JERSEY OFFICE OF THE INFORMATION COMMISSIONER

ANNUAL REPORT

R.82/2022

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

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

Contents

JOIC
JERSEY OFFICE OF THE
INFORMATION COMMISSIONER

2021 Highlights

Increased Membership of International Forums & Networks.

- Association francophone des autorités de protection des données personnelles (AFAPDP)
- Global Privacy Enforcement Network (GPEN)
- International Association of Privacy Professionals (IAPP)
- British Isles and Irish Data Protection Authorities Association (BIIDPA).

90
Complaints Handled.

100
Guests attended our lively debate 'Your Privacy – a price worth paying?'

44
Sessions delivered to Island schools as part of Young Privacy Ambassador Programme.

Following school sessions
80% of students
said they understood importance of protecting their personal information.

6692
Organisations registered.

Authority Chair & 3 Authority members reappointed.

Handled 232
self-reported data breaches.

Commended by Global Privacy Assembly for Covid-19 guidance.

180
Guests at
↓
JOIC Events
↓
75%
of attendees said information presented would benefit them personally and professionally.

Interactive Let's Go DPO network created.

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 information by:

- Implementing and ensuring compliance with the Data Protection (Jersey) Law 2018 (the DPJL) and the Data Protection Authority (Jersey) Law 2018 (the DPAJL).
- Influencing attitudes and behaviours towards privacy and processing of personal information, 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 implementing the Freedom of Information (Jersey) Law 2011 (the FOI Law). This includes encouraging public authorities to follow good practice in their implementation of the FOI Law (including adherence to the relevant code of practice) and help 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 PURPOSE

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

OUR VALUES

Our values are hugely important to us, they create our identity and inform how we do business. 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 Values

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 with 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

The people of Jersey are provided with a high level of data protection and expert service whilst resources are judiciously and responsibly managed.

To achieve this outcome, we will:

- Implement a public education programme making individuals aware of their data protection rights while facilitating public authorities and businesses in complying with their responsibilities.
- Work collaboratively with businesses, organisations, charities/not-for-profit and public authorities to assist them with meeting their legal obligations, while promoting innovation in service to the public.
- Implement an effective and fair enforcement programme.

02

The Island's approach to data protection clearly contributes to its reputation as a well-regulated jurisdiction.

To achieve this outcome, we will:

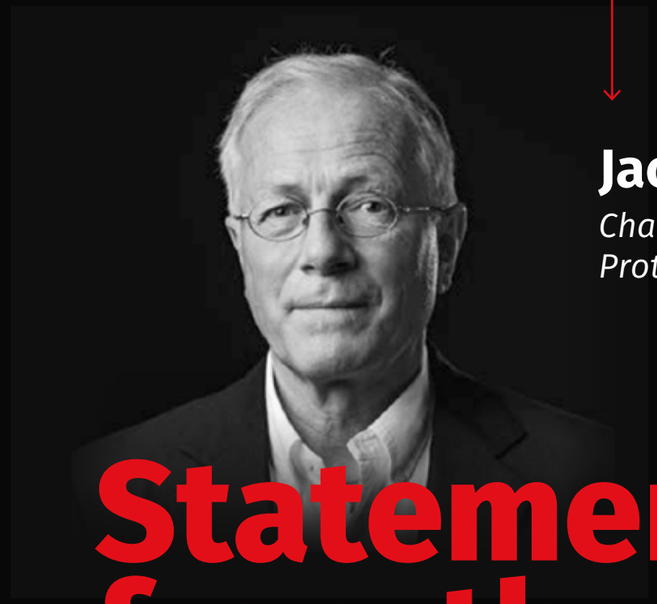
- Demonstrate an ethical approach and a commitment to regulatory excellence at all times in all of our interactions, both locally and internationally.
- Take advantage of all appropriate opportunities to speak in both local and international venues.
- Collaborate with other data protection authorities internationally and other regulators in Jersey on investigations and the development of guidance material.

03

Jersey is recognised as a world leader, embracing innovation to safely develop and implement digital technology.

To achieve this outcome, we will:

- Bring an innovative and solutions-focussed approach to all data protection issues that promotes compliance, as well as business and public policy success.
- Develop the technical expertise necessary to participate effectively in forums involving data protection and technology and to anticipate technological developments on the horizon that may have data protection implications.
- Collaborate with stakeholders in implementing a regulatory sandbox to facilitate the development of new technologies for processing personal data safely and securely.



Jacob Kohnstamm

Chair, Jersey Data Protection Authority

Statement from the Chair

Once again, it is my pleasure on behalf of the Jersey Data Protection Authority (the Authority) to present to the Minister and members of the States Assembly our Annual Report for 2021. This fulfils our statutory obligation under Article 44 of the Data Protection Authority (Jersey) Law 2018.

In last year's report, I spoke of the extraordinary challenges 2020 brought as we attempted to navigate the previously unchartered waters of a global pandemic. As well as the increased workload created by the many privacy issues surrounding track and trace regimes, we endured the social interruption of not being able to meet in person. The Covid situation also meant that we were unable to say a proper farewell to our outgoing Information Commissioner, Dr Jay Fedorak, who completed his three-year term in July. Jay has been instrumental in leading the Jersey Office of the Information Commissioner (JOIC) into the post-GDPR era, having built an excellent team and foundations for the future of the Authority. We thank him sincerely for his hard work and dedication to privacy and data protection and wish him well in his new venture as a private consultant operating from his hometown in British Columbia.

As one door closed, another opened, with our new Information Commissioner, Paul Vane, stepping into the role in July. Similarly, we were not able to formally welcome Paul in person, however we are delighted that Paul will be leading the JOIC into the next chapter and continuing to strengthen the organisation as we deal with the challenges of emerging technologies and Artificial Intelligence (AI).

Last year I also spoke of the importance of the Government of Jersey (Government) recognising data protection as a fundamental human right. As I stated then, a key value of data protection is the principle of fairness, which extends to the work of the public sector as well as private enterprise. Currently, the private sector provides 80% of the funding of the Authority, with Government paying the remaining 20% by way of a grant. However, Government is the largest user of personal data, much of which is also personal data of a sensitive nature. Citizens have little choice but to relinquish control of their personal data if they are to fully participate in society. It is therefore incumbent upon Government to recognise that there are compelling reasons to pay their fair share of the cost of regulating data protection in Jersey. Discussions on a more appropriate funding mechanism commenced in 2021, however there has been no marked step forward in resolving this issue at the time of writing. The fact remains that the private sector pays the majority of the Authority's funding, which in the long term may prove problematic in terms of the independence of the Authority. The year ended on a more positive note however, with the Minister recognising that a resolution to this issue should be a high priority in 2022.

In terms of our personal privacy, there is a sense that privacy is something we no longer have control over. Unlike many things in life, privacy is an intangible asset which we cannot easily see. That makes it more difficult to quantify or place any tangible value upon. New emerging technologies and concepts such as artificial intelligence seem far from the grasp of the everyday individual, whereas the business sector and the public sector can more readily see the benefits of AI to their human resources, productivity and profit margins. Our Authority works a lot with businesses to ensure they have the appropriate policies, procedures and technical and organisational measures in place to protect the personal data they hold about their customers. However, it is our intention to focus more on citizens to provide them with the necessary tools and education to better protect their own personal data.

> *... it is our intention to focus more on citizens to provide them with the necessary tools and education to better protect their own personal data....*

The volume of personal data recorded by governments and 'big tech' companies in the fight against and response to Covid has been unprecedented. The silver lining is that the pandemic has woken many individuals and communities to this high level of data processing, questioning the public benefits of such large-scale processing and how this impacts personal privacy. Individuals are beginning to place greater value on their personal data. There is no doubt that in the midst of a global crisis, data sharing for the public good is of paramount importance. However, such processing should not be at the expense of privacy. Governments, organisations and Data Protection Authorities (DPAs) such as ours have a shared responsibility to ensure privacy is considered throughout the data processing lifecycle and individuals are afforded the fundamental right of data protection. DPAs cannot and should not be expected to do it alone.

Returning finally to the pandemic, in addition to the national lockdowns imposed upon many jurisdictions, the global coverage of our Authority members gave rise to difficulties in travelling to Jersey. As a result, our Authority meetings were forced to move online across different time zones and like most, we learned quickly to adapt to online video conferencing platforms to carry on our business. This continued into 2021 as the second and third waves of Covid continued to prevent us from travelling and thus meeting in person. Technology has proved invaluable in bringing the Authority together in a 'virtual' boardroom and has been an adequate substitute to physical meetings. However, teams work well with face-to-face contact and over the preceding months we have very much missed the human contact. The social element to any work forms a critical part of our team cohesion and effectiveness. It has been nearly two years since we were last together in person, and as I often say jokingly, there is no such thing as a 'virtual' beer! We look forward to a time in the near future when our Authority can once again be together.

Looking ahead, we will continue to strengthen our infrastructure and strategic capabilities with investment and focus on three key areas: enhancing the resilience and reporting capabilities of our technology infrastructure, continued development of our supervision and oversight activities and the development of a data stewardship regulatory framework in collaboration with other agencies and industry stakeholders in support of Jersey's aspiration to be a leading jurisdiction for data trusts.

Jacob Kohnstamm(s)
Chair, Jersey Data Protection Authority

Paul Vane BA(Hons) Soc Pol Crim (Open)
Information Commissioner

Information Commissioner's Foreword

It is with immense pride that I present my first Annual Report as Commissioner under the Data Protection Authority (Jersey) Law 2018 and Freedom of Information (Jersey) Law 2011. The Jersey Office of the Information Commissioner has come a long way in the three years since the European General Data Protection Regulation (GDPR) came into effect along with our new laws in Jersey, and I would like to take the opportunity first of all to thank my predecessor, Dr Jay Fedorak, for his leadership, support and expertise in steering the organisation to where it is today. Jay will be missed by all of us here and we wish him every success in his new role in his homeland of Victoria, BC.

2021 was a year when we all hoped we would see a return to 'normality' following the previous 12 months of the pandemic. However, I have always said that the concepts of 'normality' and 'privacy' are very alike, in that people's ideals of privacy and what can be considered 'normal' are personal to the individual. In reality, we saw little change at the beginning of the year as Covid case numbers increased and new variants emerged. The JOIC faced similar Covid related issues in respect of data security when working from home, contact tracing and the proposed introduction of Covid vaccination certificates. The team worked hard to ensure guidance was up to date, relevant and on hand to provide advice where needed.

The effectiveness of the JOIC's suite of guidance was recognised by the Global Privacy Assembly[1] (GPA) at their international conference in October and I was asked to present on Jersey's response to the pandemic to the GPA Covid-19 working group. A number of the group's members adopted the Jersey guidance for their own authorities. Examples like this highlight the importance of our participation in international discussions around data protection and put Jersey on the international data protection map. I am extremely proud of my team for their agility, working at pace to produce a suite of guidance whilst facing their own challenges brought about by the pandemic. It also demonstrates that even as a small island jurisdiction, Jersey can have an influence on international policy development.

> ***Even as a small island jurisdiction, Jersey can have an influence on international policy...***

In terms of our other activities throughout the year, case investigations continued to dominate much of the team's work. By far the largest proportion of casework undertaken in 2021 related to complaints against the public sector. 29% of all complaints received were made against public sector organisations, with many relating to issues around data security, data sharing and lack of response to data subject access requests. In terms of self-reported data breaches, the financial and professional services sector made the largest proportion of reports. This appears to reflect their familiarity with working to a regulator driven compliance framework and speaks well to the strength of their internal controls. Whilst few complaints or breach reports were of a level that warranted any formal sanction from our office, the team used the opportunity of intervention to help educate organisations on how to improve their processes and avoid future similar occurrences.

For the first time in 2021, and despite the challenges presented by the pandemic, we completed our first compliance audits, focusing on the high-risk data processing activities, such as those organisations holding more sensitive, health-related information. The team audited 26 organisations with the aim of improving levels of data protection compliance across that sector. This first tranche of audits represented a tangible success for both the sector concerned and our office, with both benefitting greatly from the experience. Our aim for 2022 is to expand this aspect of our responsibilities significantly.

Again, despite the limitations imposed by the pandemic, we continued to adapt our education and outreach programme, combining online delivery with 'in person' events and awareness sessions. We successfully launched our Board Support Squad initiative as well as our 'Let's Go DPO' workshops and continued our school's education programme and industry awareness talks.

Perhaps one of the highlights of our events calendar for 2021 was our first debate, 'Your privacy – A price worth paying?' which attracted over 100 attendees. The event promoted some deep discussion about how much of our privacy we are willing to trade for the goods and services we all expect and need. However, the overwhelming highlight for me was the inclusion of some of the Island's young people in the discussions, who provided a different, but hugely

Transferring personal data out of Jersey is critical to the stability of our economy and a major part of the day-to-day activities of many local businesses, particularly the finance industry.

relevant perspective. We all learned a thing or two from their presence and will continue to involve our young people in future events.

Other areas of focus during 2021 included the much-debated topic of international data transfers, particularly in light of the events of the previous two years, namely Brexit, the decision of the Court of Justice of the European Union to invalidate the EU-US Privacy Shield in 2020 and the introduction of updated Standard Contractual Clauses by the European Commission.

Whilst these three factors may not mean a lot to the average person on the street, the impact of these is far reaching. Transferring personal data out of Jersey is critical to the stability of our economy and a major part of the day-to-day activities of many local businesses, particularly the finance industry. The public sector is also reliant on cross-border data transfers for some of its back-office functions, so it is easy to understand why any potential barriers to transferring data can cause such anxiety in a small jurisdiction like ours. Our office has been working hard to monitor international developments in this rapidly changing area. In September last year, we set up a working group in collaboration with our colleagues at Jersey Finance Limited to explore the issues faced by Jersey businesses, the impact on Islanders and look at options for a practical way forward. These discussions are ongoing, and I look forward to sharing the results of those discussions in next year's report.

Returning to our international work, since the re-establishment of the GPA in 2018, the JOIC has become an active member of several working groups, ranging from enforcement cooperation, digital education, artificial intelligence and data sharing for the public good. Our participation in all of these helps to shape our own strategies whilst ensuring a consistent approach with our international colleagues.

Artificial Intelligence and the continued advancement in technology and the internet is an important and growing area giving rise to many privacy issues. It is critical our office is involved in these discussions as much as possible to both influence and be influenced by our international colleagues and privacy experts. This will improve our own understanding of the impact of AI and shape how we can best educate Islanders and local businesses for the overall benefit of the Island.

In addition to the GPA, the JOIC has continued to be involved in other international forums and data protection networks. We now have a presence on a number of other international groups, including the Association francophone des autorités de protection des données personnelles[2] (AFAPDP), the Global Privacy Enforcement Network[3] (GPEN), the International Association of Privacy Professionals[4] (IAPP), and the British, Irish and Islands' Data Protection Authorities Association (BIIDPA).

Keeping an eye on the international data protection arena has become a fundamental part of our work at the JOIC and essential to fulfilling our strategic outcomes. Thanks to rapid technological advancement and the growth of the internet, the ease of movement of data has improved greatly and the accessibility and availability of data has improved significantly. As a result, the value of personal data has increased exponentially, and the controls required to protect data have strengthened as the risks associated with data transfers increase. Working together as a global data protection community benefits both businesses and individuals alike, and it is therefore critical to our Island future that Jersey continues to have a voice on the global stage.

The JOIC remains committed to ensuring our Islanders and those who interact with Jersey organisations are afforded the very highest standards of data protection for this generation and those to follow as we strive to add real value to our Island's health and prosperity and achieve our long-term vision whereby thinking privacy becomes instinctive.

Paul Vane BA(Hons) Soc Pol Crim (Open)
Information Commissioner

4

The Jersey Data Protection Authority

The Jersey Data Protection Authority is a statutory body which oversees the protection of personal data. The Authority consists of the Chair, five 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:

01 **is responsible for managing the other employees of the Authority.**

02 **is in charge of the day-to-day operations of the Authority.**

03 **has the functions conferred or imposed on him or her by the Law and any other enactment.**

The Information Commissioner has the delegated responsibilities of the Authority, undertakes the functions of the Authority under the Data Protection Authority (Jersey) Law 2018 (DPAJL) and the Data Protection (Jersey) Law 2018 (DPJL) other than, the issuing of a public statement under Article 14, the making of an order to pay an administrative fine under Article 26, 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 of 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.

Governance, Accountability & Transparency

→ The Jersey Data Protection Authority

The Authority has responsibility to:

- → Ensure that the Jersey Office of the Information Commissioner (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 ten 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 Law, 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.

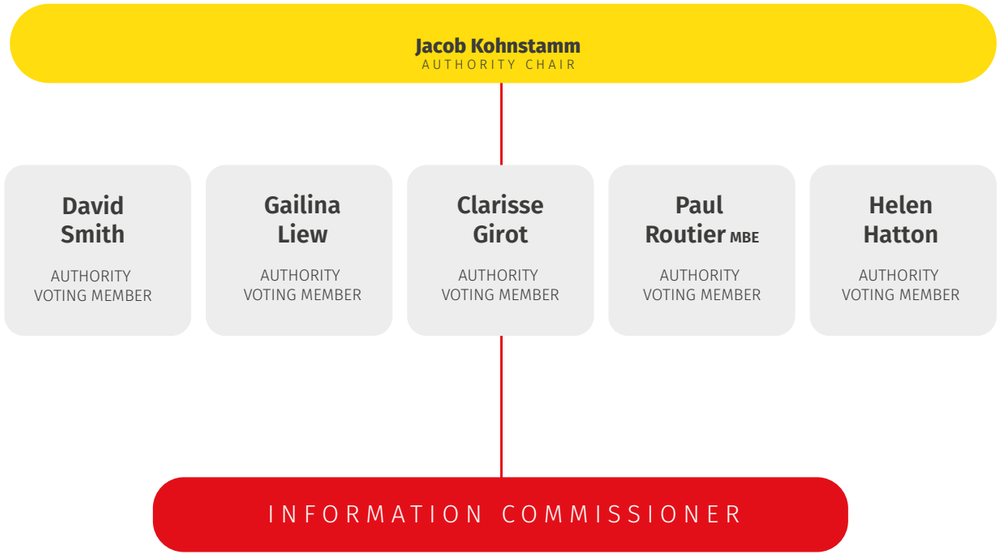
The Authority has delegated all these other powers and functions to the Information Commissioner.

There are certain functions that the Authority Law stipulates that the Authority must perform itself, and which cannot be delegated to the Information Commissioner. The most important function is that only the Authority can decide whether to issue administrative fines 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.

Authority Structure & Authority Report

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

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



Authority Members

CHAIR OF THE AUTHORITY

Jacob Kohnstamm

TENURE
Chair since May 2018, current period of office until 24 May 2024.

EXPERIENCE
Jacob has 18 years' experience in the field of data protection, having served as chairman of the Dutch Data Protection Authority for 12 years.

He also served as vice chairman of the Article 29 Data Protection Working Party for six years; the advisory body composed of the chairs of all Data Protection Authorities in the European Union. Prior to that, Jacob served as vice chairman of the Executive Committee of the International Conference of Data Protection and Privacy Commissioners for four years and hosted that conference in Amsterdam in 2015.

VOTING AUTHORITY MEMBER

Clarisse Girot

TENURE
Clarisse joined the Authority in October 2018 and has recently been reappointed for a further three years until 28 October 2024.

EXPERIENCE
Clarisse is a seasoned data privacy and Asian law expert and has unique expertise in the area of the regulation of international data flows.

She is also a well-known figure in the world of data protection globally, having been involved in major international cases in data protection and privacy.

VOTING AUTHORITY MEMBER

Helen Hatton

TENURE
Helen joined the Authority on 1 August 2019 for a period of three years. Her current term of office is due to expire on 31 July 2022.

EXPERIENCE
Helen is widely recognised as the prime architect of the modern Jersey regulatory regime. Helen retired as Deputy Director General of the Jersey Financial Services Commission in May 2009 having led the implementation of regulatory development in the Island from its blacklisted state in 1999 to achieving one of the world's best International Monetary Fund (IMF) evaluation results.

VOTING AUTHORITY MEMBER

David Smith

TENURE
David joined the Authority in October 2018 and has recently been reappointed for a further two years until 28 October 2023.

EXPERIENCE
David is an independent data protection expert, following his retirement from the role of Deputy Commissioner at the UK Information Commissioner's Office (ICO) in November 2015.

David spent over 25 years working with the ICO and its predecessors, serving in a variety of data protection roles, under four previous commissioners.

As Deputy Commissioner David had oversight of all the ICO's data protection activities, including its enforcement regime, successfully leading the introduction of the UK's first administrative fines. He played a significant role in shaping the UK position on the General Data Protection Regulation and represented the ICO on the Article 29 Working Party of European Supervisory Authorities set up under the Data Protection Directive.

VOTING AUTHORITY MEMBER

Gailina Liew

TENURE
Gailina joined the Authority in October 2018 and has recently been reappointed for a further three years until 28 October 2024.

EXPERIENCE
Gailina is a broadly-experienced independent non-executive director with a legal, scientific, operations and international business executive background. She is interested in the evolving frameworks for the regulation of privacy, data protection and their intersection with the ethical use of technology, human behaviour, artificial intelligence, and the future of human society.

Gailina brings more than 20 years of board governance experience and data protection perspectives from the listed company, investment fund, human health, economic development, education, regulatory, adjudication and voluntary sectors to the Jersey Data Protection Authority.

VOTING AUTHORITY MEMBER

Paul Routier MBE

TENURE
Paul joined the Authority on 1 August 2019 for a period of three years. His current term of office is due to expire on 31 July 2022.

EXPERIENCE
Paul was an elected member to the States of Jersey for 25 years and Assistant Chief Minister for a period of this time. During this time, he was responsible for working with officers and the public to develop a number of policy documents and legislation covering a wide cross section of commercial and social issues. Before presenting any new legislation to the States Assembly, he made it a priority to ensure that a satisfactory public consultation had been done.

During his final term of office, he successfully led the debates in data protection legislation which, after gaining the support of States Members, led to the establishment of the Data Protection Authority. He also led the time critical political work in negotiating the final version of the Data Protection (Jersey) Law 2018 and the Data Protection Authority (Jersey) Law 2018 which are in force today.

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

Governance Report

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

The following table sets out the number of full Authority and Sub-Committee meetings held during 2021 and the number of meetings attended by each voting Authority member.

	Full Authority	Audit and Risk	Governance	Remuneration & Human Resources
Number of Meetings	5	7	4	2
Clarisse Girot	5	-	4	-
Helen Hatton	5	7	-	-
Jacob Kohnstamm	4	-	4	2
Gailina Liew	5	7	4	-
Paul Routier MBE	5	-	-	2
David Smith	5	7	-	-

→ 2021 Authority Members' Remuneration

The Authority voting members received, in aggregate, £61,427 in remuneration in 2021.

Further details regarding the Authority voting member remuneration can be found at page 76.

→ Performance Evaluation and Re-appointments

The Governance Committee has established an Authority performance evaluation process which is based on an internal annual peer review of performance by voting members with an independent external review contemplated for every third year. The first internal performance evaluation took place in 2021.

The Chair's first three-year term of office expired on 24 May 2021 and three Jersey Data Protection Authority members' terms of office expired in the autumn of 2021. The outcome of the performance evaluation provided evidence upon which the Chair based formal letters to the Minister to recommend the reappointment of three Authority members. The Chair was also recommended to the Minister for reappointment based on a rigorous individual performance review.

The Governance Committee has also established a self-assessment process to survey the breadth of skills, knowledge and experience of Authority voting members. This process was undertaken for the first time in 2021 to generate a Skills Matrix for the Authority. The Skills Matrix reflects a broad mix of skills, knowledge and experience across the primary areas of governance, sectoral skills and personal attributes that are appropriate for the Authority's mandate.

→ Diversity of the JDPA

The six voting members of the Authority reflect a balance between male and female members, different nationalities, ranging in age from late 40s to early 70s, with a broad mix of formal education and professional qualifications including law, IT, sciences, business administration, education and teaching.

Authority Sub-Committees

→ Audit & Risk Committee (ARC)

The voting members who comprise the ARC are:

Helen Hatton (Chair) / Gailina Liew / David Smith

The Audit & Risk Committee'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 / Clarisse Girot

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.
- Lead the process for appointments ensuring plans are in place for the orderly succession to the Authority.
- 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.

→ Remuneration & Human Resources Committee (R&HR)

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

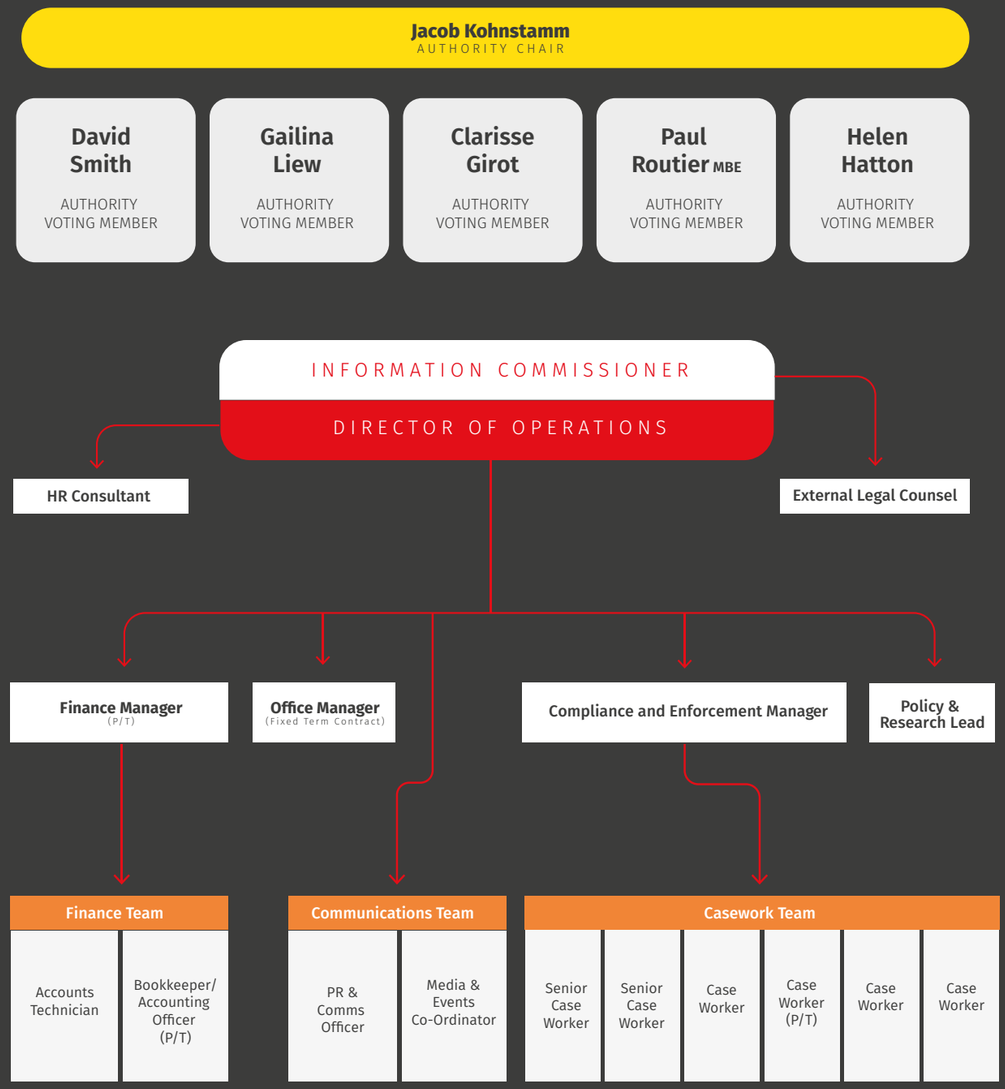
Paul Routier MBE (Chair) / Jacob Kohnstamm

The Remuneration & Human Resources 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.

Organisational Structure



5

Principal and Emerging Risks

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

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

Our low appetite for risk is due to our obligation to fulfil our statutory responsibilities as the independent body promoting respect for private lives. Maintaining trust, independence and reputation is essential for the Authority.

