JOIC

JERSEY OFFICE OF THE
INFORMATION COMMISSIONER

2020 ANNUAL REPORT

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

www.jerseyoic.org

CONTENTS

The Jersey Data Protection Authority's role, vision, mission, promise and 2020 strategic outcomes

OUR ROLE

The Jersey Data Protection Authority (the Authority) is an independent statutory body. Its mission is 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 and the Data Protection Authority (Jersey) Law 2018.
- 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.

OUR VISION

A prosperous, close-knit island community that embraces a collaborative and innovative approach to data protection, providing a leading-edge model to other similar jurisdictions.

OUR PROMISE

To promote the information rights of individuals 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.

OUR 2020 STRATEGIC OUTCOMES

1. The people of Jersey are provided with a high level of data protection and expert service whilst resources are judiciously and responsibly managed.
2. The Island's approach to data protection clearly contributes to its reputation as a well-regulated jurisdiction.
3. Jersey is recognised as a world leader, embracing innovation to safely develop and implement digital technology.

Message from the Chair

Jacob Kohnstamm
Chair, the Jersey Data Protection Authority (JDPA)

It is my pleasure, on behalf of the Jersey Data Protection Authority (JDPA) to present to the Minister and the members of the States Assembly our Annual Report for 2020. This fulfils our statutory obligation under Article 44 of the Data Protection Authority (Jersey) Law 2018.

This report covers an extraordinary year. We had just begun to implement our new registration model when the Covid-19 pandemic presented a wide range of further challenges to us all. The Voting Members of the JDPA are grateful to the employees of the Jersey Office of the Information Commissioner (JOIC) for continuing to deliver exemplary service to the people of Jersey, despite a myriad of administrative and operational challenges, as well as a further increase in workload.

In my message in the Annual Report for 2019, I described our efforts to develop a new registration model that would provide the majority of the new funding for the JDPA. I noted that the goal was to reduce Government funding from 85% to 33% of our revenue. This was to provide us with sufficient independence from Government, while ensuring that Government continued to pay a fair share. What I mean by paying a fair share is that the Government contribution should recognise that the JDPA regulates the public sector, as well as businesses, and that data protection is a human right. Consequently, supporting data protection regulation is a public good, worthy of Government support.

Data protection involves the promotion of fairness. The JDPA believes that promoting the principle of fairness should go beyond just the regulatory responsibilities of conducting investigations, but that it should also guide all of its operational and administrative functions. To that end, the JDPA recommended a registration model that would distribute the financial burden fairly. Larger organisations with greater resources should pay more than smaller organisations. Organisations that collect sensitive data that present a greater risk to the rights and freedoms of data subjects should pay more than other organisations, owing to the greater level of data protection required. The other issue was the balance between funding from Government and revenues through registration fees. As Government was exempt from paying the registration fees and any regulatory penalties, the JDPA believed that Government should provide a grant of at least a third of the total funding. In common with most jurisdictions around the world, Jersey is experiencing a significant increase in workload relating to investigating and monitoring data breaches and other types of regulation involving the public sector. This work often involves extremely sensitive personal data. Reviewing data protection impact assessments, draft laws and interagency agreements, along with creating guidance and implementation tools, are other examples of our activities that primarily involve the public sector. It would not be fair for businesses to be subsidising the costs incurred from the JOIC providing services to Government

As the JDPA approached the first year of implementing the new registration model, we did not know how much revenue it would generate. We based the model on the most accurate projections of the best data available, but we knew that even the soundest projections could not guarantee accuracy. Fortunately, the new registration model generated revenue that exceeded our target by a modest amount. This combined with spending reductions resulting from the pandemic resulted in a small budget surplus. As a result, the government reduced its grant. This meant that the business community increased its share of the costs of regulation from 67% to 85%.

While this did not cause the JDPA economic hardship, we feel that there is an important matter of principle at stake. We believe there are compelling reasons for Government to pay a fair share, rather than just top up the fee revenue received from businesses. We are involved in continuing discussions with Government to re-evaluate the current fee model, with a view to an arrangement that is just and therefore fairer for everyone.

Like everyone else, we faced new challenges from the pandemic. Because of government-imposed restrictions, our employees spent a large portion of the year working from home. Fortunately, modern technology made it possible for us to continue to provide service to the public and our stakeholders. We were able to use telephone and video conferencing to conduct investigations, present training sessions and conduct meetings both internal and external. Travel restrictions meant that some of our Authority members could not attend our meetings in person, but video conferencing was a suitable alternative. Even though the restrictions also reduced our travel and recruitment expenditure, they triggered new expenditure in information and communications technology that were necessary for employees to be able to serve the public, while working remotely. The only deficiency we experienced was in the social benefits of our work that can only be realised when people are able to meet in person. Social interaction and knowledge sharing, in the workplace and at the Board level, is important in building an efficient and effective team. It is also necessary to build effective partnerships with stakeholders. We look forward to resuming personal interaction once it is safe again to do so.

In addition to social challenges, the pandemic introduced technical and ethical challenges, as well as the need for businesses and government to rapidly collaborate. Fighting a pandemic effectively requires reducing social contact and identifying individuals who might be infected, which could have major implications for individual privacy and data protection. Data protection laws do provide the means of managing this dichotomy, whilst also protecting the privacy of individuals to the greatest extent possible. Our office advised on several contact tracing initiatives. One example was a smartphone app that can alert individuals that they might have been in contact with an infected individual, without identifying those individuals. As the result of our collective action with the Government and other public sector agencies, approximately 50% of the Jersey population downloaded this app, which constituted the highest participation of any jurisdiction in the world. We also advised government and the hospitality sector on the best means and good practices for contact tracing of customers. These issues were common to jurisdictions around the world, and we worked with our international partners to identify best practices for our communities, including as an active member of the Global Privacy Assembly task force. We anticipate that this type of international cooperation will increase.

We also implemented rigorous enforcement measures in 2020 in the form of two public statements. I announced the first in my message last year, regarding a statement we issued in January 2020. That statement related to a series of breaches by a private sector business. We issued a second statement involving a government department in October 2020. Public statements serve several functions:

- They inform the public about the existence and circumstances of significant breaches of the law.
- They provide a teaching tool that highlights the risks to personal data when it is not treated fairly or kept secure.
- They prompt both public and private sector organisations to regularly review their own data protection practices to ensure that they have the right controls in place.

A public statement holds organisations accountable for their actions, or lack of action, and provides guidance on how to improve data protection practices. Finally, it also holds the JDPA accountable by giving the public the opportunity to view its regulation practices in action. Good data protection regulation must not only be done, but also be seen to be done. Public statements, like this annual report, give members of the public information they need to evaluate the effectiveness of the JDPA.

In closing, we are sad that this will be the final annual report with Dr Jay Fedorak as Information Commissioner. We have enjoyed working with him and have benefitted from his extensive experience and international expertise. I would like to speak further about Jay's invaluable contribution to the JDPA, but I decided that this annual report is not the right time to praise him, for two reasons. The first is that he will remain in office until the first of July, and it seems risky to commend him too early. The second is that I want to 'keep my powder dry' for a tribute when we have to bid him farewell in a few months.

However, I am pleased to report that the JDPA has already selected his successor. In October 2020, we commenced a recruitment process with the assistance of the Jersey Appointments Commission (JAC). We conducted an international search in accordance with the requirements of the JAC. We attracted many good candidates from different jurisdictions. In conclusion, the best candidate to emerge from the competition was Jersey's own Paul Vane. We look forward to Paul transitioning into his new position in July 2021 and we are proud that a candidate from Jersey proved to be the most qualified.

Jacob Kohnstamm
Chair, the Jersey Data Protection Authority (JDPA)

Message from the Commissioner

Jay Fedorak PhD
Information Commissioner

It is with great pride and a little sadness that I present my third and final Annual Report under the Data Protection Authority (Jersey) Law 2018 and the Freedom of Information (Jersey) Law 2011. My three-year appointment has passed quickly. The old adage says that time flies when one is having fun, and I certainly have enjoyed my time on this unique and remarkable island.

When I began my term in 2018, my priorities were to build the capacity and capability of the Jersey Office of the Information Commissioner; to ensure that the Jersey data protection regime meets European standards to facilitate the free flow of personal data; and to harmonise data protection regulation across the Crown dependencies, the UK and European Union.

I am pleased to report that, with the support of the JOIC team and the assistance of the Jersey data protection community, we have succeeded in achieving these goals. Prior to my appointment, the office consisted of four employees. The implementation of the new GDPR-based data protection laws in 2018 required that the JOIC have greater capacity to fulfil its expanded responsibilities. We have increased our staff complement to meet our emerging needs. Including hiring we completed in 2020, our team has grown to 16 talented professionals. This has enabled us to manage the increasing workload resulting from our new laws; to improve awareness through public education of the rights of the public and responsibilities of Data Controllers; and to create new implementation tools for businesses and public authorities. Our workload has increased from 93 cases in 2017 to 479 cases in 2020. We have expanded our team of caseworkers who conduct investigations from two to six. This has enabled us to ensure that we can respond to complaints in a timely manner and maintain levels of service that the public deserve. Our caseworkers have identified and corrected lax security and other poor data protection practices. As Chair Kohnstamm has indicated above, we issued public statements on two cases in 2020 that provided good examples to the rest of the data protection community of the risks of lax data protection practices and how to address them.

