LAW SOCIETY
OF SOUTH AFRICA

An Introduction to Cloud Computing

Legal Implications for South African Law Firms

Version 2

Drafted for the
Law Society of South Africa
by Mark Heyink

An Introduction to Cloud Computing - Legal Implications for South African Law Firms

LSSA Guidelines

VERSION 1.02

MARK HEYINK

Attorney, Notary & Conveyancer
Specialising in Information Law

Table of Contents

Foreword

Please read this foreword carefully.

This guideline has been compiled for the Law Society of South Africa primarily as a tool to assist attorneys in governance and management of eMail.

By its nature the guideline is general, not exhaustive, and intended as a starting point to guide attorneys in their use of cloud computing. This guideline is not intended and must not be construed as establishing any legal obligation. Neither is the guideline intended, nor must it be construed, as providing legal advice.

This guideline is supplementary to the Information Security Guideline and the Protection of Personal Information Guideline published by the Law Society of South Africa which should also be considered in using this Guideline.

Copyright

Chapter 1

1. INTRODUCTION

1.1 The Law Society of South Africa has published guidelines entitled "Information Security Guideline 2011" and "Protection of Personal Information Guideline 2013". This Guideline was originally published in 2012 but has been revised. It is supplementary to the guidelines referred to above, which are available on the Law Society of South Africa website at **www.lssa.org.za**.

1.2 Cloud computing comes in a wide variety of forms. Some of these are quite simple and others significantly more complex. So too the legal issues relating to the use of the cloud take on many varying forms and complexity. The purpose of this Guideline is to assist attorneys to navigate some of the typical legal issues which cloud computing may present.

1.3 Also addressed very briefly, are issues that the use of tablets and Smartphones and the Apps provided for use with tablets and Smartphones, which may be facilitated by servers (in the cloud) outside of South Africa. These devices bring with them wonderful advantages but may present legal problems which may not be fully appreciated.

1.4 With the advent of wonderful new technologies in recent years the furious rate of change of how we apply technology in our daily lives has accelerated. This also dramatically impacts how we process information in our practices. The law, cumbersome slow beast that it is, has simply fallen further behind in addressing the changes that the novel technologies and practises herald. In the case of cloud computing one of the major advantages is the driving down of cost of the availability of excellent computer facilities and applications that would otherwise be beyond the financial means of many practices.

1.5 This having been said, the law relating to the governance of information and communications technologies, its management and use, requires due diligence. In the case of attorneys there are also professional obligations that must be considered. The regulation of an attorney's behaviour to meet these legal requirements and professional obligations relies to a large degree in ensuring that the implications of cloud computing are properly considered and that appropriate agreements are concluded governing an attorneys' use of the technologies.

1.6 The issue of discovery, generally and e-discovery, more specifically also raises certain issues which must be considered in determining whether cloud computing is appropriate for the processing of information by attorneys and whether information processed using cloud computing will be readily available for discovery should this become necessary.

1.7 This Guideline highlights some of the considerations which attorneys should bring to bear in deciding on the appropriateness of cloud computing within their practises.

Chapter 2

2. WHAT IS CLOUD COMPUTING?

The aim of this chapter is to:

- Explain the nature of cloud computing;
- Alert the reader to advantages that cloud computing may hold; and
- Alert the reader that there are potential legal risks in adopting cloud computing.

2.1 As indicated in the Introduction, cloud computing takes on many forms and while there are definitions that have been developed to describe cloud computing, these typically address the more technical issues and will not be particularly helpful in this Guideline. It may be more helpful to describe some of the services that cloud computing offers and the deployment of these services.

2.2 At its broadest level cloud computing is the provision of computing as a service over a network, typically the Internet. These services are usually grouped into the following categories:

- "Software as a service" which allows for the provision of software over a network rather than software being loaded directly onto a locally available computer;
- "Platform as a service" which allows for the provision of a computing platform which in turn allows the environment for other software to run on (for example operating systems) over a network rather than being loaded directly onto a locally available computer;
- "Infrastructure as a service" which allows for the access of a computer infrastructure (for example data storage or processing capability) over a network that is used to complement locally available platform resources.

