GUIDE TO ACHIEVING EMAIL COMPLIANCE

– a South African perspective

Abstract

This document highlights some of the South African rules and regulations that require the effective management of email. It looks at relevant provisions of, among other things, the ECT Act, the new interception legislation and the King II Report on Corporate Governance.

It then sets out the key requirements of an effective email management system, which are distilled from the law and regulatory requirements. What is apparent is that simple save and back-up solutions are not enough – a solution must fundamentally ensure the integrity of email.

Finally, this document outlines a process that can be used to achieve email compliance and identifies the key elements of a solution.

Table of Contents

1 INTRODUCTION

The use of email for business purposes is beginning to replace many of the more traditional ways of communicating. Indeed, it is fast becoming not a luxury, but an essential business tool.

An important question is – how does a company maintain control over such fast paced and essential business communications. And what exactly does it mean to maintain control? And why is it important?

1.1 Why email compliance?

The reason why it is increasingly important for email to be effectively managed is because of ever increasing legal responsibilities with regard to the retention, destruction and restoration of electronic records. In addition to general legislation requiring the maintenance of information, recent legislation specifically relevant to electronic communications includes the Electronic Communications and Transactions Act (ECT Act)[1] and The Regulation of Interception of Communications and Provision of Communication-Related Information Act (Interception Act).[2]

1.2 Risks of non-compliance

In addition, the King Report on Corporate Governance for South Africa (King II Report)[3] provides that directors are responsible for risk management and specifically with regard to information technology, that they have a responsibility to ensure that an effective internal control system is maintained.

Thus, electronic document management is an issue not only for the technology and legal/compliance departments, but is the concern of every part of a business, especially the board of directors.

The ultimate risks of non-compliance are potentially significant fines and the imprisonment of directors.

1.3 Benefits of compliance

There are also benefits of compliance. A good email management system well implemented should increase productivity and reduce costs. Employees will spend less individual time managing their own email and duplicative storage will be reduced. A good management system will also decrease the amount of person hours required to search and retrieve documents.

Good email management will also give a company access to email records that will assist it in a defence when a company has been falsely accused. It will also allow companies to destroy documents when appropriate thereby reducing legal risks and costs.

1.4 What needs to be done

For most companies, it will not be enough to rely on the more traditional ways of managing email, for example, directing end users to manage their individual mail boxes and backing up data periodically. The key aspect emerging from increased reliance on email for essential business purposes and legal requirements regarding electronic communications, is the maintenance of the integrity of email and being able to prove that integrity.

So, what do you do? Doing nothing is not an option. Unfortunately, neither is rushing out to buy the latest technology. A company must assemble the right team, examine the issues, including the legal requirements and find a multi-faceted solution that is right for that company.

2 THE RULES AND REGULATIONS

Before developing and implementing an email compliance solution, it is important to understand the legal requirements. In South Africa, these include the ECT Act, general rules requiring record keeping and management, interception legislation and the King II Report.

2.1 Electronic Communications and Transactions Act

One of the main purposes of the ECT Act is to make clear that electronic communications are to be treated in the same way as other more traditional forms of communications, in the eyes of the law. The Act provides that information is not without legal force and effect merely because it is in electronic form.

Because of the nature of electronic communications - including the fact that it can be manipulated fairly easily – varying and specific rules are set out in the ECT Act with regard to how electronic communications should be managed in order to maintain and prove the integrity thereof.

There are specific rules with regard to –

- Writings
- Signatures
- Agreements
- Originals
- Retention of electronic documents
- Production of electronic documents
- Admissibility of evidence

2.1.1 Writings

If the law requires a writing, the writing may be in electronic form as long as the writing is 'accessible in a manner usable for subsequent reference'. What this means is that the electronic document must be captured, retained and retrievable.

2.1.2 Signatures

If the law requires a signature, an electronic signature may be used. However, an advanced electronic signature is required, meaning that the signature must be supported by an authentication product or service, which is a product or service that identifies the holder of an electronic signature to other persons.

