

Cloud Computing guide 2024

13 March 2025  Jeanne Kelly

This was first published on [Chambers and Partners](#)

Jeanne authored the 2024 Chambers Cloud Computing Global Practice. The Guide explores the key legal considerations that businesses must consider when using cloud computing services, including compliance with data protection and privacy laws, the protection of intellectual property rights, and the negotiation of effective cloud computing contracts.

Browne Jacobson (Ireland) is pleased to present the Chambers Cloud Computing Global Practice Guide. Our team of experienced lawyers has extensive knowledge of the legal issues surrounding cloud computing and has advised numerous clients on these matters. In recent years the legal landscape has undergone a digital revolution by moving towards the use of cloud systems.

Cloud computing has become an essential part of modern business operations. Instead of data being stored on hard drives and local computers as in the past, remote servers are used. Cloud applications are often referred to as “web services” or “hosted services”, but here we simply use the term cloud services.

Cloud services might be hosted by a third party (eg, Microsoft) or, by a provider which runs its services on Microsoft, or another data centre provider.

It is a delivery model for IT services to store data on remote servers owned or controlled by third parties usually on the internet or via private networks. These remote servers are usually hosted in data centres across the world, and provide for the distribution of computing power, increased storage capacity, and provides fast delivery and on-demand bandwidth. The cloud model is very attractive in that it enables companies to meet their ever-growing IT needs with smaller capital expenditure and less reliance on their IT departments. However, the use of cloud computing also brings with it a range of legal and regulatory issues that businesses must navigate. These challenges include data protection and privacy, intellectual property, and contractual issues.

In this guide, we aim to provide businesses with a comprehensive understanding of the legal issues surrounding cloud computing in the covered jurisdictions. We will explore the key legal considerations that businesses must take into account when using cloud computing services, including compliance with data protection and privacy laws, the protection of intellectual property rights, and the negotiation of effective cloud computing contracts.

Our team of lawyers have a deep understanding of the legal and regulatory landscape surrounding cloud computing. We have advised clients across a range of industries, including healthcare, finance, and technology, and have helped them navigate the complex legal issues associated with cloud computing.

We hope that this guide will be a valuable resource for businesses looking to use or are currently using cloud computing services. We believe that by providing businesses with a comprehensive understanding of the legal issues surrounding cloud computing, we can help them make informed decisions about the use of cloud computing services and to manage the associated risks effectively.

We also look at issues contained in cloud providers' (including VARs or Value-Added-Resellers) contracts with their customers, to ensure that customers are adequately protected from the legal risks inherent in cloud service usage. That said, there are benefits, including enhanced back-up and disaster recovery, and the increased data handling capacities these services offer, which are noteworthy and should be factored in by customers in any legal/risk analysis.

Legal challenges posed by Cloud Computing

Data sovereignty

When data is stored on remote servers across different jurisdictions, it can raise concerns about data sovereignty and jurisdictional conflicts.

Data protection and privacy

One of the key legal issues surrounding cloud computing is data protection and privacy. Businesses must ensure that they comply with data protection and privacy laws when using cloud computing services. This includes ensuring that personal data is processed in accordance with the relevant data protection laws.

General Data Protection Regulation

When using cloud services, businesses need to consider the key principles of the GDPR, including:

- data minimisation;
- purpose limitation;
- data accuracy;
- accountability;
- lawfulness, fairness, and transparency;
- storage limitation; and
- integrity and confidentiality.

Businesses must also ensure that they have appropriate data protection and privacy policies in place when using cloud computing services. These policies should set out how personal data will be processed, who will have access to the data, and how the data will be protected.

In addition, businesses must ensure that they have appropriate contractual arrangements in place with their cloud computing service providers. These contracts should set out the responsibilities of the service provider in relation to data protection and privacy, and should include appropriate data protection and privacy clauses.

Consideration should be given to whether you need to prepare a DPIA (Data Protection Impact Assessment) for the cloud service, which may be a requirement under applicable laws, or as a matter of good practice.

Compliance

When companies move their information to the cloud, they must ensure they are compliant with service laws and regulations – this can create hurdles in cloud storage and back-up services.

Intellectual property

Another key legal issue surrounding cloud computing is intellectual property. Businesses must ensure that they protect their intellectual property rights when using cloud computing services. This includes ensuring that they have appropriate intellectual property policies in place, and that they have appropriate contractual arrangements with their cloud computing service providers.

Businesses must also ensure that they have appropriate measures in place to protect their intellectual property when using cloud computing services. This may include implementing appropriate access controls, encryption, and other security measures.

Contractual issues

Finally, businesses must ensure that they negotiate effective cloud computing contracts with their service providers. These contracts should set out the responsibilities of the service provider and should include appropriate service level agreements (SLAs) and other contractual provisions. Liability issues are key and go to the pricing of the underlying service. Liability caps, and exclusions from them, are a key consideration as market practice evolves in this area.

Businesses must also ensure that they have appropriate exit strategies in place when using cloud computing services. This may include ensuring that they have appropriate data back-up and recovery procedures in place, and that they have appropriate termination clauses in their contracts with their service providers.

Other issues which are core to good governance in selecting and contracting with a cloud provider include:

- access to the stored data for customers;
- access to the stored data for law enforcement;
- liability issues, including for any failure of service;
- service levels and service credits;
- jurisdiction and governing law;
- use policies;
- insurance matters;
- renewals and notice periods;
- subcontracting; and
- transitional arrangements when service migration is to occur.

Summary

Cloud computing has become an essential part of modern business operations, providing organisations with an efficient and cost-effective way to store, process, and manage data. However, the use of cloud computing also brings with it a range of legal challenges that businesses must navigate.

In this guide, we explore the key legal issues surrounding cloud computing, including data protection and privacy, intellectual property, and contractual issues. We provide practical guidance on how businesses can navigate these issues effectively and highlight the importance of having appropriate policies and contractual arrangements in place when using cloud computing services.

We hope that this guide will be a valuable resource for businesses looking to use cloud computing services, and that it will help them to make informed decisions about the use of cloud computing services and to manage the associated legal risks effectively.

Key contact

Jeanne Kelly

Partner

jeanne.kelly@brownejacobson.com

+353 1 574 3915

Related expertise

Data protection and higher education

Data protection and privacy

Data protection for retail

Data protection guidance for schools and trusts

Digital and data

Intellectual property