveness, to be conducted every three years.

# JDPA PERFORMANCE EVALUATION

The Authority is committed to regularly evaluating and reporting on its governance and effectiveness. A key element of this process is the Independent External Review (IER) of the Authority, undertaken every three years to assess the Authority's overall performance.

The IER took place over a four-month period from January to April 2024. A local, specialist provider was engaged to support the Authority in assessing and measuring the overall effectiveness of its governance and culture.

The assessment utilised technology combined with expertise in people governance, to deliver a comprehensive and insightful evaluation. The process benefitted from the full cooperation of the Authority members and the JOIC, ensuring a collaborative and comprehensive review. The three main domains that made up the evaluation framework are.

- Culture.
- Decision-making.
- Implementation.

A draft report was completed in April 2024 and its findings were reviewed and approved by the Authority.

This thorough approach delivered valuable insights, essential to the Authority's commitment to continuous improvement. Under the leadership of the new JDPA Chair, the Authority plans to revisit and build on these findings in 2025 to strengthen governance, enhance organisational effectiveness, and drive progress towards its strategic outcomes.

# DIVERSITY OF THE JDPA

At the end of 2024 the Authority comprised of five members, 40% of JDPA members were female and 60% were male. Members range in age from early 40s to early 70s and represent five different nationalities. Authority members bring a diverse range of experience, formal education and professional qualifications, including expertise in data protection, law, governance, IT, business, education and teaching.



# PRINCIPAL & EMERGING RISKS

The Authority's primary obligation is to fulfil statutory responsibilities as the independent body promoting respect for private lives. The Authority's strategic outcomes support us in the fulfilment of our mandate.

The 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, who monitor risk movements and

mitigating actions and relevance to the strategic outcomes. 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 following table identifies the principal risks and mitigating actions. The risks are categorised into five main areas:

- 1 LEGAL & REGULATORY 
- 2 OPERATIONAL 
- 3 GOVERNANCE 
- 4 STRATEGIC 
- 5 POLITICAL 





Summary of Principal Risks

OPERATIONAL	RISK DESCRIPTION	HOW WE MANAGE THE RISK
	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.  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.	<ul style="list-style-type: none"><li>→ Monitor number of entities deregistering as the economy changes.</li><li>→ Monitor the actual registered entity revenues.</li><li>→ Monitor operational costs and revenues closely.</li><li>→ Monitor entity numbers, liaise with Statistics Jersey for data analysis.</li><li>→ Stakeholder relationships to gauge industry movements.</li><li>→ Seeking 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</li><li>→ Maintain liaison with Government to progress fee discussions to contribute financially to the provision of data protection regulation in Jersey.</li></ul>
	A potential change in the AML Jersey legislation could mean a significant reduction of administered entities in Jersey.	<ul style="list-style-type: none"><li>→ Monitor with support from the Jersey Financial Services Commission and the Authority.</li><li>→ MoneyVal report in the public domain and the findings were more positive than anticipated however we are monitoring the impact of the report, and this may result in changes to the volume of administered entities in Jersey.</li></ul>
	Asset management, software and hardware security.	<ul style="list-style-type: none"><li>→ Achieving proportionate and relevant accredited security standards.</li><li>→ Testing, maintenance, asset replacement, training.</li><li>→ Undertake relevant testing and maintenance.</li></ul>
	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.	<ul style="list-style-type: none"><li>→ Embedding succession planning throughout the organisation.</li><li>→ Building skills and knowledge through personal and professional development.</li><li>→ Aligning Human Resources strategy with our strategic outcomes.</li><li>→ Striving for diversity and inclusion throughout our operational and HR activities.</li><li>→ Align our training and development with our succession planning and performance management.</li></ul>
	Training and Development – Essential the JOIC maintains sufficient and progressive knowledge to avoid poor quality advice/regulation.  Financial uncertainty limits budget and resources for training and development.	<ul style="list-style-type: none"><li>→ We have a constantly evolving learning and development programme.</li><li>→ Ensure personal training plans are in place, manage expectations.</li><li>→ Ensure job descriptions are up to date and understood.</li><li>→ Implement a Competency framework to establish the core (general) competencies needed to succeed in each role.</li><li>→ Align with talent and succession management, performance management (OBA) and career opportunities.</li></ul>
	Cyber threat and Information Security. The Authority recognises that it is a target for cyber threats.	<ul style="list-style-type: none"><li>→ Critical applications are only accessible through secure portals requiring layered authentication.</li><li>→ We undertake Disaster Recovery exercises to test systems.</li><li>→ We employ industry best practices as a fundamental part of our cyber security policies, processes, software and hardware.</li><li>→ Cyber awareness training is ongoing within our team.</li></ul>

GOVERNANCE	RISK DESCRIPTION	HOW WE MANAGE THE RISK
	Poor Stakeholder relations – impacting on inclusion in projects and Island decisions.  Authority Talent Management and Retention.	<ul style="list-style-type: none"><li>→ Using Outcomes Based Accountability to engage key stakeholders and form like-minded partnerships.</li><li>→ The heightened awareness of JDPA/JOIC due to GPA Conference and Enforcement is slightly mitigating this risk.</li><li>→ Manage stakeholder communications and mapping plan and listen and measure feedback.</li><li>→ Genuine engagement and relationships.</li><li>→ JDPA Succession planning and Authority recruitment plan for 2025 to be considered and agreed by the JDPA by end Q1 2025.</li><li>→ JDPA effectiveness review (to be completed every 3 years) and internal skills review are well overdue.</li><li>→ Maintain data protection expertise within the Authority.</li><li>→ Maintain local members to provide for an understanding of unique local landscape in which JDPA operates.</li></ul>

LEGAL & REGULATORY	RISK DESCRIPTION	HOW WE MANAGE THE RISK
	Perception – industry and Government perception that our effectiveness as a regulator is based on our fining actions.	<ul style="list-style-type: none"><li>→ JOIC focus is on outcome-based regulation.</li><li>→ Enforcing appropriate and proportional enforcement sanctions.</li><li>→ Maintaining consistent and compliant investigation, inquiry, and audit processes.</li><li>→ Publication of quarterly newsletters – explaining enforcement.</li><li>→ Increased prominence on website of decisions taken.</li><li>→ Use Outcomes Based Accountability measures to report on enforcement activity.</li></ul>
	Internal compliance – failing to comply with the Data Protection Authority (Jersey) Law 2018 in terms of case management, process and reasonableness of decisions made.	<ul style="list-style-type: none"><li>→ Understand our compliance obligations and what this looks like on a practical level.</li><li>→ Monitor how we implement and sustain our obligations.</li><li>→ Put in place effective and ongoing training, staff feedback, internal audits and reviews.</li><li>→ Application of technology to help us achieve statutory deadlines.</li></ul>

Ongoing.

- Understand our compliance obligations and what this looks like on a practical level.
- Monitor how we implement and sustain our obligations.
- Put place effective and ongoing:
  - Training.
  - Induction.
  - Recruitment.
  - Review of processes.
  - Staff feedback.
  - Internal Audits.

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.



PRINCIPAL & EMERGING RISKS

<div>STRATEGIC</div>	RISK DESCRIPTION	HOW WE MANAGE THE RISK
	Hosting GPA International Conference in October 2024. Risks associated with the conference. • Financial exposure. • Reputational. • Impact on mandated activities.	<div>→ Detailed project management, including sponsorship and conference agenda to attract sufficient ticket sales.</div> <div>→ Ensure a resilient and relevant range of speakers and panellists.</div> <div>→ Monitor sponsorship monies/commitment carefully and share the financial risk with sponsors.</div> <div>→ Collaboration with the GPA.</div> <div>→ Managing local, national and international reputational risk.</div>
	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.	<div>→ Horizon Scanning.</div> <div>→ Stakeholder management.</div>
	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.	<div>→ Measuring the impacts of resources in relation to Business Plan and Statutory Obligations.</div> <div>→ Considering the most effective options for gathering information and tracking progress/improvement. Outcomes based accountability – who is better off?</div> <div>→ Horizon scanning.</div> <div>→ Creating baselines for most vital areas to track.</div>
	A potential lack of management information on data protection trends could impact decision making, planning and evaluating issues.	<div>→ Constant horizon scanning.</div> <div>→ Consider most effective options for gathering information and tracking progress/improvement.</div> <div>→ Create baselines for most vital areas to track.</div> <div>→ Measuring impact of resources in relation to Business Plan and Statutory Obligations.</div>



<div>POLITICAL</div>	RISK DESCRIPTION	HOW WE MANAGE THE RISK
	Failure to maintain Jersey Adequacy with the EU and UK.	<div>→ Adequacy approved with the EU in 2024 and the UK in 2023.</div> <div>→ Adequacy reviews are an ongoing process and activities by both the Authority and Government need to be cognisant of this.</div>
	Insufficient and/or unpredictable Government funding for Government data protection activities.	<div>→ Frequent reviews and provision of activity data.</div> <div>→ Protecting our independence as a key priority.</div> <div>→ Discussions have been ongoing since late 2020 to effect a change in the annual grant/fee Government contribution for data protection.</div> <div>→ Reviewing grant and working agreement.</div>
	The Value for Money Review being undertaken at the request of the GoJ to help inform them as to any financial commitments/grant/fee monies to the Authority. Review in Q1 2025.	<div>→ JOIC &amp; JDPA embracing the opportunity of the evaluation.</div> <div>→ Providing timely and relevant information.</div> <div>→ Facilitating the opportunity for the auditors to understand our work and mandate.</div> <div>→ Emerging outcomes based accountability framework can be used to explain JOIC purpose and approach to performance measurement.</div>
	Ministerial decisions and the Privacy/Data protection implications. Risks not evaluated and risk of impact on Data subjects.	<div>→ Stakeholder management.</div> <div>→ Communication with Government.</div>
	Maintaining constructive dialogue with the Department of the Economy. Changes in personnel and availability of key personnel impacts our working relationship.	<div>→ Monitor relationship.</div> <div>→ Proactive approach to maintaining regular dialogue.</div>
	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.	<div>→ We strive to maintain and monitor exchanges with the relevant parties.</div> <div>→ Maintain open and fair dialogue.</div> <div>→ Clarifying and recording decisions/requests.</div> <div>→ Working constructively with GoJ policy leads.</div>
	Political unrest and wars in Ukraine and Israel-Gaza. Risks: • Cyber implications. • Economic costs. • Political instability and unpredictable landscapes.	<div>→ Monitor and liaise with stakeholders.</div> <div>→ Horizon scanning.</div>
	The impacts of the new American Presidential administration on privacy frameworks and relevant bodies.	<div>→ Horizon scanning.</div> <div>→ Collaboration.</div>

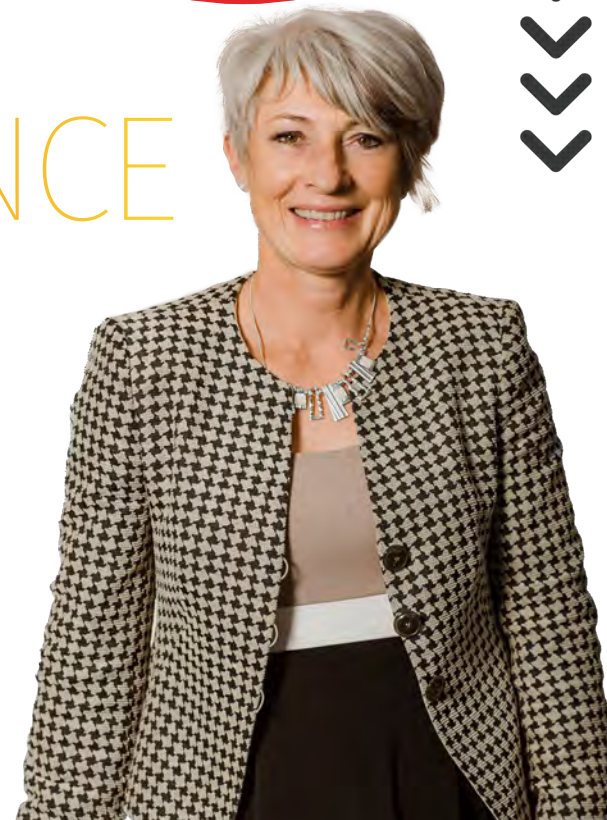




# PERFORMANCE REPORT

**Anne King**

OPERATIONS DIRECTOR



The JOIC's method for measuring and monitoring progress toward our strategic outcomes considers both the quantitative and qualitative effects of our service. 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 will aim to also find evidence of progress in these more nuanced areas and determine 'is anyone better off?' as a result of our efforts.

We already include performance measures in many of our activities, and we recognise we can expand our efforts further to include a consistent approach across all areas of our service. The following sections highlight our enforcement activities, case data, breach data, outreach and engagement activities and most importantly the impacts and effectiveness.

The JOIC has adopted an 'Outcomes Based Regulation' approach, meaning 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 learnt to be shared. Our Regulatory Action and Enforcement Policy details our approach to proportionate enforcement.

## ENFORCEMENT BY THE AUTHORITY

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

### Complaints and Inquiries

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

Upon receipt, each complaint and self-reported data breach is evaluated to determine whether or not to investigate or conduct an inquiry, as appropriate. The Authority undertakes this evaluation as soon as is practicable and in any event within eight weeks for complaints and as soon as possible for self-reported data breaches.

In the case of a complaint, once the initial evaluation has taken place the complainant is advised in writing whether or not a formal investigation will take place. The complainant has a 28-day window of appeal at this stage if the Authority decides it would not be appropriate to carry out a formal investigation and it may reject complaints if they fulfil certain criteria set out in the DPAJL 2018.

Once the investigation is underway we provide updates at least every 12 weeks. Any investigation must conclude whether the law has been contravened (Article 23 of the DPAJL 2018) and, if so, must decide whether or not to impose any formal sanction (although it does not have to do so). We will then notify the data controller or data processor of the 'proposed determination' which sets out the findings and includes details of any sanctions it is minded to impose, and they are afforded 28 days to

provide any representations on those draft findings and/or sanctions.

We must take into account any representations made before issuing our final determination which will be sent to the data controller or data processor and to the complainant. Both parties have a 28-day period to appeal that final determination to the Royal Court of Jersey but can only do so if our decision is considered unreasonable in the circumstances of the case.

The above process is almost identical in terms of an inquiry although such obviously does not involve a data subject in the same way.

As part of our formal investigation and inquiry process, we have the power to issue a formal 'Information Notice' to compel the production of information and the recipient will usually have 28 days to respond.

In the majority of cases such correspondence is requested and responded to directly by email. This is generally quicker and more efficient as most controllers are willing to cooperate fully with the investigation. This often makes for a good relationship between our office and the organisation we are investigating.

We would make use of the more formal Information Notice where we were experiencing resistance from a controller to provide us with the information requested.



# Authority Sanctions and Powers

The Authority’s Regulatory Action and Enforcement Policy <sup>3</sup>, 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:

- A. WORDS OF ADVICE

B. REPRIMAND

C. WARNING
- D. ORDER

E. PUBLIC STATEMENT

F. ADMINISTRATIVE FINE

### A. Words of Advice

Where we have identified a contravention or potential contravention of the law that does not warrant a sanction, we take the opportunity to issue Words of Advice under Art. 11(1)(e) of the DPJL 2018 in order to remind data controllers/processors of their obligations under the DPJL 2018.

### B. Reprimand

This is a formal acknowledgment that an organisation has done something wrong and is being rebuked for its conduct. This remains on the record of an organisation and could be considered if further incidents occur in the future. Generally, reprimands are issued in tandem with certain other Orders, but this is not always the case. For example, whilst there may have been a technical contravention of the DPJL 2018 for which the organisation was responsible, they might have taken steps to put things right and rectify the issues that contributed to the contravention and a formal rebuke may suffice.

### C. Warning

We may issue a Warning when the Authority considers that any intended processing or other act or omission is likely to contravene the DPJL 2018. A Warning is designed to avoid such a contravention. We have not had occasion to issue any Warnings.

### D. Order

The Authority can make a variety of Orders, but we make sure these are proportionate to the actual contravention and actually address and remediate the issues identified.

### E. Public Statement

As with everything it does, the Authority approaches the issuing of Public Statements on a proportionate basis and will only issue a Public Statement where, because of the gravity of the matter or for other exceptional reason, it would be in the public interest to do so. It

does not identify all parties involved in or otherwise report on every enforcement action taken because that is not what the law provides for. There is a strict test that must be met and the Authority reserves this power for the most serious cases.

### F. Administrative Fine

The Authority Law provides for substantive administrative fines and sanctions for contraventions of the DPJL 2018, but it is our intention to use these as a sanction of last resort.

In determining whether to impose an Administrative Fine in accordance with Article 26 of the DPAJL 2018, the Authority will consider:

- The nature, gravity and duration of the contravention.
- Whether the contravention was intentional or neglectful.
- The action taken by the controller or processor to mitigate the loss or damage, or distress suffered.

