Business Electronic Records and the Law in Papua New Guinea

Written by Keith Iduhu and Joy Tera
6.06.2017

Key Points:

- Business electronic records/documents are protected by law.
- Not all business electronic records are accepted as evidence in court.
- A production of a business electronic record must reflect authenticity requirements under the *Evidence (Amendment) Act 2016*.
- Unless provided otherwise by legislation, hardcopy business records or original paper records reflecting information that is electronically stored may be destroyed upon meeting authenticity requirements.

Introduction

Company policies change occasionally to reflect new technology advances created to bring business efficacy and foster competitive advantage. However with change come challenges and the need to be informed of the current trend in law relating to electronic records. Should I be worried if I do not know what the law in relation to electronic records demand? Yes, off course you should be worried! You run the risk of having your entire electronic record system fall short of the requirements provided by law.

What are Electronic Records?

An electronic record is a set of data that is created, generated, recorded, stored, processed, sent, communicated or received on any physical medium by an electronic system or device, that can be read or perceived by a person by means of an electronic system or device, including a display, print out or other output of those data.[1]

Are these Records protected by law?

The recent enactment to the *Cybercrime Code Act 2016* creates offences and penalties for the unlawful use of information and communication technology or cybercrime. It follows that the Act creates a safety net around electronic records and imposes penalties for the acts or omission relating to this type of records.

For example, it is a serious offence under this Act to interfere with data by means of recklessly:[2]

[1] s 4(1) Evidence (Amendment) Act 2016
[2] s 8 Cybercrime Code Act 2016

a. deleting data; or
b. altering data; or
c. obstructing, interrupting or interfering with the lawful possession of data; or
d. obstructing, interrupting or interfering with any persons lawful use of the data; or
e. denying any authorized person access to data.

The penalty for which is a fine not exceeding K100,000.00 or an imprisonment for a term of ten (10) years or more.

Are all Electronic Records admissible in court?

It is important to note that whilst an electronic evidence is accepted by the courts, not all of them can be admissible. The courts have the discretion to refuse any electronic record into evidence if the interest of justice does not favour it but will do this in light of two things:

1. Ascertaining the credibility of the electronic system itself; and
2. Ascertaining the authenticity of the document/record produced as evidence.

What does this mean for you?

The person responsible for a company's electronic file management system should strive to ensure that the company's electronic records reflect these two stages. It is only then can we say with legal certainty that our electronic records are admissible in court when the need arises to have them produced.

Stage 1 – Credible electronic system.

A credible electronic system should reflect the following:

a. The electronic storage system is certified or has been signed by a method provided by an accredited certification entity;[3]
b. the Computer System is complete and unaltered apart from the normal storage or display changers that occurs during the normal course of communication;[4]
c. the Computer System is working properly;[5]
d. the document was prepared during a period over which the computer regularly stored or processed information;[6] and
e. over the relevant period of time, information of this type was regularly supplied to the computer.[7]

Stage 2 – Document Authentication.

The onus of proving that the information produced is authentic lies on the party who wishes to introduce and rely on the relevant electronic evidence.[8] Whilst that may be the normal practice, it is desirable that the party who introduces electronic evidence should make a statement showing one of

[3] s(67A) *Evidence (Amendment) Act 2016*
[4] ibid
[5] ibid
[6] s 4(2) *Evidence (Amendment) Act 2016*
[7] ibid
[8] s(67C) *Evidence (Amendment) Act 2016*

the two things or both:

- the process of how the electronic record was produced must be described;[9] or
- all electronic systems or devices that were involved in the production of the electronic record must be described.

Additionally, where the electronic record is in the form of a 'print out' before the court, one must also seek to establish that the particular print out:

- has been consistently or manifestly acted on;[10] and
- relied upon;[11] or
- used;[12]

as the record of data recorded or stored on the printout. This would go towards establishing the authenticity of the document.

What about the original paper copies of Electronic Records? Can we destroy them?

Whether it is possible to destroy an original paper copy reflecting an electronic record is yet to be tested and proven by the courts. It is however good practice and a matter of public policy that original paper copies should be retained.

But like all other rules, there are exceptions! If an original paper copy will be scanned and kept as an electronic record, and unless required otherwise by legislation; one must prove the following before the paper copy is destroyed:

a. the electronic storage system that will be used to store the electronic record is certified or has been signed by a method provided by an accredited certification entity;[13]
b. the Computer System is complete and unaltered apart from the normal storage or display changers that occurs during the normal course communication;[14]
c. the Computer System is working properly;[15] and
d. the electronic copy of the paper copy will be consistently relied upon or used.

Conclusion

All business electronic records stored must reflect authentication requirements under the *Evidence (Amendment) Act 2016* as discussed earlier. Unless these requirements are met, the electronic document runs the risk of being inadmissible in court when the need arises to have it produced as evidence.

[9] s67A(4) supra n ii
[10] s67B *Evidence (Amendment) Act 2016*
[11] ibid
[12] ibid
[13] Supra n ix
[14] ibid
[15] ibid

Disclaimer
The information set out in this article is a general guide only about the laws in PNG and is not intended as specific legal advice.

Contact

For more information please contact:

Keith Iduhu
Principal
T +675 321 4470
E kiduhu@fairfax.com.pg

Joy Tera
Lawyer
T +675 321 4470
E jtera@fairfax.com.pg