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 scrutinised via a scoring mechanism which is linked to likelihood and consequence.

The following table identifies the principal risks and mitigating actions. The risks are categorised into five main areas.

01 **Legal and Regulatory**

02 **Operational**

03 **Governance**

04 **Strategic**

05 **Political**

Summary of Principal Risks

Legal & Regulatory

Risk Description	How we manage the risk	Covid-19 Response
Internal compliance – failing to comply with the Data Protection Authority (Jersey) Law 2018 in terms of case management, process and reasonableness of decisions made.	→ Understand our compliance obligations and what this looks like on a practical level. → Monitor how we implement and sustain our obligations. → Put in place effective and ongoing training, staff feedback, internal audits and reviews.	→ We understand that data controller/processor resources may be diverted away from usual governance and compliance work. We expect to see timely and transparent communication with data subjects and the Authority.
Perception – industry and Government perception that our effectiveness as a regulator is based on our fining actions.	→ Maintaining consistent and compliant investigation, inquiry and audit processes. → Enforcing appropriate and proportional enforcement sanctions.	→ We meet the standards as required by the Law to ensure consistency and fairness throughout our regulatory activities.

Operational

Risk Description	How we manage the risk	Covid-19 Response
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.	→ Embedding succession planning throughout the organisation. → Building skills and knowledge through personal and professional development. → Human Resources strategy aligns with our strategic outcomes. → Striving for diversity and inclusion throughout our operational and HR activities.	→ We care about our team's welfare, especially when working away from the office. Our employee communication and engagement put health and well-being first. → We cross-train where possible to ensure resilience and avoid a single point of failure.
Revenue. The revenue model is delivering sufficient monies to support the necessary activities of the Authority. Any changes in revenue streams from industry or Government funding could impact on our ability to fulfil our regulatory functions.	→ Monitor operational costs and revenues closely. → Stakeholder relationships to gauge industry movements.	→ Organisations ceasing trading impacts on our registration's revenue. → New businesses have contributed to the revenues. → Finance industry has remained stable throughout the pandemic.
Cyber threat and Information Security. The Authority recognises that it is a target for cyber threats.	→ Critical applications are only accessible through secure portals requiring layered authentication. → We undertake Disaster Recovery exercises to test systems. → We employ industry best practices as a fundamental part of our cyber security policies, processes, software and hardware. → Cyber awareness training is ongoing within our team.	→ IT vulnerabilities due to remote working have been evaluated and processes enhanced to protect our critical applications.

Governance

Risk Description	How we manage the risk	Covid-19 Response
Stakeholder relationships. Maintaining constructive and collaborative relationships to ensure key stakeholders are included in key projects. Maintaining JOIC's credible reputation.	→ Stakeholder mapping exercise coupled with genuine engagement. → Regularly reviewing relationships and keeping in touch with industry and Government assists in understanding the privacy playing field.	→ Outreach to data controllers to support them through Covid.

Strategic

Risk Description	How we manage the risk	Covid-19 Response
Jersey Adequacy – it is essential that the island maintains its adequacy status with Europe to help protect data flows.	→ Ensure that we deliver the relevant activities to help Government maintain adequacy with European Union. → Monitor effectiveness of the data protection laws.	→ Ensure that our Covid communications and advice are exemplary. → Contribute to international privacy working groups remotely.

Political

Risk Description	How we manage the risk	Covid-19 Response
Government funding for Government data protection activities.	→ Frequent reviews. → Provide activity data. → Protecting our independence as a key priority. → Reviewing grant and working agreement.	→ Government requesting to reduce data protection grant monies to help with Covid activities funding. → Authority seeking to ensure that the Government fund their data protection activities.

6

Performance Report

“The vision of the Authority is to create an island culture whereby privacy becomes instinctive...

All of our activities contribute to the delivery of our strategic outcomes. Our priorities are to ensure that Jersey achieves and maintains the highest standard of data protection.

01 **The people of Jersey are provided with a high level of data protection and expert service whilst resources are judiciously and responsibly managed.**

02 **The island’s approach to data protection clearly contributes to its reputation as a well-regulated jurisdiction.**

03 **Jersey is recognised as a world leader, embracing innovation to safely develop and implement digital technology.**

The following pages review our compliance and enforcement activities in relation to our strategic outcomes. Our communications and outreach activities also contribute significantly to the outcomes and details of these activities are detailed from page 62 of this report.

The vision of the Authority is to create an island culture whereby privacy becomes instinctive, with individuals and organisations taking a proactive approach to privacy and data protection which is embedded throughout their daily activities and business planning. The Authority aims to achieve this by engaging with the Island community to embrace a collaborative and innovative approach to data protection whilst providing a leading-edge model to other, similar jurisdictions.

This vision is an essential pillar to maintaining Jersey’s position as a well-regulated, safe place to do business and is of fundamental importance to Jersey’s economy, recognising that alongside its traditional agricultural and tourism industries, Jersey is also a globally recognised international finance centre. In addition, maintaining the social well-being of Jersey’s citizens by ensuring that individuals’ privacy is regarded as a fundamental human right is core to the Authority’s focus.

The Authority will strive to promote the data protection rights of individuals, be they our local citizens or international stakeholders, through a practical and ethical approach to business practice and regulation that supports the delivery of public services and promotes the social and economic interests of the Island.

Anne King

Operations Director

Performance Report

The Authority continued to demonstrate its operational agility throughout 2021 functioning in a pandemic environment, which meant that our team, data controllers, processors and data subjects were often working from home or in a variety of remote/hybrid locations. These restrictions impacted on our community, generating different challenges and expectations. Laws do not diminish or fall away just because we were still tackling Covid. In fact, we would argue that data protection laws are even more critical bearing in mind that data protection is about protecting the rights and freedoms of people. It supports a well-functioning democracy and protects individuals from the risks of rapid technological change. Data protection helps redress imbalance between the individual and organisations that collect, process and communicate their personal data to third parties.

The Bailiwick of Jersey boasts a wealth of culture and history. It also has a vibrant blend of economic activities across retail, agriculture and fisheries, legal, tourism, finance and public sector. Each of these areas employs thousands of staff, the finance sector represents 40% of Jersey's economic output. The finance sector is a mature, well-regulated sector which employs over a quarter of Jersey's workforce. The well-established regulatory culture and behaviours of this sector permeates through to the proactive approach and understanding of their data protection obligations. The finance sector represents 28% of the data protection registrations in 2021. The Authority welcomes the approach taken by the finance sector to data protection compliance and, indeed, other sectors that are already well-versed in the obligations surrounding regulatory compliance.

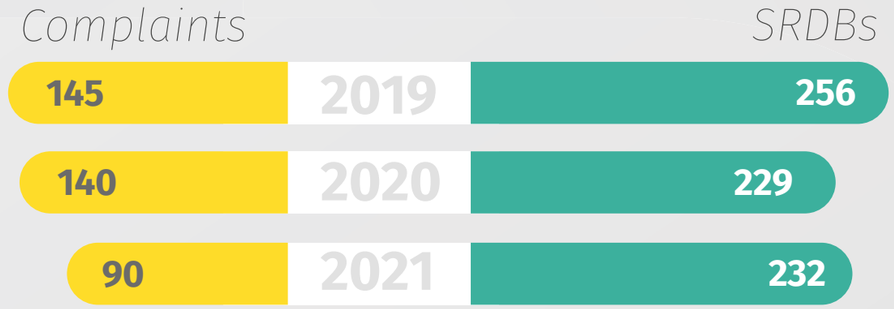
2021 Annual Registrations & Complaints by Sector	Registrations	Complaints
Agriculture & Fishing	83	-
Animal Husbandry & Welfare	42	1
Charities	288	2
Construction, Trades & Services	682	2
Education & Childcare	215	-
Faith, Worship & Religion	45	-
Financial & Professional Services	1864	14
Health & Well-being	528	2
Legal Services	113	7
Leisure & Fitness / Hospitality / Tourism / Travel / Entertainment	506	3
Manufacturing, Wholesale & Retail	439	6
Media, Communication & Advertising	136	1
Professional Bodies / Professional Associations / Professional Consultancy	261	3
Public Authority / Sector, Appointed Regulators & Statutory Bodies	110	26
Real Estate & Property Management	853	1
Social Clubs & Associations	257	-
Technology & Telecommunications	211	4
Utilities & Delivery Services	59	-
Unassigned	-	18
TOTAL	**6692**	**90**

The infographic highlights a culture of compliance and high level of reporting within the finance and professional services sector. Analysis indicates that they reported high volumes of low-level breaches and this must be considered in light of the fact that this is an industry used to reporting requirements and that takes a pro-active approach to such matters. It is worthy to note that Public Authorities, whilst only 1.6% of our data protection registrations, represent 29% of our annual complaints in 2021 and 22% of our Self-Reported Data Breaches (SRDBs).

The industry sectors representing other volumes of complaints and SRDBs are legal services, manufacturing, wholesale & retail, technology and telecommunications and charities (see diagram above). It should be noted that one initial complaint can evolve into several separate cases due to its complexity.

The industry sectors representing other volumes of complaints and SRDBs are legal services, manufacturing, wholesale & Retail, technology and telecommunications and charities. (see table/diagram above) It should be noted that one initial complaint can evolve into several separate cases due to its complexity.

Case numbers have been relatively consistent since 2019 until 2021. The complaint numbers fell during 2021, in part this could be because individuals were not placing as much emphasis on data protection as the pandemic continued to disrupt daily events. Many organisations may be more aware of their data protection responsibilities and responding appropriately to subject access requests.



The JDPA is bound by the Law to investigate complaints and SRDBs. The spirit of the DPJL 2018 is proportionality. Whilst the DPJL provides the Authority with significantly enhanced fining and enforcement powers we are pleased to report that in Jersey none of the cases investigated by our office and involving non-public authority controllers warranted the issuing of an administrative fine.

The DPJL is very prescriptive of the threshold for fining, and so far, we have not had a case that has met those criteria. Jersey does not have the large corporations which we have seen subjected to fines from Data Protection Authorities in other jurisdictions. It is also worthy of note that the number of fines issued in Europe are also very few in total when you weigh those numbers up against the number of cases those DPAs have investigated since GDPR came into force.

Additionally, we believe that a significant proportion of our population remain unaware of their rights under the Law. Experience tells us the more people who understand their rights will exercise them, will know who we are, and will result in more complaints to our office. In turn this means we see more cases where individuals have suffered harm as a result of poor data protection practices. Outreach and enforcement should work in tandem if we are to be at our most effective.

The Authority is an independent regulator and will only impose fines where proportionate and having had regard to the matters it must consider, as set out in the Authority Law, Art.26(2). We always undertake a thorough investigation and/or inquiry process, as detailed in the Authority Law. (The process is detailed on page 43). (We are specifically prohibited from issuing administrative fines against public authorities.)

During the course of 2021, the Authority issued one Public Statement reflecting the fact that the Children's Services Department, Government of Jersey had been found to have contravened Art.8(1)(f) of the Law in that it failed to comply with the integrity and confidentiality principle and ensure that it had appropriate technological and organisational measures in place to ensure the security of the data it processes. It should be noted that had the Authority not been prevented by law from imposing a fine due to the Controller being a Public Authority, the Authority would have likely considered imposing a fine in these circumstances. The Authority does not make a statement following the conclusion of every piece of regulatory action, rather, and in line with the Authority Law, it will only do so where *"because of the gravity of the matter or other exceptional circumstances, it would be in the public interest to do so."*

It is important to remember 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. Whereby both parties learn and can exchange information, helping us to understand the challenges faced by industry and the frustrations faced by complainants. That said, we will 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.

> ***Dealing with the JOIC is a breath of fresh air.***

> ***Unlike a lot of other 'official bodies' they treat you like a valued customer.***

> ***With a friendly, professional and knowledgeable team, whatever the matter, they are always ready and willing to help.***

> ***Well done JOIC. You make working with a 'Commissioner' a most pleasurable experience!"***

Constructive working relationships allow data controllers and processors to feel sufficiently comfortable to approach us to ask for help and guidance before a situation reaches crisis point. As the Authority Chair stated in 2019:

'I believe that data protection is a team sport. There are many players, and we will only succeed if everyone plays their part, and we work together. The players are the Authority, the Government, businesses, associations, and the public. The Authority is partially referee and partially coach. Like a referee, it interprets and implements the rules. Sometimes it issues warnings – a yellow card - and sometimes issues penalties – a red card. Like a coach, it provides guidance and training as to how to play effectively by the rules. The Government creates the rules through the States Assembly and then must play by those rules. Companies need to learn the rules, set up infrastructure for compliance and then follow the rules.'

> ***data protection is about protecting the rights and freedoms of people. It supports a well-functioning democracy and protects individuals from the risks of rapid technological change...***

2021 Case Data

Schedule 4 of the Authority Law 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 JOIC receives a broad range of contacts.
We classify them into the following categories:.

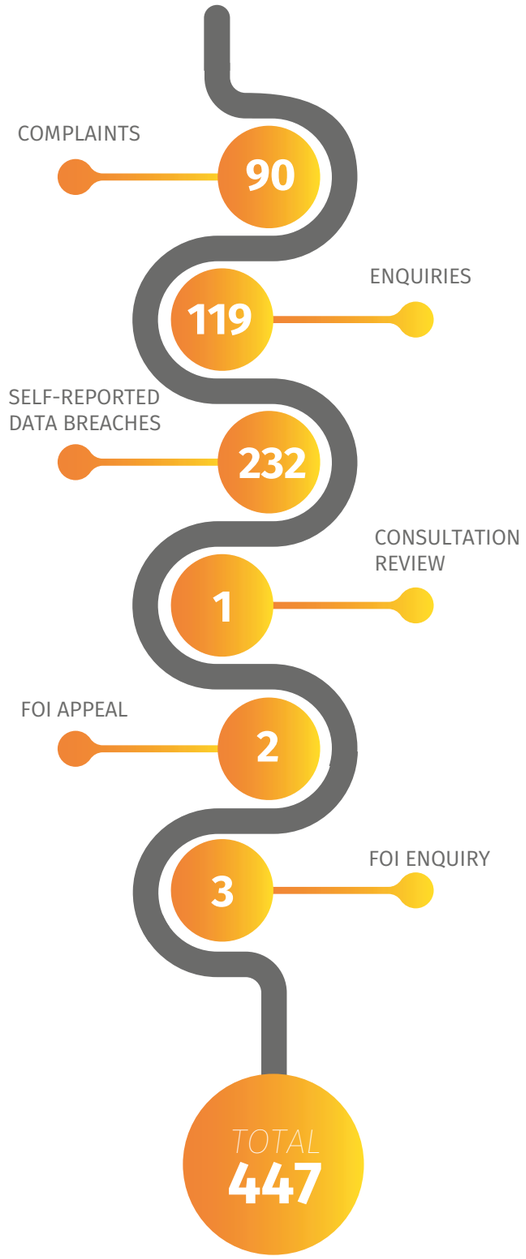
ENQUIRIES
These range from simple questions regarding our location and career opportunities to the more complex questions around guidance matters.