2.3 The deployment of cloud computing may also occur in different ways, which may also affect the legal consequences of using cloud computing. These include:

- Public Cloud (there is no restriction and any entity or person may access these services);
- Private Cloud (where access is restricted to a single entity);
- Community Cloud (where access is available for a community of entities – for example if the Law Society established services and were only available to members of the various law societies in South Africa which would accessed remotely by attorneys in a Law Society cloud facility);
- Hybrid Cloud (in this instance more than one of the cloud computing models referred to above may operate in conjunction with another and provide a level of interactivity which would not be available outside of the hybrid cloud).

2.4 Cloud computing is not to be confused with outsourcing, although it may have many similar characteristics. Typically with outsourcing control of the services provided may be exercised by having a single agreement with a service provider. This is not always the case with cloud computing.

2.5 What often happens in the case of cloud computing is that entities may establish infrastructure that may be used optimally in certain instances by offering the services to different parties at different times. So it is possible that a particular entity requires significantly more processing capacity at a particular time and that the computers and servers facilitating this capacity are relatively idle at other

times. These entities then hire out this unused computing capacity to parties that may require the computing capacity in most cases at a very favourable cost to the third party. The providers of cloud computing facilities will often take advantage of the low cost computing capacity offered in this manner. However, the computers which provide this capacity may be situate in a myriad of different geographical locations, each of which may be subject to different laws, business practices and government oversight.

2.6 The economies of scale that can be achieved through cloud computing services will in most cases significantly drive down the cost of computing. This makes cloud computing an extremely attractive option for the development of an organisation's computing infrastructure and the ability to acquire computing capacity on demand.

2.7 While the cloud computing option holds many attractions, the complications which may occur as a result of the services being provided from dispirit geographical locations which are subject to different legal jurisdictions may result in unexpected but significant legal consequences and need to be carefully considered in determining whether cloud computing is an appropriate option.

Chapter 3

3. PROTECTION OF PERSONAL INFORMATION

The aim of this chapter is to alert attorneys to:

- Their obligations to protect personal information;
- Information security obligations that are inherent in protecting personal information; and
- The restrictions on trans-border flows of personal information.

Introduction

3.1 Privacy is a constitutional right in South Africa. One of the elements of privacy is the protection of personal information.[1]

3.2 The Protection of Personal Information Act No. 4 of 2013 ("the Act") was enacted on the 26th November 2013. However, while certain of the provisions of the Act have been proclaimed to have commenced, proclamation of the commencement date, many of the operative provisions and in particular Chapter 3, which governs the Conditions for the lawful processing of personal information, is still awaited.

3.3 The importance of the Act on attorneys, who by the nature of their practices process considerable amounts of personal information, cannot be underestimated. What must be recognised by attorneys is that whoever may process personal information on the attorney's behalf, where the attorney is the responsible party as defined in the Act, the attorney remains accountable to the data subject for the lawful processing of the client's personal information and is liable for sanctions that may be imposed by the Regulator.

3.4 Cloud computing offerings may be enormously attractive as they can facilitate the reduction of cost of both software and support and significantly improve the security of the technologies used to process personal information. In many instances both the organisational and technological security which can be provided by cloud providers is simply out of reach of small entities. Thus, for many South African practices (the vast majority of which are limited to 2 or 3 attorneys) the cost and other advantages of cloud computing must not be ignored.

3.5 If cloud computing is an option that a practice wishes to take advantage of, it will be vital that proper consideration also be exercised in determining what agreements need to be concluded with cloud computing providers ("cloud providers"). In doing so the statutory obligation stipulated in Section 21 of the Act, requiring that a written contract be concluded between the responsible party and the operator detailing the security measures that the operator must comply with, is only one of the considerations that need to be brought to bear in determining the terms that would be appropriate in such an agreement. This is more fully dealt with in Chapter 8.

[1] Section 14 of the South African Constitution

Trans-Border Information Flow

3.6 Also of importance in considering the protection of personal information is Chapter 9 of the Act which deals with Trans-Border Information Flow[2], in particular the provision that a responsible party may not transfer personal information about a data subject to a third party who is in a foreign country unless the recipient is subject to a binding agreement which effectively upholds the principles of reasonable processing of the information. Alternatively, that there are adequate laws in place (substantially similar to the provisions contained in the Bill) which afford this protection. If agreements are relied upon by an attorney these must provide for substantially similar Conditions for the Lawfully Processing of Personal Information in South Africa and also include a provision preventing the third party from transferring the information to another foreign country.