On the other hand, if a signature is not required by law, then any form of electronic signature or even a simple communications of intent will suffice.

2.1.3 Agreements

Thus, an agreement may be concluded via email. Indeed, an employee may be able to bind a company via email, even where the company would not normally want them to be able to do so.

The Companies Act provides that any person acting under the authority of the company, whether express or implied, may contractually bind the company.

The ECT Act provides that an electronic communications is considered that of the originator, if sent by either the originator, someone who had authority to send it on behalf of the originator or by an automated process programmed by or on behalf of the originator.

The ECT Act also provides that an agreement is concluded at the time when and place where the acceptance of the offer is received. It also provides that an electronic message is received

when the message enters an information system and is capable of being retrieved by the addressee and that it is received at the addressee's usual place of business or residence.

The ECT Act, however, allows companies to opt out of the presumptions regarding the generating, sending, receiving, storing and processing of electronic communications.

Thus, companies will not only need to be able to capture, retain and retrieve email, but also need to be able to manage the use of the email, from a company point of view, from an employee point of view and from the point of view of the public with which the company and employees communicate via email. This can be done through employee use policies and email disclaimers, in addition to utilising appropriate technology.

2.1.4 Originals

If the law requires an original, the document may be in electronic form as long as it is 'capable of being displayed or produced to the person to whom it is to be presented', and if the integrity of the document is maintained. With regard to integrity, the ECT Act stipulates that integrity will be assessed by whether the document is unaltered, in the light of the purpose for which the document was generated, and any other relevant circumstance.

Thus, in addition to being able to manage the use, capture, retention and retrievability of electronic documents, companies must also be able to manage subsequent use of such documents and in particular, must be able to audit such use.

2.1.5 Retention of electronic documents

Where the law requires the retention of information, such information may be retained in electronic form. However, the information must be 'accessible so as to be usable for subsequent reference'. The electronically retained document must also be in the format in which it was generated, sent or received, or in a format that can be demonstrated to represent accurately the information generated, sent or received. Also, the origin and destination and the date and time it was sent or received must be determinable.

2.1.6 Production of electronic documents

If the law requires the production of a document, it may be produced electronically. However, it must have been reasonable to expect at the time the electronic message was sent that the information contained therein would be readily accessible 'so as to be usable for subsequent reference'. Further, considering the circumstances at that time, the method of generating the electronic information must have provided a reliable means of assuring the maintenance of the integrity of the information. With regard to integrity, it is maintained if the information has remained unaltered.

2.1.7 Admissibility of evidence

The ECT Act makes clear that electronic evidence is not inadmissible simply because it is electronic. The integrity and audit-ability of the integrity of the evidence is key. The Act indicates that electronic evidence must be given 'due evidential weight'. Due evidential weight depends on the reliability of the manner in which the electronic evidence was generated, stored or communicated, the reliability of the manner in which the integrity of the evidence was maintained, the manner in which the originator was identified, and any other relevant factor.

2.2 General legal requirements for records management

The general document collection, retention and production obligations for companies stems from a myriad of legislation. Some of the more uniformly applicable laws are mentioned herein, namely –

- Requirements stemming from the constitutional right of access to information
- General commercial requirements
- General requirements regarding matters in litigation
- Specific requirements for financial and similar companies
- Specific requirements for telecommunication companies
- Specific requirements for government and government-owned entities

2.2.1 The right of access to information

The Promotion of Access to Information Act[4] was enacted to give substance to the constitutional right of access to information. It indicates that once a request for access is received, steps must be taken to preserve the records requested. This legislation is applicable to private as well as government entities.

2.2.2 General commercial requirements

Various legislation and regulations require companies to keep documents. For example, the Regulations for the Retention and Preservation of Company Records, 1983 made in terms of the Companies Act[5] and the Administrative Regulations made in terms of the Close Corporations Act,[6] set out rules for the retention of company documents for certain periods of time.