Previously, we had no resources dedicated to providing communications and public education services. We now have a team of three that has revamped our office website (which won a Jersey technology award), established a social media programme and delivered training and awareness sessions to data protection officers and the public, including students in schools. Keeping children safe, physically and online, is a priority for everyone in Jersey, and we are proud of our schools programme. As an added benefit to us, we sometimes end up learning as much from the students as they do from us.

During 2020, our team also produced a suite of implementation tools to assist the data protection community, including separate toolkits for small, medium and large businesses, as well as one dedicated to financial services. We know that businesses, particularly small businesses, have unique data protection challenges and often lack the necessary expertise. These toolkits will assist them. Financial services, which represent that largest share of the island's economy, provided us with an opportunity to create guidance materials that would have a significant impact for our community. In consultation with Jersey Finance Limited and representatives from the finance industry, we created a toolkit to ensure that all members of this sector can implement the data protection law as efficiently and effectively as possible. We look forward to ongoing collaboration with members of all sectors of the Jersey economy that process personal data.

A larger office required increased financial resources. The Government of Jersey decided that this funding should come from increased registration fees paid by business. We worked at length during 2019 to develop a new registration process, through collaboration and consultation with government and businesses. We strove to find a process that would be fair, simple and based on data risk and ability to pay. We engaged an independent service provider to model a range of fees and predict the anticipated revenue. We aimed to produce a revenue target that matched the resources that we identified would be required to provide adequate service levels to the public. As Chair Kohnstamm has explained, we were successful in 2020 in meeting our revenue target, despite Covid-19 restrictions.

A larger budget, more fee revenue and further independence from Government meant that we needed to recruit our own finance department. Our team of two has been busy over the course of the year, issuing invoices, collecting payments, and processing refunds, while also implementing the entire infrastructure of an independent agency. This included obtaining new bank accounts, credit cards, insurance policies and financial systems, as well as an annual independent audit of our accounts that the team had to assist with for the first time. We also have to provide a suite of deliverables to the Government of Jersey to enable it to provide independent verification that we are providing taxpayers and customers with value for money.

We have been working closely with our international partners to harmonise data protection regulation. We signed a Memorandum of Understanding with the Guernsey Data Protection Authority in 2020. We also began negotiating a similar agreement with our counterparts in the United Arab Emirates. We continue our participation in the Global Privacy Assembly (GPA), the British, Irish and Islands Data Protection Authorities (BIIDPA), and l'Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP). We are a member of the International Enforcement Working Group and the Covid-19 Working Group of the Global Privacy Assembly. We were pleased that the Global Privacy Assembly recognised Jersey at its annual conference as having the shortest retention period for contact tracing data of any jurisdiction in the world. Through these initiatives and forums, as well as others, I am pleased to report that we have been successful in creating greater levels of awareness internationally that Jersey is serious about data protection.

In summary, I am proud that my team of talented and committed professionals has succeeded in meeting our strategic outcomes during my transitional term of office. We have laid the foundation for successful and efficient data protection regulation through an organisation whose influence extends far beyond its modest size. It will be up to my successor to take the office to the next stage of its development, by building on our existing strengths, to enable us to take advantage of emerging opportunities.

I have enjoyed my experience in Jersey tremendously. Jersey businesses and the Government of Jersey have demonstrated a greater level of interest in and commitment to data protection than I have witnessed in other jurisdictions. The quality of the people that I have encountered here also impresses me. I have met an abundance of talented, capable and successful individuals during the course of my stay. With the population of a small municipality, Jersey demonstrates the attributes of a country. Like everybody else, I find the natural beauty to be astounding. I count myself fortunate to have shared this time with a wonderful group of employees in my office and everyone in the rest of the community. After I leave office, I will remain an overseas champion for Jersey, doing my best to create further awareness of this wonderful island. If I do not have a chance to speak with you before July 1st, I say 'A bétôt'.

Dr Jay Fedorak PhD
Information Commissioner

Jersey Data Protection Authority

INDEPENDENCE

The Information Commissioner is accountable to the independent Data Protection Authority in accordance with the Data Protection Authority (Jersey) Law 2018 (DPAJL). The Jersey Data Protection Authority includes the Office of the Information Commissioner.

'In exercising or performing its functions, the Authority must act independently and in a manner free from direct or indirect external influence'

Article 12 Data Protection Authority (Jersey) Law 2018

Independence was the result of the EU Data Protection Directive 95/46, which required that supervisory authorities be independent and effective. The General Data Protection Regulation (GDPR) extended these requirements to include the power to issue fines and sanctions.

The Authority is the independent body responsible for overseeing the Data Protection (Jersey) Law 2018 (DPJL) and the Data Protection Authority (Jersey) Law 2018 (DPAJL). The Office of the Information Commissioner is also responsible for overseeing the Freedom of Information (Jersey) Law 2011.

The **Data Protection (Jersey) Law 2018** gives citizens important rights including, but not limited to, the right to know what information public authorities and companies hold about them and how they handle that information, and the right to request correction of their information. The Data Protection Law in Jersey helps to protect the interests of individuals by requiring organisations to manage the personal information they hold in a fair, lawful and transparent way, as well as being accountable to their customers and to themselves for their actions.

One of our primary functions is to make individuals aware of their rights and to ensure all organisations are aware of their responsibilities. Another is to conduct investigations into complaints by individuals about public agencies or companies concerning the management of personal data. We also manage the process of registration of public authorities and companies under the DPJL. In addition to investigating complaints that individuals bring to our attention, we can proactively investigate or audit general compliance with the laws.

The data protection laws give the Authority and the Commissioner responsibilities with respect to public education, conducting investigations, receiving reports of breaches and consulting with public authorities and companies.

The **Freedom of Information (Jersey) Law 2011** gives people a general right of access to information held by most public authorities in Jersey. Aimed at promoting a culture of openness and accountability across the public sector, it enables a better understanding of how public authorities carry out their duties, why they make the decisions they do and how they spend public money by requiring the disclosure of information in those areas.

Our primary function is to fulfil the second stage of the appeals function - a person dissatisfied with a decision of a scheduled public authority may appeal to the Information Commissioner. The JOIC fully reviews each appeal submitted and undertakes a thorough analysis of the first appeal, all case material and where applicable drawing on precedents and the public interest test. The Information Commissioner will serve a notice of the decision in respect of the appeal on the applicant and on the scheduled public authority.

Looking Forward - Privacy & Horizon Scanning

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

The progression of digital technologies has accelerated at an unprecedented pace. A McKinsey & Company study estimates that globally this progression has advanced by seven years in the wake of the pandemic, as businesses move services online and seek further innovation in providing service to their customers. For example, the urgency that the pandemic has created has led to the speedy development of contact tracing apps and the first Covid-19 vaccines.

Every one of us has been touched by the pandemic, some affected more than others. But as with every crisis, human beings are somehow able to show our true selves and demonstrate a level of resilience, adaptation and determination that in future years will be deemed remarkable. Our office has dealt with many privacy issues arising from the pandemic. There are new privacy challenges involved both with working from home and returning to the office. Test and trace initiatives, including from the implementation of tracing apps raised numerous privacy concerns. Most importantly, there is the need to ensure that data protection compliance is not neglected, while we deal with the immediate demands of the pandemic.

Digital technologies regularly process large amounts of personal information without our knowledge. Few of us question why organisations collect information from us, or what steps are being taken to ensure its security. We should question the decisions made using our information, particularly when this occurs under the pretext that it is necessary to keep us safe. We should also question the use of automated decision making technologies to decide whether we are good enough for a particular job, or whether we are eligible for credit. Sometimes these technologies deploy algorithms that incorporate bias, which may unfairly influence the outcomes. We should not assume that these technologies will always operate fairly. Custodians of our data must earn our trust.

This is why the JOIC will be focusing more than ever on individuals over the coming year; to help them take greater control, ownership and responsibility over their own information, and to challenge decisions about them with the right questions.

As privacy regulators, we are watching for the development of new technologies that might have an impact on our privacy. We have seen how the global pandemic has spawned significant growth in innovations, such as e-learning, digital health and Fintech. With so many people working from home, or studying remotely, and the vulnerable less able to access the traditional service delivery, we will need to address all privacy concerns to ensure public trust and organisational accountability. The advancement of digital healthcare in Jersey provides significant cause for excitement and optimism, with the Government of Jersey's Digital Health Team working hard to implement a forward-thinking strategy that will change the way in which healthcare data is both generated and accessed, thus providing an enhanced level of health and social care to the island. In practice, this means a healthcare transformation that puts the citizen at the heart of the process with a clear focus on the individual and their needs. In addition, Jersey will benefit from a digitally world-class healthcare system and the project provides an opportunity for the island to become a world leader in the field.

Our primary objective over the last three years has been to ensure the people of Jersey receive a high standard of data protection. Our focus has been to promote compliance through support to island businesses in the form of awareness raising and useful tools and guidance. However, everyone must do their part (regulator, businesses, government and the public) to ensure the highest standards of data protection across the island.

Compliance with the Law should not be just a tick-box exercise, but rather part of our everyday thinking.