Processing of Personal Information in Foreign Jurisdictions

3.7 While the issue of jurisdiction is more fully dealt with in Chapter 5, in the context of the Protection of Personal Information, jurisdiction is also important. In this regard the provisions governing agreements to be entered into between responsible parties and operators and trans-border information flows will require careful consideration.

3.8 It is beyond the scope of this Guideline to deal with the myriad of jurisdictional issues which relating to the processing of personal information. However, it may be helpful to understand how personal information is dealt with in other jurisdictions and with the developments which are occurring in this regard.

3.9 The **USA** does not have a general law of application governing the protection of personal information. Privacy is governed by a proliferation of several sectoral legislative instruments, including without limitation:

- The Gramm-Leach-Bliley Act which is also known as the Financial Services Modernisation Act. This Act requires financial institutions, among other things, to protect the non-public personal information if financial consumers from disclosure and addresses important information security issues.
- The Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH") govern the protection of personal health-related information in the USA.
- Sarbannes Oxley ("SOX"), among many other things, governs internal controls over financial disclosures and the Federal Information Security Management Act ("FISMA") governs how federal agencies are required to protect personal information.
- The Fair Credit Reporting Act ("FCRA") and Fair Accurate Credit Transactions Act ("FACTA") requires consumer credit reporting agencies to implement reasonable procedures that are fair and equitable to the consumer with regard to the confidentiality, accuracy, relevancy and proper utilisation of consumer credit, personal insurance, and other personal information.
- The Children's Online Privacy Protection Act ("COPPA") prohibits websites from processing, using or disclosing of personal information of a child under the age of 13 without obtaining verifiable consent from the child's parent.

[2] Section 72 of the Act

3.10 In addition to the laws referred to in 3.9 there are several other federal laws which govern the protection of personal information and a plethora of State laws regulating the processing of personal information within specific states in the USA.

3.11 One of the reasons that the USA is important in this perspective is the fact that many cloud computing platforms and applications used on tablet and mobile technologies are supported by cloud computing facilities situate in the United States. It should be noted that by the nature of cloud computing, even though the entity might be a USA entity, the support for these devices and applications used on these devices may well be in another jurisdiction. In determining whether these devices may be used for the processing of personal information, care must be taken to ensure that proper consideration of the jurisdiction of not only the entity providing the services but also where the computers are situate that provide the services needs to be established.

3.12 It should be noted that in February of 2012 President Barack Obama introduced the "Consumer Privacy Bill of Rights" to Congress for consideration. In effect this Bill will provide for a general law of application governing the privacy of personal information.

3.13 In March 2012 the Federal Trade Commission published a paper entitled "Protecting Consumer Privacy in an Era of Rapid Change – Recommendation for Businesses and Policy Makers". In essence this report recognises and in many ways supports the concept of a General Law of Application governing personal information being introduced in the USA.

3.14 In the **European Union** there have also been significant developments. The European Union is a leader in the establishment of the Protection of Personal Information principles globally. In January 2012 the European Commission introduced a regulatory framework which is far broader in application and concept than the directives which are currently in place. While many different issues are considered, the issues of primary importance in so far as jurisdiction is concerned is that previously countries within the European Union were required to legislate in terms of directives made by the European Union. It is contemplated that the new European Regulation will apply to all European countries and governs among other things the issues of cross-border transfer of information, policing and enforcement of contraventions of the regulation. This is an important development as it recognises the practical difficulties that have been experienced in the policing and enforcement of legacy legislation between different countries in Europe despite the fact that they are closely bound and related in so many ways.

3.15 The development of a law of general application in the USA and the European Union Regulation highlights the increasing importance that is being assigned to privacy by legislators globally. This is well summarised by the remarks of President Obama in his introductory note to the "Consumer Privacy Bill of Rights". President Obama remarks:

> *"One thing should be clear, even though we live in a world in which we share personal information more freely than in the past, we must reject the conclusion that privacy is an outmoded value. It has been at the heart of our democracy from its inception, and we need it now more than ever."*

Chapter 4

4. JURISDICTION

The aim of this chapter is to highlight issues of jurisdiction and choice of law in implementing cloud computing solutions.