The Income Tax Act,[7] specifically with regard to electronic documents, requires the keeping of records by persons deriving income other than from remuneration, including 'any data created by a computer relating to any trade carried on by that person in which are recorded the details from which that persons' returns for the assessment of taxes under the Act were prepared'.

The South African Revenue Service (Sars) has indicated that Value Added Tax (Vat) invoices may be sent electronically. The Value Added Tax Act[8] requires the retention of Vat records for a period of five years. As more South African companies are electronically sending Vat invoices, it will be critical for all companies (even those that just receive them) to be able to store and retrieve them.

Sars also has indicated that electronically sent Vat invoices should be sent in encrypted format and that recipients should in writing confirm that they will accept Vat invoices transmitted electronically.[9] Thus, sending Vat invoices electronically will require specific attention from a compliance point of view.

A good records management policy will not only seek to comply with relevant legal and regulatory requirements, but will also be guided by business requirements. For example, contracts should be retained for at least the period of the contract and for the prescription period for contract debts, which is three years. There may be other reasons for retaining records after that time period, such as continuing litigation or in order to protect information that would allow, for example, a company to analyse business practices.

2.2.3 General litigation requirements

In addition to legislative requirements to keep records, which would include the capture and retention of electronic records, there are corresponding requirements to be able to retrieve and produce such records. This is implicit in legislative requirements to keep documents.

It is also required by the various rules of court made in terms of the Supreme Court Act.[10] The rules with regard to the discovery, inspection and production of documents require a discovery request to be complied with within a certain time period and if it is not complied with, then a party not complying can be compelled to do so. If a discovery request is not complied with, a company ultimately may be fined or company directors jailed. This is so even if the reason for non-compliance is simply because a company's electronic document management system is inadequate.

In response to a discovery request (or in response to a production request from government or a request for documents in terms of the Promotion of Access to Information Act), a company will have to be able to separate out different types of documents based on their nature, for example, confidential documents. The same would apply to privileged documents in response to a discovery request. Thus, a good email management system must be able to categorise and separate documents in relation to storage and retrieval functions.

2.2.4 Financial and similar companies

The newly enacted Financial Intelligence Centre Act (Fica)[11] has as its principal object to assist in the identification of proceeds of unlawful activities and the combating of money laundering activities. Fica requires accountable institutions, such as attorneys, estate agents, financial and insurance institutions, and accountants to collect and keep records about clients and transactions for a period of five years, and to make such records available to the Financial Intelligence Centre. Failure to comply with Fica and in particular with regard to the requirements to collect, keep and provide information, is an offence, which could result in significant fines and imprisonment.

The Financial Advisory and Intermediary Services Act[12] requires the retention of records by financial services providers for at least a five year period. The types of records that must be retained include, among others, premature cancellations of transactions or products and complaints received.

2.2.5 Telecommunication companies

The Telecommunications Act[13] requires the retention of various types of records in order to assist in the regulation of the industry. The regulator is empowered to call for the production of certain information.

In addition, the Interception Act specifically requires telecommunications companies to collect and retain various types of information regarding customers and communications. The details of such requirements are to be set out in regulations currently under consideration.

2.2.6 Government and Government-owned entities

There is a myriad of legislation that requires government and government-owned entities to keep records. Of general importance are the National Archives of South Africa Act[14] as well as the Promotion of Access to Information Act.

The ECT Act directs government entities to specify in the *Government Gazette* various matters with respect to the creation, retention or submission of documents or payments. Although enacted before the ECT Act, the Customs and Excise Act,[15] which provides for the levying of customs and excise duties, deals specifically with the keeping and production of electronic records relating to transactions.

2.3 Monitoring and Interception

Much of the legislation requiring the retention and production of records implicitly requires companies to be able to monitor and intercept email going out and coming into their communications systems. In addition, there are other reasons for monitoring and interception.

2.3.1 Spam / viruses

Effective email management tools must include the ability to intercept and monitor email to protect the integrity of communications systems by, for example, detecting and rejecting spam and viruses.

