Consultation response released for draft cyber security law for Jersey

Insights - 22/08/2024

The Government of Jersey Department for the Economy has completed its consultation process on the new draft Cyber Security (Jersey) Law 202-.

This follows receipt of feedback from a range of entities that are proposed to be Operators of Essential Services under the draft law, along with other stakeholders and interested parties.

This article is an update to our previous article from 11 March 2024: Latest news on the draft cyber security law for Jersey. Please refer to that article for background on the policy motivation behind the draft law, the proposals in the draft law and our summary of how the draft law is proposed to be engaged in the event of a cyber incident.

In this article, co-chair of Ogier's Regulatory group in Jersey Matthew Shaxson, managing associate Tom Hall and associate Michael Ogilvy Watson explore the draft law in light of the consultation response and its implications for banks, trust company service providers and fund services businesses providing a service of that kind in Jersey. They will be referred to in this article as Banking and Financial Service Providers.

Background on the draft Cyber Security (Jersey) Law 202-

The Department for the Economy specifically requested feedback on the following areas during the consultation process:

- the definitions, scope and threshold requirements of Operators of Essential Services (**OES**) to be included
- the reporting obligations and time frame in which OES are to report incidents to the Jersey Cyber Security Centre (**JCSC**)
- definition of "significant incidents"

- when the requirements on OES should come into force

The consultation response has recently been published and a number of amendments have been proposed to the draft law by the Department for the Economy in light of the consultation response, to be incorporated in the draft law before it is laid before the States Government in the near future.

Spotlight on the banking and financial services industry sub-sectors

The following three changes have been proposed for the draft law in the consultation response:

- the banking subsector threshold will be refined and amended before the draft law is lodged
- the financial services subsector threshold will be removed for lodging to allow for further consultation on the threshold definition and re-introduced via amending regulation in future
- the Jersey Financial Services Commission (**JFSC**), among other Jersey regulators, will be included as an OES

Despite what we understand to be relatively strong opposition from industry in the consultation feedback, Banking and Financial Services Providers remain designated as OES.

There was a feeling that provision could be made to require Banking and Financial Services Providers to enhance their cyber security resilience by bolstering their existing regulatory duties, rather than creating further duties pursuant to the draft law.

However, it seems that they will nonetheless remain designated as OES, but it remains to be seen how the Banking subsector threshold will be refined and when a further consultation process might take place in relation to the appropriate threshold for the Financial Services subsector. For now, it seems that they will be included without a minimum threshold.

Possible expansion of OES to include the professional services sector, notably accountants and law firms

Under the draft law, professional services firms (other than those falling within the definition of Banking and Financial Service Providers) were not included as OES.

It was felt by a number of respondents to the consultation response that the professional services sector, notably accountants and law firms, ought to be included as OES. This is presumably on the basis that the professional services sector makes a significant economic contribution, may (in the event of a cyber incident) have an adverse reputational impact on Jersey and / or holds special category data – these factors appear to be the practical (if not technical) thresholds applied for

determining OES.

There are no current proposals to update the draft law to include the professional services sector. However, it is important to note that, as acknowledged by question one of the consultation response, the Minister may by Order (after enactment of the draft law) amend the definition of a cyber threat, and thus the scope of OES, albeit that this would likely only follow further round(s) of consultation with key stakeholders.

Deadlines for self-reports and the nature of reports

The consultation response acknowledges that it is not currently the policy intent to adopt a similar reporting policy as is seen in other jurisdictions, which requires a shorter time frame for the initial response and an obligation to submit updated information and a final report, again within specified time frames. This will be welcome news to prospective OES as this will reduce the reporting burden. Should the policy intent change, it would be subject to further consultation.

Similarly, the consultation response acknowledges a duty to report to the JCSC will overlap with existing reporting requirements, for example to the JFSC and the Information Commissioner for Jersey. It is proposed that guidance will be developed and published before the draft law is enacted as to how OES ought to comply with these overlapping reporting requirements.

The consultation response clarifies that whilst there is an attraction to a "report once" approach (that is to say, one report to satisfy all legal and regulatory reporting requirements), that is not currently envisaged albeit the Department for the Economy may consider this further in the future.

After divisive feedback about the appropriate deadline for self-reports in the event of a "significant" cyber incident, the deadline will remain 48 hours after the OES identifies that the cyber incident is "significant". The JCSC intends to host a number of workshops to assist OES to understand what "significant" means.

The JCSC remains of the view that a self-report within the first 12 hours of identifying a "significant" cyber security incident is likely to be of greatest benefit to monitor the scale and impact of the incident, and most effectively combat it.

When will the duties on OES take effect?

It is proposed that the duties on OES will take effect three months after the draft law is enacted. This should provide OES with some time to consider guidance that is likely to be issued in short order by the JCSC post-enactment of the draft law to better understand how the duties will impact on their specific sector.

Other headline changes to the draft cyber security law

The consultation response highlights (among others) the following eight amendments to the draft law following the consultation:

- updated definitions in Part 1, to include revised "cyber" definitions and refined definition of "public administration"
- incident reporting timeframe to be a maximum of 48 hours after determining the incident is significant
- refinement of the OES definition used in Article 24
- removal of the financial services subsector from OES, to work with industry on a suitable definition and threshold limits before being included
- key regulators explicitly included as OES
- removal of Article 32 which required the OES to notify all impacted service users or network users of incidents
- clarification of governance arrangements to ensure effectiveness and to be appropriate and proportionate to the size and scale of the Office of the Commissioner for Cyber Security
- information sharing gateways have been clarified to ensure reporting to JCSC do not contravene any other legal obligations an organisation may have

How can Ogier help?

If you have any questions about the draft cyber security law, please do not hesitate to contact any of the authors of this briefing.

About Ogier

Ogier is a professional services firm with the knowledge and expertise to handle the most demanding and complex transactions and provide expert, efficient and cost-effective services to all our clients. We regularly win awards for the quality of our client service, our work and our people.

Disclaimer

Key Contacts

Matthew Shaxson

Group Partner, Ogier Legal L.P.

Jersey

E: matthew.shaxson@ogier.com

T: +44 1534 514064

Tom Hall

Managing Associate

Jersey

E: tom.hall@ogier.com

T: +44 1534 514443

Michael Ogilvy Watson

Associate

Jersey

E: michael.ogilvywatson@ogier.com

T: +44 1534 514058

Related Services

Cyber security consulting

Banking and Finance

Investment Funds

Related Sectors

Technology and Web3

Trusts Advisory Group