4.1 As globalisation increasing renders our commercial activities borderless the issues of jurisdiction and choice of law have become one of the burning issues in our jurisprudential development globally.

4.2 This is all the more the case when we are dealing with something as portable as electronic information. Thus, in processing information using cloud computing solutions, consideration must be given to jurisdictional and choice of law issues which may be important.

4.3 In considering cloud computing it is important to ensure that a clear understanding of the services, their deployment, both structurally and geographically, and the information security protections employed by a service provider are understood. This should be reflected in the agreement, which in itself may provide important information determining whether the services are appropriate and whether they might lead to potential non-compliance with local legislation or professional obligations.

4.4 In instances where the principal service provider relies on sub-contractors, it may be necessary to obtain the necessary assurance and warranties from the principal contractor relating to the sub-contractors.

4.5 In considering the use in business of tablets and Smartphones, which in many cases may have limited processing power and thus rely on cloud computing services to allow users the functionality they desire, consideration needs to be given to where the processing will occur. Likewise the use of Apps, in many but not all cases, will route processing through particular computers and gateways which may have similar considerations.

4.6 Where the services are provided from third party jurisdictions, consideration of the law governing those jurisdictions is very important.

4.7 A good example would be the United States which has enacted the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intersect and Obstruct terrorism Act 2001" ("the US Patriot Act"). In response to the events of the 11th September 2001 the US Patriot Act has reduced the procedural hurdles that the USA Law Enforcement Agencies and Government need to overcome to secure access to any information held by organizations within the United States. This would include any information which emanates from a foreign jurisdiction but is processed within the United States. Thus, platforms such as the Blackberry Messaging service (BBM) and iServer-type platforms, serving many of the tablets available today, would be subject to this legislation. In certain instances governments and even companies have prohibited the use of this type of service by their employees for fear that sensitive information may fall into the hands of the United States Government or its law enforcement agencies.

4.8 The United States is not alone in efforts to counteract organized crime and terrorism in this manner. Recently the British Government has been considering proposals for similar laws and there are

numerous jurisdictions around the world that are reviewing their cyber security status in order to protect both their own resources and access to information which may assist them in these efforts.

4.9 From the perspective of an attorney in South Africa the potential risk of the processing of information in third party jurisdictions needs to be considered carefully, taking into account the nature of the information that may be processed, and if the information belongs to a client the risks that this type of processing may hold to the client. It must be borne in mind that whatever legislation may be in place in South Africa, over and above legislation, consideration to the professional duty of confidentiality demands that attorneys ensure that information which may be processed by them in using resources which are not directly available under their control, are not subject to confidentiality risks.

Chapter 5

5. INFORMATION SECURITY

The aim of this chapter is to highlight to attorneys their obligation to provide information security and complications which this may present in implementing cloud computing solutions.

5.1 In the Information Security Guideline for South African Law Firms published in 2011 (to which the reader is referred for a greater depth of information), attention is drawn to the attorney's professional duty to implement information security. In this regard it is recognised globally that lawyers have a duty to maintain confidentiality over client communications.

5.2 While our obligations as attorneys may place an even greater obligation on us to provide appropriate information security, there is an underlying obligation on all entities processing information (in both manual and electronic forms) to implement reasonable, organisational, physical and technical measures to safeguard the information. The legal obligation to provide information security is owed by all stakeholders of the entity and globally is increasingly being regarded as a non-negotiable obligation.

5.3 In South Africa the Companies Act requires that directors (and senior executives) perform their functions with the degree of care, skill and diligence that may be reasonable expected of the director having the general knowledge, skill and experience of the director. Further, that the director must properly equip him/herself to fulfil these obligations with the necessary skill. It is suggested that attorneys (even those who are not directors in incorporated practises) take heed of the provisions of the King III Code of Governance Principles for South Africa relating to ICT Governance. One of the obligations which is expressly addressed is the obligation to implement information security.

5.4 Information security is not an end in itself and in order to ensure that the information and communications processed by an attorney meets the provisions governing legal requirements for data messages (electronic records and communications), the provisions aimed at facilitating electronic transactions contained in Chapter III of the Electronic Communications and Transactions Act have to be met. A cursory reading of these provisions highlights the fact that they cannot be met without ensuring an appropriate level of information security.

