WHITE PAPER:
EMAIL ARCHIVING

Legal Compliance in Electronic Record Keeping

Who should read this paper

IT Managers, C Level Executives, Compliance Managers, Legal Officers

Symantec.cloud

Content

Introduction

In Australia there is now a complex framework of legislation regulating the retention of information for various purposes. It has never been more important to ensure that an organisation's records are properly managed. It should be noted that emails form a significant part of what is described in this paper as an organisation's "records".

The retention, storage and recoverability of records is important for three main reasons:

Reason One: Regulated Retention – Records should be retained because the organisation has a statutory obligation to retain those records; and

Reason Two: Be Dispute-Ready – Records should be retained in case they are required for a dispute or even litigation.

Reason Three: For Reference – To ascertain ongoing legal rights and responsibilities.

A 'record' can be paper or anything upon which there is writing or marks, symbols or perforations and any disk, tape or other article from which sounds, images or messages are capable of being reproduced. A 'record' is not just the physical thing (ie hard copy or paper document), but can be any data or information stored or recorded by mechanical or electronic means, such as voicemail, images, audio and video files, presentations, emails and metadata (data contained within electronic files relating to the identification, origin or history of the file itself).

This paper summarises the Regulated Retention obligations of organisations and how proper record retention is essential in order to be Dispute-Ready.

Finally, the paper sets out the key points to ensure that organisations comply with their Regulated Retention obligations and are Dispute-Ready.

Regulated Retention Obligations for the Private Sector

Regulated Retention is a major issue for non-government organisations.

Privacy legislation

The Commonwealth Privacy Act also regulates the collection, use, disclosure and handling of personal information and sensitive information for the private sector in a similar way to the way government organisations are regulated (as set out above).

Non-government organisations should ensure they are able to produce all personal information about an individual (including emails) within a reasonable time of the individual making a request.

Corporations Act

The *Corporations Act* contains a number of records management requirements. The key requirements include the following:

- Financial records (which include invoices, receipts and documents of prime entry and can include emails) must be retained for no less than 7 years.
- All reasonable precautions must be taken for guarding against destruction or falsification of any financial record. In particular, financial records must be kept in such a manner as to enable true and fair financial statements to be prepared and audited.
- Financial records may be stored electronically but hard copies are required to be made available within a reasonable time if necessary.

- A company's officers must make annual declarations that the financial records have been properly maintained for the financial year.
- There are other specific requirements for the maintenance of company registers and related documentation.

Employment legislation

The *Fair Work Act* requires employers to keep particular types of employee records for 7 years after they are created (including name, employment type, commencement dates, overtime records, pay, bonuses, superannuation contributions, leave entitlements, termination details, flexibility arrangements, hours worked and employment agreements). If any employment record is changed, it must be kept for at least 7 years from the date of the change.

Legislation in New South Wales and Victoria obliges employers to keep certain employment-related records for minimum periods of between 6 and 7 years. These records may often be in the form of email correspondence between the HR Department and the employee.

Under each State and Territory's workers compensation regime, there is also a general obligation to create a variety of records relating to an employee's injury and the management of that injury.

Further, employers may be able to avoid sexual harassment in the workplace and the resource drain in dealing with such claims by establishing strong harassment policies. These may be included in email and internet usage policies.

The key legislation includes the *Fair Work Act,* the *Workers Compensation Act* in each State (and similar legislation), the *Long Service Leave Act* (in various states and other similar legislation) and various Acts dealing with accident compensation.

It should be noted that the *Workplace Surveillance Act* in NSW and similar legislation in some other States require that employees be given notice whenever employers plan to conduct computer surveillance of employees (including the monitoring of emails).

Tax Acts

Key provisions of the *Income Tax Assessment Act* include the following:

- Any organisation subject to income tax must keep records that record and explain transactions and other acts engaged in by the person that are relevant to the Act for 5 years.
- These records must be readily available if stored electronically.
- A failure to comply may result in a fine and an unfavourable tax assessment.

Similar obligations for record retention exist for records relating to other federal taxes, such as FBT, CGT and GST. Each State and Territory also require records related to stamp duty and payroll tax to be kept for a minimum of 5 years.