Jersey is a unique place that historically has achieved influence in the world beyond the size of its land mass or population. Embracing new technologies, fostering creative innovation and working together as one, Jersey can continue to flourish on the world stage. It needs to sustain a strong culture of privacy and security to ensure Jersey can take full advantage of these new opportunities and become an even more attractive and safer place to do business. This will ensure a promising future for Jersey with obvious benefits to both the economy and our overall wellbeing.

Our aim for the future is to foster a culture where privacy becomes instinctive.

We want individuals to recognise and value their own privacy. Similarly we want businesses to consider the privacy risks associated with their processing activities right from the outset. This is an ambitious aim that requires inclusion and involvement from everyone in our community to succeed. Privacy is a fundamental human right, but it is also necessary, and a collective responsibility if we are to preserve the future prosperity of our Island.

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

Governance, Accountability and Transparency

THE DATA PROTECTION AUTHORITY

The general purpose of the Authority is to provide administrative and operational oversight of the Jersey Office of the Information Commissioner:

- It performs a non-executive function and does not participate in the daily activities of the Information Commissioner's Office, the Jersey Office of the Information Commissioner (JOIC).
- It provides direct independent oversight of the JOIC, replacing the Government of Jersey in this function.

The Authority has the public responsibility to:

- Ensure that the JOIC remains accountable to the people of Jersey, in properly fulfilling its mandate and delivering quality services to its stakeholders.
- Ensure that the JOIC provides value for money and complies with appropriate policies and procedures with respect to human resources, financial and asset management, and procurement. This includes formal approval of any single item of expenditure in excess of ten percent of the operating budget for the JOIC.

The Authority also provides an advisory function to the Office. 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. At times, the Authority may also provide strategic advice with respect to the handling of particular cases.

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 of these other powers to the Commissioner. It reserves the right, however, to exercise those functions itself in particular cases, at its discretion.

There are certain functions that the Data Protection Authority Law stipulated that the Authority must perform without delegating to the Commissioner. The most important is that only the Authority can decide whether to issue 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

The Authority is currently comprised of a non-executive chair and five non-executive members, which the Chief Minister appointed in accordance with the Law in October 2018.

The Information Commissioner is also a non-voting member of the Authority.

CHAIR OF THE AUTHORITY
JACOB KOHNSTAMM

Jacob has over 24 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 6 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 4 years and hosted that conference in Amsterdam in 2015.

VOTING AUTHORITY MEMBER
CLARISSE GIROT

Clarisse is a seasoned data privacy Asian law expert and has a 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.

Clarisse is currently a senior fellow at the Asian Business Law Institute (ABLI), a legal think tank which initiates and conducts projects that promote the convergence of business laws in Asia. Prior to relocating to Singapore, Clarisse was based in Paris where she acted as Counsellor to the President of the French Data Protection Authority (CNIL) and Chair of the group of European DPAs (now EDPB). From 2004 to 2008, she was head of CNIL's department of International Affairs.

VOTING AUTHORITY MEMBER
HELEN HATTON

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.

Helen is a Fellow of the Institute of Advanced Legal Studies, a member of the Editorial Board of the Journal of Banking Regulation, and a Liveryman of the Worshipful Company of International Bankers. She is a recognised international speaker on regulatory and compliance topics.

VOTING AUTHORITY MEMBER
DAVID SMITH

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

Gailina is an independent non-executive director with a legal, scientific, operations and international business executive background. She brings more than 20 years of board governance experience in the listed company, investment fund, economic development, education, adjudication and voluntary sectors to the JDPA. Engaging and curious, she is interested in the evolving frameworks for the regulation of privacy, data protection and their intersection with the ethical use of technology, artificial intelligence, personal information and the future of human society.

Gailina's current portfolio includes Chair of the Statistics Users Group, Member of the Committee of Management of the Public Employees Pension Fund, Commissioner for Tax Appeals, and Senior Independent Director of Digital Jersey

VOTING AUTHORITY MEMBER
PAUL ROUTIER

Paul was an elected member to the States of Jersey for 25 years and Assistant Chief Minister for a period of this time.

During his final term of office he successfully led the debates in data protection legislature 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 General Data Protection Regulations (GDPR) which are in force today.

Three Authority 'sub-committees' were established in 2020 to ensure good governance.

- Audit and Risk Committee chaired by Helen Hatton met three times in 2020.
- Governance and Nominations Committee chaired by Gailina Liew met twice in 2020.
- Remuneration and Human Resources Committee chaired by Paul Routier met twice in 2020.

Each sub-committee has a Chair, the relevant balance of expertise and defined proportionate terms of reference.

AUTHORITY MEETINGS

The Authority meets no less than four times per annum. In 2020 there were four scheduled Authority meetings and three additional meetings to discuss governance, enforcement and financial matters.

BOARD MEMBERS REMUNERATION

For 2020 the Chair of the Jersey Data Protection Authority received £11,250 for his services based on 12-days commitment. The voting Authority Members were paid £7,200 for their 12-days' commitment to the Authority.

→ RISK MANAGEMENT

The JDPA approaches risk very conservatively. The Audit and Risk Sub Committee has recommended that the Authority identifies, mitigates and reviews all risks in the following key areas;

- Legal and regulatory.
- Operational.
- Governance.
- Strategic.
- Finance.
- External and emerging.
- People.
- IT/Cyber.

→ ENVIRONMENTAL & SOCIAL POLICY

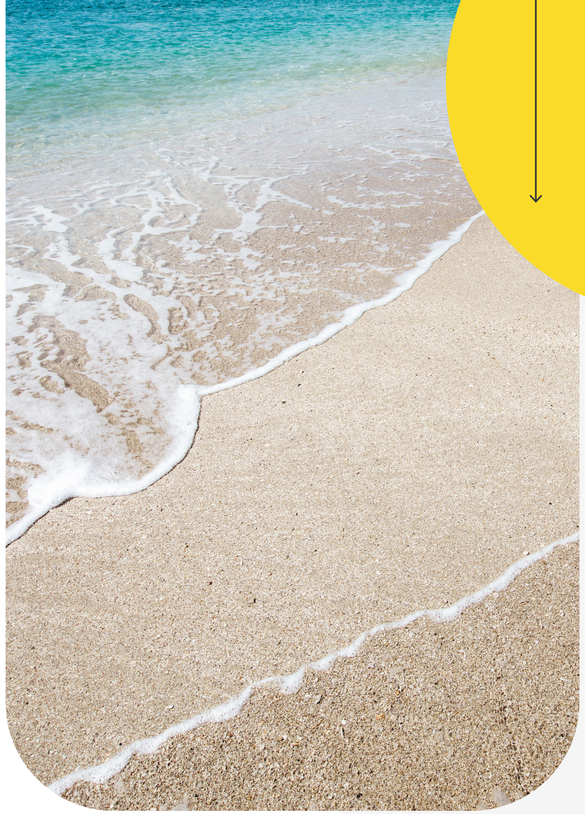
Protecting the environment is one of our priorities, and we are pursuing membership in the Government of Jersey's 'Eco Active Business Network'. This is an environmental management scheme for organisations on the island. Joining the network will assist us in protecting the environment collaboratively in a coordinated fashion to contribute to the goals of our entire community.

The JOIC is committed to:

- Improving efficiency in the use of energy.
- Reducing waste.
- Demonstrating compliance with environmental legislation.
- Reducing the risk of causing pollution or other damage to the environment.

→ SOCIAL

Supporting local charities has been a priority for the JOIC for several years. We will pursue opportunities to continue our tradition once the pandemic restrictions are lifted.



Managing Performance and Regulatory Deliverables

Anne King

Communications and Operations Manager

Measuring performance can be challenging in an organisation whose primary purpose is other than fiscal. Our objectives are to promote security, awareness and empowerment, and they require a different approach.

The Data Protection Authority (Jersey) Law 2018 defines the JOIC's role, with respect to oversight and enforcement. However our purpose is broader.

The JOIC's three over-arching strategic outcomes;

1. The people of Jersey are provided with a high level of data protection and expert service whilst resources are judiciously and responsibly managed.
2. The Island's approach to data protection clearly contributes to its reputation as a well-regulated jurisdiction
3. Jersey is recognised as a world leader, embracing innovation to safely develop and implement digital technology.

These outcomes promote the wellbeing of the entire community. We cannot achieve them without collaboration with other organisations and members of the public.

Our approach to the performance monitoring and measurement of our strategic outcomes must reflect both the quantitative and impact of our service. We must be able to demonstrate both the tangible and the intangible results of our work. That is to say not only the number of cases closed but the progress made in shifting attitudes and behaviours towards data protection and empowering islanders to exercise their rights.

Our measurement model aims to seek evidence of progress in these areas as well as to guide our strategy and inform our decision making.

Our objective, therefore, is to ensure that we undertake our activities in a focused and meaningful way and to be able to determine 'is anyone better off' as a result of our efforts?

In support of our strategic outcomes, we have established seven indicators, with fourteen performance measures.

We have incorporated measures for the entire population, whether they engage directly with us or not.

Examples of indicators include 'The level of Compliance with the Data Protection Law' and 'The percentage of islanders who are exercising their Information Rights'. They help quantify the achievement of our strategic outcomes.