5.5 Similarly, certain of the obligations imposed in the Promotion of Access to Information Act, the Consumer Protection Act and the National Credit Act, while information security is not explicitly a requirement in these Acts, cannot be achieved without appropriate information security.

5.6 The Protection of Personal Information Bill (once enacted) will be the first legislative instrument in our law which expressly requires the implementation of appropriate information security. This is dealt with more fully in Chapter 4 of this Guideline and in "the Protection of Personal Information for South African Law Firms Guideline" published by the Law Society of South Africa in 2011. Nonetheless it bears repeating that as attorneys the vast majority of the information which we process relating to our clients is personal information and is subject to the provisions of this prospective legislation.

5.7 Bearing in mind the obligations which are currently a feature of our law and the potential complexity of the relationships in cloud computing, the difficulty of ensuring that appropriate information security is established and maintained by the service providers and the many parties to whom these services may be sub-contracted is brought into sharp focus.

5.8 It should also be borne in mind that considering the professional and ethical requirement of maintaining the confidentiality of client information, this may demand that attorneys introduce security measures which are more stringent than those regarded as “Best Practice”.

Chapter 6

6. TABLETS, MOBILE PHONES AND APPS

The aim of this chapter is:

- To draw the attorney's attention to the use of mobile devices; and
- The reliance that mobile devices often place on cloud computing solutions.

6.1 Over recent years one of the most exciting developments in information and communications technologies has been the advent of tablet computers and the vastly improved facility of mobile phones to process and communicate data. Tablet computes and mobile phones are referred to as mobile devices in this Chapter.

6.2 These developments are globally of huge importance as they have exponentially increased the capacity of people around the world to effectively process information and communicate on mobile devices which makes information instantaneously available wherever they are. In the South African context the importance of these developments cannot be overstated. It should be remembered that there are slightly less than 7 million PC devices in South Africa whereas there are approximately 40 million mobile devices.

6.3 The very nature of mobile devices (much smaller and more compact) dictates that the computing capacity of these devices (while significant) does not allow for the type of processing power that operating platforms typically used in PC's provide. The platforms are for the most part cut-down versions but the development of Apps which run on mobile devices allow users to choose the processing that best suits their needs and to download onto the mobile devices. Thus, the ability to customise mobile devices provides extremely effective tools for the user in the processing of information.

6.4 One of the features of many Apps is that while in certain circumstances they may be utilised in a stand-alone form on a mobile device, in many circumstances they facilitate a link to a server or servers which will allow the mobile device to use processing facilities in that server. Thus in many cases by using the computing services provided on the tablet or mobile device as well as the Apps which may be downloaded to the mobile device, in effect the processing of the information is occurring on computers situate in the cloud.

6.5 Thus, while the use of tablet and mobile devices has many important attractions, consideration needs to be given to how these devices may be used in an attorney's practice to ensure that the potential dangers highlighted in this Guideline do not result in the attorney compromising the security and confidentiality of the information, which is the attorney's legal and professional duty to protect.

Chapter 7

7. DISCOVERY AND E-DISCOVERY

The aim of this chapter is to highlight the importance of electronic discover and issues which an attorney may have to agree with a cloud computing service provider to ensure that it can discharge these obligations.

7.1 Attorneys are indebted to Brendon Hughes for his article entitled "The Rise of Electronic Discovery" published in the January/February 2012 De Rebus. This article draws attention to the more important elements of e-discovery and attorneys are referred to this article to gain a greater depth of understanding relating to e-discovery.

7.2 In seeking to comply with the uniform rules of court and Magistrate's Court rules, obligations on litigants to make discovery on oath of all documents relating to any matter in question in litigation and produce such documents for inspection and at trial, all too often the issue of electronic communication is overlooked, or poorly dealt with.

7.3 In many instances important and sometimes critical information will be held by attorneys in electronic form only and these electronic communications may never be printed out before the requirement for discovery. As Mr Hughes points out, these documents are subject to the Electronic Communication and Transactions Act and need to be retained in accordance with the provisions of that Act to counter any challenge to the validity of the electronic communications when adduced in evidence.

7.4 In instances where this information is processed in the cloud, the obligation to discover the electronic communications and the obligation to ensure that the electronic communication meets the requirements of the Electronic Communications and Transactions Act remains unchanged.