- The degree of responsibility of the person concerned and the technical and organisational measure implemented for the purposes of data protection.
- Previous contraventions.
- The degree of cooperation with the Authority.
- The categories of personal data.

In issuing a fine, the Authority will consider the need for it to be effective and proportionate, as well as to be a deterrent.

It should be noted that the Authority does not have the power to fine a ‘public authority’ as detailed in Part 4 Article 26. (9) of the DPAJL 2018, this includes the States Assembly, the States of Jersey Police, a Minister etc.



<sup>3</sup> <https://jerseyoic.org/media/l5sfz1s0/joic-regulatory-action-and-enforcement-policy.pdf>



# ENFORCEMENT & COMPLIANCE

## Stephanie MacNeill

COMPLIANCE & ENFORCEMENT MANAGER

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.

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 DPJL 2018 applies to 'personal data' meaning any information relating to an identifiable, natural, living person who can be directly or indirectly identified in particular by reference to an identifier. The definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

Personal data is at the very heart of most organisations. Data protection legislation is in place to help ensure that all of us are provided with appropriate legal protections and remedies in today's highly digitised world.

## Investigation Process

Each complaint and self-reported data breach (SRDB) is evaluated using a standard framework as set out in Part 4 of the DPAJL 2018. The JOIC undertakes this evaluation as soon as is practicable and in any event within eight weeks for complaints and as soon as possible for self-reported data breaches.

In the case of a complaint, once the initial evaluation has taken place the complainant is advised in writing whether or not a formal investigation will take place. The complainant has a 28-day window of appeal, if the JOIC decides it would not be appropriate to carry out a formal investigation or the complaint is rejected on the grounds it does not fulfil certain criteria set out in the Law.

Once the investigation is underway the JOIC provide updates at least every 12 weeks.

As part of our investigation process and powers under Schedule 1 of the DPAJL 2018, we have the power to issue an organisation with an Information Notice. This imposes a legal requirement to provide us with any information we consider necessary to assist us in any investigation or inquiry.

An Information Notice requires we give the data controller 28 days to provide the requisite information. This is a lengthy and formal process. Often upon receipt and analysis of the requested information, we have further questions which results in a follow up Information Notice. It will be clear that such exchanges can take a number of months.

Therefore, we tend to use the Information Notice for the more complex/serious cases or where there is reluctance from a data controller to engage with us at an early stage.

The investigation must conclude whether the Law has been contravened (Article 23 of the DPAJL 2018) and, if so, must decide whether or not to impose any formal sanction (although it does not have to do so). The JOIC will then notify the data controller or data processor of the 'proposed determination' which sets out the findings and includes details of any sanctions it is minded to impose, and they are afforded 28-days to provide any representations on those draft findings and/or sanctions.

The JOIC must take into account any representations made before issuing its final determination which will be sent to the data controller or data processor and to the complainant. Both parties have a 28-day period to appeal that final determination to the Royal Court of Jersey.

The JOIC will also use the framework as set out in Part 4 of the DPAJL 2018 to conduct an 'Inquiry' on its own initiative into a likely contravention of the DPAJL 2018, which we may learn about from a whistle-blower or by observing a behaviour relating to the use of personal data by an organisation. The investigation will identify if there has been a contravention of the law.





ENFORCEMENT & COMPLIANCE

As part of our formal investigation and Inquiry process, we have the power to issue a formal ‘information notice’ to compel the production of information and the recipient will usually have 28 days to respond.

(The above process is almost identical in terms of an Inquiry although an inquiry does not involve a data subject in the same way. ‘The Authority may conduct an inquiry on its own initiative into the application of the Data Protection Law’ as per Part 4, Article 21 of the DPAJL 2018.)<sup>4</sup>

In the majority of cases such correspondence is requested and responded to directly by email. This is generally quicker and more efficient as most controllers are willing to cooperate fully with the investigation. This often makes for a good relationship between JOIC and the organisation we are investigating.

We would make use of the more formal information notice where we were experiencing resistance from a controller to provide us with the information requested.

Schedule 4 of the DPAJL 2018 details the process of enforcement by the Authority in the event it receives a complaint (which can lead to a formal investigation) or conducts an inquiry.

The Authority receives a broad range of contacts. We classify them into the following categories:

- Enquiries. These range from simple questions regarding our location and career opportunities to the more complex questions around guidance matters. In 2024 we responded to 83 general enquiries.
- Complaints. Complaints are received from individuals concerned about the use of their personal data, non-response to a subject access request or other rights which have not been fulfilled.
- Self-Reported Data Breaches. Under the DPJL, data controllers are required to report ‘certain’ breaches to the JOIC within 72 hours of becoming aware of the breach unless the breach is unlikely to result in a risk to the rights and freedoms of the individual.

184

Total Number  
Self-Reported  
Data Breaches  
reported in 2024

34%

of our caseload  
were complaints  
about Public  
Authorities

NUMBER OF COMPLAINTS AND SELF-REPORTED DATA BREACHES PER SECTOR 2024

	REGISTRATIONS		AMICABLE RESOLUTIONS		COMPLAINTS		SRDBS	
	Count	%	Count	%	Count	%	Count	%
Agriculture and Fishing	96	1%	0	0%	1	1%	0	0%
Animal Husbandry and Welfare	64	1%	0	0%	0	0%	2	1%
Charities	302	4%	1	5%	3	4%	16	9%
Construction, Trades and Services	786	10%	0	0%	2	2%	9	5%
Education and Childcare	234	3%	1	5%	1	1%	8	4%
Faith, Worship and Religion	46	1%	0	0%	0	0%	0	0%
Financial and Professional Services	1995	26%	3	14%	6	7%	53	29%
Health and Wellbeing	600	8%	1	5%	8	10%	33	18%
Legal Services	119	2%	1	5%	6	7%	8	4%
Leisure and Fitness/Hospitality/ Tourism / Travel/ Entertainment	599	8%	1	5%	3	4%	5	3%
Manufacturing, Wholesale and Retail	461	6%	1	5%	3	4%	3	2%
Media, Communication and Advertising	166	2%	1	5%	0	0%	0	0%
Professional Bodies/ Professional Associations/ Professional Consultancy	330	4%	1	5%	4	5%	6	3%
Public Authority/ Sector, Appointed Regulators and Statutory Bodies	120	2%	6	27%	28	34%	23	13%
Real Estate and Property Management	1161	15%	0	0%	2	2%	5	3%
Social Clubs and Associations	292	4%	0	0%	0	0%	0	0%
Technology and Tele-Communications	240	3%	0	0%	1	1%	2	1%
Utilities and Delivery Services	86	1%	1	5%	3	4%	10	5%
No organisation type (domestic CCTV for complaints or not completed correctly)	0	0%	4	18%	11	13%	1	1%
TOTAL	7697	100	22	100	82	100	184	100

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. Health and Wellbeing is being carefully monitored as the complaints have doubled in number from 2023.

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.

<sup>4</sup> <https://www.jerseylaw.je/laws/enacted/Pages/L-04-2018.aspx>.



ENFORCEMENT & COMPLIANCE

	COMPLAINTS AND INQUIRIES	AMICABLE RESOLUTION	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

Throughout 2024 the Amicable Resolution process has remained a positive option for matters to be resolved amicably with between the individual (the complainant) and the data controller. 50% of Amicable Resolution matters were successfully completed.

Complaints generally relate to a mix of topics but predominantly focus on right of access requests, and unauthorised disclosure of personal data.

COMPLAINTS OPENED PER YEAR BY TYPE	2020	2021	2022	2023	2024	TOTAL
Uncategorised at time of submission	16	20	5	3	3	47
I asked for access to/copies of my personal information and I've not received it/they have withheld it from me	33	18	16	30	27	124
Direct marketing	2	5	1	2	1	11
I asked for my information to be rectified/erased/sent to another controller and my request has been refused	6	3	5	7	9	30
I don't think my personal data is being/has been kept safe	37	13	5	5	12	72
My information has been shared and it shouldn't have been	30	22	18	21	22	113
Other	-	-	4	1	3	8
Someone has collected my personal data, but I didn't give it to them	13	9	2	3	5	32
TOTAL	137	90	56	72	82	437

Right of access complaints include a lack of response, refusal to respond, delays and excessive redaction. Complaints also included excessive collection, lack of required transparency information (including privacy notice), holding inaccurate personal data and concerns over security. We also received a number of domestic CCTV complaints.

The two categories of complaints attracting the higher number in 2024 are the same as in 2023:

- I asked for access to/copies of my personal data, and I've not received it/they have withheld it from me.
- My information has been shared, and it shouldn't have been.

The first of these refers to dissatisfaction raised by the complainant upon receipt of the information they request as part of the right of access. We often see over-redacting when responding to data

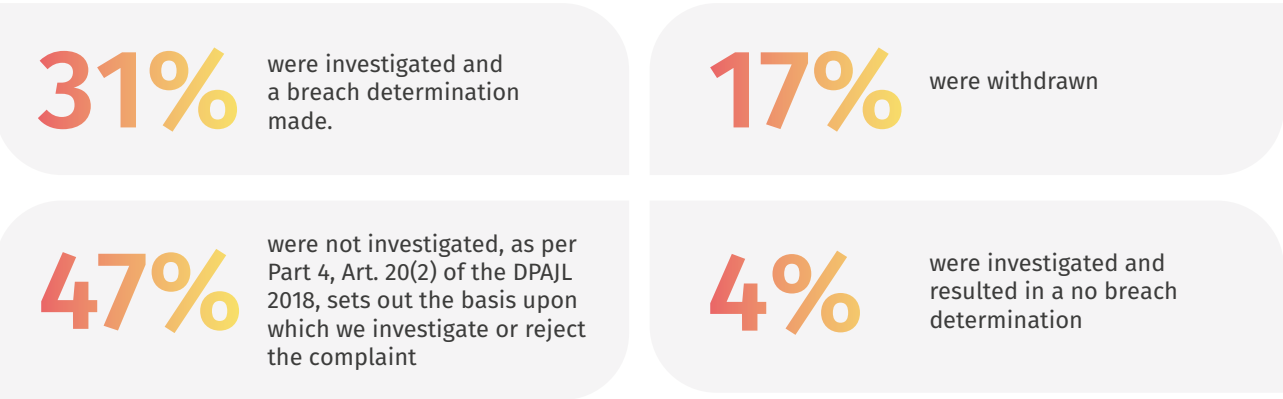
subjects, failing to respond to requests or declining to share certain aspects of information expected by the applicant.

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.

Following the structured investigations, 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 2024



ACTION WE'VE TAKEN

The complaints we have investigated have resulted in a number of sanctions issued, including Reprimands and Orders. Also in 2024 the Authority were requested to consider issuing administrative fines to two data controllers.

The Orders covered a range of topics from role specific training, software training, redaction training, lawful basis of data sharing, implementation of policies, data migration, registering with the Authority, and conducting new searches of systems in relation to a subject access request.

During 2024, the Authority issued a range of Orders including:

- 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.
- Registering with the Authority.
- Requiring a controller to rerun broader searches

- when managing a data subject access request.
- Keeping a controller under effective supervision for a period of time whilst they update data protection policies, procedures and IT systems and requiring an update report at the end of that period. For example, retention schedule, privacy policy and breach log.
- Directing that a controller should respond to a previously unanswered subject access request or any other data subject right under the DPJL 2018 within a certain timeframe (including providing previously withheld information).
- Keeping a controller under effective supervision to reevaluate/improve on internal processes and controls in relation to personal data processing.

The subject and focus of the Orders issued in 2024 were aimed at changing the behaviour of the data controllers and importantly put into context the risks associated with each topic associated with the breach determination.

Data Protection Governance

**Risk:** Without a robust governance process for evaluating the effectiveness of data protection policies and procedures there is a risk that personal data may not be processed in compliance with the DPJL 2018 resulting in regulatory action against, and/or reputational damage to, the organisation, and damage and distress to individuals.

Training and Awareness

**Risk:** If staff do not receive appropriate data protection training, in accordance with their role, there is a risk that personal data will not be processed in accordance with the DPJL 2018 resulting in regulatory action against, and/or reputational damage to, the organisation, and damage and distress to individuals.

Security of Personal Data

**Risk:** Without robust controls to ensure that personal data records are held securely in compliance with the DPJL 2018, there is a risk that they may be lost or used inappropriately, resulting in regulatory action against, and/or reputational damage to, the organisation, and damage and distress to individuals.

Records Management

**Risk:** In the absence of appropriate records management processes, there is a risk that records may not be processed in compliance with the DPJL 2018 resulting in regulatory action against, and/or reputational damage to, the organisation, and damage and distress to individuals.

Data Subject Access Requests Responses

**Risk:** Without appropriate procedures there is a risk that personal data is not processed in accordance with the rights of the individual and in breach of Art.8(f) of the DPJL 2018. This may result in damage and/or distress for the individual, and reputational damage for the organisation as a consequence of this and any regulatory action.

The Authority were requested to consider issuing administrative fines to two data controllers in late 2024. The issuing of an administrative fine by the Authority will be dependent upon a number of factors.

- The nature, gravity and duration of the failure
- The intentional character of the failure or the extent of negligence involved
- Any action taken by the controller or processor to mitigate the damage or distress suffered by the data subjects
- The degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by the controller or processor in accordance with Articles 8, 14, 15, 21 and 22 of the DPJL
- Any relevant previous failures by the controller or processor
- The degree of co-operation with the JOIC, in order to remedy the failure and mitigate the possible adverse risks of the failure
- The categories of personal data affected by the failure
- The manner in which the infringement became known to the JOIC, including whether, and if so to what extent, the controller or processor notified the JOIC of the failure

- The extent to which the controller or processor has complied with previous notices, determinations, recommendations or orders
- Adherence to any applicable approved codes of conduct or certification mechanisms
- Any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, as a result of the failure (whether directly or indirectly)
- Whether the penalty would be effective, proportionate and dissuasive.

Considering the above criteria, the Authority noted that in both cases the aggravating factors warranted the issuing of a fine as set out in the Regulatory Action and Enforcement Policy.

In one case the controller was aggressive and brash in their actions and behaviour, the Authority noted the duration of the contravention and evaluated the harms/impacts caused on the complainant over the course of the complaint. In the other case there was improper disclosure for the second time in a matter of months combined with a threat to further publish the personal data concerned and linked with the controller’s dismissive nature the Authority felt that a relevant/proportionate penalty should be awarded.

The current approach to determining the amount of the administrative fine is set out in the Authority’s [Regulatory Action and Enforcement Policy](#).

THE TRUE IMPACTS OF POOR DATA PROTECTION PRACTICES ARE BEST ILLUSTRATED IN THE FOLLOWING CASES.

The precis of some investigation and enforcement actions highlight the reality of the mis-handling of personal data and the potential impact on the data subjects and the data controllers. These cases bring to life the reality of our mandate, powers and remedies.

A COMPLAINT REGARDING A SUBJECT ACCESS REQUEST AND CONFUSION OVER A THIRD-PARTY CONTRACT

An individual submitted a subject access request. The recipient organisation would not provide the personal data stating they ‘did not hold it’. They claimed that a third party, which they contracted as their DPO, held the information. Our investigation revealed that there were complexities surrounding the working relationship and in particular the contract in place between the organisation and the third party. Both parties held copies of the data requested at various stages during its processing. The recipient organisation could not get to grips with the data processing responsibilities between them and their third party DPO service. This complexity and lack of clarity prolonged the investigation and made it difficult to pinpoint the controller of the personal data which had been requested.

The Regulatory Framework

*The right of access, more commonly referred to as subject access or a subject access request, is created by Art.28 of the DPJL18. It is most often used by individuals who want to see what information an organisation holds about them. An individual who makes a written request is also entitled to be:*

- *told whether their personal data is being processed by the organisation.*
- *given a description of the personal data, the reasons it is being processed, how long it will be kept for and whether it will be given to any other third parties, including those located in a third country.*
- *given the details of the source of the data (where available).*

SUMMARY OF FINDINGS, CONTRAVENTIONS AND ORDERS

REPRIMAND ISSUED

FINDINGS

FINDING 1

→ Contravention of Art.27(1) of the DPJL 2018

FINDING 2

→ Contravention of Art.28(1) of the DPJL 2018



ENFORCEMENT & COMPLIANCE

ORDERS

ORDER 1

→ The controller was ordered to provide specific details regarding the improvements that were to be made following an internal structural framework review; and timeframes for these improvements.

ORDER 2

→ Confirmation of the controller and third-party contractor was ordered to be provided. This was to include the data protection aspects of the contract and any instruction relating to the DPO provision from the controller to the third party.

FORMAL WORDS OF ADVICE & GUIDANCE

The controller was reminded of their obligation to cooperate with the Authority during an investigation, as per Art.6(i) of the DPJL 2018. During the investigation, the Authority:

- a. Experienced significant delays in the controller’s engagement with the Authority, and
- b. Noticed a lack of clarity and transparency in the way in which the controller responded to both the Authority and the Complainant.

The Authority noted that this should have been a relatively straightforward complaint for the controller to deal with, however, the points raised above made the investigation more difficult than it needed to be, for all involved.