COMPLAINTS
Complaints are received from individuals concerned about the use of their personal information, non-response to a subject access request or other rights which have not been fulfilled.

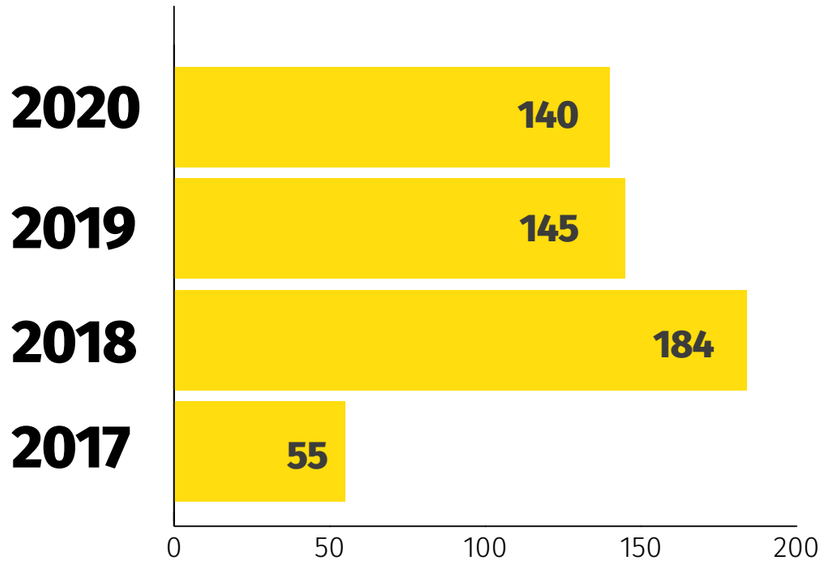
SELF-REPORTED DATA BREACHES
Data controllers, under the DPJL, are required to report 'certain' breaches to the JOIC within 72 hours of becoming aware of the breach unless the breach is unlikely to result in a risk to the rights and freedoms of the individual.

FREEDOM OF INFORMATION
Enquiries exploring if there are grounds for an appeal or for further guidance.

FREEDOM OF INFORMATION
Appeals. An applicant who is dissatisfied with a response to a request for information from a public authority may appeal to the Information Commissioner.



The volume and type of cases submitted to the Authority is consistent with the pattern of activity over the years since the introduction of the Data Protection (Jersey) Law 2018. The Authority presents this report to demonstrate that we handle each complaint, breach and enquiry with fairness, consistency and respectfully.



The above table shows the number of complaints received by the JOIC over the last five years.

Article 19 of the DPAJL summarises the parameters of the 'Right to make a complaint'

An individual may make a complaint in writing to the Authority in a form approved by the Authority if –

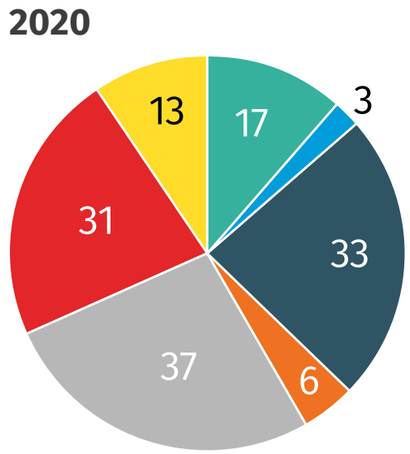
(a) the individual considers that a controller or processor has contravened or is likely to contravene the Data Protection Law; and

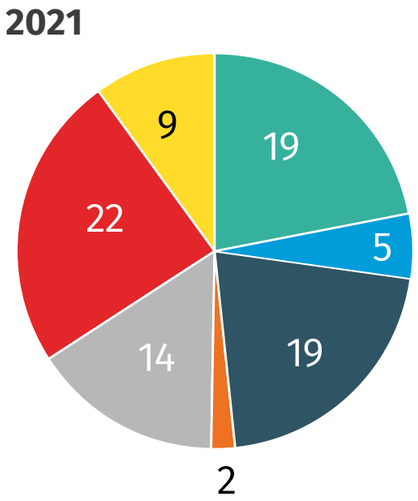
(b) the contravention involves or affects, or is likely to involve or affect, any right in respect of personal data relating to the individual.

Individuals complain to our office about their concerns in relation to the processing and use of their personal information.

Each complaint and self-reported data breach (SRDB) is evaluated using a standard framework as set out in Part 4 of the Data Protection Authority (Jersey) Law 2018

What were people complaining about?	2020	2021
Direct marketing	3	5
I asked for access to/copies of my personal information and I've not received it/they have withheld it from me	33	19
I asked for my information to be rectified/erased/sent to another controller and my request has been refused	6	2
I don't think my personal data is being/has been kept safe	37	14
My information has been shared and it shouldn't have been	31	22
Someone has collected my personal data, but I didn't give it to them	13	9
Unassigned	17	19
TOTAL	**140**	**90**





Each complaint and self-reported data breach (SRDB) is evaluated using a standard framework as set out in Part 4 of the Data Protection Authority (Jersey) Law 2018. The JOIC will also use this framework to conduct an inquiry on its own initiative into a likely contravention of the DPAJL, which we may learn about from a whistle-blower or by observing a behaviour relating to the use of personal information by an organisation. The investigation will identify if there has been a contravention of the Law.

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 Law.

Once the investigation is underway the JOIC will provide updates at least every 12 weeks. The investigation must conclude whether the Law has been contravened (Article 23 of the Authority Law) 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.

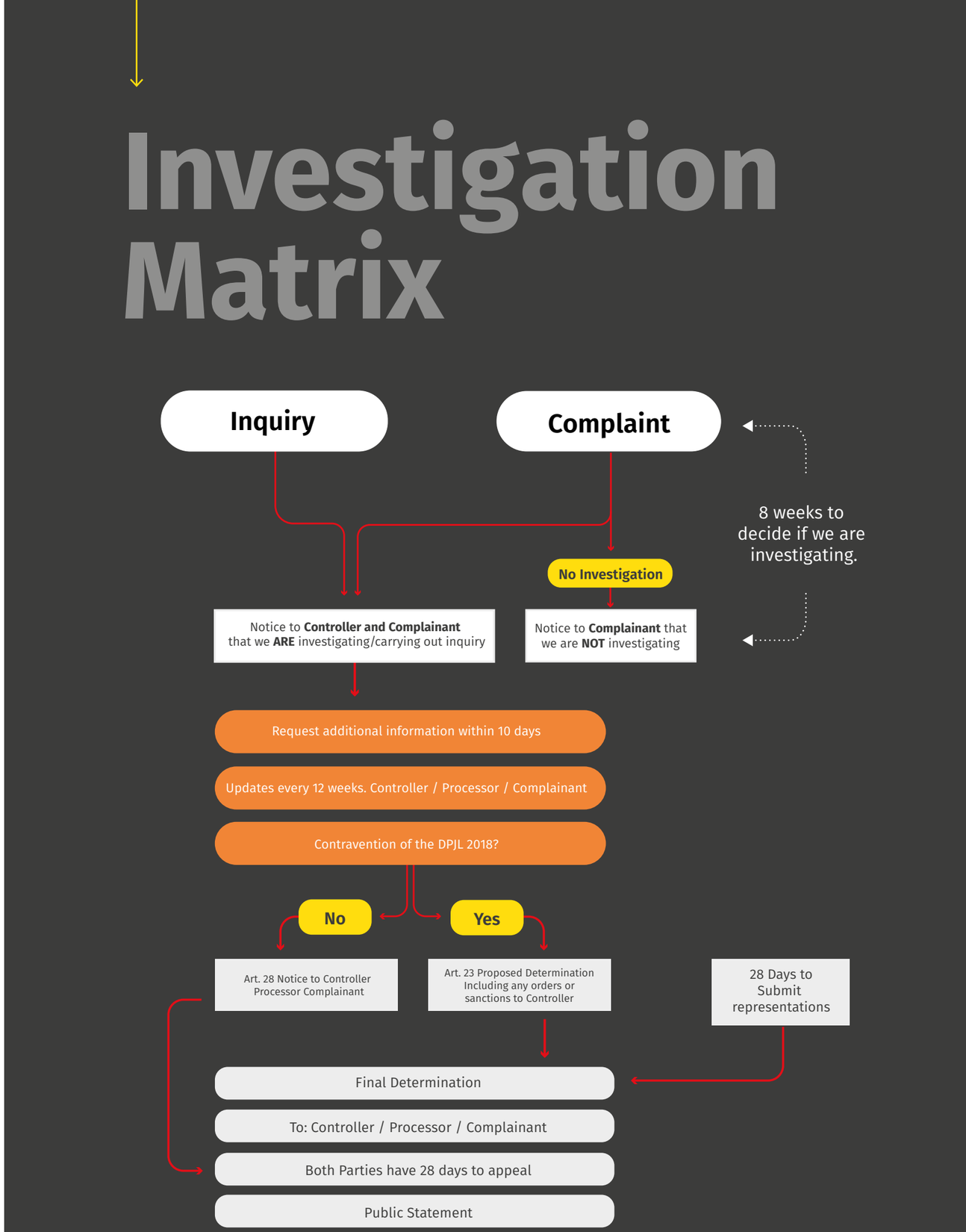
The JOIC must take into account any representations made before issuing its final determination which will be sent to the data controller or data processor and to the complainant. Both parties have a 28-day period to appeal that final determination to the Royal Court of Jersey.

(The process (right) 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 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.



8

2021 Case Outcomes

The JOIC's Regulatory Action and Enforcement Policy [7], introduced in 2020 supports the Authority's Strategic Outcomes as detailed above and the Business Plan.

[7] *https://jerseyoic.org/media/l5sfz1s0/joic-regulatory-action-and-enforcement-policy.pdf*

This policy is based on five key principles:

01 **Proportionality.**

02 **Targeted.**

03 **Accountability.**

04 **Consistency.**

05 **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.

Throughout 2021, the Authority continued to review and improve its regulatory approach, tailoring any enforcement action appropriately and proportionately to the actual contravention and the harm suffered by the individual. Our philosophy is to work collaboratively with the community to educate and guide data controllers, processors and data subjects to reduce breaches, complaints and contraventions. Whenever we apply sanctions, it must be fair and reasonable in the circumstances.

→ Authority Sanctions

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

- → Reprimand
- → Warning
- → Orders
- → Public Statement
- → Administrative Fine

→ 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 Law 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. For example, we issued a formal reprimand where an organisation had failed to consider a staff member's specific request not to share a report which contained special category data. Due to a failure in internal processes, the organisation proceeded and shared the report anyway although ultimately such sharing did not cause any lasting issues for the data subject. Notwithstanding, it was felt that case was serious enough to issue formal reprimand.

→ Warning

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

→ Orders

The Authority can make a variety of Orders but we make sure these are proportionate to the actual contravention. During 2021, the Authority issued a range of orders including:

- → Ordering a controller to provide certain staff members with appropriate training and to report back to the Authority within a stipulated timeframe, confirming that training had been provided, who it had been provided to and with a copy of the course materials, this for review by the Authority.
- → Keeping a controller under effective supervision for a period of time whilst they updated certain policies, procedures and IT systems and requiring an updating report at the end of that period.
- → Directing that a controller should respond to a previously unanswered subject access request within a certain timeframe (including providing previously withheld information).
- → Directing that a controller properly actions a request for rectification, including giving notice to third parties previously in receipt of inaccurate information/information it should not have received.

→ 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 report on every formal action taken because that is not what the Law provides for and the Authority reserves this power for the most serious cases such as that issued in October 2021 involving a very serious breach of a data subject's special category data by a Government of Jersey entity. This Public Statement involved Orders to update policies and procedures in respect of data sharing and training of relevant staff on these matters and their data protection obligations more generally.

The Public Statement confirmed that a breach of Article 8(1)(f) of the Data Protection (Jersey) Law 2018 had occurred, as the data controller failed to comply with the Integrity and Confidentiality Principle and ensure that they had appropriate technological and organisational measures in place to ensure the security of the data they process.

→ Administrative Fines

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

In determining whether to impose an administrative fine in accordance with Article 26 of the Law, 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 have a deterrent effect. It has not had to issue any fines.

→ Information Notices

As part of our investigation process and powers under Schedule 1 of the Authority Law, 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.

9

Breach Reporting

Investigating self-reported data breaches represented 52% of our Compliance and Enforcement caseload during 2021. In 2020 self-reported data breaches made up 47%.

A third 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. Article 20 of the Law states that:

'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 in the manner required by the Authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.'

2021

52% **self-reported data breaches**

2020

47% **self-reported data breaches**

From our records it is evident that just under half of the reported breaches were unlikely to 'result in a risk to the rights and freedoms of natural persons'. However, we continue to encourage organisations to report breaches to enable us to understand the breach landscape in Jersey to help shape our guidance and advice.

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

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.

