Jersey Finance

Delivering Insight ▪ Driving Innovation

Data Protection: Jersey Finance Talks to Jersey's Information Commissioner

2 March 2020

Introduction

The Data Protection (Jersey) Law 2018 and the Data Protection Authority (Jersey) Law 2018 came into force on 25 May 2018. Both were intended to bring in an updated data protection framework for Jersey in line with the EU's General Data Protection Regulation (GDPR), helping to preserve our strong track record in this area and cementing the Island's GDPR equivalence.

In 2019, the Jersey Office of the Information Commissioner (JOIC) and the Government of Jersey launched a consultation process with the intention of replacing the old data controller notification and fee regime, which had been grandfathered over from the previous data protection law, with a new registration model and risk-based system of tiered annual charges.

In December 2019, the States Assembly approved the Data Protection (Registration and Charges) (Amendment) (Jersey) Regulations 2019 (amending the previous regulations), and the new model of registration and charges for data controllers and processors went live on 1 January 2020. Jersey Finance has been collaborating with JOIC on the rollout of this new model and the development of its Guidance Note on the treatment of administered entities.

As the initial deadline for registration of existing data controllers and processors passes, Jersey Finance put some questions to Jay Fedorak, Jersey's Information Commissioner, to find out more about his team's plans for 2020.

Q&A with Jay Fedorak

JOIC has had a very busy start to the year. With the initial window for registration and payment under the Data Protection (Registration and Charges) (Jersey) Regulations 2018 (as amended) having closed on 29 February 2020, can you tell us a bit more about JOIC's priorities for 2020?

Jay Fedorak: Our Board has approved a strategic plan for the next three years and a business plan for 2020. The new fee model is part of our move to greater independence from the Jersey Government, which includes developing our own financial management infrastructure and we will be taking control over our own financial accounts. One of our main priorities is to issue sector specific guidance on complying with the data protection laws including for the Jersey financial services industry. It will provide practical advice, in plain language crafted to the

circumstances and challenges that the industry is facing in order to help members comply with the data protection laws. We will be launching three implementation tools kits specifically tailored for small, medium and large businesses.

Our caseload of complaint files continues to increase, and we must ensure that we can continue to resolve these complaints in a reasonable period. We are developing a new enforcement strategy that we plan to implement later this year. We have room in our budget for a few additional employees, and we will begin recruiting when we have completed a workload needs assessment.

You mention that you are working on a new enforcement strategy. Can you tell us what JOIC's priorities are likely to be in terms of enforcement in the coming year? Where do you see the key risks?

Jay Fedorak: Our enforcement strategy is a comprehensive overview of our enforcement objectives and the approach we will take in achieving them. This includes policies on issuing sanctions, including administrative fines, and cooperation with other international data protection regulators.

Enforcement is just one part of our compliance programme. We start with educating organisations and the public about their rights and responsibilities.

We also assist organisations in dealing with data protection issues. We investigate all complaints with a risk-based approach. That is to say we will likely take more serious action when the personal data at issue is special category data; a breach affects a large group of individuals; or the data subjects are vulnerable.

The keys risks relate to information technology. We are anticipating complaints involving artificial intelligence and will be looking into the growing use of surveillance technologies.

One of the key concerns for Jersey's finance industry is that the compliance requirements for administered entities with limited personal data should be proportionate. What can you tell us about your expectations in that respect?

Jay Fedorak: We are adopting the standard international approach to data protection compliance, which is that the measures organisations adopt while processing personal data should be proportionate to the size and nature of the organization and the processing, the risks to data subjects and the costs involved.

For example, we expect that hospitals and police services would provide a comprehensive level of security to the personal health records and criminal records

because they process large volumes of sensitive special category data. This would involve secure facilities for paper records with restricted access on a need to know basis, such as locked file rooms. The same would apply to access controls on electronic information systems, which should have individual user IDs and passwords and industry standard firewalls and virus protection. Encryption is essential when transmitting this data. The same would not necessarily apply to a small company with a minimal amount of information about directors or shareholders. In that case, we would expect more modest security controls.