A SELF-REPORTED DATA BREACH THAT LED TO AN INQUIRY

An employee of an organisation in the health and well-being sector carelessly caused unauthorised disclosure of an individual’s information and submitted a self-reported data breach (SRDB) to notify us of the unauthorised disclosure that occurred. We dealt with the SRDB to ensure they took appropriate actions in relation to mitigating further risk, including consideration of whether to inform affected data subject and dealt with the employee who caused breach appropriately.

Based on our findings following a review of the SRDB, which included seeking clarification on basic data protection obligations and regime, it transpired that the controller did not have adequate data protection

policies, procedures, and training in place, nor were they registered with our office. We therefore launched a formal Inquiry to investigate these other areas of non-compliance which had arisen during course of the SRDB. The formal Inquiry also tackled the lack of engagement and time taken to get back to us during the SRDB process. We held a face-to-face meeting which was useful as this provided the opportunity for them to explain that they did not have a great deal of data protection experience or knowledge, plus other difficulties they were facing with some business changes. It was still a challenging Inquiry at times however, with persistence and the help of an external DPO service (who they chose to hire), satisfactory compliance was achieved.



The Regulatory Framework

A ‘personal data breach’ is defined in Art.1 of the DPJL 18 as a ‘breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed’. Under Art.20(1) of the DPJL 18, controllers have a specific obligation to notify the Commissioner that a personal data breach (a breach) has occurred without undue delay and at the latest, within 72 hours of becoming aware, unless the breach is ‘unlikely to result in a risk to the rights and freedoms of natural persons’. If full details are not available at the time of notification, further details should be provided as soon as possible. Where the breach is likely to result in a high risk to the rights and freedoms of the individuals affected, the controller is also required to notify them without undue delay. Controllers are required to keep a log of those breaches. It is important for organisations to consider the types of personal data they use and how any breach could adversely affect individuals, for example by causing financial loss, reputational damage or identity fraud.

OUTCOME

Although the formal Inquiry did not result in a formal determination, we worked very closely with the controller to ensure that they had implemented a satisfactory level of data protection technical and organisational measures. This included registering with our office, creating appropriate policies and procedures such as a privacy policy, a data breach log and a retention schedule. The controller also ensured that all employees undertook adequate data protection training that was suitable and relevant for their roles and responsibilities within the organisation.

Once we began working closely with the controller, they understood their obligations and took them seriously. They had learnt a valuable lesson following the SRDB and wanted to ensure satisfactory compliance, so also decided to take on the assistance of a third-party data protection consultant to ensure their duties were fulfilled in line with the Authority’s expectations.





## A COMPLAINT REGARDING THE MISUSE OF PERSONAL DATA AND THE PROCESSING OF IT ON SOCIAL MEDIA

An individual complained to the Authority that a small trades and services organisation had disclosed their personal data on social media. The individual had asked the organisation to remove the information/post, but they were not co-operating

and raised a concern with us as a 'complaint'. This resulted in a formal investigation during which it quickly came to light that the organisation did not have adequate measures of data protection in place.

### The Regulatory Framework

Art. 6(1)(a) of the DPJL 2018 confirms that a controller is responsible for and must be able to demonstrate compliance with the data protection principles. The data protection principles detailed in Art.8 of the DPJL 2018 relevant to this particular matter included the following:

- (a) which requires that a controller only process personal data where they have a lawful basis to do so, it is fair for them to do so and they do so in a transparent manner, i.e. with a privacy policy detailing the required information. This is known as the 'lawfulness, fairness and transparency' principle.
- (b) which details that a controller should only collect and use personal data for a specific, explicit and legitimate purpose and should not further use that personal data for a purpose that is not compatible with the original purpose for which it was collected. This is known as the 'purpose limitation' principle.
- (f) which requires that an organisation has appropriate technical and organisational measures to ensure that all personal data is handled in a manner that keeps it secure and protected from unauthorised or unlawful use and accidental loss, destruction or damage. This is known as the 'integrity and confidentiality' principle.

## SUMMARY OF FINDINGS, CONTRAVENTIONS AND ORDERS

### FINDING 1

- Contravention of Art.6(1)(a) of the DPJL 2018

### FINDING 2

- Contravention of Art.8(1)(a)(b) and (f) of the DPJL 2018

### FINDING 3

- Contravention of Art.9(1) of the DPJL 2018

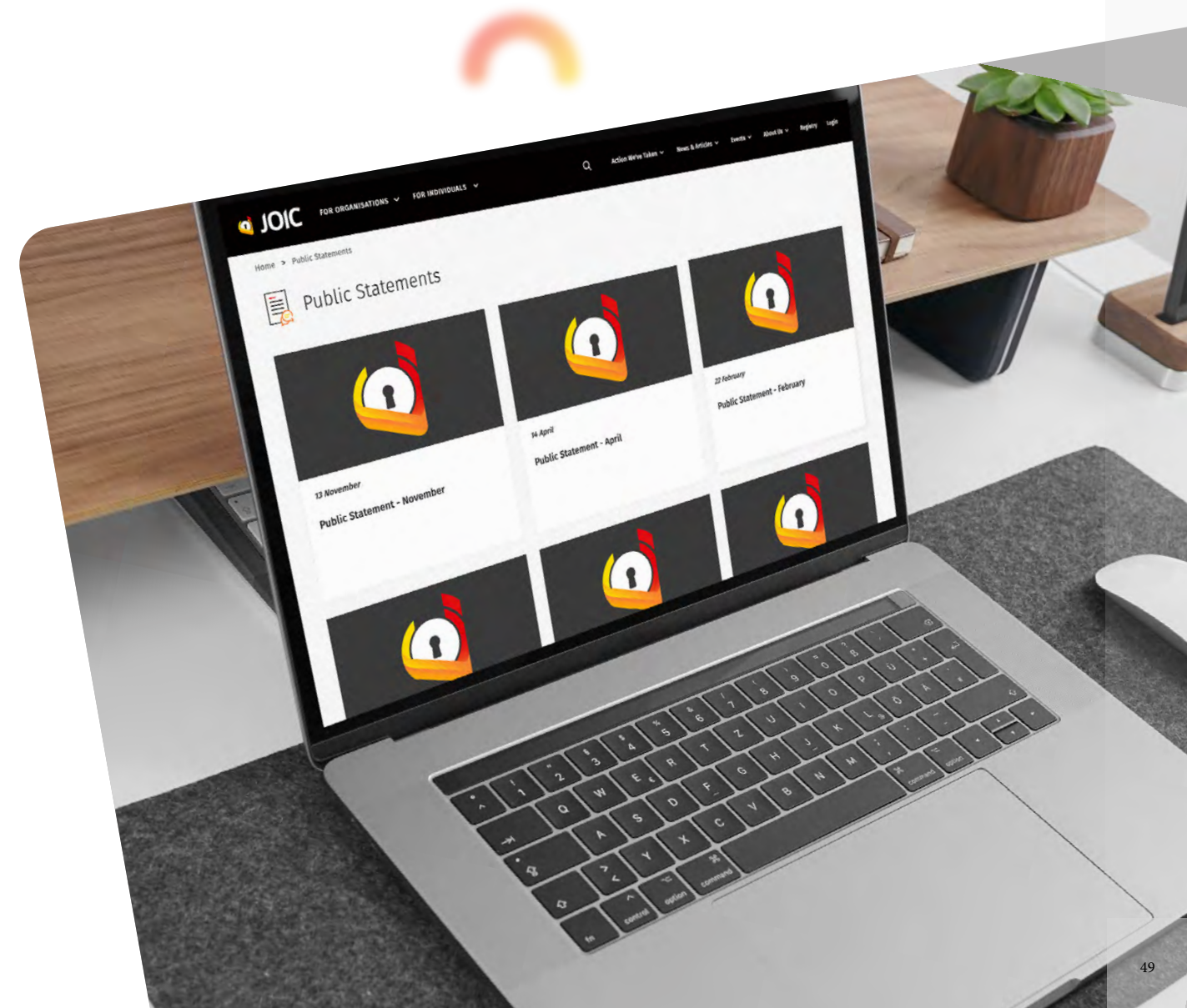
## ORDERS

### ORDER 1

- The Controller will take steps to review its policies and procedures regarding its obligations as a controller under the Data Protection (Jersey) Law 2018.

### ORDER 2

- The Controller will ensure that all staff are aware of their obligations under the Data Protection (Jersey) Law 2018 and have a sufficient understanding to fulfil their responsibilities. Therefore, the Authority requests that all staff will receive a level of data protection training that is appropriate for the role they are carrying out.
- We did not issue any Words of Advice or a Reprimand on this occasion as it was the first time the controller had any interaction with our office. We had a lot of difficulty getting the controller to engage at first and we had to work very closely with them by having regular meetings, until they had completed all of the orders. It became evident that the lack of initial engagement was due to feeling very overwhelmed and out of their depth.
- After working closely with the controller to ensure they better understood their obligations and practical measures to help with compliance, they recognised the importance of data protection and the importance of correctly handling personal data.

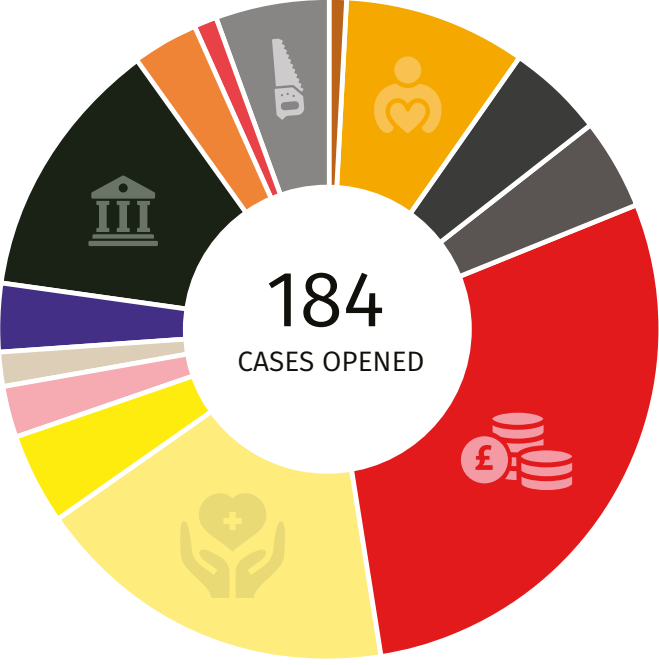


# Breach Reporting

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). In relation to breaches we also have an obligation under Art 11 1. (e) of the DPAJL 2018 ‘to promote the awareness of controllers and processors of their obligations under this Law and the Data Protection Law’.

## 2024 SRDB CASES OPENED BY ORGANISATION TYPE

Agriculture & Fishing	0
Animal Husbandry & Welfare	2
Charities	16
Construction, Trades & Services	9
Education & Childcare	8
Faith, Worship & Religion	0
Financial & Professional Services	53
Health & Wellbeing	33
Legal Services	8
Leisure & Fitness / Hospitality / Tourism / Travel / Entertainment	5
Manufacturing, Wholesale & Retail	3
Media, Communication & Advertising	0
Professional Bodies / Professional Associations / Professional Consultancy	6
Public Authority / Sector, Appointed Regulators & Statutory Bodies	23
Real Estate & Property Management	5
Social Clubs & Associations	0
Technology & Telecommunications	2
Utilities & Delivery Services	10
No organisation type	1
Total	184



The chart above highlights that 29% of the breaches reported to us were from the financial and professional services sector. It should be noted that this sector has a culture of reporting and monitoring breaches throughout their activities.

Due to the severity, nature of the data (for example, special category data) and the possibility of repeat breaches following the submission of a self-reported breach, we may open a formal Inquiry. Two Inquiries were commenced following the submission of self-reported data breaches in 2024, the entities involved were from leisure and fitness and public authority.

As previously noted, we take every opportunity to educate and support any organisation reporting a breach. Breaches can be traumatic for organisations to manage and can carry serious reputational damage for businesses. The JOIC team works sympathetically, yet professionally, when responding

to breach reports, that said we are not shy in holding organisations to account if they fail to mitigate a breach and reappear with a similar breach.

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.

29%

Breaches from Financial & Professionals Sector

## SELF REPORTED DATA BREACHES OPENED FOR 2024, BY BREACH TYPE

	2024
Alteration	1
Destruction	1
Lack of Availability / Access	2
Loss	2
Unauthorised Access	62
Unauthorised Disclosure	116
Total	184

### SPECIFICALLY

116

Self-reported data breaches were due to unauthorised disclosure (emails sent and received in error) but in all circumstances, the breaches were appropriately mitigated, presenting no risk to the data subject.

62

Self-reported data breaches involved a number of different issues including malware, phishing attacks, lost data and other processes leading to breaches. In all circumstances, the breaches were appropriately mitigated, presenting no risk to the data subject.



Enforcement Audits

Enforcement audits contribute to our Strategic Outcome - ‘Achieving and maintaining the highest standard of data protection in Jersey’. The primary purpose of an enforcement audit is to provide the Authority with an insight into the extent to which the audited entities are complying with the particular areas audited and highlight any deficient areas in their compliance.

We will be executing risk-based enforcement audits, commencing with a virtual desk-top approach and if necessary, developing into a face-to-face audit. We will also be undertaking remedial audits to track progress and the effectiveness of implementing the recommendations.

We will be executing risk-based enforcement audits, commencing with a virtual desk-top approach and if necessary, developing into a face-to-face audit. We will also be undertaking remedial audits to track progress and the effectiveness of implementing the recommendations.

Article 22(7) of the DPAJL 2018 details our power to conduct or ‘require data protection audits’

- 1. The Authority may –
  - (a) conduct a data protection audit of any part of the operations of the controller or processor; or
  - (b) require the controller or processor to appoint a person approved by the Authority to –
    - (i) conduct a data protection audit of any part of the operations of the controller or processor, and
    - (ii) report the findings of the audit to the Authority.

- 2. The Authority must specify the terms of reference of any audit carried out under sub-paragraph (1).
- 3. The controller or processor concerned must pay for an audit required under sub-paragraph (1)(b).

In 2024 we undertook 54 virtual compliance audits, conducted across two different sectors both of which process significant amounts of special category data. Complaints have been submitted to us in relation to one of the sectors regarding personal data security/

unlawful sharing. Whistleblowers raised concerns over the absence of data protection registrations in the other sector.

The lessons learned and key findings from the virtual audits will be published early in 2025.

The full audit, which began in 2023, was completed in 2024 and the lessons learned published on our website. The full audit focused on one important local Public Sector data controller which processes significant volumes of personal data. The scope of the audit focussed on the risk of non-compliance with applicable data protection principles, with specific reference to two key areas.

- 1. Training and awareness – The provision and monitoring of staff data protection training and the awareness of data protection requirements relating to their roles and responsibilities; and
- 2. Security of personal data – The technical and organisational measures in place to ensure that there is adequate security over personal data held in manual or electronic form.

We consider that it is important to highlight areas of good practice in industry, as well as areas for improvement and to explain what remedial action was required, and why.

We identified strengths in the controller’s breach management procedures, with the majority of employees stating they were able to identify a data protection breach and felt comfortable reporting breaches.

A number of deficiencies in systems and controls were identified, however, which if left unremedied, would have likely resulted in further enforcement activities taking place, as such will expose the controller to risk in terms of the potential exposure of the personal data handled by them (which could, in turn, impact on affected data subjects).

Organisations must have in place robust controls, policies, procedures, technology, and provide appropriate training to ensure the safety of individuals’ data and mitigate potential risks and we publish lessons learned so industry can learn from the audit outcomes.

The audits, complaints and self-reported data breaches appear to have common threads evident in each outcome or breach.

- Lack of relevant data protection training and refreshers.
- Effective, proportionate, implemented and communicated data protection policies and procedures.
- Personal data security- including access and visibility.

Organisations should be getting the basics right to avoid breaches which can cause distress and harm to individuals and reputational damage.

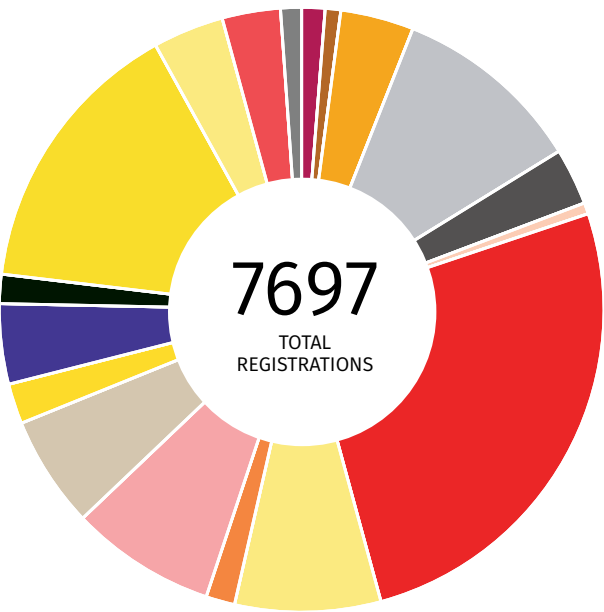


Data Protection Registrations

The number of entities registered with the Authority for the purpose of processing personal data increased by 4.5%, from 7,366 in 2023 to 7,697 in 2024. This growth is net of de-registrations, as organisations cease trading, in total we had 297 de-registrations in 2024. This figure was slightly down on de-registrations for 2023 which stood at 330.

