White Paper

Improved Delivery and Management of Critical Information:

Solicitors Regulation Authority Compliance

Author	:	Ben Martin
Document Number	:	WHP-1010
Revision	:	V2.2
Issue Date	:	January 2015
Copyright	:	© 2015 Safe4 Information Management Limited

Safe4 Information Management Limited

1 Kingsmill Park
London Road
Loudwater
Buckinghamshire
HP10 9UB
United Kingdom

☎ +44 845 094 8045
@ enquiries@safe-4.co.uk
www.safe-4.co.uk

Safe4 Information Management (Africa) (Pty) Ltd

Building No 2, Pinewood Office Park
33 Riley Road
Woodmead
Johannesburg
PO Box 555
Strathavon 2031
South Africa

☎ +27 11 234 2563
www.safe-4.co.za

Contents:

1. Introduction

A recent SRA paper [1] recognises that cloud computing can provide security and cost benefits for the law firm and its clients.

> *"The use of cloud computing can improve general data security. Data service providers will usually have more experience in protecting data than their clients will, and have access to stronger security and encryption."*

One area for law firms to take quick advantage of cloud technology is in secure online document delivery and storage services. Removing the need for insecure email, providing secure, audited access to documents from any location and enabling better communication with clients and other lawyers are strong reasons to engage with an online document service. Using an effective outsourced provider to supply these services is permitted under the SRA code of conduct and the SRA identifies risks and compliance issues for the law firm to manage in its use of cloud computing.

Safe4's document delivery and storage service addresses these issues and is a silver lining for law firms seeking efficiencies from working in the cloud. As a secure and compliant partner ***Safe4*** can reduce costs and improve security for document sharing with other law firms and clients.

[1] Solicitors Regulation Authority (SRA) Risk Centre paper "Silver Linings: cloud computing, law firms and risk" November 2013

2. Controlling Risk

In requiring solicitors to keep the affairs of clients confidential[2] the SRA notes that this does not prevent firms outsourcing services, for example to cloud computing service providers. Although cloud computing can involve risks to regulatory objectives in the Legal Services Act 2007, it can also help to control risk. When it comes to information or document sharing, the SRA identifies a number of areas of concern, including:-

- Theft or loss of mobile devices including laptops and USB drives. Cloud storage reduces the need for storing data on these vulnerable devices.
- USB drives are also particularly vulnerable to spreading viruses and other malware. Eliminating them provides a general improvement in data security.
- Transmitting working files or other documents by email is an inherently insecure form of data transmission.
- Public Wi-Fi is not guaranteed to be secure.

Using a reputable cloud based document storage and delivery provider, such as ***Safe4***, eliminates these concerns. With ***Safe4***, all documents are encrypted and held securely at UK based data centres complying with the key information security standard ISO 27001 2005. All users access documents through a secure SSL login via their internet browser (to prevent eavesdropping) with password and optional PIN. Confidential documents are held securely in the cloud, reducing the need to store them on vulnerable laptops, USB drives or other mobile devices.

In terms of general work efficiency, the use of an internet accessible document store by all participants – lawyers, paralegals, professional advisors, clients and others – can ensure that all parties are referring to the same versions of documents, reducing the risk of error.

In using such cloud based services, the law firm is still responsible for monitoring risks[3] and requires an enforceable agreement with the provider contracting to the relevant security and compliance measures. The SRA suggests this is one reason why free public cloud services will not generally be suitable for confidential client information.

[2] SRA Code of Conduct: Outcome 4.1
[3] SRA Code of Conduct: Outcome 7.3

3. Contracting for Compliance

Law firms are expected to establish clear contractual agreement with cloud providers to provide a framework around regulatory compliance as well as the management of security and other risk. The key aspects of this identified in the SRA paper are:-

- **SRA access**: The law firm should have terms in the agreement allowing the SRA to access information stored[4]. To be effective, the SRA asks for such terms to be binding notwithstanding any dispute between the law firm and cloud provider or any breach of the agreement on the part of the law firm.
- **Data Centre security**: The agreement should identify specifically what the security measures for the data centre must be. These may be included in an ISO 27001 compliant process.
- **Data Centre Location and Reporting**: It is advisable that the agreement requires the provider to report any requests for confidential information from third parties and any security breaches. This may be complicated by the location of the Data Centre and any local laws which apply to the provider. The best solution for a UK based law firm is to have all data securely held in a UK data centre and within UK jurisdiction.
- **Loss of data control**: The agreement should confirm that law firms retain full ownership of information stored and have the right to get back data in a usable format on demand. The agreement should identify data back-up frequency and data availability in the event of provider business failure.
- **Downtime**: Advisable that the agreement identifies what redress is available to the law firm in terms of (excessive) downtime.

These requirements are all incorporated in the ***Safe4*** Professional Practice Agreement for law firms and other bodies subject to SRA regulation and associated Service Level Agreement (SLA).

[4] SRA Code of Contact: Outcome 7.10

4. Data Protection Act 1998 (DPA)

Law firms have to comply with the DPA, which allows data to be transmitted to an outsourced (cloud) provider. However, personal data storage demands a written contract to be in place requiring the provider to act only on the law firm's instructions. Also the DPA asks for the provider to have a level of security meeting the information security provisions of the *seventh* principle of the DPA, essentially measures against unauthorised access and against accidental loss or destruction of or damage to personal data.

