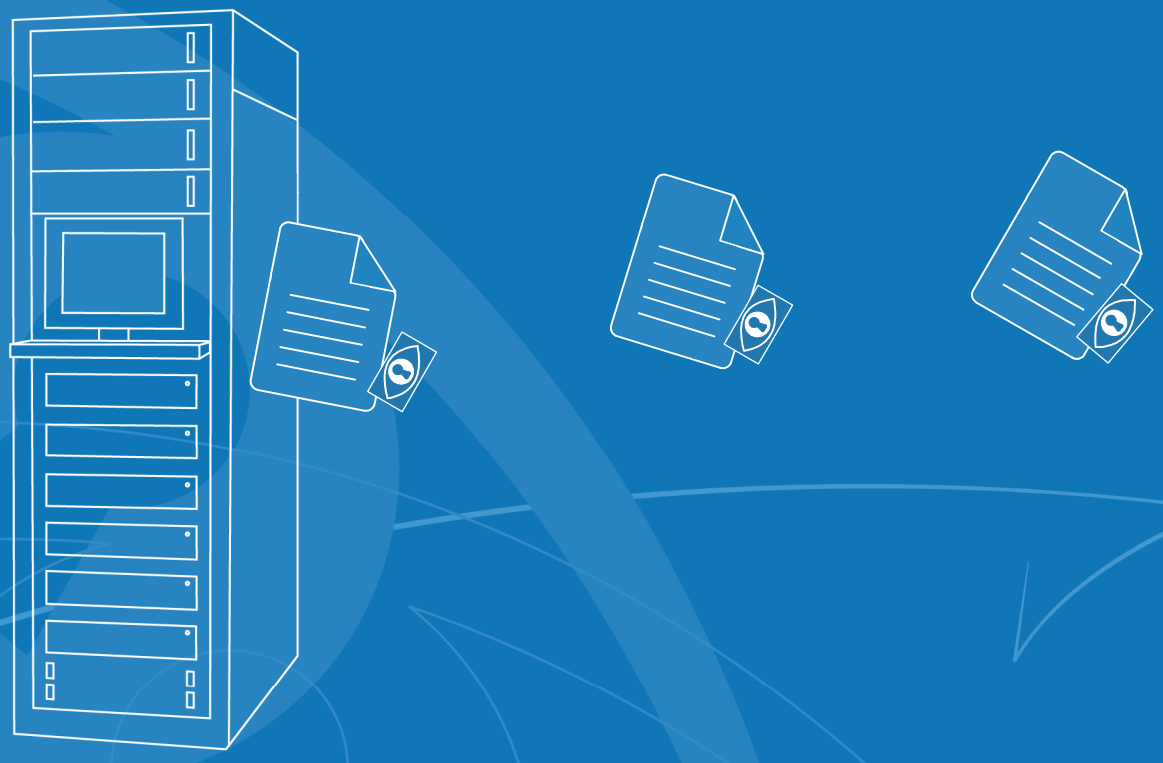
SOFTECTION

The 5 Golden Rules of Data Protection when Outsourcing



SOFTECTION
DIGITAL ASSET PROTECTION

The 5 Golden Rules of Data Protection when Outsourcing

www.softection.com

The 5 Golden Rules of Data Protection when Outsourcing

Rule 1: Keep IT Under Your Control

If there is not a very sound reason to send data overseas, then don't. The latest data protection policies in most western countries holds the originating company responsible for the protection of the data even when they are dealing with a third party supplier. You are outsourcing a business process, not the responsibility of protecting the data.

You are responsible for the protection of that data and in many cases required by law to report on who accessed the data and what was done to it. Outsource Providers in many countries can access a reasonable amount of information over a network, which can be protected and the data can be held encrypted and controlled. If the data is required to be sent overseas, then you should implement controls which can be managed remotely.

Rule 2: Get It Right and Get It In Writing

Data protection and security considerations must feature in the initial vendor due diligence. This should be supplemented by audit rights exercisable during the life of the contract so that the business may reassure itself that data is lawfully processed and protected by adequate security.

The outsource provider needs to be aware of the data protection laws imposed on the data he is working with. The laws of the originating country follow that data regardless of where in the world it is stored and processed.

Some common question that need to be asked: is data gathered overseas, where is it stored, who has access, is it encrypted, is there a log of who accessed the data and what was done with it, can the outsourcing provider use third party contractors etc. Layout the rules and make sure everyone understands them and ensure they are enforced.

Rule 3: Control Access to data required

Allow access only to the data required to do the job. If you have a package sent to your house, you need to provide the courier with your address; you don't give them the keys to your house and the combination to your safe.

The same rule applies here. Only give access to the data that is relevant to the job, AND NOTHING MORE.

Rule 4: Control the Use: Stop Internal Leakage

This is an important rule often overlooked and is possibly the best defense against internal leakage of sensitive information. The technology to stop internal leakage is available today and if ever there was a need to use it, Outsourcing is it.

Usage control allows the required use of protected information, but stops the unnecessary use of the protected information. (control copy, paste, screen-grabs, printing, etc.)

Rule 5: Log actions and access to Sensitive Data

Keep a Log of all activity of your sensitive data. This has a three fold benefit.

SOFTECTION
DIGITAL ASSET PROTECTION

The 5 Golden Rules of Data Protection when Outsourcing

www.softection.com

1. Review activity in case of a breach.
2. Report on compliance.
3. Set rules that notify of unusual activity.

Conclusion

Outsourcing has many business benefits, mostly financial, but with the good comes the bad. Failure to deal with the data protection issues from the beginning could result in long lasting damage to a business' reputation… with only one data breach.

Web: www.softection.com
Email: outsource@softection.com
Phone: +61 2 9816 3433

SOFTECTION
DIGITAL ASSET PROTECTION