The economic climate, business confidence and disposable income all impact on our registration income as businesses start-up, thrive and grow. As productivity and the economy shrinks so do the number and size of entities registering for the purpose of processing personal data.

Agriculture & Fishing	96
Animal Husbandry & Welfare	64
Charities	302
Construction, Trades & Services	786
Education & Childcare	234
Faith, Worship & Religion	46
Financial & Professional Services	1995
Health & Wellbeing	600
Legal Services	119
Leisure & Fitness / Hospitality / Tourism / Travel / Entertainment	599
Manufacturing, Wholesale & Retail	461
Media, Communication & Advertising	166
Professional Bodies / Professional Associations / Professional Consultancy	330
Public Authority / Sector, Appointed Regulators & Statutory Bodies	120
Real Estate & Property Management	1161
Social Clubs & Associations	292
Technology & Telecommunications	240
Utilities & Delivery Services	86
Total	7697





SECTION 8

COMMUNICATIONS,  
ENGAGEMENT  
& OUTREACH

**Sarah Moorhouse**  
COMMUNICATIONS AND PR LEAD

**Susan Fernandes**  
COMMUNITY ENGAGEMENT LEAD



Industry Engagement

Part 2 Article 11e of the Authority Law states one of the functions of the Jersey Data Protection Authority is ‘to promote the awareness of controllers and processors of their obligations under this Law and the Data Protection Law’.

Our industry engagement activity for 2024, aligned with our strategic outcome to ‘achieve and maintain the highest standard of data protection in Jersey,’ was to connect with organisations of all sizes to raise awareness of their obligations and how they are embedding data protection policies and procedures within their organisations, to drive a culture whereby privacy feels instinctive for all.

Our programme aimed to enhance organisations’ awareness to meet their obligations by:

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

Our events programme for 2024 began with an opportunity for organisations to hear directly from the Information Commissioner regarding our mandate and regulatory and enforcement philosophy, which set the scene for our further guidance sessions throughout the year.

“  
**All the information I was given has been useful and helpful.** *Event Attendee*

Our Let’s Go DPO network, a forum which provides Data Protection Officers and those that lead on data protection in Jersey the opportunity to explore common scenarios with industry peers, tackled key challenges industry were telling us about. These interactive sessions also gave attendees the chance

**99%**

Of individuals representing a controller/processor reported their knowledge of data protection obligations improved following participation in a JOIC outreach session.

to gain direct updates and feedback from our senior leadership team, including our Operations Director and Compliance and Enforcement Manager.

Interactive workshops explored:

- JOIC’s enforcement activity and Data Protection Compliance Audit Programme.
- Myth busting about local data protection law and application.
- Subject Access Request handling.
- The Dos and Don’ts of Employee Surveillance.

Let’s Go DPO continues to be popular, with those that attend reporting they appreciate the opportunity to explore common data protection themes and network whilst gaining support, insight and guidance from our office. Of those that completed our post Let’s Go DPO event feedback surveys, 98.5% said the session would benefit them personally and/or professionally. For 2025, we are seeking to significantly increase membership and attendance at these sessions and link the topics to our thematic enforcement areas.

Our Board Support Squad initiative continues to be well received by the Island’s senior leaders. The programme gives board level teams the opportunity to work with us to stress test their data protection practices in a safe space, whilst embedding positive and impactful data protection cultures and behaviours within their organisation.

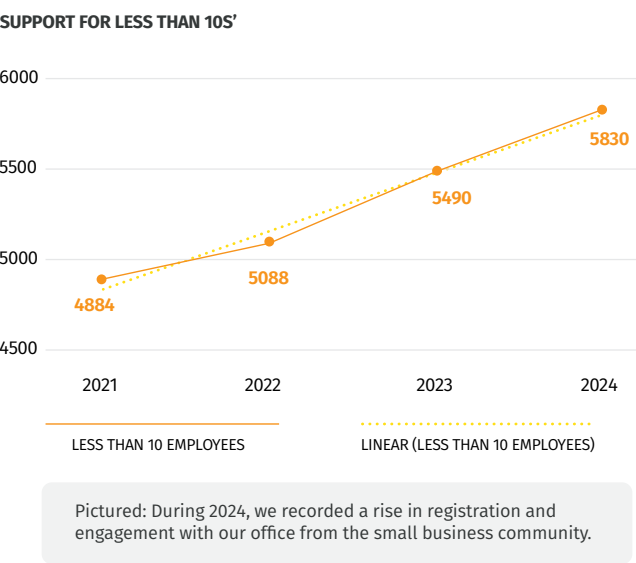
# Support for ‘Less than 10s’

Our ‘Excelling in Regulation’ cornerstone demonstrates our commitment to maintaining strong data protection standards for the Island’s economic growth and we lead by example in compliance and enforcement to ensure others understand and act on their data protection obligations. The Jersey economy is comprised of over 89% of businesses with less than 10 employees.

Given the economic landscape, business profile and to benefit our Island community, we recognised we needed to engage with smaller sized organisations to improve data protection compliance and understanding, with the aim of:

- Engendering a greater understanding of the data protection law and the obligations of organisations with less than 10 employees
- Increasing compliance via awareness of registrations obligations.

Our interventions and engagements led to a 6.25% increase in the number of registered small businesses during 2024.



We recognised there is a need to raise awareness of data protection obligations among organisations with less than 10 employees in the Health and Wellbeing, Trades and Construction and Retail sectors.

To raise awareness, in line with our business plan deliverables, we delivered a mix of face-to-face sessions, drop-in clinics, radio advertising and social media communications.

“  
**Thank you for a really informative session. I now feel more confident about my data protection obligations.** *Event Attendee*

## COLLABORATION AND PARTNERSHIPS

We also partner with and supported Jersey Cyber Security Centre as an advisory panel member for a series of incident response exercises specifically tailored for small businesses, charities and the finance and hospitality sector.

We continually collaborate with other local stakeholders, and this continued throughout 2024 to help us cascade and amplify our key messages. We liaise and work with Jersey Business and Jersey Chamber of Commerce, as well as industry bodies and associations, to help us communicate with a broad range of data controllers/processors. Including the Construction Council, Association of Jersey Charities, Genuine Jersey and Customer and Local Services business hub.

## FOCUS GROUPS

To gain a deeper understanding of the needs and opinions of organisations with less than 10 employees, we undertook moderated focus groups. Outcomes from those focus groups included:

Increasing the frequency of our information sessions.

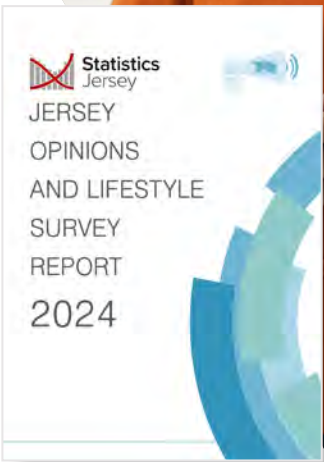
- Using more accessible language and avoiding technical jargon in our communications.
- Raising awareness of our physical location and contact details.

## JERSEY OPINIONS AND LIFESTYLE SURVEY

To further gauge an understanding of attitudes towards privacy and data protection among our community, during 2024, we submitted questions to the Government of Jersey for inclusion in their Jersey Opinions and Lifestyle Survey<sup>5</sup> (JOLS).

Issued annually, the survey seeks to explore the experiences and opinions of Islanders to help inform Government policy by gathering views on a wide range of social issues.

More than 3,500 households were selected at random to statistically represent islanders. We are able to glean extremely helpful insights from our questions.



**98%**

Respondents indicate it is very or quite important that **companies implement strong privacy measures** to protect their personal data.

**80%**

Respondents are very or quite **concerned about the security of their personal data** when making transactions online.

**64%**

Respondents agree they **felt pressure to share personal data, such as at a checkout counter, on the phone or on a website.**

**71%**

Respondents agree they **felt pressure to share more personal data** than they were comfortable with when signing up to an app or service.

From this survey and our own research, we will continue with the outreach programme to raise awareness to empower islanders to make informed decisions regarding their personal data to help protect the community, privacy becoming instinctive and Jersey is a good place to do business. The results are shaping the 2025 communications plan, deliverables and activities.

We are collaborating with the Government of Jersey Statistics Unit and we have formulated privacy focussed questions to be incorporated in future JOLS survey so as to measure privacy at the population level as part of the broader Island Indicators. We hope to rerun the 2023 privacy JOLS question in due course to help measure the impacts of outreach from us and other partners.

<sup>5</sup> Jersey Opinions and Lifestyle Survey (JOLS) - <https://www.gov.je/StatisticsPerformance/StatisticsCommunityPeople/pages/socialstatistics.aspx>



# Outreach and Education

Part 2 Article 11 (d) of the Authority law states one of the functions of the Jersey Data Protection Authority is to ‘promote public awareness, risks, rules, safeguards and rights in relation to processing especially in relation to children’.


In line with our strategic outcome to ‘protect our future generations by putting children and young people first’ the learning outcomes of our young persons’ programme for 2024, were as follows.

To raise awareness of our role and obligations and how they can support individuals in protecting their personal data and privacy rights.


- To raise individuals’ awareness of their privacy rights.
- To increase knowledge of key privacy issues and promote good privacy behaviours for privacy to become instinctive.
- To provide practical, actionable insights to help individuals confidently protect their personal data.

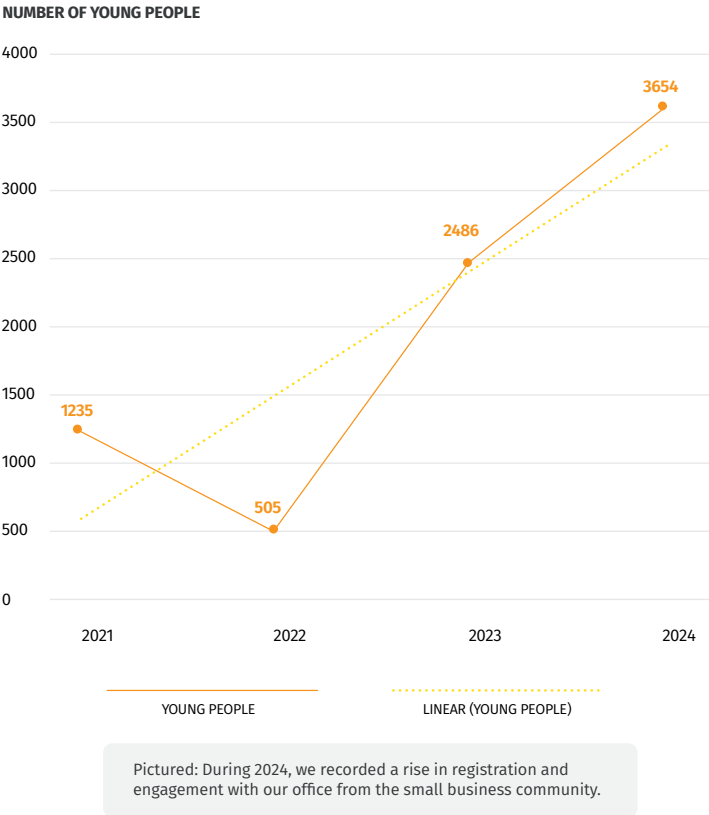
## IN 2024:

We engaged with **26% of the total population of Jersey’s under 18** year olds across 18 different schools.



86% of the young people we engaged with said their ‘**knowledge of JOIC, protection of their personal data and understanding their personal data rights improved as a result of participating in one of our outreach sessions’.**





# In line with our business plan deliverables, during 2024 we delivered the following:

**10 x**

**Privacy Awareness assemblies** for Key Stage 2 students (7-11 years old)

**28 x**

Sessions highlighting ‘**The Importance of Protecting Personal Data**’ and Awareness of Digital Footprint, for Key Stage 3 students (11-12 years old)

**19 x**

Sessions highlighting ‘**Understanding Information Rights**’ for students in years 8 and 9 (12-14 years old)

**25 x**

Sessions about ‘**Data Protection responsibilities in the Workplace and Data Protection Principles**’ for students at Key Stages 4 and 5 (14 – 18 years old) who are undertaking industry work placements

**3 x**

‘**Privacy Debate**’ sessions allowing students at Key Stage 4 (15-16 years old) to research, reason and deliver arguments around privacy themes

**3 X**

Bespoke ‘**Courtroom Challenges**’ bringing data protection law to life for students at Key Stage 5 (16-18 years old)

Given the exponential advances and uses of technology, it is critical, now more than ever, that we take steps to educate young people on how online behaviours can affect their opportunities in later life and provide them with the tools to protect themselves against the many harms associated with a digital environment and ensure they are empowered and equipped with the tools to protect their own personal data and that of others as they enter employment.

The aim of our measured programme of engagement activities and educational events for community members of all ages from sports clubs, to schools, youth clubs, cultural associations and volunteering groups was to educate participants about privacy and data protection matters and further embed our vision to create an Island culture whereby privacy is instinctive.



COMMUNICATIONS, ENGAGEMENT & OUTREACH

From January 2025 we will focus our energies with our young persons' programme with students aged 11 to 18, only. This is in response to session survey feedback, as well as reflections that the curriculum and teaching professionals were already addressing the essential topics for younger children. Our strategy for 2025 will include further sessions which prepare young people for data protection compliance in the workplace and understanding responsibilities as employees.

“

**What a fab team you have. My child took something away from the session without it being overwhelming.**



“

My child found the discussion around the difference between special category data and other data insightful.

“

**My daughter told me about a visit from JOIC at her PSHE lesson. She said it was the best PSHE lesson of the year.**



“

What a great conversation. Great job JOIC team for an engaging and interesting session that got the girls thinking.



“

**Thank you so much for delivering such a brilliant session.**

## CREATING YOUNG PRIVACY AMBASSADORS

Our Courtroom Challenge is an interactive mock privacy trial 'court case' that brings privacy law to life for young people, requiring them to delve into certain aspects of data protection law whilst developing life skills and personal values.

The challenge, operated using real life court etiquette, helps young people to understand privacy in an ethical context and encourages them to be curious, question and feel confident interpreting data protection law, whilst developing their decision-making to make appropriate judgements when it comes to privacy and personal data.

The challenge's fictional character 'Jade' is accused of taking a customer database from her old company and sharing with her new employer. The students take on the roles of defence and prosecution teams, preparing questions based on their courtroom bundle and witness statements. The defence set out to prove Jade's innocence, in that taking the database was lawful. The database contained personal data which identified certain special characteristics which could lead to prejudice. The prosecution must show that Jade has no lawful basis for her actions. Each courtroom challenge explores whether Jade can defend her actions. The students enjoy competing to find out who will emerge victorious.

Student benefits of our Courtroom Challenge include:

- Helps equip young people with the decision-making tools to make a judgement when it comes to privacy and personal data.
- Helps young people to understand privacy in an ethical context.
- Provides extra-curricular experience for university applications, curriculum vitae, references and interviews.
- Helps to create a team of young privacy ambassadors ready to be curious, question and feel empowered and confident.



## Connecting with our Community

Privacy is a fundamental human right and in line with our vision, it was essential to develop a trusted connection with our community throughout 2024, raising awareness about the role of our office and mandate, data protection law itself and educating and empowering Islanders about their personal data rights and how to exercise them.

We respect all members of our community whilst recognising that some populations may be at higher risk and need greater protection. Our role as regulator is to ensure we target our support accordingly and apply the law in a fair and consistent

manner, protecting those who need it most.

Our public awareness campaigns included hosting drop-in sessions at key spots Island wide including family groups and social activity groups for senior citizens. Further sessions took place at community hubs including Jersey Library and on St Helier's high street and all sessions promoted our guidance, resources and support available for individuals regarding how to safeguard their personal data as well as their personal data rights, the risks surrounding it and how our office can support them in the event of a personal data breach.



COMMUNICATIONS, ENGAGEMENT & OUTREACH

To provide awareness to the more vulnerable members of our community and their carers, we engaged with Island charities including Eyecan, Age Concern, Autism Jersey, Mind Jersey, The Good Companions Club and the St John's Ambulance Carers group. This also involved guidance sessions for staff and volunteers.

Our Community Outreach team also attended Island events throughout 2024 accompanied by our privacy superhero life-size characters enabling families to engage with our educational activities and learn about the importance of protecting personal data. The largest of these was the Government of Jersey's Children's Day for 2024 which attracted more than 10,000 members of Jersey's community. Other activity

**I learnt a great deal at your event. It's reminded me to be more careful with my personal data.**

**I feel so much more knowledgeable about the data protection principles and my responsibilities when handling client and staff personal data.**

included a presence at a Jersey adventure park, Jersey Library's Summer Reading Challenge and a privacy themed bear hunt, as well as a privacy trail through St Helier.