7.5 Mr Hughes raises the very important point of the value of meta data. Very often important information relating to the document itself, for instance, when it was created and on what computer it may have been created, when and on what computer it may have been amended, and when it may have been communicated, is retained with the electronic communication. In these circumstances the meta data itself takes on important evidential value. In the 21st century no lawyer should discount the critical evidential value that meta data provides.

7.6 Against this background it is clear that when using cloud computing one of the issues that needs to be considered and where appropriate contractually guaranteed, is that the electronic information processed in the cloud will be processed in a manner which meets with the provisions of the Electronic Communications and Transactions Act and that the information can be readily retained for the purposes of discovery should this become necessary. In addition the retention of all appropriate meta data should also be required.

Chapter 8

8. CLOUD COMPUTING AGREEMENTS

The aim of this chapter is to highlight certain important points relating to agreements which may govern cloud computing and an attorney's obligations in this regard and the terms necessary to be included in agreements with cloud providers.

General

8.1 This Chapter is not intended to be an exhaustive review of the nature of cloud computing agreements and provisions which attorneys should address in considering cloud computing. The nature of cloud computing, the proliferation of different cloud computing models and the multitude of parties who may provide services within those models, militate against this. Nonetheless, it may be useful for attorneys to consider the following issues as a checklist in determining whether the cloud computing services are appropriate to the processing of information and particularly personal information in the conduct of their practice.

European Union Approach

8.2 In providing this guidance, in the absence of the Regulator having been established in South Africa or specific guidance relating to the Act being in evidence, consideration has been given to the directions provided by the European Union in this regard. As the wording of the Conditions for the lawful processing of personal information in Chapter 3 of the Act are materially similar to the principles on which the European Union Privacy Directive is based, the guidance given by the Article 29 Data Protection Working Party, a European Union institution which deals specifically with data protection ("Working Party") will, it is submitted, not only be persuasive but probably authoritative in the South African context.

8.3 In addressing the issue of cloud computing, the Working Party has warned that the imbalance in the contractual power of a small controller (data controller is synonymous with responsible party in our Act) with respect to large service providers should not be considered as a justification for the controller to accept clauses and terms of contracts not in compliance with data law protection. On this basis, given that the responsible party is accountable for the protection of the personal information of the data subject, if it is to use cloud computing services, it must negotiate appropriate terms governing the relationship between it and the cloud provider. Against this background the following issues require consideration.

Terms of Cloud Computing Agreements

8.4 **Accountability.** It must be made clear that the cloud provider can only process the information provided to it by the attorney in terms of the express provisions of the agreement concluded between the parties and ensuring that the cloud provider understands that as the operator, processing personal information on behalf of the attorney as the responsible party, that the processing is circumscribed strictly in terms of the agreement.

8.5 In considering cloud computing services the actual model and who will be processing the information should be disclosed and where necessary service providers contractually bound to not change or use

other services outside of the configuration contemplated. This will allow the proper consideration of whether the processing of the information in the cloud is appropriate and provides the necessary protections.

8.6 Where providers of cloud computing services are unable to provide an agreement for consideration this should immediately raise an alarm that the provider has not considered potential obligations and liability issues, including without limitation, protection of personal information, information security, access to information by third parties, agreements with sub-contractors, record management, business continuity, termination of the agreement and return of information and choice of law.

8.7 Considering the legal issues which this Guideline touches on, any lack of transparency in arrangements with the providers of cloud computing services, however technologically or commercially attractive the services may be, should be treated with great caution.

8.8 **Openness.** Openness is of key importance for the lawful processing of personal information in a reasonable manner that does not infringe the privacy of the data subject. In essence the Openness Condition allows the data subject to have knowledge of who will be processing the data subjects personal information, what mechanisms are available to allow the data subject access to the information and to allow the data subject to correct personal information (which is incorrect), or object to the further processing of the information.

8.9 Openness in regard to cloud computing means that it would be necessary for the attorney to make clients aware that the information is being processed by a cloud provider, who the cloud provider is, locations at which personal information may be processed and the details necessary to allow the client to exercise its rights in terms of the Act.

8.10 **Purpose Specification.** This Condition provides that personal information may only be processed for specific, explicitly defined and lawful purposes and that further processing which is incompatible with this purpose is prohibited. Contracts with cloud providers should include technical and organisational measures to mitigate against this risk and the cloud provider should provide assurances for the logging and auditing of relevant processing operations on personal information, which are sufficient to ensure that the personal information is not processed for another purpose.