These requirements are covered in the operational design of ***Safe4*** and in the ***Safe4*** Professional Practice Agreement for law firms.

The *eighth* principal of the DPA states that personal data may not be transferred to a country outside the European Economic Area (EEA) unless the country meets particular safeguards and maintain a "Safe Harbour" status with the EEA. The USA is the prime country of concern in this respect as weak US protection for personal data, the provisions of the PATRIOT act and recent developments involving NSA access to data have evidenced. Recently the EU Justice Commissioner spoke of the need to strengthen Data Protection throughout Europe [5] and included particular reference to the need for the USA to strengthen the Safe Harbour process or have it suspended.

The implication of this is that the law firm should know in which jurisdiction their data is stored and manage risk accordingly. There should be particular concern if a provider uses USA jurisdiction data centres. The least risky situation is generally to have data stored in the UK under the jurisdiction of English. This is the solution adopted by ***Safe4*** under their standard agreement which uses a "UK cloud" from a world leading supplier incorporating UK data centres with ISO 27001 2005 and other certifications. English law applies.

[5] Viviane Reding, EU Justice Commissioner: A data protection compact for Europe: 28 January, 2014. http://europa.eu/rapid/press-release_SPEECH-14-62_en.htm

5. Law Firm Security Responsibility

In addition to having a SRA compliant contract with an outsourcing "cloud" supplier in a suitable jurisdiction, a law firm entrusting documents to such storage and delivery services still has to manage its internal administration in a compliant and security conscious manner.

There should be suitable procedures to manage the security of and access to documents held within the law firm's own operating environment, including proprietary practice or case management software. These procedures should be reviewed against the enhanced security offered by the outsourced provider. Areas for consideration should include:-

- Proper authorisation procedures for users, including their permissions to access documents and act on them.
- Application of normal confidentiality precautions such as regularly changing passwords and not writing passwords down to avoid unauthorised access.
- Restrictions on use of insecure email for sending documents.
- Eliminating where possible the use of USB drives or similar temporary storage devices and, where used, to ensure data is encrypted on these devices.
- Requirements to password protect mobile devices including laptops.
- The ability to audit access to documents.

6. The Need for Encryption

The Information Commissioner has consistently stated, over the years, that it is not appropriate for customer data to be taken offsite on laptops or other portable devices which are not encrypted[6]. This guidance has been reinforced, not just by the SRA, but also by the Financial Services Authority / Financial Conduct Authority (FSA / FCA) and it extends to the need to consider encryption for emails and email attachments depending on the level of confidentiality.

A compliant online document delivery and storage provider, such as ***Safe4***, will use a Transport Layer Security (TSL) connection to the internet to take the document securely offsite from the Law firm systems. This effectively provides a security tunnel through the internet to the provider's data centre, where an encryption process should immediately take place. When an authorised user seeks to access a document, the exact reverse process takes place to deliver the decrypted document to the user's workstation, laptop or other device.

The SRA also recognises there may be situations where it is advisable that a document is encrypted within the law office and this can be done with a range of proprietary technology. This will mean that any authorised user will also need decryption keys in addition to standard Username / password / PIN access to the online document provider.

All document files uploaded to ***Safe4*** are encrypted immediately they reach the server, after being virus-checked.

[6] http://ico.org.uk/news/current_topics/Our_approach_to_encryption October 2012 et al.

7. Summary

Outsourced Cloud Computing solutions can deliver information security and cost benefits to law firms and their clients, particularly in relation to secure online delivery and storage of documents. This methodology bypasses inherently insecure email transmission and helps avoid the risks of theft and loss associated with mobile devices including laptops and USB drives.

For regulatory compliance, the SRA requires the law firm and outsourced cloud provider to enter an appropriate contract which includes data ownership, SRA rights of access to data and various data centre security commitments including the jurisdictional and physical ability to report on information requests and security breaches. With increasing concerns about USA data security law and European requirements to upgrade data protection, UK data centre location provides the lowest risk for UK law firms and their clients.

Safe4 secure online document delivery and storage, in conjunction with appropriate law firm internal security measures, provides a compliant and secure solution to allow UK law firms to take advantage of the business benefits of working with the cloud delivering efficiency, security and cost improvements.

8. Additional Information

SRA Code of Conduct principles

As a law firm, you must:

1. uphold the rule of law and the proper administration of justice;
2. act with integrity;
3. not allow your independence to be compromised;
4. act in the best interests of each *client*;
5. provide a proper standard of service to your *clients*;
6. behave in a way that maintains the trust the public places in you and in the provision of legal services;
7. comply with your legal and regulatory obligations and deal with your regulators and ombudsmen in an open, timely and co-operative manner;
8. run your business or carry out your role in the business effectively and in accordance with proper governance and sound financial and risk management principles;
9. run your business or carry out your role in the business in a way that encourages equality of opportunity and respect for diversity; and
10. protect *client* money and *assets*.

9. Data Protection Act 1998: Principles

Schedule 1 to the Data Protection Act lists the data protection principles in the following terms:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

   (a) at least one of the conditions in Schedule 2 is met, and

   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

End of Document

If you have any comments on this document, or if you would like to discuss any of its contents with *Safe4*, please visit our website:

- **Articles:** http://safe-4.co.uk/blog/
- **Contact:** http://safe-4.co.uk/contact/

www.safe-4.co.uk
ben.martin@safe-4.co.uk