Other collaborations included working with the Jersey Fraud Prevention Forum to raise awareness about frauds and scams. We partner with local agencies to amplify our key messages for the protection and safety of our community.

These sessions provided the opportunity for us to hear directly from Jersey's community about any challenges they face related to data protection, levels of understanding of the law and how it helps to protect and empower them, as well as common misconceptions.

MEDIA AND PUBLIC RELATIONS

Another step in our business plan was to further establish relationships with media outlets in Jersey during 2024 to forge positive working relationships, resulting in greater and more meaningful local coverage for our office. As well as this, we committed to forging connections with international journals.

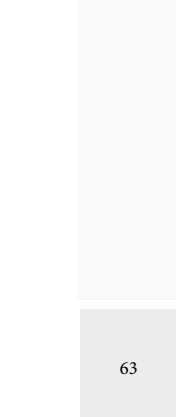
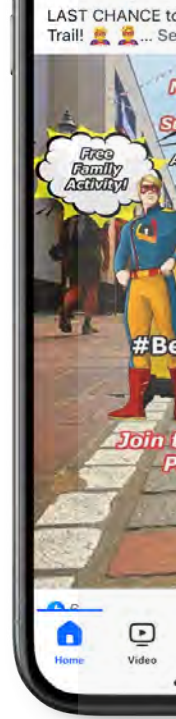
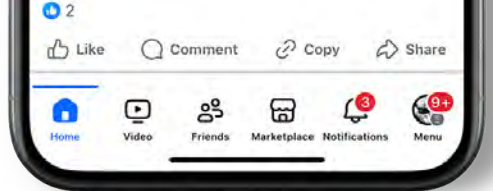
Media and Public Relations themes from our office for the year highlighted our regulatory action and enforcement activity and powers, as well as updates regarding the data protection regulatory landscape and our community outreach programme.

MEDIA RELEASES ISSUED INCLUDED:

- Jersey successfully retaining its adequacy status
- Promoting international Data Protection Day and Data Protection Week 2024
- The announcement of the new Chair of the Jersey Data Protection Authority
- The publication of our findings and lessons that industry could learn from the outcomes of our JOIC Data Protection Compliance Audit Programme

We also highlighted our involvement with the Global Privacy Enforcement Network's international enforcement sweep that examined more than 1,000 websites and mobile applications and found nearly all used one or more deceptive design patterns that made it difficult for users to make privacy-protective decisions.

Further media updates included the signing of Memorandums of Understanding (MoUs) with the Jersey's office of the Comptroller and Auditor General, the Isle of Man Information Commissioner, Gibraltar Regulatory Authority, the Abu Dhabi Global Market Office of Data Protection and the UK Information Commissioner's Office. The signing of these MoUs with national and international counterparts underlines our





COMMUNICATIONS, ENGAGEMENT & OUTREACH

commitment to strengthen our cooperation with data protection regulators worldwide, serving not only to reinforce existing ties but to also build upon joint efforts in areas of common interest and concern. When working to protect the privacy and information rights of individuals, we believe we are stronger together.

Other public relations activity surrounded raising awareness of the role of our office, controller and processor obligations, how we deal with Freedom of Information appeals, our regulatory action and enforcement policy and the guidance available from our office for individuals as well as organisations. Further updates included the potential impacts and harms of privacy breaches, the importance of data protection for consumers and promoting awareness and empowerment of personal data rights.

A significant part of our promotional activity for 2024 centred around the launch of the 46th Global Privacy Assembly and our event theme ‘The Power of i’ including the announcement of the event programme and international sponsor and speaker lineup as we explored the social, moral and commercial considerations of data privacy and the need for global citizens to maintain control and dignity over their personal data.



Paul Vane and John Edwards, UK Information Commissioner.

NATIONAL AND INTERNATIONAL WORKING GROUPS

The Information Commissioner is proud to remain on the Executive Committee of the Global Privacy Assembly and is now Chair of the GPA Reference Panel – a group of non-DPA experts who assist the GPA with strategy and direction.

He is also a member of the Strategic Direction Sub-Committee and remains a member of the Working Group on Data Sharing for the Public Good. JOIC senior team members contribute to other GPA working groups such as the International Enforcement Working

Group, the Digital Economy Working Group, the Digital Education Working Group, the Ethics in Data Protection and Artificial Intelligence Working Group and the International Development, Humanitarian Aid and Crisis Management Working Group.

We are members of the Global Privacy Enforcement Network, British, Irish and Islands’ Data Protection Authorities regional network of privacy commissioners and our senior team attends and contributes to the International Conference of Information Commissioners and the International Association of Privacy Professionals.



Paul Vane and Alexandra Delaney-Bhattacharya, Isle of Man Information Commissioner.







# 46TH GLOBAL PRIVACY ASSEMBLY

**Paul Vane**

INFORMATION COMMISSIONER



**It was an honour and a privilege for the Jersey Data Protection Authority to welcome attendees to its shores and showcase Jersey and all it has to offer.**

An infographic with an orange-to-red gradient background. It features various icons and statistics related to the 46th Global Privacy Assembly. At the bottom, there is a black and white image of a stone tower on a rocky shore.

<b>70</b> countries represented	<b>7</b> venues	<b>500</b> delegates
<b>80</b> speakers over 3 days	<b>122</b> Data Protection Authorities	

**8 pillars of the 'Power of I' theme**

**THE POWER OF I**

- Icon 1: A solid circle.
- Icon 2: A shield with a checkmark.
- Icon 3: A cluster of small circles.
- Icon 4: A circle with concentric rings.
- Icon 5: A circle divided into four quadrants.
- Icon 6: A circle with a network of dots.
- Icon 7: A 3x3 grid of small circles.
- Icon 8: A circle with a clock face and arrows.



46TH GLOBAL PRIVACY ASSEMBLY

I am thrilled and deeply honoured to have welcomed international colleagues and friends to the beautiful island of Jersey to host the 46th Global Privacy Assembly, one of the largest and most prestigious events in the global privacy calendar that connects the efforts of more than 138 Data Protection Authorities worldwide to discuss major issues impacting upon privacy and data protection and create the roadmap for the future of privacy regulation.

The overarching aim of the conference was to create a roadmap for the future, both short-term and long-term, to improve individuals' ability to self-manage their data, achieve greater equity in data sharing and foster better behaviours and culture around the use of personal data. The event attracted more than 500 delegates from 70 different countries to Jersey.

I, along with my team, wanted guests to enjoy the spirit and hospitality of their island nation, steeped in history and a place where collaboration and innovation thrives. A wealth of local leaders, industry bodies, event suppliers and experts came together to make the Jersey conference unforgettable and I must first pay tribute to the speakers, sponsors, advisers, creative designers and events team that worked tirelessly over two years to bring our concept and vision to life.

The other, perhaps hidden objective of holding a conference of this scale in Jersey was to provide a boost to the local economy in what would otherwise be a relatively quiet period for local businesses. I was delighted that so many local organisations were involved in the planning and delivery of the event, not to mention the welcome boost to the hospitality industry in terms of hotel and restaurant bookings and retail sales across the week.

***'The Power of I'***

The overarching conference theme 'The Power of I', highlighted the significance of our eight chosen themes of Innovation, Individual, Independence, International, Intercultural, Indigenous, Integrity and Information, which are intrinsically linked to encompass the harms, values and enrichment of our human lives. The conference sought to establish and explore how we can respect and balance the power of information with the need for citizens across the world to have power, control, and dignity over their personal data. The discussions challenged and questioned who controls this power, for what purpose and for whom. They also examined the effectiveness of current regulatory models, questioning whether they are still fit for purpose in a rapidly changing world.



THE  
POWER  
OF **I**

The 46th GPA was an unforgettable experience filled with inspiring discussions and thought leadership.

COMMON ACTIONS  
ARISING ACROSS ALL  
PILLARS INCLUDED:

- Ensure indigenous communities have a consistent seat at the table, develop new data governance principles, establish a working group within the Global Privacy Assembly and engage directly with indigenous populations.
- Prioritise data privacy as a human right, address biases in data handling, build trust across diverse communities, promote transparency and consent, evolve company cultures to prioritise ethics and privacy, hold tech companies accountable, involve diverse community representatives in policy development, and educate the public on data privacy rights.
- Seek early adopters for a digital privacy charter for schools, implement the '3E' strategy (Educate, Engage, Empower) for children's privacy education, advocate for a digital media literacy strategy and provide support to regulators and innovators globally.
- Find solutions that reconcile privacy protection with innovation, create a flexible approach to data minimisation and consider proportionality in data collection.







# KEY OUTCOMES ARISING FROM DISCUSSIONS WERE:

- We're operating in a complex regulatory environment.
- Collaboration is key.
- We need to do more involving young people.
- We must not forget about the impact on humanity or how to address real harms.
- Privacy needs to be a human right available to all.
- Privacy and Innovation need to work together.
- We need to deal with the complexity of rules around international data flows.
- We need to focus more on privacy concerns around Internet of Things.

All of the outcomes from the 46th Global Privacy Assembly will be detailed in a comprehensive report which will be published in 2025.

# DELEGATE FEEDBACK

“JOIC did a fantastic job as host



“I think the biggest theme that became apparent was the need for more collaboration

“The ideas on data protection authorities being fit for the 21st century is also important for Data Protection Authorities to change to be better regulators in the digital/AI world’



“Loved the new perspectives and focus on topics outside of what we hear all the time. Fantastic conference’



“The youth panel was particularly powerful and thought provoking’



“Involving young people's voices in the children's privacy panel in the open session was an excellent idea’





# ENVIRONMENTAL, SOCIAL AND GOVERNANCE

We are proud to have retained 'Eco Active' status from the Government of Jersey's Eco Active business network.

Our team is committed to fostering positive change and is committed to:

- Improving energy efficiency and eco awareness among staff.
- Taking a proactive approach to office recycling.
- Enhancing energy awareness in the workplace.



- 1 IMPROVING EFFICIENCY.
- 2 PREVENTING WASTE.
- 3 REDUCING THE RISK OF POLLUTION OR OTHER NEGATIVE ENVIRONMENTAL IMPACTS.

We regularly review our office to identify opportunities for energy savings. Our workplace has energy-efficient lighting and we switch off computers, monitors and communal equipment at the end of each day. We use 100% recyclable printer paper.

We also have a dedicated eco active champion who takes responsibility for raising awareness among staff of beach clean-up activities and promoting eco-friendly transportation options.



Conducting regular reviews and office walk arounds, to identify where energy can be saved.



Having energy saving lighting in place across our workplace and switching off computers, monitors and communal equipment at the end of each day.



Using 100% recyclable printer paper.







# PEOPLE AND ORGANISATIONAL DEVELOPMENT

**Sam Duffy**  
PEOPLE AND ORGANISATIONAL DEVELOPMENT PARTNER

2024 was a dynamic year of challenge and change for the JOIC and the Authority. Our priorities remained focused on developing our people, aligning our efforts with strategic outcomes and fostering a culture of performance, engagement and retention. Financial uncertainty means we have delayed recruitment on vacant roles. We prioritised initiatives that supported the growth and development of our teams while ensuring alignment with our business plan and strategic outcomes.

Key achievements included enhancing our performance measurement framework through Outcomes Based Accountability (OBA), offering leadership development opportunities and advancing professional qualifications. Our talent and succession planning discussions matured, identifying opportunities for internal career progression, ensuring we remain prepared for the future.

Despite resource challenges and setbacks, we maintained focus on employee engagement through regular communication and a review of pay and reward, reinforcing our dedication to fairness and recognition. Whilst there is still much to do, together our efforts in 2024 have strengthened our foundation, positioning us to meet future challenges with a skilled, motivated and cohesive team.

## Workforce Composition

### JERSEY DATA PROTECTION AUTHORITY

The Jersey Data Protection Authority Chair retired in October 2024 and was succeeded from within the JDPA. In addition, one voting member left the Authority and was not replaced.

At the end of 2024, the Authority headcount was five members, including the new Chair. This was two members less, than the year before. The average length of tenure of a JDPA member at the end of 2024 was 3.2 years.

### JERSEY OFFICE OF THE INFORMATION COMMISSIONER

At the end of 2024 there were 19 (18.6 FTE) permanent employees within the JOIC. There was one leaver, one new starter and one promotion in 2024. The headcount therefore remained the same as the year before.

In the current climate of financial uncertainty we have made a policy decision to either postpone recruitment or not recruit into vacancies.

In total, 90% of the JOIC's employees were female and 10% were male in 2024. The JOIC senior leadership team comprised of four permanent employees, three female and one male, supported by two external consultants.



**90%**  
Female Employees

## JERSEY DATA PROTECTION AUTHORITY CHAIR RECRUITMENT

A comprehensive recruitment and selection process was undertaken to appoint a new JDPA Chair in 2024. The process was designed to reflect our commitment to fairness, transparency and equal opportunities. Conducted in close collaboration with the Jersey Appointments Commission (JAC), the process adhered to best practices and governance standards. A four-member panel, comprising two representatives from the JDPA, one from the Government and one independent member carefully evaluated the applications under the oversight of the JAC. The process attracted a diverse and talented pool of candidates from both local and international backgrounds, resulting in the appointment of Elizabeth Denham as the successful candidate, in September 2024.

## PERFORMANCE MEASUREMENT

Throughout 2024 we enhanced our approach to performance measurement using Outcomes Based Accountability (OBA) methodologies across several JOIC functions. This involved selecting key programmes and services, identifying metrics and capturing meaningful data to accurately reflect our progress and the impact of our service. By focusing on outcomes, we aim to align our efforts more closely with our vision and strategic goals.

Additionally, we collaborated with the Government of Jersey's Statistics department to identify possible measures for the Island Outcomes Indicators.

As part of this initiative, we provided OBA training for a number of JOIC team members, who will have some responsibilities for performance measurement, within their roles. This work will continue into 2025.

## EMPLOYEE DEVELOPMENT

This was a pivotal year for employee development at JOIC, marked by a variety of learning initiatives. These efforts aimed to support the continuing professional growth of our team while meeting the demands of a busy conference year.

## PERSONAL LEADERSHIP PROGRAMME

A cornerstone of our development efforts was a 12-month Personal Leadership Programme, designed to enhance leadership skills and achieve specific organisational outcomes. Five team members, selected for their current or potential leadership responsibilities, participated in this programme. The training equipped them with essential skills and support to enhance their personal leadership skills and performance.

## PROFESSIONAL QUALIFICATIONS

Despite the challenges posed by reduced budgets and the need to carefully balance time away from the office with the demands of hosting the GPA conference, JOIC remained committed to employee development. We are proud to report that six team members successfully completed or made progress towards professional qualifications at levels 3 to 7. These qualifications spanned key areas including Freedom of Information, Data Protection, Company Direction, Accounting, Education and Training, further enhancing the skills and expertise of our workforce.

## IN-HOUSE LEARNING AND WELLBEING PROGRAMME

The JOIC Learning and Wellbeing Programme delivered a variety of short, impactful sessions tailored to both personal and professional development. Topics included neurodiversity, mental toughness, networking, health and wellbeing and specialist/technical updates, ensuring our team remained informed and supported in their busy work environment.

## CONTINUING PROFESSIONAL DEVELOPMENT

In 2024, we reviewed and enhanced our policies, procedures and knowledge across several important areas. The entire JOIC team completed Cyber Security training and selected members completed Safeguarding training, reinforcing our commitment to best practices and professional excellence.

## 46TH GLOBAL PRIVACY ASSEMBLY

Hosting the 46th Global Privacy Assembly conference served as a unique and valuable learning experience for the JOIC team. From programme design and event organisation to teamwork and active participation, the conference provided excellent opportunities for professional growth. Team members expanded their knowledge and networks while contributing to the success of this high-profile event.

## LOOKING AHEAD

By providing diverse learning opportunities and investing in the growth of our team, we will continue to build a skilled and motivated workforce prepared to meet future challenges and opportunities.

## PAY & REWARD REVIEW

Between April and June 2024, an in-depth review of the JOIC/JDPA's pay and reward structure and policy was undertaken. This review takes place approximately every four years to ensure that JOIC's pay and benefits are comparable with market rates. Conducted by a local independent specialist, the review benchmarked JOIC and JDPA pay structures against ten organisations, including regulatory bodies and public interest organisations in Jersey, Guernsey, the Isle of Man and Bermuda.

One organisation remained anonymous, and the Government of Jersey did not take part, however their publicly available pay data was included. Findings were shared with participating organisations to support their pay practices. The Remuneration and HR Committee reviewed the recommendations, and these were used to inform pay increases later in 2024.