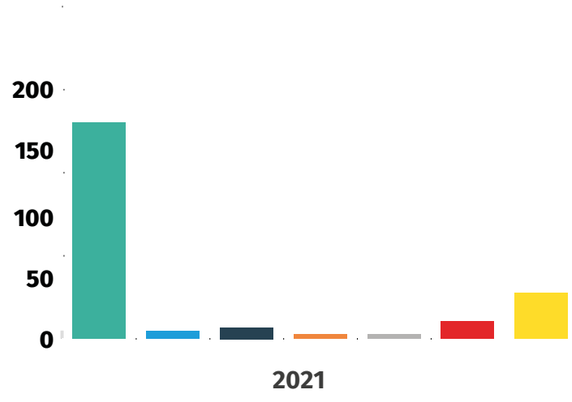
To help mitigate the possibility of increased breaches as our community adapted to working from home (either wholly or in part) in response to the Covid pandemic, we maintained a vibrant and broad range of relevant guidance. We improved and regularly updated our Covid website hub, recognising this resource was vital in helping organisations by providing timely and effective communication to support the business community to remain compliant.

We were very proud to be commended by the Global Privacy Assembly[8] (GPA) at their international conference in October for our work in this area and it was suggested that other data protection authorities refer to our guidance.

[9] https://globalprivacyassembly.org/

→ Types of Breaches Reported in 2021

Types of Breaches Reported	2021
Unauthorised disclosure	168
Unassigned	2
Alteration	3
Destruction	1
Lack of availability/access	1
Loss	11
Unauthorised access	46
TOTAL	232



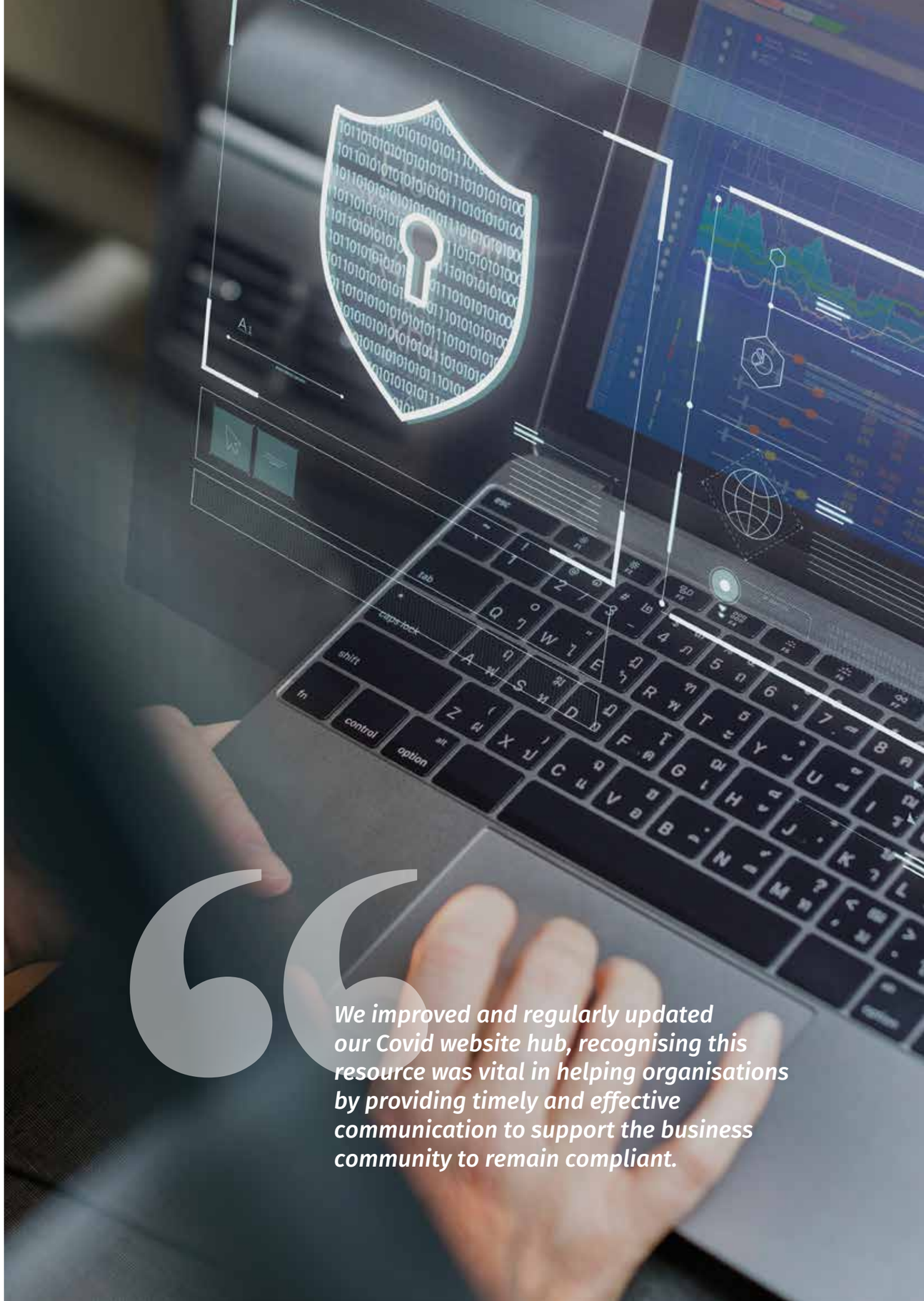
Of the breaches reported in 2021, one resulted in a formal inquiry and a **determination** that there had been a contravention of the Data Protection (Jersey) Law 2018.

Of the remaining self-reported data breaches, many did not cross the threshold for reporting to the Authority and were of a minor nature. Once reported, the Authority makes enquiries of the data controller to obtain a full picture of the breach that has occurred, and what steps have been taken by the organisation to deal with the breach and, where appropriate, stop similar occurrences in the future.

Specifically:

- → 168 self-reported data breaches were due to unauthorised disclosure (e.g. emails sent in error) but in all circumstances, the breaches were appropriately mitigated, presenting no risk to the data subject.
- → Of the remaining 64 incidents there were a number of different issues including malware, phishing attack, lost data and technical/ procedural errors leading to breaches. In all circumstances, the breaches were appropriately mitigated, presenting no risk to the data subject.

As indicated above, there is an element of over-reporting self-reported data breaches of matters that do not necessarily need be reported, but, at present we do not discourage such reporting as it gives us an opportunity to identify patterns and offer guidance, support and words of advice to organisations to help increase understanding and improve their internal processes (including educating on breaches that reach the threshold criteria for reporting).



We improved and regularly updated our Covid website hub, recognising this resource was vital in helping organisations by providing timely and effective communication to support the business community to remain compliant.

10

Enforcement Audits

We will significantly enhance our audit capability, frequency and breadth from 2022 onwards following our investment in audit software, team recruitment and training.

One of our key 2021 business plan deliverables was to assess the level of compliance of data protection in Jersey. To help achieve this we exercised our power to conduct data protection compliance audits to begin to assess the percentage of businesses reaching a competent standard of data protection practice in certain key areas.

The primary purpose of the 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 faced the challenge of carrying out this function whilst in the midst of ongoing pandemic restrictions.

The first tranche of audits started in November 2020 and were completed in January 2021. We undertook the second tranche of desktop audits in June 2021 and completed these in November 2021. We took a risk-based approach to selecting the industry sector to audit first. The industry area selected processes a high volume of special category data and it was felt could most benefit from a targeted audit following issues that had been raised against controllers in that sector.

Article 22 (7) of the Data Protection Authority (Jersey) Law 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 concernedx must pay for an audit required under sub-paragraph (1)(b).

Thus prior to undertaking compliance audits of any nature we are required to carefully consider and document the audit terms of reference. The following is an extract from the information passed to the data controllers being audited in both tranche one and tranche two.

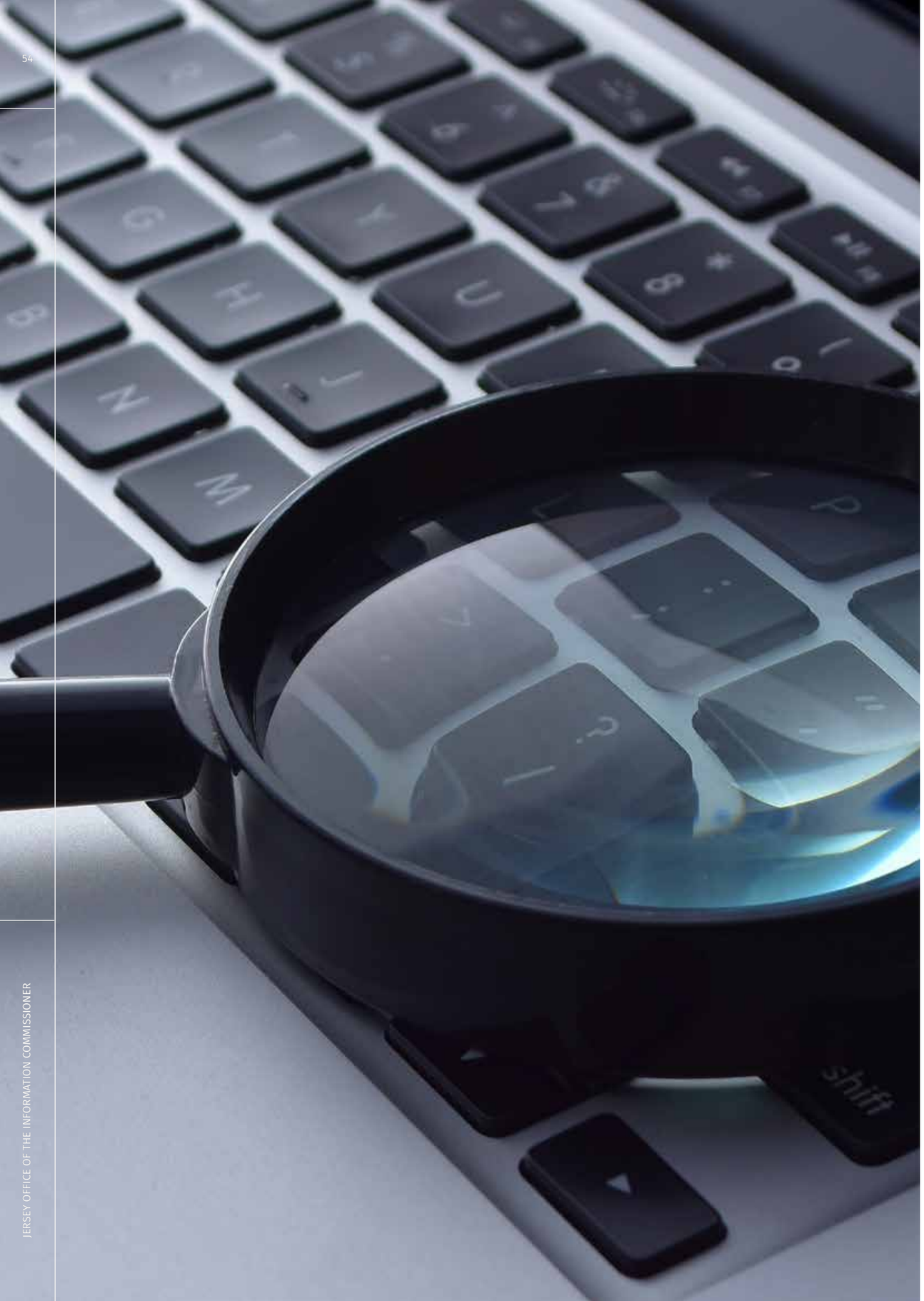
→ Scope/terms of reference

We are required to specify the terms of reference of the audit.

The compliance audits we conduct are mandatory for recipients to complete. That said we are very keen to work with the industry to help improve data protection compliance and forge a positive, collaborative relationship.

The audit scope is limited to the following matters and seeks to gauge the controller's compliance with appropriate data protection principles and obligations:

→ Transparency, lawfulness and fairness. Article 8(1)(a) of the DPJL requires personal information to be processed lawfully, fairly and in a transparent manner in relation to the data subject. In other words, how does the relevant controller demonstrate that they are able to explain to data subjects what information is being collected, for what purpose and what is done with it, etc.



- Integrity and confidentiality: Article 8(1)(f) of the DPJL requires that personal data are processed in a manner that ensures appropriate security of the data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. We will ask about personal information breach provisions and what policies/procedures the controllers have in place to deal with breaches should they occur.
- The broader aspects of data protection management and staff training.

Respondents were asked a range of simple questions to assess their compliance, for example, existence of an appropriate privacy policy, staff training and the use of an internal data breach log. We also requested documentation to evidence the responses given. We assessed each response fully and a Red-Amber-Green (RAG) indicator rated each controller. At the end of the process, we looked at all the data to assess common themes.

One common issue was the suitability of data protection training and the appropriateness of its delivery. We found that training was infrequent and did not reflect the local data protection law. We provided supportive guidance and suggestions as to how each audited organisation could better protect their clients and staff with more relevant and timely training, not necessarily relying on just an online platform.

Encouragingly, this was the only common issue identified in the first audit tranche.

All of the audited organisations engaged fully with our office and responded to the guidance and recommendations offered. Their training plans were updated to reflect the needs of the organisation and we were satisfied with the improvements made.

In the second tranche of audits carried out between June 2021 and November 2021 we audited 25 organisations from one business sector using the same online process, using the same terms of reference with slightly modified questions to better reflect the industry sector.

This industry sector revealed that a frequent issue was the quality of privacy policies. The Privacy Policy/Notice is a key document as it lets employees, customers, suppliers and contractors know that organisations take their privacy responsibilities seriously. It spells out how organisations use personal information and what individuals can do if they would like clarification as to how that information is being used. The policies which existed and were shared as part of the second tranche of audits highlighted that often they failed to contain the specified information required in Article 12(4) of the DPJL.

Again, all of the responses were reviewed thoroughly and feedback given where appropriate. We worked closely with the organisations in question to provide guidance that would assist them in preparing a privacy policy that would be fit for purpose for their organisation without actually preparing it for them.

Overall, the standard of compliance we found was encouraging. Where issues were identified, the feedback from our office was well received and any issues identified were generally dealt with promptly.

Undertaking compliance audits is a detailed and resource intensive activity. However, the results are essential to help us to fulfil our strategic aim of **achieving and maintaining the highest standard of data protection in Jersey.**

We will significantly enhance our audit capability, frequency and breadth from 2022 onwards following our investment in audit software, team recruitment and training.

11

Annual Report of Freedom of Information Activities

The Freedom of Information (Jersey) Law 2011

> *The aim of the FOI Law is to promote a culture of openness and transparency across the public sector*

The Freedom of Information (Jersey) Law 2011 (the FOI Law) provides the public with a legal right for individuals to request access to, and be provided with, information held by Scheduled Public Authorities (SPA).