We build measures into all of our activities whether it is a communications campaign, data protection audit or case management. We want to ensure that we deploy our limited resources well, that we target our efforts in areas that make a difference for people and that we are making steady progress towards our longer term outcomes.

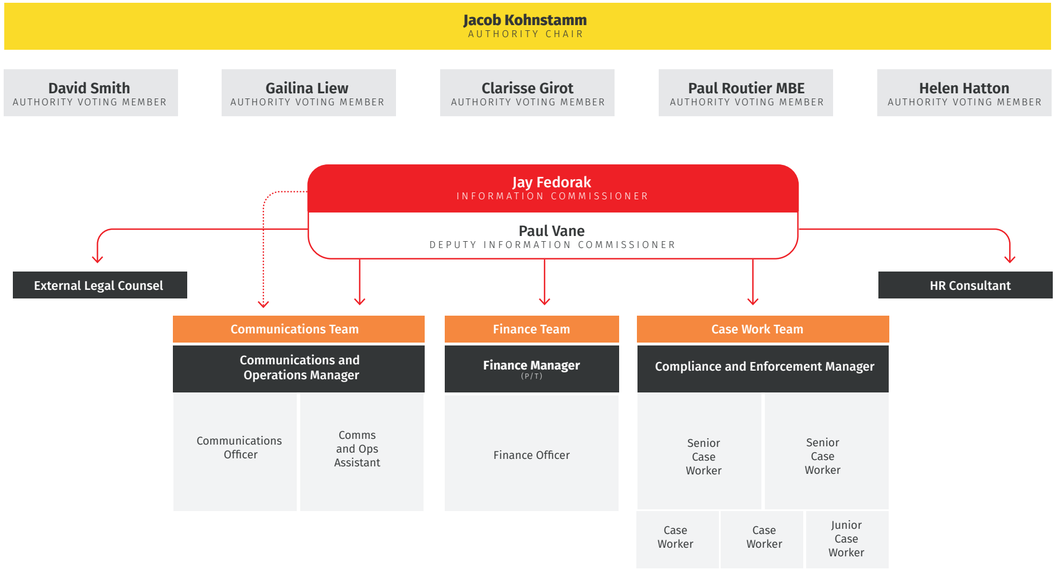
As our performance management system is still relatively new, we will adjust it as necessary to ensure that we are on the right track. We will be monitoring and measuring our case management, how well we educate and communicate and to what extent we have made a positive difference to the community.

Organisation

About the Jersey Office of the Information Commissioner

THE STRUCTURE

The JOIC team began 2020 with 12 permanent employees. The organisation structure is shown below:



THE TEAM

During the global pandemic, maintaining business continuity and employee wellbeing were key challenges, with team members working in different locations. However, new technologies combined with particular attention to regular team communication and engagement helped us to deliver the level of service that the Jersey public expects.

The new registrations process tested the team in January and February 2020, as they responded to receiving up to treble the volume of communications per week and having to facilitate 5,720 renewals and new registrations. This enabled us to exceed the 2020 Business Plan target of 4,600 registrations and £1,300,000.

We created a new performance development and review process (PDR) to connect individual performance to organisational performance, while ensuring staff received the support and training they needed to meet their objectives. The PDR process also promotes individual development and succession planning to promote the development of employee skills and knowledge, using both formal and informal strategies, from certification courses to 'lunch and learns'.

Our team is relatively new with low turnover. In 2020, we added a new Communications and Operations Assistant and a Junior Caseworker.

As the current Information Commissioner will retire in July 2021, the Authority wished to complete a competition for his replacement by the end of December 2020. A comprehensive recruitment and selection process began in October, overseen by the Jersey Appointments Commission. The role attracted approximately 20 candidates from Jersey, the UK, Europe and North America. As Chair Kohnstamm announced in his annual message, the successful candidate was Jersey's own Paul Vane. We are pleased with the stability that this will provide to our existing team and look forward to Paul leading us into our next phase of development.

2020

5,780
REGISTRATIONS

£1.8M
GENERATED INCOME

Summary of 2020 Data Protection Activities

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.

"Compliance with the Law should not be just a tick-box exercise, but rather part of our everyday thinking".

Paul Vane, Deputy Information Commissioner

Organisations that implement good data protection promote consumer and staff confidence and are more successful in retaining both. Customers who believe that companies are keeping their data secure and collecting, using and disclosing it properly, will have more trust and confidence in those companies.

2020 OPERATIONAL PERFORMANCE

→ INTRODUCTION

During 2020, the Compliance and Enforcement team faced fresh challenges from Covid-19. One example is that we reviewed the Data Protection Impact Assessments for new privately funded contact tracing apps and the Government of Jersey's own app. Our job was to ensure that these necessary new initiatives complied with Data Protection requirements while promoting community safety and individual health.

The newly introduced Data Protection annual registration system was introduced following approval on the 10 December 2019 of the Data Protection (Registration and Charges) (Amendment) (Jersey) Regulations 2019. The risk-based system started on the 1 January 2020. Data Controllers and processors responded generally positively, but the necessary changes to the process generated problems for service users and a high volume of requests for help. The complexities of the structures and operations of financial services organisations meant their employees required assistance to navigate and understand the system.

There were 5,780 data protection registrations created during 2020. See the table (right) for a breakdown.

2020 Annual Registrations by Sector		
	Agriculture & Fishing	79
	Animal Husbandry & Welfare	36
	Charities	275
	Construction, Trades & Services	624
	Education & Childcare	206
	Faith, Worship & Religion	42
	Financial & Professional Services	1721
	Health & Wellbeing	437
	Legal Services	100
	Leisure & Fitness / Hospitality / Tourism / Travel / Entertainment	381
	Manufacturing, Wholesale & Retail	381
	Media, Communication & Advertising	127
	Professional Bodies / Professional Associations / Professional Consultancy	220
	Public Authority / Sector, Appointed Regulators & Statutory Bodies	105
	Real Estate & Property Management	578
	Social Clubs & Associations	224
	Technology & Telecommunications	185
	Utilities & Delivery Services	59
	TOTAL	**5780**

"The teams were stretched dealing with these issues on top of their regular work, but I am proud to say that they held everything together and performed admirably."

Adrian Hayes

Compliance and Enforcement Manager

A priority in 2020 was to strengthen our enforcement action. Whilst we continue to focus on collaboration and engagement with Data Controllers, Data Processors and all stakeholders to encourage compliance, the JOIC made a conscious decision that with the Data Protection (Jersey) Law 2018 having been in place for two years, it was time to raise expectations for compliance and take stronger action in response to breaches.

There were some unanticipated problems with the new registration system, but we have made changes to the software to ensure that registrations will be easier in 2021.

One key 2020 business plan deliverable was the commencement of a proactive programme of data protection audits to measure levels of compliance in the absence of complaints. Schedule 1 part 7 of the Data Protection Authority (Jersey) Law 2018 (DPAJL) allows the JOIC to conduct a data protection audit of any part of the operation of Data Controller or Data Processor. The audit approach follows best practice as detailed by the UK Information Commissioner 'Guide to Audits'.

We had planned a series of on-site audits, but Covid restrictions made this less practical. Therefore, we modified our approach by implementing an online survey.

We take a risk-based approach in selecting organisations to be audited. The primary purpose of our audits is to provide the JOIC with an insight into the extent to which a Data Controller is complying with the Data Protection (Jersey) Law 2018 and to identify and remedy any deficiencies.

With each audit, we communicate the scope clearly to the controller, highlighting the relevant applicable articles of the Law.

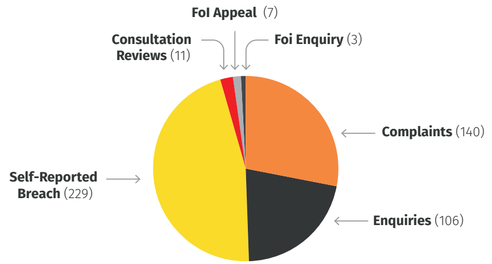
We generally restrict our enforcement activities to the specified scope of the audit. The audit will not usually address individual cases, other than to the extent that it may demonstrate good practice. We do, however, retain the right to comment on any other weaknesses observed in the course of the audit that could compromise good data protection management.

→ 2020 CASE DATA

Schedule 4 of the Data Protection Authority (Jersey) Law 2018 details the process of Enforcement by the Authority in the event of a complaint.

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

- Enquiries. These range from simple questions regarding our location, 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 Breaches. Data Controllers, under the DPJL, are required to report 'certain' breaches to the JOIC within 72 hours of becoming aware of the breach.
- 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 decision responding to their request may appeal to the Information Commissioner.



→ COMPLAINTS

The overall volume of case data has steadily increased on a quarterly basis since the beginning of 2019.

The JOIC handled 384 cases in 2019 and 486 in 2020, of which 140 in 2020 were complaints.

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

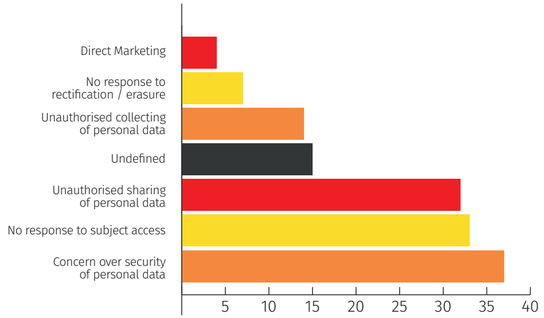
Article 19 of the DPAJL summarises the parameters of the 'Right to make a complaint'

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.