8.11 **Retention and Destruction of Personal Information.** The Act provides, save in limited circumstances that include the requirements of law, that personal information must not be retained for any longer than is necessary for achieving the purpose for which the information was collected and subsequently processed. The agreement with the cloud provider should make adequate provision for this Condition to be fulfilled. Thus, it should provide that personal information either be returned to the responsible party for destruction and a certificate be provided that no copies of the information have been retained in any form, alternatively that the personal information is destroyed and a certificate provided evidencing the destruction.

8.12 Allied to this is that during its retention by the cloud provider, personal information be properly safeguarded against unauthorised access, amendment or destruction. This is more fully dealt with in the provisions relating to Security Safeguards.

8.13 **Security Safeguards.** Sections 19 to 22 of the Act deal specifically with the security safeguards that need to be established to ensure the integrity and confidentiality of personal information, as well as notification of security compromises. The provisions expressly provide that the integrity and confidentiality of personal information is protected and appropriate technical and organisational

measures aimed at the prevention of unlawful access or unauthorised destruction of personal information are maintained, in terms of generally accepted information security practices and procedures. As there are international standards and other recognised industry-specific standards governing the security of information, there is more than sufficient guidance as to what would be appropriate in particular circumstances. With regard to cloud providers agreements should address the following specific security issues:

8.13.1 **Availability**. Responsible parties must obtain appropriate assurances from cloud providers that reasonable measures have been established and are maintained to cope with the risk of disruptions, including proper backup of Internet networked links, storage and business continuity and disaster recovery.

8.13.2 **Confidentiality.** In a cloud environment encryption will significantly contribute to the confidentiality of personal information and assurances as to the encryption of personal information "in transit" and "at rest" should be considered. There are also other technical measures which mitigate against breaches of confidentiality. These include authorisation mechanisms, other access controls which should have the appropriate strength in considering the nature of the information which is being processed. Requirements that employees of the cloud provider also conclude appropriate confidentiality agreements should be considered.

8.13.3 **Integrity.** Cloud providers should provide assurances that the information and communication technologies used for facilitating the cloud services ensure against malicious or accidental alteration of information under the control of the cloud provider.

8.13.4 **Transparency.** Cloud providers should afford the attorney or representatives of the attorney reasonable rights to audit or obtain certificates from independent third parties confirming that the assurances provided in the agreement have been fulfilled.

8.13.5 **Isolation.** Where appropriate, and to ensure personal information provided to the cloud provider is not processed with other third party information (personal or otherwise), the responsible party should require assurances that there is proper governance of the information being processed by the cloud provider, as well as technical measures to facilitate the separation of personal information from third party information.

8.13.6 **Access by Data Subject.** The cloud provider must verify that it has not imposed technical or organisational obstacles against data subjects accessing personal information that is being processed by the cloud provider. On the contrary the cloud provider should provide the necessary assurances that there are mechanisms that are established and will be maintained allowing data subjects access to their data in appropriate circumstances.

8.13.7 **Portability.** Agreements should provide that standard data formats and interfaces are used by the cloud provider to ensure that should the responsible party seek to remove the data from the cloud provider that this can be readily ported to another cloud provider for further processing.

8.13.8 **Accountability.** Agreements between attorneys and cloud providers should include the obligation to report to the responsible party immediately a data breach occurs, to be able to facilitate identification of the data breach and its limitation and to cooperate with the responsible party in determining the actions that should be taken to mitigate the damage which may be caused by a data breach.

8.14 **Attorney and client confidentiality** is dealt with in this Guideline in considering privacy and security but it is worth emphasising the professional duty of lawyers to maintain the confidentiality of client information.

Jurisdiction and Choice of Law

8.15 If the operator (provider of cloud computing facilities) is not domiciled within the Republic, the responsible party must take reasonably practicable steps to ensure that the operator complies with the laws, if any, regulating the protection of personal information of the territory in which the operator is domiciled.