2.3.2 Defamation / harassment / pornography

Because employers are generally vicariously liable for the actions of their employees, employers will need to be able to detect and control the content of email communications, so that they can deal with instances, for example, of alleged or actual defamation, harassment or the sending or receipt of illegal pornography.

2.3.3 Contractual obligations

In addition, a company might have contractual obligations that require it to be able to manage email. Many contracts contain obligations to keep certain information received from other companies confidential. Employers must be able to utilise appropriate tools to effect compliance with such obligations, including the employment of effective email management technology.

2.3.4 Interception legislation

There is current legislation regulating the monitoring and interception of communications, the Interception and Monitoring Prohibition Act.[16] It does not deal specifically with a companies' ability to monitor and intercept email.

Furthermore, there currently is no specific data protection legislation in South Africa, although the South African Law Reform Commission has recently released proposals in this regard.[17] Certain data privacy protections are currently found in the Promotion of Access to Information Act.

Despite this somewhat legal lacunae, there is nevertheless a need to balance the need to monitor and intercept email and the need to protect data.

The newly enacted, but not yet in force, Interception Act deals with the issue. The section 6 exemption to the prohibition on monitoring and intercepting recognises a company's need to monitor and intercept electronic communications – for example, to detect and reject unsolicited and unwanted communications and viruses and to monitor and take action against users who might create unwanted or inappropriate company liability. Such communications may be monitored and intercepted if -

- The purpose of the interception coincides with one or more of the purposes set out in the Act, i.e., monitoring or keeping a record of communications in order to establish the existence of facts, for purposes of investigating or detecting the unauthorised use of a telecommunication system, or in order to secure the effective operation of the system; or monitoring communications to a confidential counselling or support service.
- The interception must be affected by or approved by the system controller, i.e., the CEO or person authorised by the CEO.

- The telecommunication system involved must be provided for use in connection with the relevant business.
- The system controller must use all reasonable efforts in advance to inform employees and those persons with whom employees personally communicate that e-mail may be intercepted; alternatively, such interception must be expressly or impliedly consented to.

Companies must maintain a balance between the imperatives to monitor and intercept electronic communications and the right to privacy. The Interception Act gives guidance on how to do this. Communications systems use polices and email disclaimers should be utilised along with good email management system technology.

2.4 King Report on Corporate Governance - 2002

The King II Report deals with, among other things, directors responsibilities with regard to risk management. It states that when risk management cannot be managed through more traditional internal control mechanisms, risk issues should be addressed using flexible and forward looking mechanisms. The King ll Report also makes clear that directors are obligated to have dealt comprehensively with the issue of risk management.

With regard to accounting and auditing, the King II Report deals specifically with information technology and indicates that directors 'have a responsibility to ensure that an effective internal control system is being maintained'. It also recommends that directors must ensure, inter alia, adequate skills are in place, and that appropriate technology for reporting and transparency is embraced.

Thus, electronic document management is not just a matter of concern for the technology department or the legal department, but is increasing becoming critical to ongoing operations of a business at all levels, including at board level.

3 Key Requirements of an Email Management Solution

The myriad of laws and other obligations (both those discussed herein and those not) must be examined in detail in the creation and implementation of an email management system for any particular company. However, what can be concluded on examination of the legal requirements mentioned herein is that the core requirements of a good management system are as follows –

- The ability to monitor and intercept email
- Effective capturing of all email
- Cost effective storage of all email and efficient discarding of email that has lost its business value or is no longer required for legal or regulatory compliance
- Efficient and cost effective restoration of email
- The ability to maintain the integrity of email and the contents thereof
- The ability to audit email use (and subsequent use) in order to be able to prove integrity

The legal imperatives of an email management system are increasingly integrity and being able to prove integrity.

3.1 Monitoring and Interception

The ability to monitor and intercept email and to do so in line with relevant legislation, such as the Interception Act is a critical component of an effective email management system.

It is important for a number of reasons, for example, in managing unsolicited and unwanted email – sometimes known as spam. It also allows control over the technical operation of the communications system by allowing the detection and deletion of viruses. The ability to intercept should also allow content analysis of email.

A side benefit to being able to monitor and intercept is the discouraging effect on illegal or inappropriate use of email by employees or others allowed to use a company's communications system.

3.2 Capture

A good email management system must capture all outgoing and incoming email as they exit or enter the company's communications system. Email also must be captured and identified in a way that leads to the maintenance of the integrity of the email and the ability to prove integrity. The audit process must begin with capturing.

Software allowing users to send and receive email, although they include some management functions, are by and large inadequate, as the integrity of the email can be compromised easily by individual users.

In addition to capturing email, an email management system must be able to use and control the use of electronic signatures, advanced electronic signatures, cryptology and authentication, in line with the provisions of relevant legislation, including the ECT Act.

3.3 Storage and Deletion

Records should be stored for the mandated period of time, whether the mandate period is imposed by law or is for business reasons. The mandated period of time will differ for different types of documents or information. Further, the mandated period will have to be re-considered from time to time and the management system must be flexible enough to accommodate changes.

After the mandated time period, email should be deleted. This is important for risk reasons and for cost reasons.

Email storage should also be cost effective, avoiding duplication where appropriate, for example with regard to bulky email attachments sent or received by a number of different end users.

It is also important to ensure that the audit process continues throughout the storage life of the email in question, and with regard to deletion of email.

3.4 Retrieval

Without the ability to efficiently and cost effectively retrieve email, an email management system would be worthless.

As with the capturing and storage of email, the process must be auditable and audited. In other words, every time an email is retrieved, audit information must be stored and ideally stored away from the email itself. Even unsuccessful attempts to retrieve email must be audited.

The ability to retrieve email, like the ability to delete email, also should be controlled. This requires adequate policies with regard to who has access to what email, and adequate technology and in particular appropriate search and sort software.

3.5 Integrity

The most important requirement with regard to electronic communications brought about by the ECT Act is that the integrity of electronic communications must be maintained in order for electronic documents to be treated legally like paper based counterparts. Thus, a good email management system must ensure the integrity of email and in particular must comply with the specific requirements set out in the ECT Act with regard to various issues such as signatures, agreements, retention of documents, production of documents and admissibility of evidence.

This will require the adoption and implementation of appropriate policies, email disclaimers and the use of appropriate technology. What is important in developing and implementing an email management system is to understand and remember that the integrity of email must be maintained throughout its lifespan – from capturing, retrieval and deletion.

Another aspect of maintaining integrity is getting control and accountability right. Although the King II Report makes the ultimate responsibility rest with boards of directors, delegations of responsibility must be clear and persons delegated responsibility must be held accountable.

3.6 Auditing / Proof of Integrity

Protecting the integrity of email will be of not much value unless the integrity can be proved. Therefore, audit-ability is important in an email management system.

Ideally, separate records should be kept of auditing functions, and such records should be kept beyond the mandated period for the email in question.

Further, as with maintaining the integrity of email, auditing the maintenance of the integrity of email must be maintained through the lifespan of email.

4 Putting Compliance into Practice

The exact details of an effective email management solution will be specific to a particular organisation, depending on a number of factors, including the specific industry or industries the company operates in. In addition to complying with the relevant rules and regulations, however, there are other important aspects of an effective email management system, including the cost effectiveness of the system and the usability of it. An examination of the existing communications systems as well as the business operations of the company are all integral to finding the right solution.

What is important is not to rush into a quick fix. The solution chosen will not be inexpensive and will impact on every part of the company's operations. Getting it wrong can be very costly.

4.1 Selecting the team and finding a solution

A compliant email management solution will have to be designed and implemented with input by the entire company, from users to the board of directors. The process ultimately though must be the responsibility of the board of directors.

The company will have to choose the most effective team to deal with the various aspects of finding and implementing the right solution.