Complaint Types 2020



Each complaint (and self-reported data breach) 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 into a likely contravention of the DPAJL, on its own initiative, which we may learn about from a whistleblower or by observing a behaviour relating to the use of personal information by an organisation.

Upon receipt, each complaint is evaluated to determine whether or not to carry out an investigation. The Authority undertakes this evaluation as soon as is practicable and in any event within eight weeks.

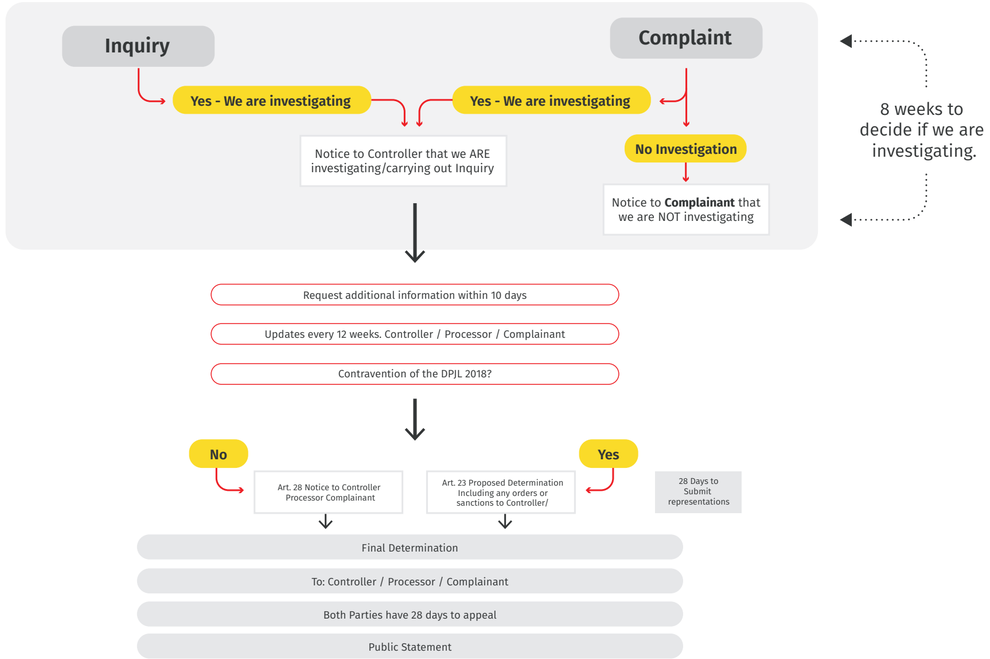
Once the initial evaluation has taken place the complainant is advised in writing whether or not an investigation will take place. The complainant has a 28-day window of appeal at this stage.

Once the investigation is underway the JOIC provide updates at least every twelve weeks. The investigation must conclude whether the DPJL has been contravened (Article 23 DPAJL). At this time the JOIC notify the Data Controller or Data Processor of the 'proposed determination' including any sanctions to be implemented, along with their 28-day right of representation.

If any further information is submitted as part of this appeal the JOIC may take this into account and then issue a final determination to the Data Controller or Data Processor and to the complainant. Both parties have a 28-day period of appeal.

As part of our formal investigation process, we use a formal 'Information Notice' to compel the production of information. This instrument gives the recipient 28-days in which to respond.

→ INVESTIGATION MATRIX



→ 2020 CASE OUTCOMES

The 140 complaints reviewed in 2020 produced a range of outcomes.

Following investigations of each case, 60 complaints were deemed as contravening the Data Protection (Jersey) Law 2018. Of these, 58 contraventions involved unsatisfactory or non-responses to right of access requests plus unauthorised sharing of personal information and unauthorised collection of personal information. The Data Controllers or Processors involved were subject to informal sanctions, from 'Words of Advice' to 'Guidance' as the majority of the complaints were not considered serious enough to warrant formal sanctions.

Words of advice are given in light of a minor infraction. The JOIC decided to only give words of advice in these circumstances as they would be sufficient to improve compliance.

Guidance is given to the Data Controller or Processor as to the steps and approach they should consider taking to avoid repetition of the contravention. The investigatory process highlights the main areas of concern and where appropriate the JOIC direct the Data Controller to particular guidance which will help them to mitigate future occurrences.

For example, a local company experienced a technical issue which led to their payslips being printed off on a domestic printer belonging to an individual who had nothing to do with the company themselves. The JOIC issued words of advice regarding their printer and Wi-Fi security. During our investigation it quickly became apparent that the company was not registered. Therefore, we provided guidance as to their obligations and how to register.

Another example involved an employee who complained about their line-manager sharing information about their performance and health with a third party outside of the organisation. This was investigated by the employer who found the line-manager to be in breach of their internal policies and started disciplinary action against the line-manager.

https://jerseyoic.org/news-articles/public-statements
https://jerseyoic.org/news-articles/public-statements/public-statement-january-2020/

Our investigation examined the company's data protection policies and procedures, with particular reference to the data protection training regime. We were satisfied with evidence we found in these areas. The investigation concluded that the controller did not breach the DPJL but the line-manager employee did and this was dealt with appropriately by the employer. The complainant advised they may take civil action against the line-manager.

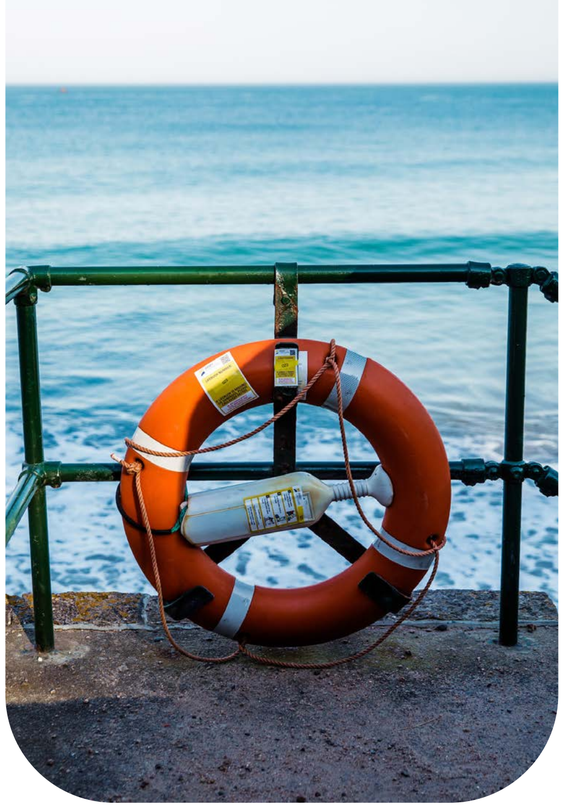
However, two of the contraventions in 2020 resulted in the JDPA issuing public statements, both following lengthy investigations into data breaches that were serious enough to publicise.

One of these two cases was brought to our attention by a whistleblower, and following a thorough investigation, the Authority has determined that the company has contravened Art.8(1)(f) of the DPJL in that it:

- failed to implement appropriate technological and organisational measures to ensure the security of the data it processes and to prevent unauthorised access to that information, including: failure to have adequate firewalls in place, a failure to properly train staff in data protection, and a failure to exercise due diligence in the selection and monitoring of its IT provider.
- failed to respond appropriately once it was aware of a personal data breach; and
- failed to notify the Authority and relevant data subjects of a personal data breach.

The second case which resulted in a public statement arose following a complaint, and following the investigation the Authority determined that the controller had also contravened Art.8(1)(f) of the DPJL. Two separate breaches were identified.

- The first breach of significant gravity related to insufficient redaction being applied to information that had been uploaded to the controller's online registry of planning applications (the "Registry"). The redactions were insufficient to prevent piecing together of information so as to allow identification of a vulnerable minor and allude to the fact that the published information related to certain highly sensitive health information.



The second breach was of even greater magnitude, as it related to the disclosure of extremely sensitive special category data (health information) about a vulnerable minor. This information was published in error and the Department has accepted that the relevant document should not have been publicly disclosed nor been uploaded to the Registry.

In this case, it should be noted that special category data (including health data) are afforded higher levels of protection in the DPJL, reflecting the harm and distress that can result from a breach. The Authority makes it clear that, where organisations do not take their legal responsibilities to protect such data seriously or where they are negligent as to their responsibilities, these considerations will determine the appropriate sanction (including the issuing of a fine, where available). Had the Authority not been prevented by law from imposing a fine due to the Controller being a Public Authority, the Authority would have considered a fine in this case.

In both cases, the Controllers acknowledge our conclusions and accepted our recommendations. As a result, they made marked improvements in processing activities and practices. They also commented publicly about their experience of a breach and commended our professional approach to the investigations.

'A public statement holds Controllers accountable for their actions, or lack of action, and provides guidance on how to improve data protection practices. Finally, it also holds the JDPA accountable by giving the public the opportunity to view its regulation practices in action. Good data protection regulation must not only be done, but also be seen to be done. Public statements, like this annual report, give members of the public information they need to evaluate the effectiveness of the JDPA.'

