Obligation to notify data storage or processing providers

Subsection 12F(3) *Security of Critical Infrastructure* (SOCI) *Act 2018* Factsheet

What is the obligation?

The responsible entity for a critical infrastructure asset is required to notify their third-party data storage or processing provider that the provider is storing or processing business critical data for a critical infrastructure asset. This obligation applies to all critical infrastructure assets.

Data storage or processing organisations often handle sensitive data on behalf of critical infrastructure assets, and play an important role in ensuring the security of that data, and in turn, the security of the asset. This obligation ensures that those providers know of the sensitivities associated with the data they are handling and can implement appropriate protections, as well as possibly triggering obligations for the provider under the SOCI Act.

Who is a responsible entity?

A responsible entity for a critical infrastructure asset is an entity defined in section 12L of the SOCI Act. The definitions vary for each class of critical infrastructure asset to reflect the entity with ultimate operational control of the asset.

Which providers need to be notified?

The obligation only applies when the responsible entity is aware that:

— a data storage or processing service is being provided by a third party
— the service is being provided on a commercial basis, and
— the service relates to the storage or processing of **business critical data.**

What is business critical data?

— Personal information (within the meaning of the *Privacy Act 1988*) of at least 20,000 individuals;
— Information related to research & development of a critical infrastructure asset;
— Information related to any systems needed to operate a critical infrastructure asset;
— Information needed to operate a critical infrastructure asset; or
— Information relating to risk management and business continuity of a critical infrastructure asset.

How do I fulfil the obligation?

As soon as practicable, the responsible entity must take reasonable steps to notify the third-party provider that they are providing data storage or processing services relating to the business critical data of a critical infrastructure asset on a commercial basis.

Reasonable steps may include writing to or emailing the provider.

Case Study 1

Eastern University is a critical education asset as it has a program of research focused on supporting Australia's defence force. Eastern University has a contract with Cloud Computing for the provision of cloud storage for data relating to the defence research.

The responsible entity for Eastern University is required to notify Cloud Computing that it is storing business critical data on a commercial basis.

The Chancellor of Eastern University writes a letter to the Chief Technology Officer of Cloud Computing, notifying them that they are storing business critical data of Eastern University on a commercial basis.

Case Study 2

Growth Wealth Ltd is the responsible entity for a critical banking asset. Growth Wealth Ltd stores information relating to its customers, product research & development, risk management and business continuity on internal systems. However, it also has a contract with Data Store for the storage of publicly available corporate and administrative arrangements. As Data Store is not storing business critical data for Growth Wealth Ltd, Growth Wealth Ltd does not have a notification obligation.

Case Study 3

Fast Trucking Ltd is the responsible entity of a large critical freight services asset. Fast Tracking Ltd has purchased account managing software from Office Solutions which it uses on its network to manage its own data in relation to customers. Fast Trucking Ltd is not required to notify Office Solutions as Office Solutions is supplying software, but does not manage data on behalf of Fast Trucking Ltd.

Contact Us | 1300 27 25 24 | enquiries@CISC.gov.au | CISC.gov.au

October 2022

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

I've been notified by a responsible entity that I store or process business critical data. What should I do?

If you have been contacted by a responsible entity for a critical infrastructure asset, it is important that you consider the following actions:

1. Consult section 12F of the SOCI Act 2018 to determine if your asset meets the definition of *'Critical data storage or processing asset.'*

An asset is a 'critical data storage or processing asset' if:

— it is owned or operated by an entity that provides a data storage or processing service, and

— the asset is not already covered as a different type of critical infrastructure asset, and

— The asset is used wholly or primarily to provide a data storage or processing service that relates to **business critical data** and is provided to an end-user that is:

- Commonwealth, State or Territory government, or
- a critical infrastructure asset.

What is business critical data?

— Personal information (within the meaning of the *Privacy Act 1988*) of at least 20,000 individuals;

— Information related to research & development of a critical infrastructure asset;

— Information related to any systems needed to operate a critical infrastructure asset;

— Information needed to operate a critical infrastructure asset; or

— Information relating to risk management and business continuity of a critical infrastructure asset.

Obligations for critical data storage or processing assets include:

2. — Reporting entities must provide operational, interest and control information to the Register of Critical Infrastructure Assets. For more information about this obligation see Register of Critical Infrastructure Guidance.

— Responsible entities must report cyber security incidents that impact their asset. For more information about this obligation see Mandatory Critical Incident Reporting Guidance.

Case Study 1

The CTO of Cloud Computing received a letter from Eastern University, alerting them that they store business critical data on behalf of Eastern University.

Cloud Computing consider the definition of a 'critical data storage or processing asset' in section 12F of the SOCI Act and, now aware of the nature of their services with Eastern University, determine that they meet the definition and are a critical infrastructure asset.

Cloud Computing consider the obligations they have as a critical data storage or processing asset.

Case Study 2

Consulting R'Us provide an accounting service to Big Power which is a critical electricity asset. The arrangement involves Consulting R'Us dealing with business critical data on behalf of Big Power.

Following notification from Big Power, Consulting R'Us consider the definition of a 'critical data storage or processing asset' in section 12F of the SOCI Act. Consulting R'Us determine that they are not a critical data storage or processing asset as the data processing is ancillary to the core accounting services being provided to Big Power.

Contact Us | 1300 27 25 24 | enquiries@CISC.gov.au | CISC.gov.au

October 2022

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE