



JERSEY
Chamber of Commerce

Chamber House, 25 Pier Road, St. Helier, Jersey, Channel Islands, JE2 4XW.

Tel: 01534 724536

E-mail: admin@jerseychamber.com

Website: www.jerseychamber.com

4th December 2018

Response From: Jersey Chamber of Commerce - Digital Committee

Dear Mr Harris, Deputy Ward,

Thank you for inviting Jersey Chamber of Commerce to provide the Education and Home Affairs Scrutiny Panel with feedback on the Draft Cybercrime (Jersey) Law 20 –to be debated in January 2019.

Please find herewith responses from the Digital Committee summarised with detailed discussion points listed in the table below.

1. Whether what is being proposed is fit for purpose and proportionate;

The Chamber Digital Committee agrees that subject to final review such amendments to the law are fit for purpose and proportionate.

It is noted in our detailed comments that this law should be reviewed more regularly to support rapid advances in technology and our dependency on digital services.

2. Whether it will effectively protect Jersey against cybercrime;

Jersey Chamber of Commerce believes these amendments will improve the islands ability to investigate and respond to Cyber related crimes, but in its own right the law will not protect our island. It is noted that the Information Security industry and its practitioners rely on such legislation to deal with incidents but must also to train on and test services. The law may require guidance on ethical hacking and testing of service for those involved in such services.

3. What impact it will have on Jersey business community;

Unless there were a sudden increase in the number of requests for data access, there should not be a significant impact. The business community is already impacted by recent amendments to Data Protection Legislation therefore appropriate guidance on any actions business must take to improve or change their processes should be carefully announced.

4. Whether we think any improvements or changes could be made to enhance the law;

We have listed a number of points raised in our workshop or submitted by attendees in the following table.

Chamber Workshop Feedback

Our approach to the response was to bring together a selection of interested professionals from varied industries including Technology, Information Security, Retail, Finance and Legal Services. Our feedback comes from our workshop in the following set of statements or questions.

Comment
In terms of providing power to investigate and obtain access to data, it must be clearly defined as to the circumstance access is allowed.
Any sudden increase with respect to the amount of data requests would have a business impact, however if the amendments to legislation simplify the processes and improve the speed in which a request can be made? For the right reasons this would have a positive impact and benefit businesses.
The update of the definitions overall has a positive impact
Several security practitioners raise the point that there needs to be guidance around their work including training in and around ethical security.
People whom cannot remember their encryption passwords should not be deemed criminals, what guidance is available on this. What is the guidance on mental health?
More guidance around who is being asked for access to what data or systems. For example, a helpdesk operative in a managed service provider being asked for access to a client's systems.
Article 12.4 – the law is not extended to all of the civil service?
The suggestion that recklessness unspecific to any computer or system is vague and somewhat confusing. Is carrying a laptop to work in a bag not seen as sufficient protection or does kicking the PC under the desk, warrant criminal recklessness?
Page 23, 27A (disclosure by operator): How does the law work if the operator is using contractors? Surely that would be an implicit disclosure as the operator would be disclosing to another company? We need to be sure that the law allows for the realism of using third parties to do BAU work.
Define properly economic wellbeing. This has been the most significant feedback from any who have reviewed the amendments.
The legislation does not seem to be updated very often. Does this current set of amendments offer futureproofing against technology such as Artificial Intelligence and the Internet of Things?
Can the authorities demand a key to data that has been obtained unlawfully?
What if decrypting a drive provides access to significant other information not related to the investigation?

The Jersey Chamber of Commerce Digital Committee would like to thank contributions from the following people;

Justin Clapham (Chair, Finance Committee)

Nadine Nicolas (Digital Committee)

Stephanie Luce (Channel Island Information Security Forum and Jersey Data Protection Association)

Andre Gorvel (Channel Island Information Security Forum)

David Cartwright (Digital Committee, BCS & Channel Island Information Security Forum)