Jacob Kohnstamm, Chair JDPA.

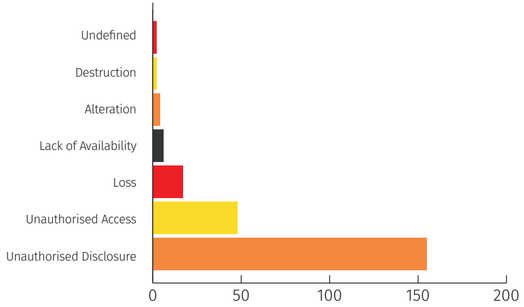
→ BREACH REPORTING

Investigating self-reported data breaches represented 47% of our compliance and enforcement case load in 2020.

Breaches can be traumatic for employees 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 exercise of a formal sanction power. However, the Authority may impose a 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.

We received notice of 229 data breaches in 2020. With the event of Covid-19, lockdown and working from home, we anticipated higher numbers of reported breaches. The JOIC created a web page for Covid-19. To help organisations to avoid the risk of neglecting data protection during the pandemic, we provided timely and effective communication to support the business community to remain compliant.



Of the breaches reported in 2020, 162 resulted in determinations that there had been a breach of the data protection law.

It is important to note that most of the breaches reported did not meet the legal threshold for mandatory reporting, because they did not result 'in a high risk to the rights and freedoms of natural persons'. Nevertheless, we encouraged organisations to report breaches to enable us to understand the breach landscape in Jersey to help shape our guidance and advice.

→ ENFORCEMENT

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

Two of the JOIC's core outcomes are: (1) to provide individuals with a high level of data protection, and (2) to raise the profile of data protection in Jersey in support of the Island's reputation as a well regulated jurisdiction and a safe place to do business.

Achieving these objectives requires a Regulatory Action and Enforcement approach that aims to increase levels of compliance across all industry sectors and recognises five key principles:

1. *Proportionate - Any action taken, or intervention required by the JOIC, including monitoring, compliance or investigation, is proportionate to specific, identified risk.*
2. *Targeted - Those involved in high risk data processing activities, those carrying out activity in high risk areas such as the medical profession, those involved in novel or complex activities, and/or those with a previous history of non - compliance can expect a greater level of monitoring.*
3. *Accountable - The JOIC is accountable to Ministers, for the effectiveness of its regulatory action. The JOIC is also accountable to the Courts for its regulatory action in specific cases. As a broader principle, the JOIC is accountable to the JDPA and the public at large;*
4. *Consistent – The JOIC's actions are consistent, in that it should be mindful to make coherent (but not necessarily the same) decisions about action with a similar factual matrix, in accordance with its delegated responsibilities, statutory objective and guidance;*
5. *Transparent – The JOIC's approach to regulatory action is transparent by publishing information to its regulated stakeholders, indicating for example, what enforcement action it can and may take in appropriate circumstances (for example by publication of this document).*

This policy not only guides the work of our staff, but also informs regulated organisations and the general public about what they can expect from us. Our regulatory approach strives to render Jersey a safe place to store data and do business. It seeks ways 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.

Aims of the Policy are to;

- Outline the JOIC's powers and indicate how and when they will be deployed;
- Ensure the JOIC takes fair, proportionate and timely regulatory action to best protect individuals' rights;
- Guide the staff of the JOIC to ensure that regulatory action is targeted, proportionate, consistent and effective;
- Assist in the delivery of the JOIC's strategic outcomes.
- Ensure the JOIC acts in accordance with its statutory obligations under the Data Protection (Jersey) Law 2018 and the Data Protection Authority (Jersey) Law 2018.

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

The 2018 Law provides for substantive fines and sanctions for contraventions of the Data Protection (Jersey) Law, but it is our intention to use these as a position of last resort. Our vision 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.

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 measures.
- 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.

Annual Report of Freedom of Information

THE FREEDOM OF INFORMATION (JERSEY) LAW 2011

The Freedom of Information (Jersey) Law 2011 provides the public with access to information held by Scheduled Public Authorities (SPA). It creates a legal right for individuals to request information from a SPA. The Law covers all recorded information in the custody of a SPA in Jersey. Recorded information includes 'printed documents, computer files, letters, emails, photographs, and sound or video recordings. It includes 'information recorded in any form'.

The benefits of effective Freedom of Information are that it improves accountability of scheduled public authorities and promotes good governance and transparency.

The Law does not give individuals a right of access to their own personal data because this right is available under the Data Protection (Jersey) Law 2018.

Our role in regulating the Freedom of Information 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; and
- To hear 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.

The Information Commissioner must decide on the appeal as soon as is practicable but may decide not to do so if the Commissioner is 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 Information Commissioner must serve a notice of his or her decision in respect of the appeal on the applicant and on the scheduled public authority. The notice must specify:

- 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.

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

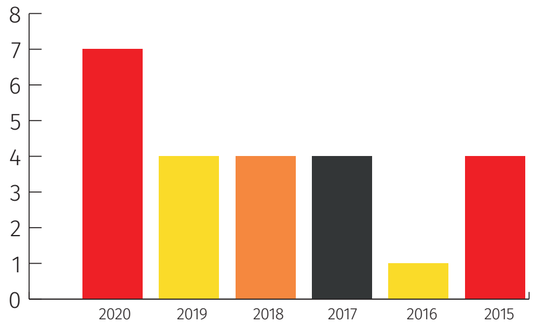
→ 2020 OPERATIONAL PERFORMANCE & APPEALS

The Central Freedom of Information Unit of the Government of Jersey reported that it received 880 valid FoI requests during 2020.

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

Source; Freedom of Information Central Unit, Government of Jersey

The table below highlights the number of appeals received by the JOIC.



The total number of valid FoI requests decreased from 933 in 2019 to 880 in 2020 but the number of appeals increased from four to seven.

→ SIGNIFICANT 2020 DECISION NOTICES

We issued four formal Decision Notices in 2020 following the appeals submitted to us. Article 46 of the Freedom of Information (Jersey) Law 2011 defines that;

(5) The Information Commissioner must serve a notice of his or her decision in respect of the appeal on the applicant and on the scheduled public authority.

And that

(6) The notice must specify –

(a) the Commissioner's decision and, without revealing the information requested, the reasons for the decision; and

(b) the right of appeal to the Royal Court conferred by Article 47.

The decision notices issued relate to the following information regarding:

1. Information from Health and Community Services relating to insurance cover for compensation paid by the Government in respect of certain personal injury claims.
2. Information from Andium Homes relating to a certain development carried out by the SPA and monies paid to a third party contractor.
3. Information from Health and Community Services regarding the Jersey Care model.
4. Information from Health and Community Services regarding Orchard House.

The three ongoing appeals were submitted in the final quarter of 2020, and are still under review.

In each case, the Commissioner conducts a formal hearing adhering to the principles of administrative fairness and the laws of natural justice. The Commissioner provides the public authority and the applicant with an opportunity to make formal submissions in support of their position. It is essential that both parties make full and complete arguments and provide adequate evidence. The Commissioner presumes that when making its submissions, each party is providing all relevant material that is available at the time of the assessment.

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.

Communications

"Communication is giving, receiving or exchanging ideas, information, signals or messages through appropriate media, enabling individuals or groups to persuade, to seek information, to give information or to express emotions."

https://www.communicationtheory.org/definitions-of-communication/

The challenges of 2020 required enhanced Communications to Jersey on pressing issues such as working from home, contact tracing, employees returning to the workplace, in addition to our planned Communications activities.

The year commenced with a drive to raise awareness of the requirements of the new registration system and to inform Data Controllers and Processors who were unaware of their obligations.

→ ANNUAL REGISTRATIONS

The 2020 Business Plan set a target of 4,600 registrations for the year. We disseminated key registration messages via a variety of mediums:

- Radio adverts on Channel 103.
- Advertising on the back of local buses.
- Newspapers, media and social media.
- Representative bodies of key stakeholders – Chamber of Commerce, Jersey Business, the Hospitality Association, Jersey Finance, Motor Trades Federation, Primary Healthcare Body, Law Society, Association of Jersey Charities, Jersey Estate Agents Association and Charities Commissioner.

These campaigns contributed to our overall success in promoting registrations.

→ DATA PROTECTION TOOLKITS

The Toolkits are a quick and easy way to learn about data protection requirements through a blend of infographics, step-by-step guidance, templates, checklists and videos.

We have created six toolkits:

→ PANDEMIC MESSAGING

With everyone becoming preoccupied by the pandemic and the collective response, we needed to ensure that businesses, public authorities and the public did not overlook data protection requirements. This is particularly important as traditional business and the volunteer taskforce landscape rapidly changed beyond recognition. We developed simple, effective and practical guidance covering a range of topics:

- Working from Home: Practical tips for keeping client, staff, volunteer and all personal information safe.
- Guidance for ALL existing and new volunteers.
- 5 Messages about Transparency, Data Protection and Statistics.
- Tips on Data Protection and Video Conferencing.
- Contact tracing checklist.

We hosted all of the material in a dedicated area on the website and ensured that all of our communication channels provided regular updates and links to guidance and documents.