The requirements in the law relating to the formal appointment of data protection officers and completions of data protection impact assessment apply only in cases involving large numbers of individuals or where the risks to those individuals is high.

With respect to requirements to document processing activities and draft data protection policies and the level of detail entailed, expectations will differ depending on the size of the organization and the level of risk.

Small companies with low-risk data would likely only need to provide brief, simple and basic documentation.

Larger entities with high-risk data should provide more detailed and extensive documentation.

In recent discussions with industry, you talked about JOIC's "graduated" approach to enforcement action, which focusses on remediation first and foremost. Can you tell us a bit more about this approach?

Jay Fedorak: Our overarching goal is to promote the greatest level of compliance across the community. Our powers are generally remedial rather than punitive. Our approach is forward-focussed rather than backward-looking. We reserve the application of administrative fines and more stringent sanctions as an avenue of last resort, where a less punitive approach is, or has been, unable to achieve compliance and it is in the public interest.

When we receive a complaint, we attempt to resolve the matter through negotiation or mediation. For example, if a complaint about a minor issue of compliance appears to be substantiated in part, and the organization agrees to change its processing practices to the satisfaction of the complainant and our office, we may close the file with the agreement of the parties.

If the complaint is more serious, the organization denies the contravention and we make a formal finding that the complaint is substantiated, we may need to compel a change of practice or issue a sanction. In a case of unconscionable neglect or

inattention resulting in significant harm to data subjects, where the organization refuses to cooperate with the investigation, we may issue an administrative fine. For those wishing to avoid serious enforcement action, our recommendation to all organisations is to comply with the laws in good faith, to the best of their understanding and to document the steps they have taken towards compliance and evidence their thought processes.

In the event of an investigation, cooperate in good faith and implement measures to remediate the breach, if applicable, as soon as possible. If they are unsure whether their current practice is in compliance, they may consult us. If they have suffered a breach, it is better to report it to us as soon as possible, rather than have us hear about it from another source.

Are any changes planned in respect of the registration model, particularly in relation to administered entities?

Jay Fedorak: Any changes to the Data Protection (Registration and Charges) (Jersey) Regulations 2018 (as amended) would be within the jurisdiction of the States Assembly. We will remain in communication with the Government of Jersey about the experience of implementing the model and may offer recommendations for change, if any appear warranted.

We also are working with the JFSC to explore whether we could combine the registration process for companies that are subject to both of our registration requirements. Ideally, we would like to see a process where these companies could make one registration and one payment, where the data and funds would be apportioned to each registry as appropriate.

One of our overriding priorities is to make complying with the registration requirements as easy and convenient as possible to ensure that more companies are able to fulfil more easily their compliance obligations.

Jersey is one of the few third countries to enjoy GDPR adequacy. How do we ensure that we maintain this going forwards?

Jay Fedorak: For the European Commission to continue to treat Jersey as adequate for the purpose of cross-border data transfer, we must accomplish three goals.

The first is to have a law that provides an adequate level of data protection.

The second is to ensure that my office, as the supervisory authority, is independent and effective.

The third is that there is a general level of compliance throughout the public and private sectors in Jersey. I think we have a good law that mirrors GDPR in every meaningful sense for a country outside of the EU. It is important that we do not undermine the effectiveness of that law by giving the police and security services additional privacy-intrusive powers through legislation on the UK model. The European Commission has already expressed concerns that UK national security legislation is overly intrusive. My office is moving towards greater levels of independence and strives to be effective in promoting compliance through education, collaboration and enforcement.

Members of the Jersey business community can do their part by implementing appropriate and effective data protection programmes and ensuring that their employees take data protection seriously. I am cautiously confident that Jersey is currently doing what is necessary, but we must ensure that we do not become complacent.

And finally, where can our members find more information and guidance from JOIC about the data protection requirements in Jersey?

Jay Fedorak: Please visit our website at www.jerseyoic.org for a wide range of guidance materials. If you have questions, or require more in-depth advice, please call us on 01534 716530.

Thanks very much for your time Jay, we look forward to further opportunities for collaboration between industry and JOIC in the coming year.