8.16 The issue of jurisdiction and problems relating to jurisdiction and conflicting laws are dealt with in Chapter 5. From the perspective of potential agreements it must be point out that "forum shopping" is not possible in relation to certain of our legislation. Thus, choice of law clauses which may make more lenient regulation of another jurisdiction applicable to the contract will not protect a South African attorney, who will remain subject to the laws of South Africa in so far as South African clients are concerned.

Subcontractors

8.17 One of the issues which needs to be taken into account in these circumstances is that the principal cloud provider relies on third parties for the processing of information, the agreements concluded with the cloud provider must also provide assurances that the principal cloud provider will enter into written agreements with its sub-contractors providing services relied on by the cloud provider, securing appropriate back-to-back assurances.

8.18 In theory this may be possible but where cloud computing models are more complex the practicality of obtaining the necessary assurances may prove extremely difficult. Nonetheless, it must be borne in mind by attorneys who wish to use cloud computing services that where personal information is processed they remain the responsible party and accountable to the data subject for any breaches that may occur in the processing of the personal information, regardless of the fact that the compromise is occasioned by negligence of the cloud provider or sub-contractors engaged by the cloud provider.

8.19 Sub-contractors must be identified, if they are processing personal information, and satisfactory assurances must be provided that there are written agreements in place between the principal service provider and the sub-contractor which satisfy the requirement of the Protection of Personal Information Bill.

Protection of Information

8.20 **Protection of personal information** is dealt with in Chapter 3 of this Guideline and needs no further elaboration.

8.21 **Security** is dealt with in Chapter 5 of this Guideline and needs no further elaboration.

8.22 **Record retention and destruction**. Issues of record retention and destruction are particularly important against the background of the legislative requirements which may apply to the information by virtue of South African law, as well as the considerations relating to discovery and electronic discovery which are dealt with in Chapter 7 of this Guideline.

8.23 **Audit** arrangements may be appropriate to ensure that the privacy and security contemplated in the provisions protecting the information are properly established and maintained through the term of the agreement.

Performance Management

8.24 Service levels should be agreed and appropriate provisions included in the agreement to allow for the measurement and enforcement of the service levels.

8.25 Response times and guarantees of uptime should be part of the service level arrangements.

Business Continuity and Disaster Recovery

8.26 One of the information security obligations of an attorney is to ensure that a client's information is not compromised by virtue of either the attorney or service providers to the attorney having their business interrupted or going out of business. In the context of electronic information issues of backup, offsite storage of documentation and disaster recovery arrangements are important in this context. While provisions governing business continuity and disaster recover should be a feature of any outsourcing arrangements where the attorney may lose direct control of the information, in the context of cloud computing this becomes even more important, considering that there may be different levels of processing. The complexity in this regard will be one of the considerations which must be brought to bear in considering whether cloud computing is appropriate for processing of the particular information.

Microsoft's Status as a Cloud Provider

8.27 While there is no intention to promote the products and services of Microsoft above those of any other service providers, in light of the fact that many South African practitioners use Microsoft products it is worth noting that the European Union Article 29 Data Protection Working Party concluded that the Microsoft agreement *"Enterprise Enrolment Addendum Microsoft Online Services Data Processing Agreement"* complies with the standard contractual clauses required by the European Union in dealing with transborder information flows.

8.28 The Working Party states that in practice, this will reduce the number of national authorisations required to allow the international transfer of data (depending on the national legislation).

8.29 It is understood that in contracting with Microsoft for the provision of its cloud computing services it is possible to contractually restrict the transfers of data to within the European Union. As South African law is materially similar in wording and identical in intent to the European Union Privacy Directive of 1995 on which the national laws of European Union members are based, the wisdom of ensuring that the processing of personal information is restricted to South African and the European Union provisions, subject to the Act and the privacy laws of European Union members, appears obvious.

Chapter 9

9. CONCLUSION

9.1 While exploring the advantages of novel technologies and how they may improve the services that we provide to our clients as well as how we may become more competitive in the provision of our services, as with most novel technologies and the application of these technologies, care must be taken to ensure that risks attendant on the use of the technologies can be avoided.

9.2 Cloud computing and portable devices, the application of which is supported by cloud computing, brings into sharp focus some of the legal issues which are taxing jurisprudential systems globally. Attorneys are well advised to not discount the huge advantages that evolving technology brings to our profession, which has at its core the processing of information, but equally to consider carefully what risks these novel technologies may hold.