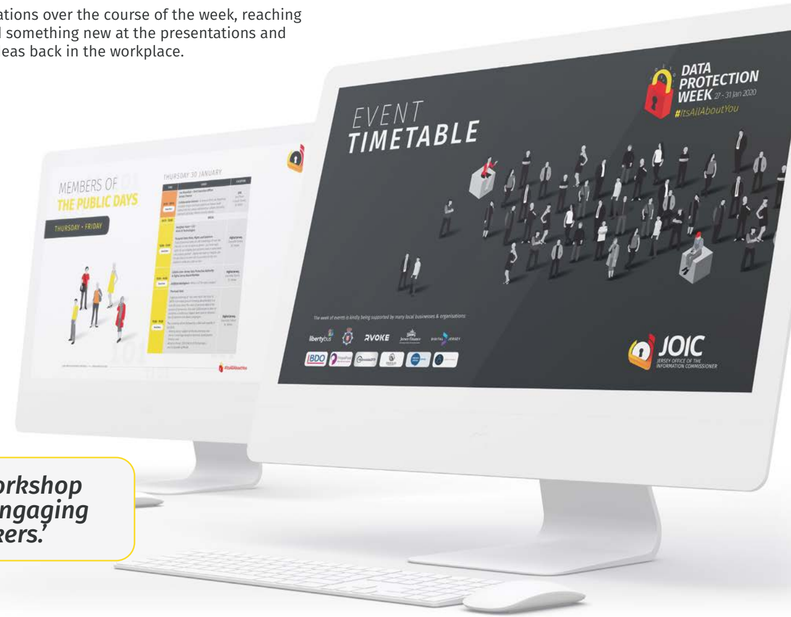
→ DATA PROTECTION WEEK 2020

The JOIC and invited contributors delivered 21 presentations over the course of the week, reaching 270 islanders. Over 70% of those who attended learned something new at the presentations and 38% said that they will be using the information and ideas back in the workplace.

The talks ranged in subject from Surveillance and Privacy, Demystifying Subject Access Requests; Why it needn't be a 'DSARster', CCTV and surveillance in the workplace, 10 essential data protection questions every Board should ask, Artificial Intelligence – What is it? Do ethics matter? Data Transfers, the Breach of 2019 – Coping with the immediate impact, how it felt, what we did and lessons learned and more.

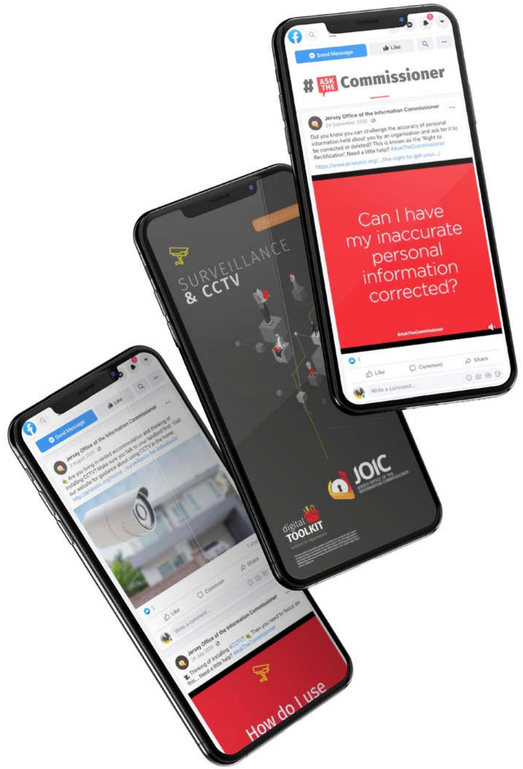
With support from Digital Jersey we arranged for a public viewing of the feature film 'The Great Hack' and were delighted to have a pre-recorded special closure of the event with questions and answers from one of the individuals involved in events detailed in the film.

We would like to extend our thanks to everyone who contributed and attended.



'Great workshop & great engaging speakers.'

Definitely useful information to further consider.'



→ #ASKTHECOMMISSIONER CAMPAIGNS 2020

We developed a campaign brand called #AskTheCommissioner. The short question and answer videos are ideal for all social media platforms and provide simple, concise messaging in an appealing and engaging way.

In 2020 we ran three #AskTheCommissioner campaigns alongside the pandemic messaging;

→ CCTV.
→ Data Protection obligations.
→ Individual Rights.

→ CCTV

We put CCTV in the spotlight in June and July of 2020. CCTV and other types of surveillance are hot topics in the field of data protection. The explosion of affordable surveillance devices both in the domestic market and the commercial workplace has given rise to increased cases within our Casework team.

The JOIC developed guidance for both sectors.

The CCTV campaign objective was to help raise awareness of the obligations under the DPJL for everyone who deploys CCTV. Islanders need to understand when the DPJL applies to domestic use of CCTV as well as being aware of individual rights.

Our key message for the campaign was to highlight that CCTV should only be used as a last resort.

The topic of CCTV captured the interest of our social media followers, with 2.5k views on Facebook posts. The media also responded positively by helping us to raise awareness.

We are working collaboratively with the States of Jersey Police and the Honorary Police regarding the correct use of CCTV in the home.

→ DATA PROTECTION OBLIGATIONS

The short videos, approximately 30 seconds in duration, asked the following questions and provided simple answers;

1. Does my organisation need to comply with the data protection law?
2. What basic steps do I need to take to comply with data protection in Jersey?
3. What else should I do once I have registered my business with JOIC?

The short videos were particularly helpful for Jersey Business and Jersey Chamber of Commerce to share and help raise awareness. We were pleased to see increased engagement on our social media platforms for the campaign.

→ INDIVIDUAL RIGHTS

This short campaign asks four questions about the right of access, erasure, transfers and correction.

The #AskTheCommissioner campaigns saw the engagement on social media double for these posts.

→ BLOGS

We published our first blog in early April 2020. Throughout 2020, we presented readers with a variety of blogs covering topics ranging from the pandemic, to CCTV, algorithms, data protection on your board radar, and the EU-US privacy shield agreement. We also invited a range of guest bloggers to write about the impact and relevance of data protection in their industries. These insightful blogs generated huge interactions on social media. The success of the JOIC blogs are set to continue throughout 2021.

a https://jerseyoic.org/blogs/

EDUCATION 2020

Our Young Privacy Ambassador Programme that teaches students about privacy issues and exercising their personal data rights continued in 2020 and will continue throughout 2021/22. The programme contributes to the Jersey school citizenship curriculum. Students learn about the implications of their decisions regarding managing their own personal data, as well as what are their rights and responsibilities. Our sessions also help to develop employment skills and knowledge about the current economic and business environment.

We began the year with a target of speaking to over 1,000 children within key stages 3 and 4 and for them to attain a 'competent' level when tested for awareness of data protection and privacy rights affecting their everyday lives.

We tailor our sessions to the appropriate age group and make them as engaging as possible, with games, quizzes and lively debate. We explore the following topics:

- Privacy and why it matters.
- Personal information rights.
- Where and how data protection fits into their worlds.

We had the pleasure of talking about privacy, individual rights, the JOIC's role and data protection to 590 young people at Le Rocquier school.

At the end of the lessons, we always verified the students' understanding of the issues discussed and we were pleased with an 80% understanding of the topics.

→ PRIVACY COURTROOM CHALLENGE

We worked in partnership with Advocate Davida Blackmore and collaborated with Hautlieu School to create a case based on a breach of personal information to give the students the opportunity to delve into certain aspects of the DPJL, whilst developing life skills and personal values.

The students involved were studying Law, Finance and technology-related industries such as Artificial Intelligence (AI), Media and Journalism. Stuart McSherry, Teacher in charge of Geography and the Core Programme at Hautlieu School, said:

'The session gave the students the opportunity to network with industry, work with a lawyer and data protection professionals from the JOIC team, equipping them with the decision-making tools to make a judgement when it comes to privacy and personal information, whilst bringing privacy and the law to life.

Working with transferrable skills and peers in developing high-level communication skills under pressure is useful for many varying careers. The session gave the students invaluable extra-curricular experience for their UCAS applications, CVs, references, interviews and bringing law to life.'

The JOIC team and Advocate Blackmore worked with the students to set a cast list and provide witness statements in preparation for the mock trial. Students benefitted from a short courtroom etiquette lesson.

'Privacy' Courtroom Challenge Objectives

- To equip young people with the decision making tools to make a judgement when it comes to privacy and personal information.
- Bringing privacy and the law to life.
- To increase the respect amongst young people for their personal information.
- To help young people to understand privacy in an ethical context.
- To create a team of young privacy ambassadors ready to be curious, questioning, empowered & confident.

Student Benefits

- Providing meaningful insights into data protection for students who want to study and work in law, finance, health, and technology-related industries such as artificial intelligence (AI), media and journalism.
- Obtaining extra-curricular experience for UCAS, CVs, references and interviews.
- Learning to interpret a law and see how it interacts with 'real life'.
- Networking with industry, meeting lawyers, data protection officers and other key professionals who may be able to assist with career path guidance.
- Working with transferable skills and peers in developing high-level communication skills under pressure, useful for many careers.
- Developing website & media content which may be used by the JOIC as part of its work with schools across Jersey.
- Working in a multidisciplinary team. Participating in mock interview and possible work shadowing opportunities.

