Cloud Computing Due Diligence Checklist

✓ TERMS OF SERVICE

- ☐ Does the cloud computing provider have a clear and accessible Terms of Service and Privacy Policy?
- ☐ What uptime does the vendor guarantee as part of their Service Level Agreement?
- ☐ Is there an initial setup fee?
- ☐ Is there a cap or limitation on the cloud provider's ability of service? (bandwidth caps, storage limits, etc.)
- ☐ Are there additional usage or bandwidth fees?
- ☐ Does the cloud provider recognise and agree to abide by the duties of lawyer/client confidentiality?
- ☐ Does the cloud computing provider explicitly recognise your ownership of any intellectual property?
- ☐ Does the cloud provider have a contractual obligation to notify you of any demands for client information in time for you to intervene?

✓ BACKUP OF DATA/BUSINESS CONTINUITY

- ☐ Are you able to easily retrieve your data from the cloud computing provider?
- ☐ Are you able to maintain a local backup of your data?
- ☐ Is the retrieved data in a usable, non-proprietary format?
- ☐ Does the cloud provider have documented (and tested) business continuity/disaster recovery procedures?

✓ GEOLOCATION

- ☐ Where are the cloud provider's servers located?
- ☐ Does the cloud provider have multiple storage locations—and if so, how often are they synced?
- ☐ Does the cloud provider provide you a means to satisfy any data residency requirements (if applicable)?

✓ REASONABLE SECURITY

- ☐ Has the cloud provider implemented controls to reasonably prevent unauthorised access or disclosure of information, including penetration testing?
- ☐ Does the cloud provider offer features to provide user authentication and prevent unauthorised access? *(Ex: Two-factor authentication, IP monitoring, strong password requirements, role based access control, etc.)*
- ☐ Does the cloud provider employ encryption at rest and in transit to protect your data?
- ☐ How often does the cloud provider have their security audited (ad hoc, annually, other)?
- ☐ Will the provider allow you to obtain copies of any security audits performed?
- ☐ Does the cloud provider offer support/remedies in the event of data breaches and service availability failures?

✓ TERMINATION OF SERVICES

- ☐ Are there any additional costs or penalties for terminating the cloud computing service?
- ☐ Will your information be returned/deleted by the cloud provider upon termination?
- ☐ Can your data be sanitised from the cloud provider in the event of termination?

✓ ADDITIONAL CONSIDERATIONS

- ☐ Does the cloud provider integrate with your other office systems?
- ☐ Have you evaluated the cloud provider's history, including how long the provider has been in business, and funding and stability?

Have more questions about evaluating cloud solutions for your firm?

Read our free article *The Quick Guide to Cloud Computing for Law Firms*