This covers 'information recorded in any form' held by a SPA and includes printed documents, computer files, letters, emails, photographs, and sound or video recordings. SPAs covered by the FOI Law include Government of Jersey departments, Parishes, States of Jersey Police and Andium Homes.

The aim of the FOI Law is to promote a culture of openness and transparency across the public sector, improve accountability and promote good governance by providing individuals with a better understanding of how SPAs carry out their duties, make the decisions they do and spend public funds.

(The FOI Law does not give individuals a right of access to their own personal data because this right is available under the DPJL.)

Our role in regulating the FOI Law includes the following functions:

- To encourage public authorities to follow good practice in their implementation of this law and the supply of information.
- To supply the public with information about the Law.
- To deal with appeals.

An applicant who is dissatisfied with a decision of a SPA in responding to their request may, within six weeks of the notice of that decision being given or within six weeks of the date the applicant has exhausted any complaints procedure provided by the SPA, appeal to the Information Commissioner on the basis that the decision of the SPA was not reasonable.

The Information Commissioner must decide the appeal as soon as is practicable but may decide not to do so if satisfied that:

- The applicant has not exhausted any complaints procedure provided by the scheduled public authority.
- There has been undue delay in making the appeal.
- The appeal is frivolous or vexatious; or
- The appeal has been withdrawn, abandoned or previously determined by the Commissioner.
- The Commissioner must serve a notice of his or her decision in respect of the appeal on the applicant and on the SPA. This is done by way of a formal Decision Notice that will set out:
- The Commissioner's decision and, without revealing the information requested, the reasons for the decision; and
- The right of appeal to the Royal Court conferred by Article 47.

In each case, the Commissioner conducts a formal appeal process adhering to the principles of administrative fairness and the laws of natural justice. Both sides are provided with an opportunity to make formal written submissions in support of their position. The Commissioner presumes that when making its submissions, each party is providing their full and complete arguments and all relevant evidence in support.

The Commissioner issues a Decision Notice based on the submissions of the parties, the precise wording of the legislation and any relevant case law. The decision is objective and includes adequate reasons. If a party is dissatisfied with the Decision Notice, the only avenue of appeal is to the Royal Court. The Royal Court may review the Commissioner's decision to determine whether it was reasonable.

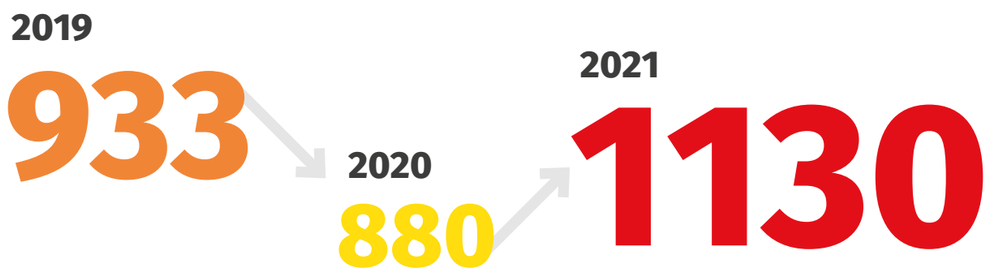
The Commissioner's team also provides informal advice and assistance to both members of the public and SPA prior to any formal appeal.

→ 2021 Operational Performance and Appeals

The Central Freedom of Information Unit of the Government of Jersey reported that it received 1,130 valid FoI requests during 2021.

Freedom Of Information Statistics	2020	2021
Office of the Chief Executive	100	74
Infrastructure, Housing & Environment	157	180
Children, Young People, Education and Skills	71	70
Health and Community Services	173	216
Justice and Home Affairs	74	123
Judicial Greffe	14	18
Customer and Local Services	31	91
States Greffe	21	24
States of Jersey Police	62	81
Treasury and Exchequer	48	67
Strategic Policy, Planning and Performance	36	101
Chief Operating Office	93	85
Total Valid Requests	**880**	**1130**

The total number of valid FoI requests decreased from 933 in 2019 to 880 in 2020. The numbers increased to 1,130 in 2021.



The increase in requests from 2020 to 2021 appear to have been generated by individuals seeking information on topical health and political issues.

- → Fishing licences
- → Covid-19
  - Track and trace
  - Vaccines
  - Deaths
  - PCR testing
- → Planning - Skatepark and Ann Street.
- → Health treatments.
- → Drones

→ Significant 2021 Decision Notices

We issued two formal Decision Notices in 2021 both relating to information sought from the States of Jersey Police regarding disciplinary complaints [9].

As of 31 December 2021, there were no active appeals under review.

[9] https://jerseyoic.org/news-articles/decision-notices/

Environmental, Social and Governance (ESG)

Environmental, Social and Governance are the three central the three central factors in measuring the sustainability and societal impact of a company or business. Sustainability is 'Development that meets the needs of the present without compromising the ability of future generations to meet their own needs'.

Protecting the environment is one of our priorities, and we are a member of the Government of Jersey's 'Eco Active Business Network'. This is an environmental management scheme for organisations on the island.

The Authority continues to be committed to:

01 **Improving efficiency in the use of energy.**

02 **Reducing waste.**

03 **Demonstrating compliance with environmental legislation.**

04 **Reducing the risk of causing pollution or other damage to the environment.**

The Authority is actively considering a meaningful and proportionate ESG policy that will include the development and implementation of appropriate metrics over the coming weeks and months.

13

Outreach and Communications

Sarah Moorhouse

Communications Lead

Winning the hearts and minds of islanders was at the forefront of the JOIC's communications outreach, campaigns and activities for 2021 with each project complementing the work of the JOIC's Compliance and Enforcement team and in line with our business promise to promote the data protection rights of individuals through a practical and ethical approach to business practice and regulation.

JOIC DEBATE

Your privacy – a price worth paying?

100 guests gathered for our lively debate titled 'Your privacy - a price worth paying?' during October 2021 to explore the value of privacy, ownership of personal information and under what circumstances are we prepared to trade our privacy in order to access goods and services.

The debate was structured to allow the young guests to challenge the 'grown-ups' and ask what was being done, how and when, to protect their personal information in a world where the relentless pace, ability and invasive nature of technology and artificial intelligence shows no sign of slowing down.

Guests from a wide range of industry sectors including business, education and charity contributed to the discussion which was held in line with our strategic aim to ensure the people of Jersey are provided with a high level of data protection as well as striving to ensure Jersey is recognised as a word leader embracing innovation to safely develop digital technology.

The aim of the event, the first of its kind for our organisation, was to establish what the audience was most concerned about regarding their privacy and personal information. Students from a number of island schools including Highlands College, Jersey College for Girls and Beaulieu School attended and guest speakers from The Diversity Network, Jersey, the Digital Jersey Academy, Highlands College, Government of Jersey, MIND Jersey, Jersey College for Girls, Jersey Finance, Trax.je and Jersey Consumer Council shaped and ignited our debate.

The debate audience strengthened the message that islanders need the tools to navigate the personal information challenge and feel equipped and empowered to understand the privacy landscape, ask the right questions and know how to check.

We received extremely positive feedback following our debate.

JOIC Debate guest experiences

Huge congratulations for organising a superb event. Despite running to a tight schedule, it still allowed plenty of time for some important discussions to be had, even on the individual tables. I would happily remain involved in anything similar you decide to do in the future.

It was a bit daunting being invited to a big corporate event. We were welcomed, made to feel important and the JOIC person on our table chatted through the event structure. It was great to be able to participate in the discussion and see the debate unravel around me.

I thoroughly enjoyed it and very much appreciated the food for thought. I think you and your team are doing great things.

Thank you so much again for inviting me. I really enjoyed it and there were some great discussions.

I really enjoyed the event and thought the content and debate was really engaging. So many different viewpoints and opinions. I also really like it that the event engaged with younger people. A very worthwhile afternoon indeed.

→ Community Education and Outreach

In line with our mandate, we're committed to raising awareness across our community about the importance of individuals taking ownership and control of their personal information. Our Young Privacy Ambassador Programme expanded during 2021 and our team delivered 44 sessions to island schools via a mix of in person and virtual delivery of our key messages.

The Young Privacy Ambassador Programme educates Jersey's young people about why their personal information must be protected and aims to equip them with the tools they need to do so. Sessions include video content, props and age-appropriate quizzes to engage the students and check their learning.

Our Young Privacy Ambassador sessions reinforce the fact privacy is a fundamental human right.

Performance Measure

To ensure the students:

- → Understand the meaning of Personal Information and how the DPJL protects them and their personal information.
- → Are equipped with the tools to protect their personal information, with a particular focus on digital advancements and technology.
- → Get to grips with their individual rights as citizens under the Data Protection (Jersey) Law 2018.
- → Are aware of the legal obligations those that are processing their personal information must adhere to under the law.

The sessions reinforce the fact that privacy is a fundamental human right and aim to ensure students have the relevant knowledge, are able to explore their rights and responsibilities and acquire the skills they need to lead fulfilling, responsible and balanced lives.

As the students progress through their school journey, our workshops offer a deeper level of education around understanding privacy rights and ethics. Following the sessions during 2021, 80% of young people we engaged with commented they understood the importance of protecting their personal information.

'The team at the JOIC have delivered a range of engaging, high quality sessions, giving our students an introduction into the world of data protection, highlighting the value of their personal data and demonstrating ways to safeguard themselves in this area. We would like to thank the team for their support and are looking forward to further sessions in the near future.'

PSHE Leader

→ Courtroom Challenge

Year 12 students at Hautlieu School stepped out of the classroom and into the courtroom once again during 2021 to learn more about data protection law via a privacy trial 'court case'.

The challenge required the students to evaluate a fictional courtroom bundle, then split into prosecution and defence teams for a two-hour hearing.

The aim of the challenge was to:

- Bring privacy law to life.
- Increase young people's understanding of privacy law in an ethical context.
- Encourage the students to explore a fictional data protection case and question privacy issues.
- Inspire the next generation of privacy professionals.

Our outreach team hosted assemblies for local sixth formers during 2021 to inform them about how to exercise their personal information rights and responsibilities and explore privacy issues as they enter adult life. Our team also delivered Data Protection Basics virtual sessions to first year degree students studying business law. Feedback confirmed the sessions supported the students in learning more about the foundations, principles and obligations of Jersey data protection law.

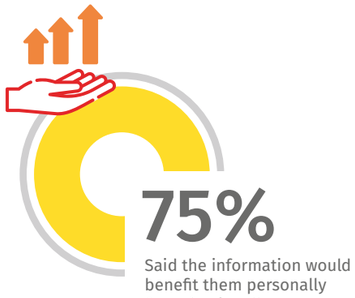
> ***The courtroom challenge was my favourite activity so far held by JOIC to teach us about the Data Protection (Jersey) Law 2018. It made the law more relevant to real life and helped us to understand why and how the law is in place to protect our personal information. It was one of the most helpful activities that we have done regarding protecting our data because we all actively and consciously took part debating about the nuances of the law and how it works. This further helped us to understand our rights as young adults'***
>
> **International Baccalaureate Student**

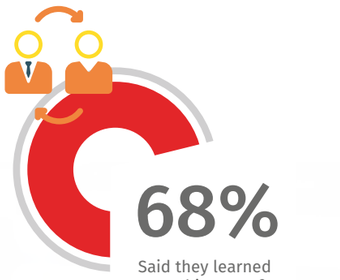
→ Events

The aim of our JOIC events programme of presentations and interactive workshops for 2021 was to educate, guide, inform and engage.

Due to the Covid pandemic, sessions were presented via a mix of face to face and virtual delivery. Themes ranged from International Transfers to Subject Access Step-by-Step, to the Dos and Don'ts when dealing with Rectifications and Erasure requests and what makes a good Data Protection Impact Assessment. The events programme included a data protection workshop designed specifically to support small businesses and sessions raising awareness of our office, who we are and what we do.

We also delivered presentations following requests from organisations including teams from the healthcare, property and charitable sectors. Our events attracted 180 guests, with 75% of attendees commenting the information presented would benefit them personally and professionally. 68% of attendees said they learned something new from the session they attended. Whilst overall guest numbers were lower than anticipated, smaller groups prompted more in-depth conversation around each subject.





→ Data Protection Day 2021

Due to the pandemic meaning we could not host in person events, we invited guests to celebrate Data Protection Day 2021 with us virtually. Presentations included 'CovidCop2021 – The Rise of Employee Spyware' which explored the implications of ethics, data protection and employee monitoring as well as 'Inclusive or Intrusive' a discussion about the importance of striking a balance between employee engagement and employee privacy. The Deputy Information Commissioner appeared live on Jersey local radio discussing the impact of data breaches, employee health data and how islanders can best protect their personal information against the threat of Covid-19 related scams.

Our office was proud to attend events during 2021 as part of the Jersey Fraud Prevention Forum and collaborate with Jersey Chamber of Commerce and Jersey Library to extend our reach to industry and individuals.

→ 'It's All About You'

Our It's All About You campaign was launched during 2021 to maximise our engagement with islanders as part of our citizen privacy brand.

The campaign launch was in line with our strategic deliverable to ensure the island's approach to data protection clearly contributes to its reputation as a well-regulated jurisdiction. It centred around a bespoke Privacy Toolkit, an online, practical go-to-guide to help islanders protect their personal information and understand their individual rights. The campaign was promoted via local television advertising and resulted in an increase in visits to the dedicated It's All About You section of our website.

It's All About You aims to:

- → Empower Islanders and provide them with the tools to protect their personal information.
- → Grow the conversation around the value of privacy.
- → Support and encourage Jersey's community to enjoy a healthy privacy self-esteem.

→ 'It's All About You' Survey

During February 2021 we launched a confidential survey as part of our 'It's All About You' campaign. Aimed citizens in Jersey, the purpose of the survey was to find out how aware islanders were about their personal information rights.

The survey, the first of its kind for our office, will be repeated each year. This initial survey will be used as a benchmark for future research and importantly, will help us shape our outreach activities.

Survey questions ranged from asking respondents to rate their knowledge of their personal information rights to asking them how concerned they would be if their personal information was lost or shared without their permission. 381 Islanders took part in the survey.