Jersey College for Girls – 180 sixth form students reached

We joined with Jersey Financial Services Commission (JFSC) to present to the College. We collaborate as regulators so as to introduce the regulatory landscape. The JFSC highlight financial fraud and risks. Our key message being 'think twice before you share your personal information'. We encourage students to exercise their personal information rights, responsibilities and question privacy issues.

Our objective for this session was to ensure the students were equipped with the tools to protect their personal information and reputation as they prepare for the world of work and adult life.

Total Number of Students Reached: **790 with 80% success rate of understanding our key messages**

Unfortunately, the remainder of the schedule fell away due to lockdown and Covid-19 restrictions.

Education continues to feature highly in the 2021 Business Plan. We are offering virtual sessions for Les Quennevais, Le Rocquier, Hautlieu and hopefully other Jersey secondary schools.

→ THE JOIC TALKS FOR INDUSTRY

Following Data Protection Week in late January we focused our Education Programme to arrange talks for Easter and beyond.

As circumstances evolved we had to adjust and deliver talks virtually. We rekindled the talks starting in September which included;

- → The Right of Access - Recognising and Responding to a SAR.
- → The JOIC's Regulatory Action and Enforcement Policy.
- → International Transfers/Data Protection Impact Assessments.

We spoke to over 100 attendees over these talks. We received positive feedback on our first few virtual talks. We recognise that we are improving on the delivery and measuring if 'anyone was better off'.

Jersey Fraud Prevention Forum (JFPF)

We actively participate in the JFPF alongside the States of Jersey Police and Jersey Financial Services Commission.

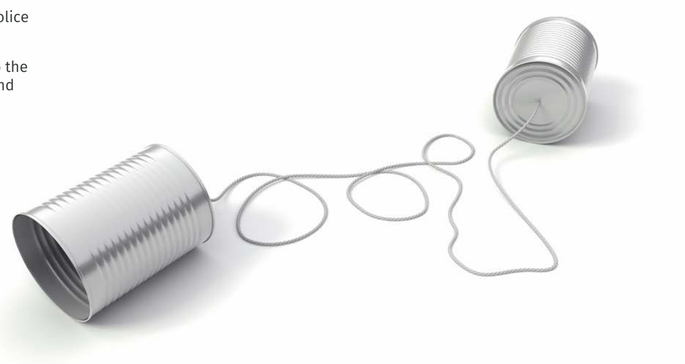
The JFPF seeks to develop a coordinated and strategic approach to the protection of the Island's general public from investment frauds and scams between the agencies concerned.

→ COMMUNICATIONS SUMMARY

The Communications and Operations team is continuing 'to promote public awareness of risks, rules, safeguards and rights in relation to processing, especially in relation to children' (Article 11 DPAJL). We will be running bespoke campaigns throughout 2021 focusing on 'people' – raising awareness of the value of their personal information and their rights.

The Chair of the Data Protection Authority says 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 more impressive results happen when we all work well together.'

That said we fully recognise that impressive results go beyond case investigations and outcomes. The JOIC strive to maintain an open dialogue with industry, work collaboratively and improve understanding of the practical implications of the Law.



https://www.fraudprevention.je/about-us/

PUBLIC ENGAGEMENTS AND AWARENESS

Our Commissioners, Communications and Operations Manager and Compliance and Enforcement Manager spoke on invitation at a limited number of industry events in 2020 owing to the pandemic.

We spoke to a variety of local companies (virtually) to deliver data protection awareness sessions, including:

- → Jersey Landlords' Association.
- → Chamber of Commerce Contact Tracing Webinar.
- → Local commercial organisations invited us to provide data protection Q&A sessions for their teams.

NATIONAL/INTERNATIONAL LIAISON 2020

The Commissioner and Deputy Commissioner attended key international conferences in person but mostly virtually throughout 2020 promoting collaboration and consistency of enforcement while raising awareness of data protection in Jersey.

The Commissioner attended in person a subgroup of the Association Francophone des Autorités de Protection des Données Personnelles, in Berne, Switzerland in February 2020.

The Compliance and Enforcement Manager virtually attended the Global Privacy Assembly in October 2020, the e-Conference covered a variety of topics; COVID-19, Artificial Intelligence, Charter of Fundamental Rights, Rights of the Individual, International Cooperation, and Biometrics.

The Deputy Commissioner attended a range of virtual conferences throughout the year including:

- → OECD (Organisation for Economic Co-operation and Development) Workshop - Addressing the Data Governance and Privacy Challenges in the Fight against COVID-19 (April 2020).
- → Covid Task Force Webinars throughout the year.
- → GPA Webinar: Enablers and Protectors: the Role of DPAs confronting COVID-19 - Contact tracing and the recovery (July 2020).
- → OECD/GPA COVID-19 Workshop: The Road to Recovery (September 2020).
- → Annual PDP (Professional Data Protection Practitioners) Compliance Conference in the autumn, which examined the developments in data protection; the continued practical implications for organisations of complying with the GDPR, as well as what could be next for organisations in a post-COVID/Brexit era.
- → OECD - Being iHUMAN: How can we lead better digital lives? (November 2020) .
- → Westminster eForum on the future of the UK's data protection frameworks (November 2020).
- → World Trade Organisation - Different models to facilitate the cross-border exchange of personal data (November 2020)Ogier: Three part webinar series: Equality in the Workplace - Discriminatory bias in algorithms and AI (November 2020).

The Management Team also participated in Diversity and Inclusion talks coupled with well-being events, including a 'Man Down' Men's mental health awareness conference.

The JOIC actively participates in the Global Privacy Enforcement Network (GPEN). GPEN is a network of 52 Privacy Enforcement Authorities. The network is tasked to:

- → Discuss the practical aspects of privacy law enforcement co-operation;
- → Share best practices in addressing cross-border challenges;
- → Work to develop shared enforcement priorities; and
- → Support joint enforcement initiatives and awareness campaigns.

Financial Report

"The financial management of the Jersey Office of the Information Commissioner always keeps the ethos of data protection in mind, by operating fairly and transparently"

Claire Le Brun
Finance Manager

Our main focus this year has been on developing the financial infrastructure necessary to operate independently from Government, including implementing our new registration and revenue model. This included educating businesses about the requirements of the new model and and facilitating registrations.

→ SUMMARY

The draft year-end position for the JOIC shows an operating surplus of £75,417* against the budget of £1,712,345.

This budget surplus was the result of the following variances:

Surplus registration fee income	**£136,345***
Underspending on staff costs	**£111,942**
Underspending on non-staff costs	**£67,130***
Reduction in grant from Government	**(£240,000)**
BUDGET SURPLUS FOR 2020	**£75,417**

** Year-end adjustments are ongoing and these figures may change as we prepare the 2020 financial statements.*

→ GRANT

The total grant payment received from Government in 2020 was £260,000. This was £240,000 less than stipulated in our Partnership Agreement with Government (£500,000). The Government reduced this grant in response to financial circumstances that arose as a result of the Covid-19 pandemic.

→ REGISTRATION FEE INCOME

The total income in the draft year-end position has been recorded as £1,778,414 (budget of £1.6m) which is made up of the following categories of fees, as required under amendments to the Regulation to the Data Protection Law:

Full-time equivalent employees fee	**£407,783**
Past-year revenues fee	**£73,050**
Proceeds of Crime fee	**£103,150**
Administration services fee	**£1,217,324**
Special Category data fee	**£52,650**

We returned £75,543 to entities at the time of registering, in the form of a credit for portions of fees that they paid in 2019. This was owing to the new requirement to register and pay by the end of February, rather than on the anniversary of their previous registration. The entities were invited to register again for 2020 and the portion of their 2019 registration that was carried into 2020 was returned to them in the form of a credit against their new registration.

There were further credits applied after the initial registration period and the totals above are net of these amounts.

→ EXPENDITURE

Staffing remains the largest resource and item of expenditure.

The total underspend on staffing at the end of December 2020 was £111,942. Throughout the year we had seen the underspending develop due to vacancies resulting where recruitment was delayed due to Covid 19. Two of these vacancies were for entry level roles, one in Casework and one in Communications. These roles were originally advertised in February 2020 but were not recruited in to until late November 2020.

→ YEAR AHEAD

A great deal of work is going into improving the finance systems during 2021 to incorporate all of the financial transactions, from producing our invoices, to paying our suppliers and financial reporting. Having all our financial information contained within one system will provide greater control and oversight, which in turn will allow resources to be directed as necessary to better support the delivery of the business plans set objectives.

The JOIC introduced a new pay scale on 1st January 2021, following an external pay review in 2020. The introduction of the pay scale ensures our salaries are set at a level consistent with similar roles in Government and industry. The pay scale will also allow for more accurate staff forecasting and development of staff performance and review process.

The JOIC has taken control over accounts payable and no longer relies on the shared services of the Government payment department for procurement and payment of suppliers. We now make all supplier payments using our own finance systems, which has allowed us greater flexibility when paying our suppliers. The JOIC has maintained strict internal controls, standards and processes when making payments externally, but we are able to take advantage of early payment discounts offered or negotiate better terms with our suppliers now we are able to utilise other payment methods such as standing orders.

We are committed to providing a high level of service, whilst attaining the best value for money as we further develop our financial policies and processes through 2021.

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