4.1.1 Legal / Regulatory compliance

The team should include personnel familiar with the legal and regulatory requirements. This would include all of the general requirements in the jurisdictions in which the company

operates as well as specific requirements to the industry or industries in which the company operates.

4.1.2 IT / Security

IT personnel will be critical in the implementation of the technological aspects of the system chosen and therefore are critical to the team. Such personnel should be familiar with existing communications systems as well as with new technology and services.

Personnel familiar with existing security and the security needs of the company must also be included on the team. The needs will have to reconciled with the legal requirements.

4.1.3 Business

In addition to legal requirements with regard to the management of email, there are also relevant business requirements, which makes it important that business operations personnel be represented on the team. Legal and business requirements must be coordinated to create coherent policies.

4.1.4 Financial

Likewise, the cost effectiveness of a solution is important and thus, financial personnel should also be represented.

4.1.5 HR

Policies will have to developed and put in place that will affect the use of email by employees and therefore HR personnel should be involved on the team.

4.1.6 End users

Ultimately, the email management system will have to be used. Thus, it is also important that end users be represented on the team.

4.2 Components of a solution

Ultimately, an effective solution will need to be able to meet the existing requirements of a company and be flexible enough to meet future requirements. It must be integratable into existing communications and IT systems. It also must be cost effective.

The critical component parts of an effective solution will include:

- A document management policy
- A communications system use policy
- Email disclaimers, if appropriate
- Hardware and software capable of implementing company policies and complying with the key requirements, namely
    - The ability to monitor and intercept email
    - Effective capturing of all email
    - Cost effective storage of all email and efficient discarding of email that has lost its business value or is no longer required for legal or regulatory compliance
    - Efficient and cost effective restoration of email
    - The ability to maintain the integrity of email and the contents thereof
    - The ability to audit email use (and subsequent use) in order to be able to prove integrity

5 CONCLUSION

Email is increasingly becoming an essential business tool. The legal requirements are becoming more prescriptive about how we use that tool and how we manage the records that are generated as a result.

For most companies, it will not be enough to rely on existing ways of managing email. Unfortunately, rushing out to buy the latest technology will also not suffice. A company must assemble the right team, examine the issues, including the legal requirements, and find a multi-faceted solution that is right for that company.

References

[1] Electronic Communications and Transactions Act 25 of 2002, www.gov.za/gazette/acts/2002/a25-02.pdf.

[2] The Regulation of Interception of Communications and Provision of Communication-Related Information Act, 70 of 2002, www.gov.za/acts/2002/a70-02/index.html.

[3] King Committee on Corporate Governance, King Report on Corporate Governance for South Africa – 2002, March 2002, see www.iodsa.co.za/ for purchasing information.

[4] Promotion of Access to Information Act 2 of 2000, as amended.

[5] Companies Act 61 of 1973, as amended.

[6] Close Corporations Act 69 of 1984, as amended.

[7] Income Tax Act 58 of 1962, as amended.

[8] Value Added Tax Act 89 of 1991, as amended.

[9] South African Revenue Service, VAT news, No. 20, September 2002, www.sars.gov.za/v_a_t/vatnews/SARS%20VAT%20News%2020.pdf.

[10] Supreme Court Act 59 of 1959, as amended.

[11] Financial Intelligence Centre Act 38 of 2001, www.gov.za/gazette/acts/2001/a38-01.pdf.

[12] Financial Advisory and Intermediary Services Act 37 of 2002, www.gov.za/gazette/acts/2002/a37-02.pdf.

[13] Telecommunications Act 103 of 1996, as amended.

[14] National Archives of South Africa Act 43 of 1996, as amended.

[15] Customs and Excise Act 91 of 1964, as amended.

[16] Interception and Monitoring Prohibition Act 127 of 1992, as amended.

[17] South African Law Reform Commission, Issue Paper 24, Project 124, Privacy and Data Protection, Closing Date for Comments: 1 December 2003, wwwserver.law.wits.ac.za/salc/issue/ip24-01.pdf.