In response to the question 'To what extent are you aware of the role of the Jersey Office of the Information Commissioner?,' 52% of recipients said they were unaware of the role of our office. Raising awareness of our office is an important part of our JOIC business plan and communications for 2022.

Another key finding was 96% of respondents said it was important to them that organisations kept their personal information safe and secure. The table to the right highlights how concerned respondents said they would be if their sensitive personal information was lost or shared without their permission.

	Very concerned	Fairly concerned	Not very concerned	Not at all concerned
Genetic data (DNA, blood type etc.)	48.13% (180)	26.20% (98)	18.45% (69)	7.22% (27)
Health data	59.68% (225)	23.34% (88)	12.20% (46)	4.77% (18)
Political, religious and other beliefs data	23.47% (88)	27.20% (102)	30.93% (116)	18.40% (69)
Biometric data (Fingerprint, facial recognition, CCTV image)	78.31% (296)	14.81% (56)	3.97% (15)	2.91% (11)
Nationality	15.24% (57)	18.18% (68)	35.83% (134)	30.75% (115)
Sexual orientation	18.62% (70)	14.10% (53)	33.24% (125)	34.04% (128)
Criminal record information	40.27% (151)	17.87% (67)	15.73% (59)	26.13% (98)
Contact details such as name, address, email address	70.45% (267)	19.00% (72)	6.33% (24)	4.22% (16)
Date of birth	49.07% (185)	24.40% (92)	15.92% (60)	10.61% (40)
Passport data	86.60% (323)	9.92% (37)	1.07% (4)	2.41% (9)
Credit and debit card details	95.76% (361)	2.65% (10)	0.00% (0)	1.59% (6)
ID information (driving licence etc.)	80.95% (306)	15.08% (57)	0.00% (0)	0.00% (0)

**Not all respondents answered every question.*

→ Guest Bloggers

Influencers continued to support our mission to bring privacy themes to life during 2021. Thought leading industry professionals contributed to our website blog pages in line with our vision to embrace a collaborative and innovative approach to data protection. Blog themes ranged from the relationship between contact tracing and data protection to data protection in the workplace and privacy and sustainability. Our contributors promoted their blogs on social media which resulted in increased engagement and more islanders joining the privacy conversation.

Blog extract

'I've always been told that a good starting point for data protection is to ask if you'd be happy if your information was being treated the way you're planning to treat someone else's. And I was not happy.'

Business

→ Board Support Squad

How do you hold the executive to account when it comes to data protection? How do you stress test the effectiveness of the data protection policies and procedures embedded in the organisation?

Set up in line with our mandate to help to help boards and Non-Executive Directors be fully conversant with the role they must play when it comes to privacy needs, the Board Support Squad has been a popular addition to our JOIC portfolio.

Its purpose is to help industry leaders to understand both board and manager data protection risks and responsibilities and to provide them with an opportunity to work with our office in a safe space to stress test the data practices in their organisation and identify any privacy risks before they are realised. The launch of our Board Support Squad has resulted in stronger working relationships and collaboration with industry and supported the development of relevant guidance material.

→ Guest experiences

> ***Let's Go DPO! is just the tip of the iceberg in terms of the support the JOIC provides. That the sessions are so well attended is evidence of a collective experience of them being prepared to listen and engage on any subject.***

> ***The Let's Go DPO! sessions have been invaluable to me as a recently appointed DPO. They provide a safe space for confidential peer-to-peer discussions and a forum to seek guidance from JOIC on issues faced by businesses.***

→ Let's Go DPO! Network

Autumn 2021 saw the launch of our interactive Let's Go DPO! support network created to provide Data Protection Officers and Data Protection Leads in Jersey a safe and confidential environment in which to:

- Discuss the highs and lows of being a DPO or DP Lead.
- Share skills, explore common experiences and ideas to help overcome some of the challenges faced by DPOs or DP Leads.
- Build working relationships for future collaborations.

Collaboration with members is at the heart of this network. Each session is structured around a specific theme chosen following discussion with members. The launch sessions explored JOIC's Compliance and Enforcement role, Subject Access Requests and this included a discussion about the support DPOs feel they need as well as data breaches explored via case studies.

'Let's Go DPO' was launched in line with our strategic aim to ensure the island's approach to data protection clearly contributes to its reputation as a well-regulated jurisdiction.

Its purpose extends to promote compliance and awareness of the DPJL and demonstrate the JOIC's commitment to providing support to those working within the field of data protection locally by offering them the opportunity to discuss and contribute to our strategic outcomes, where appropriate.

→ Small Business Focus

Our small business self-assessment tool was launched during 2021 to support and empower small business owners and sole traders to improve their understanding of their data protection obligations and find out what they need to do to ensure they are keeping personal information secure, in line with our commitment to ensure the people of Jersey are provided with the highest standards of data protection. Once small business owners or sole traders complete the self-assessment, they are presented with practical steps and links to guidance to assist them with data protection compliance.

→ Media Engagement and Partnerships

Regular features throughout 2021 included a monthly Ask the Commissioner column in Jersey's print media to demystify data protection issues as well as articles highlighting topical privacy issues, written by JOIC senior management. Media releases issued during 2021 included a Public Statement and an update regarding our JOIC Data Protection Audit Programme.

We continue to use television, print and radio advertising to inform islanders about their obligations and individual rights under the Data Protection (Jersey) Law 2018. Local television advertising during 2021 focused on the legal requirement for businesses, charities and organisations of any shape or size that process personal information to be registered with our office and adhere to their obligations under data protection law and led to greater awareness and new business registrations. A second television campaign focused on individuals being equipped with the tools to protect their personal information and led to an increase in visits to the 'Privacy Toolkit' area of our website.

The JOIC Communications team continues to nurture and develop working relationships with key stakeholders such as Jersey Business, Jersey Chamber of Commerce, Digital Jersey, Jersey Finance, Law Society of Jersey and MIND Jersey for the benefit of the Jersey community. We were also pleased to partner with States of Jersey Police, Jersey Consumer Council and Citizens Advice Jersey to raise awareness about the importance of protecting personal information as part of a social media campaign during Spring 2021.

Information Commissioner & Deputy Information Commissioner Event Highlights

2021

JANUARY 2021

Global Privacy Assembly - Artificial Intelligence Working Group

Information Commissioner participated in working group exploring Artificial Intelligence. Deputy Information Commissioner participated in working group exploring the response to Covid-19 and the data protection/privacy issues associated.

FEBRUARY 2021

Annual Privacy & Security Conference, Victoria, BC.

Information Commissioner and Deputy Information Commissioner remotely attended one of world's largest privacy conferences.

MARCH 2021

Global Privacy Assembly - International Enforcement Working Group

Deputy Information Commissioner participated in working group regarding International Enforcement, exchanging information about global enforcement strategies.

Webinar - A World View on Privacy: Commissioners in Discussion

Deputy Information Commissioner joined discussion about data privacy with regulators across several continents and what key issues they are addressing in today's landscape.

APRIL 2021

Global Privacy Assembly - Humanitarian Aid Working Group

Information Commissioner participated in round table discussion about the role of personal data protection in international humanitarian aid and crisis management.

JUNE 2021

British, Irish and Islands Data Protection Authorities (BIIDPA) meeting

Information Commissioner and Deputy Information Commissioner participated in annual small jurisdiction meeting over two days.

Westminster eForum Keynote Seminar

Deputy Information Commissioner remotely attended session about next steps for UK data protection.

Deputy Information Commissioner attended International Conference of Information Commissioners (Freedom of Information)

AUGUST 2021

Centre for Information Policy and Leadership

Information Commissioner spoke remotely at Centre for Information Policy and Leadership event 'Covid-19's Impact on Data: Lessons Learned and the New Future,' co-hosted with Dubai International Finance Centre.

SEPTEMBER 2021

Information Commissioner attended Exporting Data Stewardship Services project workshops (series) hosted by Digital Jersey.

Building a Digital Jersey

Information Commissioner participated in two-day workshop hosted by Digital Jersey.

OCTOBER 2021

Information Commissioner attended International Enforcement Working Group Governance Meeting.

NOVEMBER 2021

Transform 2021

Information Commissioner attended Jersey conference exploring data strategies.

14

Remuneration and Staff report

Sam Duffy

Human Resources Manager

> ***We recognise the value of a diverse team and welcome candidates who bring new experiences, skills, thinking styles and opinions to enhance our team.***

→ Employee Composition

As at the end of 2021 there were six Authority voting members and 12 (11.4 FTE) permanent employees within the JOIC. In total, 67% of employees were female and 33% were male.

The senior leadership team is comprised of four permanent employees, 50% female and 50% male, supported by two external consultants.

→ Remuneration

Against a backdrop of skill shortages in the island, in 2020, the HR and Remuneration Committee commissioned a comprehensive review of pay and reward for both the Authority members and the JOIC employees. This was undertaken by an independent consultant with the purpose of:

a) Developing a Pay and Reward Philosophy for the JOIC, to include guiding principles against which reward decisions are made.

b) Identifying the components that constitute pay and reward within the JOIC.

c) Establishing an appropriate method of determining pay between different levels of work.

d) Drawing benchmark comparisons with other relevant organisations and posts.

e) Designing a new pay structure and the surrounding policy.

As a result of this review a new pay structure was implemented in January 2021. The JOIC pay structure now consists of ten pay bands, containing three pay points within each band.

All pay decisions are underpinned by the JOIC Pay and Reward policy, which includes our reward principles and details of our job evaluation methodology.

Transparent	Ethical	Enabling
Openness and accessibility	Fairness and equitability	Promotes facilitation and collaboration
Honesty and Integrity	Objectivity and impartiality	Drives innovation and a solutions-focussed approach
Evidence based	Accountability	Drives regulatory excellence

It is the Authority's intention to monitor the effectiveness of the JOIC pay and reward policy, every 12-24 months. The aim is to ensure that pay and reward are competitive, reward good performance and support the JOIC in attracting and retaining key talent.

→ Remuneration of directors

Director roles, which includes the Information Commissioner, are positioned between pay bands 8 and 10 on the JOIC pay structure, as described previously.

Directors' pay and reward follow the same principles as all posts. Appointments at director level are based on clear criteria and require demonstrable evidence of management and leadership capabilities. At the current time all posts, including director level receive accrued pension benefits. See the finance report on page 78 for further information. At the current time no posts, including director level, receive allowances or performance related pay. The only additional benefit available at director level is parking.

→ Recruitment

All staff appointments are made on merit and based on fair and open competition. All vacancies are openly advertised using a number of channels to encourage a broad range of applications from all backgrounds and sectors of our community. Criteria are defined before interviews and used to objectively assess candidates' suitability for the role. We recognise the value of a diverse team and welcome candidates who bring new experiences, skills, thinking styles and opinions to enhance our team.

→ Employee turnover

One member of staff left the team in 2021 and one retired. This equated to an employee turnover of 16% in 2021.

→ Employee engagement

During the Covid pandemic, employee health, well-being and engagement was a priority for the JOIC, particularly whilst the team was working remotely and for individuals who were new to the office. An engagement survey was conducted in October 2021 focusing on seven key areas of employment. Overall, the engagement scores were high, with job satisfaction, pay and benefits and teamwork returning the highest levels of engagement. Areas for improvement were also identified, such as internal communication and more structured training. Plans are ongoing with the team in these areas.

→ Talent Management

As a small employer working in a specialist field, talent retention is vital to our success. We require a broad range of skills and knowledge, not only in data protection, but in communication, outreach, case management, finance, legal, HR and general business management. Building on our engagement work, we have put in place a comprehensive programme of training sessions to support continuing professional and personal development. It can be challenging in a small organisation to provide a breadth of career opportunities, however in 2021 we achieved three internal promotions and two progressions (employees receiving an incremental pay increase on account of exceptional performance). Our progress in the area of reward and remuneration also supports our plans to retain and engage talent.

→ Employee policies relating to disabled persons

The JOIC have a number of policies and procedures in place to ensure employees with a disability are treated fairly at all stages of the employee lifecycle (such as recruitment, training and development, absence, career progression etc.) Candidates and employees with a disability are supported in a number of ways, such as adjustments to the interview process, providing an appropriate working environment and flexible working patterns where possible. Our aim is to ensure that those who are, or become, disabled, are treated fairly and can continue to perform effectively and contribute to our goals.

15

Finance Report

Claire Le Brun

Finance Manager

> ***Registrations continued to be received over the course of the year due to the success of the community awareness programmes.***

2021 was a challenging year for JOIC but not in the typical way you would expect to have challenges during the normal course of business. Budgeting and forecasting during a pandemic (which brought with it a high degree of uncertainty) was something we had not expected to face, and we had no comparisons with a 'normal' trading year that we could draw upon but we knew we were not alone and many other businesses were facing similar struggles.

With the Covid-19 pandemic still a very real issue, the budget for 2021 was set conservatively. Noting the pressures faced by local businesses and the expectation that the pandemic would cause many businesses to cease trading we anticipated a drop in registration revenue for 2021.

The opposite of our assumptions was true, however, and we saw registration income exceed our original budget (£1.5m) by almost 40%.

All fee bands have seen an increase in fee income with the exception of the Special Category Data fee which has fallen by 37% compared to 2020. Rather than this being due to a reduction in entities holding special category data it is likely that entities are not passing the revenue threshold to become eligible to pay a fee in this banding. We are likely to see increases in this area as businesses return to pre-pandemic levels of activity.

.

	Full year 2021	Full year 2020	
Full time equivalent employees fee	£463,240	£407,783	13.6%
Past year revenues fee	£78,400	£73,050	7.3%
Proceeds of Crime fee	£106,600	£103,150	3.4%
Administration services fee	£1,412,121	£1,217,324	16%
Special Category data fee	£33,050	£52,650	-37.2%
Total	**£2,093,410**	**£1,853,957**	**12.9%**

The largest increase has been seen in the Administration services fee category which has increased by 43% on budgeted figures and a 16% overall increase when compared to 2020.