Australian Standards and APRA Guidelines

Standards Australia has issued several relevant Australian Standards and related documentation, including Standards Australia handbook "HB 171 2003: *Guidelines for the Management of IT Evidence*". Although not legally binding, they provide guidance for best practice.

The Australian Prudential Regulation Authority (**APRA**) has issued a number of guidelines for records management in relation to the financial services industry, which are applicable to organisations such as banks, credit unions and insurance companies.

Intellectual Property Issues

All records pertaining to the registration of a trade mark should be kept while ever the trade mark is registered because they may be necessary to enforce that trade mark in litigation. Similarly, records relating to any patent should be kept for the life of the patent (normally 7 years) and records relating to any copyright work should be kept for at least as long as the copyright continues to subsist (50-70 years depending on the work). These records may be stored electronically.

Regulated Retention Obligations for the Government Sector

Regulated Retention is not just an issue for non-government organisations, government bodies have statutory obligations as well.

Privacy legislation

The Commonwealth *Privacy Act* sets out privacy obligations for Commonwealth and ACT government agencies. There is also state-based legislation, including the New South Wales *Privacy and Personal Information Protection Act* and the Victorian *Information Privacy Act*, which apply to state government agencies. The state legislation is generally modelled on the Commonwealth legislation.

The Commonwealth *Privacy Act* regulates the collection, use, disclosure and handling of personal information and sensitive information. The Act contains 11 Information Privacy Principles (**IPPs**), which apply to Commonwealth and ACT government agencies. Since the IPPs have been effective, the Federal Privacy Commissioner has also issued a number of public interest determinations relating to the government sector.

The *Privacy Act* applies to any information that falls within the definition of "personal information". Personal information includes information such as names, addresses, telephone numbers, credit card details, information gathered on websites and mobile telephone numbers linked to user names and mailing lists. It also includes information like that set out above where it is contained in emails.

Under this privacy legislation it is essential for the government organisation that is holding "personal" information about an individual to make it available to that individual within a reasonable time after the individual has requested it. It is also essential that the information be protected by security safeguards against loss, unauthorised access, use, modification or disclosure, and against other misuse.

Freedom of Information Act

Similar legislation applies to the Commonwealth and in each Australian state. The Freedom of Information Act provides a right to individuals to gain access to information in the possession of agencies. To comply with the act, agencies must have protocols and systems allowing for retrieval of accurate information in a timely manner.

Archives Act

The *Archives Act* is an overarching Act that applies to all Commonwealth government recordkeeping. The Act includes wide powers to ensure preservation of Commonwealth records by implementing best practice standards of recordkeeping. It contains certain restrictions on the destruction of Commonwealth records and gives the public the right to access Commonwealth records that are more than 30 years old. Emails fall within the definition of government records that must be retained. Similar obligations are contained in State legislation (eg *State Records Act* in NSW).

Legislation specific to statutory authorities and government departments and bodies

Some statutory authorities and government departments and bodies are regulated by legislation specific to that particular authority, department or body. It is often the empowering statute that sets out the electronic records management obligations of the particular authority, department or body. There may also be agency specific policy and business requirements that apply. Symantec.cloud services may assist agencies to comply with any such requirements.

Dispute resolution and electronic records management

As a negotiation tool

The party with the best evidence often prevails in the event of a dispute. If an organisation has maintained comprehensive and easily searchable records, it will be in a better bargaining position in the event of a dispute.

Discovery

In litigation the "discovery" process is where a court orders each party to make its relevant documentary records available to the other party for inspection. The concept is that neither party should be taken by surprise during the court proceedings by undisclosed documentary evidence. It also sets the boundaries for the case in dispute.

An organisation should be prepared to comply with a court order for discovery of documents quickly and efficiently. In order to achieve this, records should be initially recorded and maintained in a way that allows them to be recovered and sorted quickly. If this is left until a dispute actually reaches the courts, the costs of the discovery process can be significant.

One of the major factors affecting the cost of discovery is the method of record (including email) storage. If the records are easily recovered, searched and printed, the costs of discovery are likely to be lower.

Relying on electronic evidence in court

Electronic evidence is generally admissible in court proceedings. However, an organisation should always be in a position to prove the integrity of its electronic evidence. This means in the case of email being able to establish a valid and secure email trail, in other words, the time of sending or receipt of an email and demonstrating that this information, and the content of the email itself, cannot have been subsequently altered.