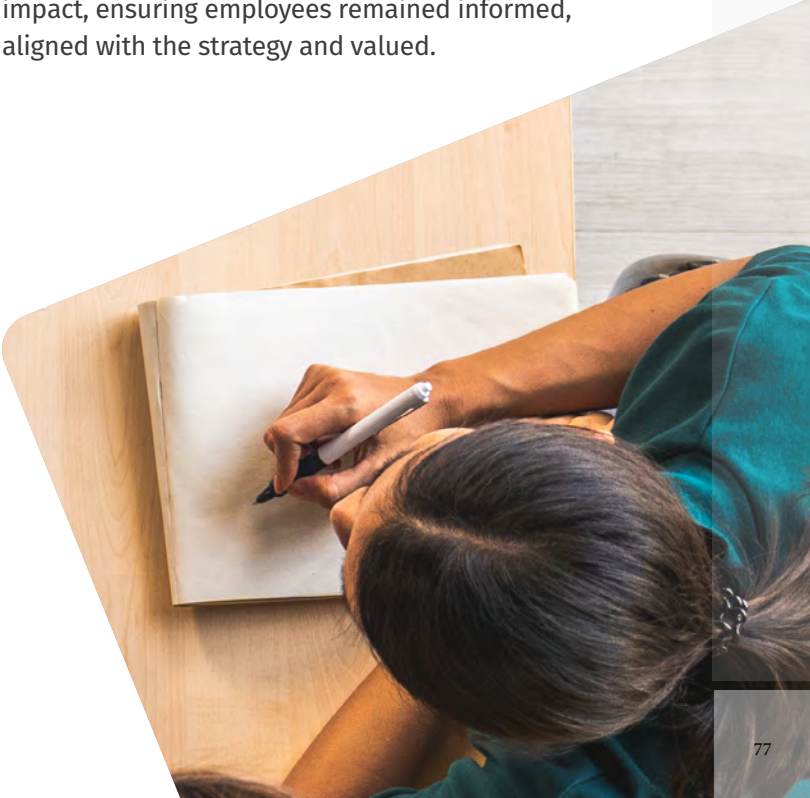
## TALENT AND SUCCESSION PLANNING

The JOIC leadership team completed talent and succession planning discussions for key roles within the organisation, in the last quarter of 2024. These discussions aimed to identify potential internal successors and prioritise development and career progression opportunities for motivated and qualified employees. The outcomes will guide the leadership team in fostering and retaining key talent throughout 2025.

As part of our broader talent strategy, we explored offering work placements to local students to promote careers in data protection. Despite extensive research and collaboration with local educational providers, budgetary constraints required these plans to be postponed at the end of 2024. We remain committed to revisiting these initiatives in the future, supporting local students eager to build careers in our industry.

## EMPLOYEE ENGAGEMENT

In 2024, we adjusted our approach to employee engagement to align with resource demands, opting to conduct our engagement survey every other year. Instead, we focused on strengthening engagement through regular communication, ad hoc 'pulse' surveys, connecting employees with our business plan and undertaking a review of pay and reward (as above). These efforts collectively made a positive impact, ensuring employees remained informed, aligned with the strategy and valued.







# FINANCE OVERVIEW

**Claire Le Brun**  
FINANCE DIRECTOR

2024 presented a challenging financial landscape, business as usual operations remained steady but due to decreased funding from Government, the JDPA took a prudent approach which resulted in streamlining, prioritising and making adjustments to ensure that our mandated services were protected and as many of the business plan deliverables to achieve our strategic outcomes to drive towards our vision were delivered.



## 46th Global Privacy Assembly

A key highlight in the year was hosting the 46th Global Privacy Assembly (GPA) annual conference. Not only did it provide a platform for important data protection discussions the conference also had a positive economic impact on local businesses which was distributed across several sectors. The hospitality industry benefited from the delegates staying in local hotels and dining at local restaurants, we also had local suppliers supporting the conference with everything from event management and logistics through to the catering services received.

The Conference was funded through two revenue streams: Ticket sales and Sponsorship. These two sources of funding provided a good financial foundation ensuring the financial viability of

the event whilst providing a quality offering for delegates, key stakeholders and sponsors.

The funding raised covered the operational costs of the event which included venue hire, the technical infrastructure, speaker costs and logistics.

The ticket sales and sponsorship not only made the event financially feasible it also helped showcase Jersey. The sun shone all week and Jersey businesses shone alongside.

At the time of writing the conference numbers are still being finalised. The total income generated from tickets sale and sponsorship is in excess of £735,000. The associated conference expenses of approximately £724,000 has resulted in a near breakeven outcome.

## Financial Summary 2024

Business Operations (DP & FoI)	Budget to Q4	Actual to Q4	Variance
Income	£2,381,727	£2,394,730	+£13,003
Staff	£1,689,511	£1,553,907	+£135,604
Non-Staff	£973,838	£932,839	+£40,999
Total Variance			+£189,606

## INCOME

Budget Area	Budget for the full year 2024	Actual as at 31.12.24	Surplus/ Deficit
Interest	£6,000	£11,873	+£5,873
Fees	£2,305,727	£2,325,260	+£19,533



# Government Funding

The JDPA took receipt of two grant payments during 2024.

The first was received solely for Freedom of Information (Fol). The Grant is paid to the Information Commissioner as part of the Fol Partnership Agreement, with the Authority being the grant receiving body/authority which enables the grant to be received and utilised to fulfil our Fol statutory obligations.

The second grant was received to enable delivery of the 46th Global Privacy Assembly.

The uncertainty in Government Grant income for our data protection mandated activities resulted in a cost saving approach being adopted throughout our work during 2024. Whilst this is prudent, this does impact negatively on recruitment, training, development and opportunities.

	Freedom of Information	GPA Conference sponsorship	Data Protection
Grant paid in 2024	£57,597	£50,000	£0

# Registration Fee Income

Fee income totalling £2,325,260 has been received which represents 100.8% of the budgeted fee income set for the year. (2023: £2,275,510. 96.4% of budget)

There were 7,366 entities registered with the Authority in 2023, in 2024 the number of entities registered increased by 4.5% to 7,697. It should be noted that not all registrations pay fees.

The below table shows a comparison of fees in each registration fee band at year end for 2023 and 2024.

	2024	2023	% +/-
Full time equivalent fee	£554,060	£524,100	+5.72%
Past year revenues	£95,750	£90,400	+5.92%
Subject to proceeds of crime	£115,250	£110,050	+4.73%
Administered Services	£1,510,650	£1,506,600	+0.27%
Special Category Data	£49,550	£44,450	+11.47%

It is challenging to forecast the fee income per fee band due to the number of differentials making up the fee.

For instance, in the 'FTE equivalent' fee banding (FTE – Full Time Equivalent), an entity is required to select the number of FTEs currently employed. This affects which level of fee is paid and can change

depending on the circumstances of the entity from year to year. Additionally, if the entity increases its revenue this also impacts on the fee to be paid for their processing.

The below table highlights how the fee could change for one single registration from one year to the next.

	Company A, year 1: 9 employees, Special cat data processing and revenue of £4.5m	Company A, Year 2: 10 employees, Special cat data processing and revenue of £5m
Full time equivalent fee	£70	£90
Special Category Data	£50	£150
Past year revenues	£0	£150
Total fee Generated	£120	£390

In the example above the same registration has increased by 225% in year 2, there would be no way to anticipate these changes in each registration. We could also see registrations doing the reverse and reducing their fee payable by the same %. The fee income could fluctuate quite significantly while registration numbers remain static.

This is something to remain mindful of when we are seeing negative impacts on business growth due to the current economic climate.

# Remuneration and Staff

The below table shows the Authority remuneration and time commitments for the Authority members based on their role on the authority. Authority remuneration has seen a 7% uplift in 2024, this is the first uplift since the creation of the Authority in 2018. The rate was subject to an external review during 2024, the findings were submitted to the Minister who approved the following:

Role	Time Commitment Days per Annum	Day Rate	Annual Remuneration
Authority Chair	18	£1,016.50	£18,297
Committee Chair and Voting Member	15	£802.50	£12,037.50
Voting Member	12	£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.

Total JOIC staff costs for the year were underspent at year end.

Budget 2024	Actual 2024	Variance
£1,689,511	£1,553,907	£135,604



PEOPLE AND ORGANISATIONAL DEVELOPMENT

There were 23 roles recorded in the 2024 budget with 19 of these in post at year end. Recruitment was delayed through the year to utilise the staff savings to offset the reduction in funding in the year.  
Staff costs include the Commissioner’s salary\*.

Commissioner Salary 2023	Commissioner Salary 2024	% increase on 2023
£152,208	£163,309	7%

\*The budgeted 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 and this was increased by 7% for cost of living from 1 January 2024.

Non-Staff Costs

Strategic decisions were taken to scale back on non-staff costs in face of the reduced Government funding. By carefully managing expenditure and focusing on efficiency we ensured we can deliver our mandate and met our deliverables whilst reducing costs.

Budget 2024	Actual 2024	Variance
£973,838	£932,839	£40,999

The action taken has resulted in budget underspends at the end of 2024 to ensure the Authority can service its financial obligations.





AUDITED  
FINANCIAL  
STATEMENTS

**JERSEY DATA PROTECTION  
AUTHORITY (JDPA)  
AUDITED FINANCIAL STATEMENTS  
FOR THE YEAR ENDED 31 DECEMBER 2024**



JERSEY DATA PROTECTION AUTHORITY (JDPA)  
AUDITED FINANCIAL STATEMENTS  
FOR THE YEAR ENDED 31 DECEMBER 2024

CONTENTS	Page
General Information	1
Authority Report	2
Statement of Authority's Responsibilities	3
Independent auditor's report to the Minister	4 - 9
Statement of Comprehensive Income and retained earnings	10
Statement of Financial Position	11
Notes to the Financial Statements	12 - 17

JERSEY DATA PROTECTION AUTHORITY (JDPA)  
AUDITED FINANCIAL STATEMENTS  
FOR THE YEAR ENDED 31 DECEMBER 2024

GENERAL INFORMATION		
<b>Members of the Authority</b>		
Jacob Kohnstamm	Chair	(Appointment ended October 2024)
Elizabeth Denham CBE	Chair	(Appointed October 2024)
Elizabeth Denham CBE	Voting Member	(Until October 2024)
Paul Breitbarth	Voting Member	
Stephen Bolinger	Voting Member	
Gailina Liew	Voting Member	(Appointment ended October 2024)
Paul Routier MBE	Voting Member	
Helen Hatton	Voting Member	
Paul Vane	Information Commissioner (non-voting member)	
<b>Registered Office</b>		
2nd Floor		
5 Castle Street		
St Helier		
Jersey		
JE2 3BT		
<b>Banker</b>		
HSBC		
15-17 King Street		
St Helier		
Jersey		
JE2 4WF		
<b>Independent Auditor</b>		
Baker Tilly Channel Islands Limited		
2nd Floor		
Lime Grove House		
Green Street		
St Helier		
Jersey		
JE2 4UB		

JERSEY DATA PROTECTION AUTHORITY (JDPA)  
AUDITED FINANCIAL STATEMENTS  
FOR THE YEAR ENDED 31 DECEMBER 2024

AUTHORITY REPORT

The Authority present their report and the audited financial statements of the Jersey Data Protection Authority (JDPA) (The "Authority") for the year ended 31st December 2024.

Incorporation

The JDPA was incorporated in Jersey under the Data Protection Authority (Jersey) Law 2018 ("DPAL") on 25 May 2018.

Corporate governance and delegation of authority

The JDPA, through the Authority, carries the ultimate responsibility for the discharge of the responsibilities under the DPAL. The JDPA operates under the name of the Jersey Office of the Information Commissioner (JOIC).

The JDPA is the guardian of independence, sets the organisation’s strategic direction, holds the Commissioner to account and provides the Commissioner with advice, support and encouragement. It ensures that JOIC provides value for money and complies with appropriate policies and procedures with respect to human resources, financial and asset management, and procurement.

The JDPA has the authority to appoint (or re-appoint) the Commissioner or remove the Commissioner from office. The JDPA has very limited operational responsibilities and these do not include day-to-day operations, individual casework or most enforcement decisions. The Authority has the ability to delegate functions to the Commissioner, but cannot delegate the following functions: this power of delegation; the function of reviewing any of its decisions; the issuing of a public statement under Article 14 of the DPAL; the making of an order to pay an administrative fine or the preparation of the Annual Report. By an Authority Resolution of 7 January 2019, the JDPA delegated all of its functions to the Commissioner, in accordance with Article 10, except 'Reserved Functions'. In performing the 'Reserved Functions' the Authority will have the assistance of the Commissioner.

Results

The financial statements provide an overview of the Jersey Data Protection Authority's income and expenditure for 2024.

Going Concern

The Authority consider, given that there is sufficient funding in place for mandated activities, the use of the going concern basis is appropriate for the current period and at least 12 months from the date of signing these financial statements.

Auditor

The Comptroller and Auditor-General exercised their power under Article 43(3)(a) of the Data Protection Authority (Jersey) Law 2018 (as defined by the Comptroller and Auditor General (Jersey) Law 2014), to appoint Baker Tilly Channel Islands Limited as auditor of the authority for 3 years to include the financial statements from the year ended 31st December 2024 to 31st December 2026. This appointment can be extended each year until 31st December 2028.

APPROVED

Paul Vane  
Information Commissioner  
on behalf of the JDPA

Date  
25th April 2025

JERSEY DATA PROTECTION AUTHORITY (JDPA)  
AUDITED FINANCIAL STATEMENTS  
FOR THE YEAR ENDED 31 DECEMBER 2024

STATEMENT OF AUTHORITY'S RESPONSIBILITIES

The JDPA is responsible for preparing the Authority's report and the financial statements in accordance with applicable law and regulations.

The Data Protection Authority (Jersey) Law 2018 requires the Authority to prepare financial statements for each financial period. Under that law, the Authority have elected to prepare the financial statements in accordance with United Kingdom Accounting Standards, including Section 1A of the Financial reporting Standards 102, the Financial Reporting Standard in the United Kingdom and Republic of Ireland ("FRS 102 1A") (collectively, United Kingdom Generally Accepted Accounting Practice ("UK GAAP"). The Authority must not approve the financial statements unless they are satisfied that they give a true and fair view of the state of affairs of the Authority and of the surplus or deficit for that period.

- In preparing these financial statements, the Authority is required to:
- select suitable accounting policies and then apply them consistently;
  - make judgements and estimates that are reasonable and prudent;
  - state whether applicable accounting standards have been followed, subject to any material departures as disclosed and explained in the financial statements; and
  - prepare the financial statements on a going concern basis unless it is inappropriate to presume that the JDPA will continue in business.

The voting members are responsible for keeping adequate accounting records that are sufficient to show and explain the JDPA's transactions and disclose with reasonable accuracy at any time the financial position of the Authority and enable them to ensure that the financial statements comply with the Data Protection Authority (Jersey) Law 2018. They are also responsible for safeguarding the assets of the JDPA and hence for taking reasonable steps for the prevention and detection of fraud and other irregularities.

- The JDPA at the date of approval of this report confirm that:
- So far the Authority are aware, there is no relevant audit information of which the Authority's auditor is unaware; and
  - each Authority member has taken all steps that they ought to have taken as a member to make themselves aware of any relevant audit information and to establish that the JDPA's auditor is aware of that information.

APPROVED

Paul Vane  
Information Commissioner  
on behalf of the JDPA

Date  
25th April 2025





# Independent auditor’s report

To the relevant Minister of the Government of Jersey (the “Minister”) on behalf of Jersey Data Protection Authority and the Comptroller and Auditor General

### Opinion

We have audited the financial statements of Jersey Data Protection Authority (the “Authority”), which comprise the statement of financial position as at 31 December 2024, and the statement of comprehensive income and retained earnings for the year then ended, and notes to the financial statements, including a summary of significant accounting policies.

In our opinion, the accompanying financial statements:

- give a true and fair view of the financial position of the Authority as at 31 December 2024, and of its financial performance for the year then ended in accordance with United Kingdom Accounting Standards, including Section 1A of FRS 102, The Financial Reporting Standard applicable in the UK and Republic of Ireland (“UK GAAP”); and
- have been prepared in accordance with the requirements of the Data Protection Authority (Jersey) Law 2018 (the “Law”).

### Basis for Opinion

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

### Key Audit Matters

Key audit matters are those matters that, in our professional judgement, were of most significance in our audit of the financial statements of the current period and include the most significant assessed risks of material misstatement (whether or not due to fraud) identified by us, including those which had the greatest effect on: the overall audit strategy; the allocation of resources in the audit; and directing the efforts of the engagement team. These matters were addressed in the context of our audit of the financial

statements as a whole, and in forming our opinion thereon, and we do not provide a separate opinion on these matters.