The full year fee in this category makes up 67.5% of the total registration revenue in 2021. (2020: 65.6%)

The next highest fee band is the full-time equivalent employees fee which makes up 22.1% of the total registration revenue received in 2021. (2020: 21.9%)

Registrations continued to be received over the course of the year due to the success of the community awareness programmes and events detailed earlier in this annual report and new businesses registering with us for the first time. This additional registration revenue was unbudgeted and contributed to the surplus generated in the year.

→ Working in Partnership with Government

JOIC receives a Government of Jersey grant and during 2021 the grant received was £500,000 (2020: £260k).

The grant income represents 19.3% of the total income received during 2021 and in line with the Partnership Agreement between JOIC and the Government of Jersey this grant income was used for the purposes of administering the Authority Law, oversight and enforcement of the DPJL and the oversight and enforcement of the FoI Law.

JOIC is still in a growth phase. Registration fee income is targeted to grow by 5% each year but there will be a point in time where we reach saturation and fee income will level off.

JOIC's operating expenses are set to grow at a higher rate with forecasts showing large increases during 2022/2023 as the full staff complement is reached with further increases in non-staff areas through 2024 and beyond.

→ Remuneration and Staff

Remuneration for the Authority was subject of an external review by Kojima. The findings were submitted to the Minister who approved the following time commitments and rates for the Authority members:

It is with the full picture in mind that the Government grant value is set along with the fee bandings which are reviewed on an annual basis.

Role	Time Commitment	Day Rate	Annual Remuneration per Authority member for the relevant contribution
Authority Chair	18 days p.a	£950	£17,100
*Sub-Commitee Chair	3 days p.a	£750	£2,250
Voting Members	12 days p.a	£750	£9,000

* *The Sub-committee Chair is a new duty in 2021 attached to an existing Voting Member role. The Sub-committee Chair has an additional three days allocated to allow for the increased workload but is paid at the same day rate as a voting member.*

There are no other payments made to the Authority members. The Chairman and the other voting members are 'appointed by the Minister who must have particular regard to the need to ensure that voting members of the Authority.

(a) have the qualifications, experience and skills necessary to exercise and perform the functions of a member, in particular relating to the protection of personal data;

(b) have a strong sense of integrity; and

(c) are able to maintain confidentiality. (Art. 3 DPAJL)'

Authority members do not constitute an employee for the purposes of the Employment (Jersey) Law 2003 or other local legislation.

Total staff costs for the year were underspent at year end due to delayed recruitment as a result of the pandemic.

[12] https://www.kojima.je/

Budget 2021	Actual 2021	Variance
£1,092,734	£965,689	£127,045

Staff costs have increased by 7% compared to the 2020 spend.

Staff costs include the Commissioner's salary. There was a change in Commissioner during 2021 but the grading applied to the role remained consistent with the change of personnel. The Commissioner's grade was subject to the same external review detailed in the Human Resources report from Kojima.

Commissioner Salary 2020	Commissioner Salary 2021	% Increase on 2020
£134,750	£143,693	6.6%

The actual payment made to the Commissioner in 2020 included a payment for a double taxation reimbursement which is not included in the figures above. The taxation reimbursement was specific to the agreement with the previous Commissioner and not part of the considerations for grade setting.

→ Non-Staff Costs

There are underspends, throughout the non-staff budget areas that are related to the previously mentioned delayed recruitment and the pandemic causing delays in planned operations.

The underspends, along with the over achievement in registration income, has meant a large underspend has been generated.

It is with the full picture in mind that the Government grant value is set along with the fee bandings which are reviewed on an annual basis.

Budget 2021	Actual 2021	Variance
£807,266	£654,207	£153,059

The surplus generated in the year will be carried forward and utilised in 2022 to fund a number of projects and initiatives that are currently undergoing detailed discussion and analysis.

16

Audited Financial Statements

JERSEY OFFICE OF THE INFORMATION COMMISSIONER

JERSEY DATA PROTECTION AUTHORITY (JDPA)
AUDITED FINANCIAL STATEMENTS
FOR THE YEAR ENDED 31 DECEMBER 2021

CONTENTS	Page

→ General Information

Members of the Authority

Jacob Kohnstamm	Chair
Clarisse Girot	Voting Member
David Smith	Voting Member
Gailina Liew	Voting Member
Paul Routier MBE	Voting Member
Helen Hatton	Voting Member
Dr Jay Fedorak	Information Commissioner (non-voting member) up to 1st July 2021
Paul Vane	Information Commissioner (non-voting member) from 2nd July 2021

Registered Office

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

Banker

HSBC
15-17 King Street St Helier
Jersey JE2 4WF

Independent Auditors

Baker Tilly Channel Islands Limited
1st Floor Kensington Chambers
46/50 Kensington Place
St Helier Jersey Jersey
JE4 0ZE

→ 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 31 December 2021.

Incorporation

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

Corporate governance and delegation of authority

The JDPA carries the ultimate responsibility for the discharge of the responsibilities under the DPJL. 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 DPJL; the making of an order to pay an administrative fine; the preparation of the Annual Report. By a Authority Resolution of 7 January 2019, the JDPA delegated all 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 2021.

Going Concern

The Authority consider, given the financial condition of the Authority, 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.

Auditors

The Comptroller and Auditor-General exercised her 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 the 5 years from the year ended 31 December 2018 to 31 December 2022.

Jacob Kohnstamm
Chair

31st March 2022

→ 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 regulation.

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 JDPA 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 Authority will continue in business.

The voting members are responsible for keeping adequate accounting records that are sufficient to show and explain the Authority'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 as 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.

Jacob Kohnstamm
Chair

31st March 2022

→ Chairman's Statement

2021 has been a successful year in terms of operational development, enhancing governance, improving infrastructure and financial independence.

The JDPA introduced the new revenue model early in 2019. The revenue generated through registration fees, as detailed in the DPAJL, is allowing us to grow and meet the advancing requirements imposed on all data protection authorities as a result of rapidly emerging technologies. Such technologies include synthetic data, AI and emotional recognition software.

Currently, the private sector provides 80% of the funding of the Authority, with Government paying the remaining 20% by way of a grant. In recent years, on occasion, Government has reduced the grant figure to 10% of our funding. Discussions on a more appropriate and representative funding mechanism commenced in 2021, the Minister recognises that a resolution to this issue should be a high priority in 2022. The casework generated from the public sector represents 29% of the investigations undertaken in 2021, which is not dissimilar to other years. Hence the discussions are focussing on equity between funding from public and private sector whilst critically protecting the Authority's independence.

The registration fees provided an annual income of £2,091,353 in 2021. The fees generated increased by 18% from 2020. We anticipate the fees levelling out or potentially declining as the full impacts of Covid begin to impact the economy and we reach saturation point of organisations required to register with the JDPA as per the Law.

We are closely monitoring the registration fee income year on year; we are being prudent In our planning as the JOIC Is a relatively young organisation and is still in a growth phase. Registration fee income is set to grow at 5% each year but there will be a point In time where we reach saturation and fee income will remain stagnant or drop when this occurs. Operating expenses are set to grow as fee income levels off and we meet an equilibrium.

Our new three-year strategic plan details new strategic outcomes 2022 - 2025. Looking ahead, we will continue to strengthen our infrastructure and strategic capabilities with investment and focus on three key areas: enhancing the resilience and reporting capabilities of our technology infrastructure, continued development of our supervision and oversight activities, and the development of a data stewardship regulatory framework In collaboration with other agencies and industry stakeholders in support of Jersey's aspiration to be a leading jurisdiction for data trusts.

Jacob Kohnstamm
Chair

31st March 2022

→ 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 2021 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 2021, and of its financial performance and surplus for the year then ended in accordance with United Kingdom Accounting Standards, including Section 1A of Financial Reporting Standard 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). 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, and we have fulfilled our other ethical responsibilities in accordance with these requirements. We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Conclusions relating to Going Concern

In auditing the financial statements, we have concluded that the Authority'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 Directors 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 of the Authority (the "Board") with delegation to the Information Commissioner (the "Commissioner") 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

As explained more fully in the Board's responsibilities statement set out on page 85, the Board is 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 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 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 is 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 Board;
- Review of legal invoices;
- Review of management's significant estimates and judgements for evidence of bias;
- Review for undisclosed related party transactions;
- Regarding revenue derived from registrations made to the Authority, obtain an understanding of the process from initial registration through to the income being recognised and received, including walkthroughs and detailed control testing;
- Undertake substantive analytical procedures to assess the completeness of the reported income derived from registrations made to the Authority;
- Review agreements correspondence and conditions related to the funding from the Government of Jersey, to ensure an appropriate level of grant income has been recognised in the reporting period;
- Undertake test of controls to gain assurance over the procedures relating to staff starters, leavers and the payroll process;
- 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.

This description forms part of our auditor's report.

Use of this Report

This report is made solely to the Minister, as a body, in accordance with section 43 of the Law. 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.

Baker Tilly Channel Islands Limited
Chartered Accountants St Helier,
Jersey

Date: 31 March 2022

→ Statement Of Comprehensive Income And Retained Earnings

	Notes	2021 £	2020 £
Income from activities	4	2,091,353	1,778,154
Operating expenses	5	(1,619,896)	(1,597,212}
Surplus on ordinary activities		471,457	180,942
Other income			
Government grant	6	500,000	260,000
Interest		25	
Surplus on ordinary activities		500,025	260,000
Taxation	7		
Surplus for the year		971,482	440,942
Retained Surplus as at 1st January 2021		580,402	139,460
Retained Surplus as at 31st December 2021		1,551,884	580,402

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 92 - 97 form part of these Audited Financial Statements

→ Statement Of Financial Position

Assets	Notes	2021 £	2020 £
Non-current assets			
Tangible assets	8	8,267	23,744
Intangible assets	9	96,517	128,879
		104,784	152,623
Current assets			
Trade and other receivables	10	54,340	40,799
Cash and cash equivalents	11	1,439,574	462,442
Total Current assets		1,493,914	503,241
TOTAL ASSETS		**1,598,699**	**655,864**
CREDITORS – amounts falling due within one year	12	(46,815)	(75,462)
Trade and other payables		(46,815)	(75,462)
TOTAL NET ASSETS		**1,551,884**	**580,402**
EQUITY	13		
Share Capital		-	-
Reserves		1,551,884	580,402
TOTAL NET ASSETS		**1,551,884**	**580,402**

The financial statements on pages 92 to 97 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 92 - 97 form part of these Audited Financial Statements.

The accounts were approved and authorised for issue on 31st March 2022 by the Authority and signed on its behalf by:

Jacob Kohnstamm
Chair

31st March 2022

→ Notes to the financial statements for the year ended 31 December 2021

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, Jersev. 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 FRS 102{1A), 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 Section 1A of Financial Reporting Standard 102 (FRS 102) The Financial Reporting Standard applicable in the UK and Republic of Ireland' issued by the Financial Reporting Council and the Data Protection Authoritv (Jersev) 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.

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 judgment 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.

(i) Going concern

The Authority consider, given the financial condition of the Authority, the use of the going concern basis is appropriate for the current period and for 12 months from the date of signing these accounts.

(ii) 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 obliqations can be reliablv estimated.

(iii) 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.

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 from 19-21 Broad Street, St Helier JE2 3RR or online at:

http://www.gov.je/Working/WorkingForTheStates/Pensions/PubiicEmployeePensionFund/Pages/PublicServicePensionPubiications.aspx

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 alreadv been incurred. The grant is recognised in income when it is received or receivable.

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 profit or loss and other 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.

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 of 5 years. 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.

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.

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 llabilltles 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.

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.

Notes to the financial statements (continued)
For the- year ended 31 December 2021

4. Income from activities

Income from activities is made up of registration fees under the terms of Data Protection Authority (Jersey) Law 2018.

5. Operating expenses

	2021 £	2020 £
Staff including Commissioner and Deputy Commissioner	965,689	901,657
Services and Communications	410,376	426,623
Administrative Expenses	17,988	66,880
Audit and accountancy fees	24,506	15,135
Premises and Maintenance	126,675	111,572
Bank charges	8,809	14,749
Depreciation and amortisation	65,853	60,595
	1,619,896	**1,597,211**

6. Government grant

Any net deficit of the Authority is financed by the Government of Jersey under the Partnership Agreement.

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

	2021 £		
Cost	Office equipment	IT equipment	Total
As at beginning of year	35,815	35,413	71,228
Additions in the year	1,239	11,162	12,401
	37,054	**46,575**	**83,629**
Accumulated depreciation			
As at beginning of year	23,876	23,608	47,484
Depreciation charge for the year	12,352	15,526	27,878
	36,228	**39,134**	**75,362**
Net book value			
As at 31 December 2021	826	7,441	8,267
As at 31 December 2020	11,939	11,805	23,744

9. Intangible assets

	2021 £
Software Cost	
As at beginning of year	184,264
Addition	5,614
	189,878
Accumulated amortisation	
As at beginning of year	55,385
Charge for the year	37,976
	93,361
Net book value	
As at 31 December 2021	96,517
As at 31 December 2020	**128,879**

10. Trade and other receivables

	2021 £	2020 £
Trade Debtors	19,459	13,122
Prepayments	34,882	27,677
	54,341	**40,799**

11. Cash and cash equivalents

The Authority has 1,439,574 at the end of the year (2020: 462,442). All balances are cash and are held in the Authority's own bank accounts.

12. Trade and other payables

	2021 £	2020 £
Accruals and trade creditors	(46,815)	(75,462)
	(46,815)	**(75,462)**

13. Share capital

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

14. Related Party Transactions

	2021 £	2020 £
Commissioner until 1st July 2021	88,227	154,582
Commissioner from 2nd July 2021	69,224	-
Chair	14,177	11,250
Voting member (Non Executives)	8,100	7,200
Voting member (Non Executives)	10,350	7,200
Voting member (Non Executives)	8,100	7,200
Voting member (Non Executives)	10,350	7,200
Voting member (Non Executives)	10,350	7,200
	218,878	**201,832**

Key management personnel includes the Commissioner (change of personnel in the year) 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 JPDA has recognised £500,000 (2020: £260,000) as grant income from the Government of Jersey. The JDPA is accountable to the Government of Jersey, who incorporated it by means of the Partnership Agreement

15. 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.

JOIC
JERSEY OFFICE OF THE
INFORMATION COMMISSIONER

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

+44 (0) 1534 716 530

www.jerseyoic.org