Consequences of destruction of electronic records

Destruction of records

Legislation in various jurisdictions makes it a criminal offence to destroy a record that is or may be required as evidence in a judicial proceeding. Victoria has a specific offence of corporate criminal responsibility for the destruction of evidence. Provisions to similar effect exist in other State Crime Acts and Criminal Codes, although none are as expressly directed towards the behaviour covered by the Victorian legislation.

A party that destroys a record may also be liable for the criminal offence of contempt of court or attempting to pervert or obstruct the course of justice.

Failing to produce a record in litigation because it was destroyed (inadvertently or otherwise) may also result in the court:

- making an adverse inference regarding the contents of the record; and
- making an order that that the evidential burden of proof be reversed in relation to a fact or issue, or that certain evidence not be adduced, or that a fact in issue between the parties be presumed to be true in the absence of evidence to the contrary.

Recent Australian cases

- *British American Tobacco Australia Services Ltd v Cowell:*

The court considered that destruction of documents could be seen as an attempt to pervert the course of justice.

- *Cashflow Finance Pty Ltd v Westpac:*

In this case a company was held not to have had a proper system of controls or a sufficient review process to prevent unauthorised conduct by personnel or officers of the company. The court considered that the company's director may have breached his duty as a director.

What does the future hold

Recent trends in the United States may hold the key to assessing future trends in statutory electronic record retention policies in Australia. There have been two major changes in the US legislative framework in recent years

- **Sarbanes–Oxley Act of 2002**

This Act, together with other corporate governance record retention related legislation, was enacted largely in response to a number of major US corporate collapses. It has resulted in record retention policies that are far more prescriptive in terms of the period of record retention, format of record retention and minimum period for record recovery than similar regulations in Australia.

- **Patriot Act**

This Act arose following the incidents of 9/11. It gives the US Government extensive powers in the name of combating terrorism. The Act imposes a range of records management obligations on the operations of US organisations, both within and outside the US.

Given these developments, it may be that Australia is likely to get more prescriptive electronic record management regulations in the future. Symantec.cloud services may assist both private and public sector organisations with their obligations to comply with future electronic records management regulations.

Key rules for compliance

(1) Become familiar with the statutory obligations on the organisation regarding electronic record management to ensure compliance with the relevant legislation.

(2) Prepare and implement an electronic record retention policy, including an email and internet use policy, which complies with the relevant statutory obligations on the organisation.

(3) Notify all employees and, where applicable, contractors of these policies. Notification of policies should be in writing and evidence that the employee or contractor has agreed to the policies should be retained.

(4) Ensure that policies are enforced. This should include regular education of employees and contractors.

(5) Ensure that the organisation's electronic record management system:

(a) allows records to be searched reasonably easily;

(b) allows records to be recovered within a reasonable time for reference purposes and in the case that a dispute ever require that records be made available; and

(c) prevents the destruction of records unless the following process is first conducted:

- identify which records are to be destroyed;
- confirm that the destruction of the records will not contravene any policy of the organisation;
- confirm that the destruction of the records will not contravene any statutory obligations;
- confirm that the records are no longer relevant for a any future dispute; and
- ensure that the final decision on destruction of the records is made at the appropriate level.

Annexure

Summary of Regulated Retention Obligations – private records

Specific Acts	Minimum Retention
Tax Acts	5 years
Corporations Act	7 years
Financial Transaction Reports Act	7 years after completion
Industrial Relations Act	6 years after last entry
Long Service Leave Act	6 years after last entry
Workers' Compensation Act	7 years after last entry

About Symantec.cloud

Symantec.cloud, a division of Symantec Corporation, offers customers the ability to work more productively in a connected world. More than 55,000 organizations ranging from small businesses to the Fortune 500 use Symantec.cloud to administer, monitor and protect their information resources more effectively. Organizations can choose from 14 pre-integrated applications to help secure and manage their business even as new technologies and devices are introduced and traditional boundaries of the workplace disappear. Services are delivered on a highly scalable, reliable and energy-efficient global infrastructure built on 18 datacenters around the globe.

For specific country offices and contact numbers, please visit our website www.symanteccloud.com/en/au/

Symantec.cloud
Level 14, 207 Kent Street
Sydney NSW 2000
AUSTRALIA
Main: +61 2 8220 7000