Key audit matter	Identified audit risk per the Audit Planning Letter	Key observations communicated to those charged with governance
<p><b>Revenue</b></p> <p>Revenue recognised during the reporting period may be incorrectly allocated or materially misstated.</p> <ul style="list-style-type: none"><li>• Accounting policies in Note 3</li><li>• Note 4 and Note 6</li></ul> <p>Revenue for the year was £2,387,730 (PY: £2,439,474).</p>	<p>Revenue derived from registrations made with the authority and renewals, or grant income, being materially misstated.</p>	<p>We have reinforced our understanding of the process, from initial registration or renewal through to the income being recognised and received, including walkthroughs and detailed controls testing, confirming key controls were appropriately implemented and operated effectively.</p> <p>We undertook substantive analytical procedures to assess the completeness of the reported income.</p> <p>We have reviewed the agreements, correspondence and conditions related to funding received from the Government of Jersey (GOJ), to ensure that the appropriate level of income is recognised in the reporting period. This amount was £nil for 2024 (PY: £85,419)</p> <p>In addition, we have reviewed post balance sheet minutes of the Members of the Authority and correspondence to confirm that no 2024 government grant was subsequently agreed after the conclusion of the financial period.</p> <p><b>Freedom of Information (Fol) grant audit procedures:</b></p> <p>We have obtained an understanding of the Fol grant through discussions with management and review of the agreement. We have agreed receipt of grant to bank and recalculated the clawback mechanism assessing if this will be applicable in 2024 for accuracy of the amount disclosed in the financial statements.</p> <p>We have assessed the correlating expenses, including assumptions made, for the Fol grant for reasonableness and performed a re-calculation.</p> <p>We reviewed the disclosure requirements for the Fol grant under FRS 102 and discussed requirements with a second Director.</p> <p><b>We have no issues to report from our testing.</b></p>

<p><b>Exceptional items – General Privacy Assembly (GPA) conference</b></p> <p>Sponsorship/ticket income or GPA related expenses during the period could be incorrectly accounted for or disclosed.</p> <ul style="list-style-type: none"><li>Accounting policies in Note 3</li><li>Note 19</li></ul> <p>Revenue relating to the GPA conference was £745,663 (PY: £nil).</p> <p>Expenses relating to the GPA was £708,860 (PY: £33,581).</p>	<p>There is a risk that the grant/donation income and related expenses incurred for the purposes of hosting the GPA conference are not correctly accounted for and disclosed in the financial statements.</p>	<p><b>Ticket Income</b></p> <p>We have obtained an understanding of the process, from registration through to the income being recognised and received.</p> <p>We undertook substantive procedures as well as communication with management, to assess the reported income. This amount was £258,855 for 2024 (PY: £nil).</p> <p><b>Sponsorship Income</b></p> <p>We have obtained an understanding of the processes surrounding sponsorship income through discussions with management, including how they reach out to potential sponsors, to how the sponsors paid the authority.</p> <p>We have reviewed the material sponsorship agreements and invoices, related to the GPA conference, to ensure that the appropriate level of income is recognised in the reporting period, as well as ensuring the money was appropriately accounted for and held separately in bank. This amount was £478,998 for 2024 (PY: £nil).</p> <p><b>Expenditure</b></p> <p>We have obtained an understanding of the process, with the expenses being budgeted and invoiced by the event organiser.</p> <p>We obtained and reviewed material contracts related to the GPA, as well as substantively sampling a selection of the GPA conference expense invoices to ensure they were classified correctly. The expenses relating to the GPA conference were £708,860 for 2024 (PY: £33,581).</p> <p>We have reviewed post balance sheet minutes of the Members of the Authority and correspondence to confirm that no additional income/expenses relating to the GPA conference arose after the 2024 year end.</p> <p>We performed a Pentana disclosure checklist to ensure correct disclosures in accordance with applicable financial reporting frameworks.</p>
--	---	--

Our Application of Materiality

Materiality for the financial statements as a whole was set at £42,000 (PY: £42,000), determined with reference to a benchmark of total revenue/expenses, of which it represents c1.8% (PY: c1.8%).

In line with our audit methodology, our procedures on individual account balances and disclosures were performed to a lower threshold, performance materiality, so as to reduce to an acceptable level the risk that individually immaterial misstatements in individual account balances add up to a material amount across the financial statements as a whole.

Performance materiality was set at c70% (PY: c70%) of materiality for the financial statements as a whole, which equates to £30,000 (PY: £29,000). We applied this percentage in our determination of performance materiality because we have not identified any significant corrected misstatements or material uncorrected, misstatements in the prior year audit. We also based the percentage on results and experience in the prior year audit and understanding of the entity therefore we deem the likelihood and effects of misstatements to be low.

We have reported to the Audit and Risk Committee any uncorrected omissions of misstatements exceeding £2,000 (PY: £2,000), in addition to those that warranted reporting on qualitative grounds.

Conclusions relating to Going Concern

In auditing the financial statements, we have concluded that the Board of Member’s use of the going concern basis of accounting in the preparation of the financial statements is appropriate.

Based on the work we have performed, we have not identified any material uncertainties relating to events or conditions that, individually or collectively, may cast significant doubt on the Authority’s ability to continue as a going concern for a period of at least twelve months from when the financial statements are authorised for issue.

Our responsibilities and the responsibilities of the Board of Members with respect to going concern are described in the relevant sections of this report.

Other Information

The other information comprises the information included in the annual report other than the financial statements and our auditor’s report thereon. The Board of Members are responsible for the other information contained within the annual report. Our opinion on the financial statements does not cover the other information and, except to the extent otherwise explicitly stated in our report, we do not express any form of assurance conclusion thereon. Our responsibility is to read the other information and, in doing so, consider whether the other information is materially inconsistent with the financial statements, or our knowledge obtained in the course of the audit, or otherwise appears to be materially misstated. If we identify such material inconsistencies or apparent material misstatements, we are required to determine whether this gives rise to a material misstatement in the financial statements themselves. If, based on the work performed, we conclude that there is a material misstatement of this other information, we are required to report that fact. +

We have nothing to report in this regard.

Responsibilities of the Board of Members

As explained more fully in the statement of Authority’s responsibilities set out on page 3, the Board of Members are responsible for the preparation of financial statements that give a true and fair view in accordance with UK GAAP, and for such internal control as the Board of Members determine is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error.



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

The Board of Members are responsible for overseeing the Authority's financial reporting process.

**Auditor's Responsibilities for the Audit of the Financial Statements**

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

The extent to which our procedures are capable of detecting irregularities, including fraud, is detailed below:

- Enquiry of management to identify any instances of non-compliance with laws and regulations, including actual, suspected or alleged fraud;
- Reading minutes of meetings of the Authority;
- Reading compliance reports and key correspondence with regulatory authorities;
- Review of legal invoices;
- Review of management's significant estimates and judgements for evidence of bias;
- Review for undisclosed related party transactions;
- Using analytical procedures to identify any unusual or unexpected relationships; and
- Undertaking journal testing, including an analysis of manual journal entries to assess whether there were large and/or unusual entries pointing to irregularities, including fraud.

A further description of the auditor's responsibilities for the audit of the financial statements is located at the Financial Reporting Council's website at [www.frc.org.uk/auditorsresponsibilities](http://www.frc.org.uk/auditorsresponsibilities).

This description forms part of our auditor's report.

**Other Matters which we are Required to Address**

We were initially appointed by the Comptroller and Auditor General on 4 March 2020 to audit the financial statements and subsequently reappointed on 7 October 2024 for a period of at least two more years. Our total uninterrupted period of engagement is 7 years.

The non-audit services prohibited by the FRC's Ethical Standard were not provided to the Authority and we remain independent of the Authority in conducting our audit.

Our audit opinion is consistent with the additional report to the audit committee in accordance with ISAs.

**Use of this Report**

This report is made solely to the Minister in accordance with Article 43 of the Data Protection Authority (Jersey) Law 2018. Our audit work has been undertaken so that we might state to the Minister those matters we are required to state to them in an auditor's report and for no other purpose. To the fullest extent permitted by law, we do not accept or assume responsibility to anyone other than the Authority and its Minister, as a body, for our audit work, for this report, or for the opinions we have formed.



Sandy Cameron

For and on behalf of Baker Tilly Channel Islands Limited

Chartered Accountants

St Helier, Jersey

Date: 25 April 2025

JERSEY DATA PROTECTION AUTHORITY (JDPA)  
AUDITED FINANCIAL STATEMENTS  
FOR THE YEAR ENDED 31 DECEMBER 2024

STATEMENT OF COMPREHENSIVE INCOME AND RETAINED EARNINGS

	Notes	2024 £	2023 £
<b>Income from activities</b>	4	2,325,260	2,275,510
<b>Operating expenses</b>			
Data Protection	5	(2,429,095)	(2,612,360)
<b>Deficit on ordinary activities</b>		<u>(103,835)</u>	<u>(336,850)</u>
<b>Other expenditure</b>			
GPA Conference Expenditure	19	(703,355)	(33,581)
Freedom of Information	18	<u>(57,651)</u>	<u>(62,945)</u>
		(761,006)	(96,526)
<b>Other income</b>			
Data Protection Fines Issued	20	4,500	-
GPA Conference ticket income	19	268,272	-
GPA Conference Sponsorship income	19	478,998	-
Government grant - Data Protection	6	-	85,419
Government grant - Freedom of Information	18	57,597	70,000
Interest		<u>11,873</u>	<u>8,545</u>
		821,240	163,964
Taxation	7	-	-
<b>Deficit for the year</b>		<u><b>(43,601)</b></u>	<u><b>(269,412)</b></u>
<b>Retained Surplus as at 1st January 2024</b>	17	<u><b>1,678,579</b></u>	<u><b>1,947,991</b></u>
<b>Retained Surplus as at 31st December 2024</b>		<u><b>1,634,978</b></u>	<u><b>1,678,579</b></u>

The JDPA's turnover and expenses all relate to continuing operations. There are no recognised gains or losses other than those shown above.

The notes on pages 12-17 form part of these Audited Financial Statements.

JERSEY DATA PROTECTION AUTHORITY (JDPA)  
AUDITED FINANCIAL STATEMENTS  
AS AT 31 DECEMBER 2024


STATEMENT OF FINANCIAL POSITION

ASSETS	Notes	2024 £	2023 £
<b>Non-current assets</b>			
Tangible assets	8	11,026	16,789
Intangible assets	9	<u>30,679</u>	<u>73,367</u>
		41,705	90,156
<b>Current assets</b>			
Trade and other receivables	10	160,983	144,383
Cash and cash equivalents	11	<u>1,649,153</u>	<u>1,667,814</u>
<b>Total Current assets</b>		1,810,136	1,812,197
<b>TOTAL ASSETS</b>		<u><b>1,851,841</b></u>	<u><b>1,902,353</b></u>
<b>CREDITORS – amounts falling due within one year</b>			
Trade and other payables	12	(204,460)	(219,987)
Deferred Income	13	<u>(12,403)</u>	<u>(3,787)</u>
		(216,863)	(223,774)
<b>TOTAL NET ASSETS</b>		<u><b>1,634,978</b></u>	<u><b>1,678,579</b></u>
<b>EQUITY</b>			
Share Capital	14	-	-
Reserve - Retained surplus	17	720,275	1,471,525
Reserve - Operating Reserve	17	707,703	-
Reserve - Legal Contingency Reserve	17	200,000	200,000
Restricted Reserve - Freedom of Information	18	7,000	7,054
<b>TOTAL EQUITY</b>		<u><b>1,634,978</b></u>	<u><b>1,678,579</b></u>

The financial statements on pages 12 to 17 have been prepared in accordance with the Data Protection Authority (Jersey) Law 2018 and Section 1A of Financial Reporting Standard 102.

The notes on pages 12 - 17 form part of these Audited Financial Statements.

The accounts were approved and authorised for issue on 25th April 2025 by the Authority and signed on its behalf by:

  
Paul Vane  
Information Commissioner  
on behalf of the JDPA



JERSEY DATA PROTECTION AUTHORITY (JDPA)  
AUDITED FINANCIAL STATEMENTS

NOTES TO THE FINANCIAL STATEMENTS  
FOR THE YEAR ENDED 31 DECEMBER 2024

1. General Information

The Jersey Data Protection Authority (JDPA) (the "Authority") was created by the Data Protection (Jersey) Law 2018 on 25 May 2018 and is responsible for the registration and regulation of Data Protection in Jersey. This law transferred all responsibilities for registration and regulation of Data Protection prescribed as the duty of the Minister or other States bodies to this new Authority. The Authority is a body corporate and its registered office is 2nd Floor, 5 Castle Street, St Helier, Jersey, JE2 3BT.

Basis of accounting

The financial statements have been prepared on the going concern basis, under the historical cost convention. The Authority has applied the small entities regime under Section 1A of the Financial Reporting Standard 102 (FRS 102), which allows qualifying entities certain disclosure exemptions. The Authority has taken advantage of the exemption from preparing a statement of cash flows under paragraph 7.1b.

Functional and presentational currency

The financial statements are prepared in Pounds Sterling (GBP or £) which is the functional and presentational currency of the Authority.

2. Statement of compliance

The financial statements have been prepared in compliance with FRS 102(1A) 'The Financial Reporting Standard applicable in the UK and Republic of Ireland' issued by the Financial Reporting Council and the Data Protection Authority (Jersey) Law 2018.

3. Summary of Accounting Policies, Estimates and Significant Judgements

The principle accounting policies applied in the preparation of these financial statements are set out below. These policies have been consistently applied to all years presented, unless otherwise stated or a new or amended accounting standard is applied.

The preparation of financial statements requires the use of certain accounting estimates. It also requires management to exercise its judgement in the process of applying accounting policies. Accounting estimates involve management's judgement of expected future benefits and obligations relating to assets and liabilities (and associated expenses and income) based on information that best reflects the conditions and circumstances that exist at the reporting date. There have been no changes to the accounting estimates from the previous financial period.

Going concern

The Authority consider, given that there is sufficient cash in place to fund mandated activities, the use of the going concern basis is appropriate for the current period and for 12 months from the date of signing these accounts.

Provisions

Provisions are recognised when the Authority has a present legal or constructive obligation, as a result of past events, for which it is probable that an outflow of economic benefits will be required to settle the obligation in future and the amount of the obligations can be reliably estimated.

Economic useful lives of intangible and tangible fixed assets

The Authority's fixed assets are depreciated on a straight-line basis over their economic useful lives. Useful economic lives of equipment are reviewed by management periodically. The review is based on the current condition of the assets and the estimated period during which they will continue to bring an economic benefit to the Authority.

Revenue recognition

Registration fees

Under the terms of Data Protection Authority (Jersey) Law 2018 registrations made to the Authority are valid for one year. The registration fees are non-refundable and fall due each year on 1st January. Income from registrations is recognised when it is earned. Deferred revenue represents revenues collected but not earned as of December 31. This is primarily made up of Grant income for Freedom of Information.

Operating Expenses

Expenses are accounted for on an accruals basis.

Employment benefits

Pension costs

As the Authority is an admitted body, past and present employees have been eligible to accrue post-employment benefits under the provisions of two possible defined benefit pension schemes, namely the Public Employees Contributory Retirement scheme ("PECRS") or the Public Employees Pension Fund ("PEPF").

The assets are held separately from those of the Government of Jersey and the responsibility to discharge accrued liabilities are held by those Funds. The Authority is not responsible to fund any deficit or to maintain the specific level of the pension assets to meet pension liabilities. In light of this, the scheme is accounted for as though it is a defined contribution scheme, with the annual cost to the authority taken to be equal to the employer's pension contributions payable to the scheme for the accounting period. The contributions are charged to operating expenses as and when they become due.

Contribution rates are determined on a triennial basis by an independent qualified actuary, so as to spread the costs of providing benefits over the members' expected service lives. The main purposes of the valuations are to review the operation of the scheme, to report on its financial condition and as noted, to confirm the adequacy of the contributions to support the scheme benefits. Copies of the latest annual accounts of the scheme, and Government of Jersey, may be obtained online at:  
<http://www.gov.je/Working/WorkingForTheStates/Pensions/PublicEmployeePensionFund/Pages/PublicServicePensionPublications.aspx>

JERSEY DATA PROTECTION AUTHORITY (JDPA)  
AUDITED FINANCIAL STATEMENTS

NOTES TO THE FINANCIAL STATEMENTS (CONTINUED)  
FOR THE YEAR ENDED 31 DECEMBER 2024

Interest receivable

Interest receivable is accounted for on an accruals basis.

Government Grant

Grants are recognised in other income in the year the related costs are incurred by the Authority for which the grant is intended to compensate. For grants which are received by the Authority for compensation for expenses or deficit which have already been incurred, the grant is recognised in income when it is received or receivable. Any residual grant income is held in deferred Income.

Tangible assets

Tangible assets consists of office equipment which is stated at historical cost less accumulated depreciation. Cost includes all costs directly attributable to bringing the asset to working condition for its intended use. Depreciation is calculated on the straight-line method to write-off the cost of equipment to their estimated residual values over their expected useful lives as follows:

- Office equipment 3 years
- IT equipment 3 years

The useful lives and depreciation methods used are reviewed regularly and any adjustments required are effected in the charge for the current and future years as a change in accounting estimate. Gains and losses on disposal of equipment are determined by reference to their carrying amounts and are taken into account in determining net profit. Repairs and renewals are charged to the statement of comprehensive income when the expenditure is incurred. The carrying values of the plant and equipment are reviewed for impairment when events or changes in circumstances indicate the carrying values may not be recoverable. If any such indication exists, and where the carrying values exceed the estimated recoverable amounts, the plant and equipment are written-down to their recoverable amounts. One full year of depreciation is charged in the year of acquisition. Items with a value in excess of £1,000 are capitalised. Items under this amount are expensed in the year.

The Authority's policy is to review the remaining useful economic lives and residual values of property, plant and equipment on an ongoing basis and to adjust the depreciation charge to reflect the remaining estimated useful economic life and residual value.

Intangible assets

Externally acquired intangible assets (website and software) are initially recognised at cost and subsequently amortised on a straight-line basis over their useful economic lives. The carrying amount of each intangible asset is reviewed periodically and adjusted for impairment where considered necessary.

Due to the revenue generation, regulatory function and API connection to Dynamics CRM, an expert opinion was sought on the useful economic life and 5 years was considered to be appropriate and in line with the Digital Strategy for the JDPA.

Intangible assets (website and software) held solely for the GPA conference are initially recognised at cost and subsequently amortised on a straight line balance basis over their useful economic lives of 16 months being the end date of the GPA conference.

The Authority's policy is to review the remaining useful economic lives on an ongoing basis, and to adjust the amortisation charge to reflect the remaining estimated useful economic life and residual value if appropriate. One full year of amortisation is charged in the year of acquisition.

Financial assets

Basic financial assets, including trade and other receivables, and cash and bank balances, are initially recognised at transaction price, unless the arrangement constitutes a financing transaction, where the transaction is measured at the present value of the future receipts discounted at a market rate of interest. Subsequent measurement shall be at fair value with the change in fair value recognised in profit or loss.

Financial assets are derecognised when (a) the contractual rights to the cash flows from the asset expire or are settled, or (b) substantially all the risks and rewards of the ownership of the asset are transferred to another party or (c) despite having retained some significant risks and rewards of ownership, control of the asset has been transferred to another party who has the practical ability to unilaterally sell the asset to an unrelated third party without imposing additional restrictions.

Trade and other receivables

Trade and other receivables are initially recognised at their fair value and are carried at their anticipated realisable values. An allowance is made for impaired trade and other receivables based on a review of all outstanding amounts at the year-end. Bad debts are written-off during the year in which they are identified. Subsequent measurement will see the change in the realisable value recognised in profit or loss.

Cash and cash equivalents

Cash and cash equivalents comprises of cash in hand.

Financial liabilities

Basic financial liabilities, including trade and other payables are initially recognised at transaction price, unless the arrangement constitutes a financing transaction, where the debt instrument is measured at the present value of the future receipts discounted at a market rate of interest. Financial liabilities are derecognised when the liability is extinguished, that is when the contractual obligation is discharged, cancelled or expires. Subsequent measurement shall be at fair value with the change in fair value recognised in profit or loss.

JERSEY DATA PROTECTION AUTHORITY (JDPA)  
AUDITED FINANCIAL STATEMENTS

NOTES TO THE FINANCIAL STATEMENTS (CONTINUED)  
FOR THE YEAR ENDED 31 DECEMBER 2024

Trade and other payables

Trade payables are obligations to pay for goods or services that have been acquired in the ordinary course of business from suppliers. Accounts payable are classified as current liabilities if payment is due within one year or less. If not, they are presented as non-current liabilities. Trade payables are recognised initially at transaction price and subsequently measured at amortised cost using the effective interest method.

Contingencies

Contingent liabilities, arising as a result of past events, are disclosed when it is possible that there will be an outflow of resources but the amount cannot be reliably measured at the reporting date. Contingent liabilities are disclosed in the financial statements unless the probability of an outflow is remote. Contingent assets are disclosed in the financial statements, but not recognised, where an inflow of economic benefits is probable.

Reserves

Unrestricted reserves include surplus funds arising from registration fees. The use of the reserves for business operations or one-off projects must be approved by the Authority.

Where a restricted reserve exists, the funds within it are appropriately disclosed, held separately, and ring-fenced for their intended purpose.

The Operating Reserve is maintained at a minimum level equivalent to three months of operating costs, with the specific amount determined by the Authority. This reserve is intended to support ongoing business operations and may be drawn upon with approval through established internal governance processes.

The Legal Contingency Reserve is maintained to support potential legal actions, including the pursuit of complex cases, initiating or defending litigation, and securing additional legal counsel. Use of this reserve is subject to approval in line with internal governance processes.

The Retained Surplus has been generated from registration fees earned in prior periods. Its use for business operations or one-off projects must be approved in line with internal governance processes.

The Freedom of Information Reserve is a restricted reserve comprising grant funding specifically allocated to support activities mandated under FoI legislation. Its use is restricted to purposes aligned with the terms of the original grant agreement issued by the Government of Jersey. Refer to Note 18 for further details.

4. Income from activities

Income from activities is made up of registration fees under the terms of Data Protection Authority (Jersey) Law 2018. The registration fee income in the year was £2,325,260 (2023 £2,275,510)

5. Operating expenses - Data Protection

	2024	2023
	£	£
Staff including Commissioner and Deputy Commissioner	1,529,294	1,550,930
Services and Communications	590,489	789,450
Administrative Expenses	27,697	25,040
Audit and accountancy fees	32,345	26,254
Premises and Maintenance	172,034	172,493
Bank charges	11,007	11,152
Depreciation, Amortisation and Provisions	66,229	70,622
	<u>2,429,095</u>	<u>2,645,941</u>

JERSEY DATA PROTECTION AUTHORITY (JDPA)  
AUDITED FINANCIAL STATEMENTS

NOTES TO THE FINANCIAL STATEMENTS (CONTINUED)  
FOR THE YEAR ENDED 31 DECEMBER 2024

6. Government grant

The Government Data protection grant provided in the year was £nil (2023:£85,419). Any net deficit of the Authority's operating costs is financed by the Government of Jersey under the Partnership Agreement. The current partnership agreement has been extended until 30 June 2025.

The Government provided a 'top up' grant of £50,000 as sponsorship of the Global Privacy Assembly conference.

The Government also provided a grant for Freedom of Information activity in the year £70,000 (2023:£70,000). This amount was reduced to £57,651, as the activity cost was lower than the grant amount. £7,054 has been retained as part of a restricted reserve for future expenditure. This grant payment is subject to a separate Partnership agreement. Please refer to Note 18 for further details.

7. Taxation

Article 42 of the Data Protection Authority (Jersey) Law 2018 provides that the income of the Authority shall not be liable to income tax under the Income Tax (Jersey) Law 1961.

8. Tangible assets

	2024		
	£		
	Office equipment	IT equipment	Total
Cost			
As at beginning of year	49,531	73,261	122,792
Additions in the year	-	10,913	10,913
Disposals in the year	-	(9,379)	(9,379)
	<u>49,531</u>	<u>74,795</u>	<u>124,326</u>
Accumulated depreciation			
As at beginning of year	45,372	60,630	106,002
Depreciation charge for the year	4,159	3,139	7,298
	<u>49,531</u>	<u>63,769</u>	<u>113,300</u>
Net book value			
As at 31 December 2024	-	11,026	11,026
As at 31 December 2023	<u>4,158</u>	<u>12,631</u>	<u>16,789</u>

9. Intangible assets

	2024		
	£		
	Website and Software	GPA Conference Website	Total
Cost			
As at beginning of year	246,968	20,822	267,790
Additions in the year	3,969	-	3,969
	<u>250,937</u>	<u>20,822</u>	<u>271,759</u>
Accumulated amortisation			
As at beginning of year	188,603	5,820	194,423
Charge for the year	31,655	15,002	46,657
	<u>220,258</u>	<u>20,822</u>	<u>241,080</u>
Net book value			
As at 31 December 2024	30,679	-	30,679
As at 31 December 2023	<u>58,365</u>	<u>15,002</u>	<u>73,367</u>

10. Trade and other receivables

	2024	2023
	£	£
Trade Debtors- Data Protection	5,641	7,000
Trade Debtors- GPA sponsorship	104,000	-
Other Debtors	13,917	9,359
Grant receivable	-	85,419
Prepayments	37,425	42,605
	<u>160,983</u>	<u>144,383</u>



JERSEY DATA PROTECTION AUTHORITY (JDPA)  
AUDITED FINANCIAL STATEMENTS

NOTES TO THE FINANCIAL STATEMENTS (CONTINUED)  
FOR THE YEAR ENDED 31 DECEMBER 2024

11. Cash and cash equivalents

The Authority has £1,572,279 at the end of the year (2023: £1,660,760). £76,874 (2023:£7,054) is within a restricted account which can only be used for Freedom of Information activities. All balances are cash and are held in the Authority's own bank accounts.

12. Trade and other payables

	2024	2023
	£	£
Accruals and trade creditors	(204,460)	(219,987)
	<u>(204,460)</u>	<u>(219,987)</u>

13. Deferred Income

	2024	2023
	£	£
Freedom of Information Grant	12,403	-
Conference ticket sales	-	3,787
	<u>12,403</u>	<u>3,787</u>

14. Share capital

The JDPA was incorporated in Jersey under the Data Protection Authority (Jersey) Law 2018 and has no share capital.

15. Related Party Transactions

The Related Party Transactions for the JDPA solely relate to the Authority remuneration.

Authority Remuneration

	2024	2023
	£	£
Information Commissioner	132,949	124,252
Chair Term ended October 2024	15,247	17,291
Chair November 2024 onwards	3,049	-
Voting member (Non Executives) Term Ended October 2024	10,031	11,250
Voting member (Non Executives)	4,815	4,500
Voting member (Non Executives)	12,038	11,250
Voting member (Non Executives)	12,038	11,250
Voting member (Non Executives)	8,025	6,134
Voting member (Non Executives)	9,630	6,132
Voting member (Non Executives)	<u>9,630</u>	<u>6,000</u>
	<u>217,452</u>	<u>198,059</u>

Key management personnel includes the Commissioner and the Voting Members who together have authority and responsibility for planning, directing and controlling the activities of the JDPA.

All amounts paid to key management personnel were in line with the contractual agreement and entirely related to remuneration for the above described services.

The JDPA has recognised £nil (2023: £85,419) as grant income from the Government of Jersey. The JDPA is accountable to the Government of Jersey by means of the Partnership Agreement.

16. Controlling Party

The JDPA was incorporated in Jersey under the Data Protection Authority (Jersey) Law 2018 and works as an independent Authority. As such, it is not considered to have a controlling party.

17. Retained Surplus

The retained surplus has been generated through registration fees earned in prior periods. To enhance the accuracy of the financial statements and to give greater clarity on the use of the surplus the following structure for the retained earnings has been put in place.

	2024	2023
	£	£
Reserve - Retained surplus	720,275	1,671,525
Reserve - Operating Reserve	707,703	-
Reserve - Legal Contingency Reserve	<u>200,000</u>	<u>-</u>
	<u>1,627,978</u>	<u>1,671,525</u>

JERSEY DATA PROTECTION AUTHORITY (JDPA)  
AUDITED FINANCIAL STATEMENTS

NOTES TO THE FINANCIAL STATEMENTS (CONTINUED)  
FOR THE YEAR ENDED 31 DECEMBER 2024

18. Freedom of Information  
Income

A grant of £70,000 was received in the year under a partnership agreement between the Information Commissioner and the Government of Jersey with the JDPA receiving the grant on behalf of the Information Commissioner ("Recipient of the Grant"). Freedom of Information (FoI) functions are funded solely by way of this annual funding from the Government of Jersey and the sole purpose of this funding is for FoI related activities. FoI cash is held in a separately named bank account as per note 11.

Operating expenses

	2024	2023
	£	£
Staff including Commissioner and Deputy Commissioner	24,613	24,158
Services and Communications	24,491	30,975
Administrative Expenses	924	974
Audit and accountancy fees	1,000	550
Premises and Maintenance	4,839	4,509
Bank charges	180	-
Depreciation and Amortisation	<u>1,604</u>	<u>1,779</u>
	<u>57,651</u>	<u>62,946</u>

The Freedom of Information grant was calculated using an assumption that 3% of operating activity within the JDPA was solely attributable to Freedom of Information functions. This assessment was used to form a baseline for the value of the grant. The agreement with the Government of Jersey contains clearly defined mechanisms to enable additional funding to be requested or for unutilised grant funding to be reimbursed to the Government. During 2024 £57,651 (2023:£62,946) of costs, made up of actual and apportioned costs based on the 3% allocation, were incurred leaving an underspend against the full grant funding of £12,350 (2023:£7,054). The total cost incurred was transferred from the FoI bank account and the remaining grant funding is expected to be returned to the Government of Jersey in 2025.

19. Significant items of Expenditure of note

The JDPA hosted the 46th International Global Privacy Assembly (GPA) Conference in October 2024. Due to the size of the event, work commenced on the construction of the website and on the planning and budgeting of the event during 2023. These items are expensed through the Profit and Loss account. 2023 saw £33,581 expensed. A portion of the retained surplus for the JDPA had been set aside as a cashflow however, the Conference was funded by ticket sales and event sponsorship so has an overall net nil impact on the operating costs for the JDPA. The surplus funds are held within the retained surplus to allow for clearance of unexpected items of expenditure should any occur.

	2024	2023
	£	£
Jersey International Conference		
Opening Balance	(33,581)	-
Ticket Sales	268,272	-
Sponsorship	478,998	-
Expenditure incurred	<u>(703,354)</u>	<u>(33,581)</u>
	<u>10,335</u>	<u>(33,581)</u>

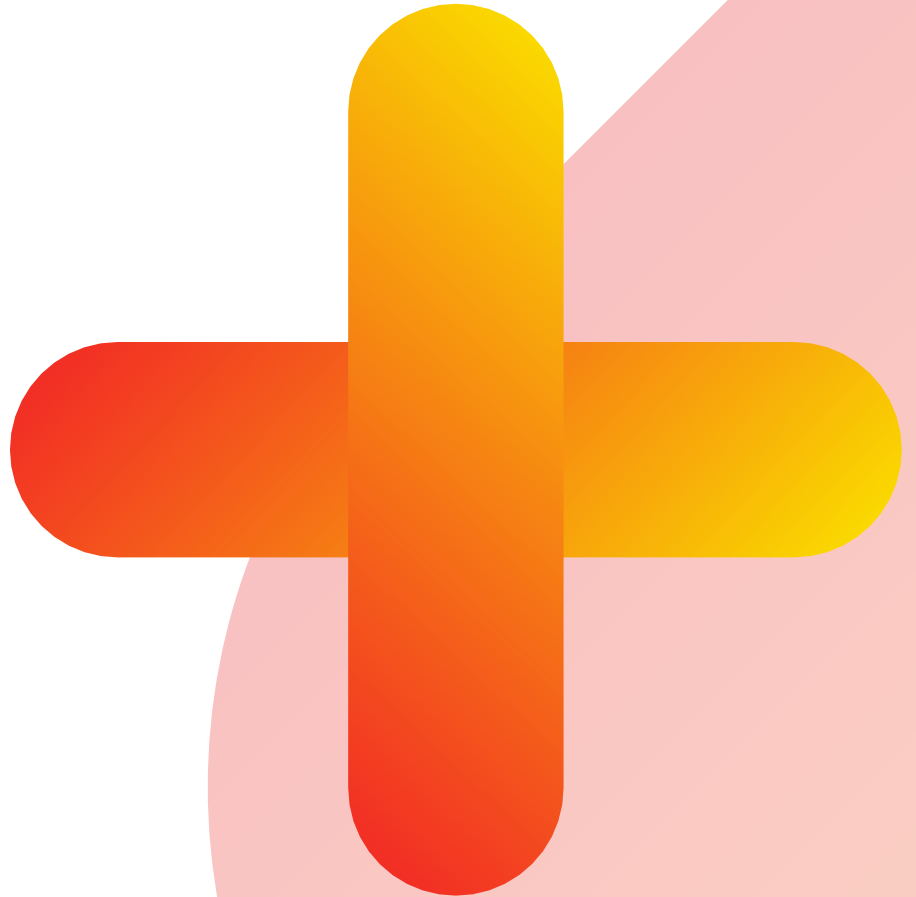
20. Data Protection Fines

The JDPA can issue administrative fines under Article 26 of the Data Protection Authority Jersey Law 2018. In December 2024 two fines were issued with a combined value of £4,500 (2023:£nil). The fine income is paid over to Government when it is collected and is not retained by the JDPA. The JDPA are able to offset any costs incurred in the collection of the fine monies.

	2024	2023
	£	£
Administrative Fine 1	500	-
Administrative Fine 2	<u>4,000</u>	<u>-</u>
	<u>4,500</u>	<u>-</u>



**JOIC**<sup>®</sup>  
JERSEY OFFICE OF THE  
INFORMATION COMMISSIONER



+44 (0) 1534 716 530

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

**[www.jerseyoic.org](http://www.jerseyoic.org)**

