Navigating your way to the cloud

# Getting Started:

# Key questions to ask

Organisations all over Europe —from small business owners to large global corporations —are embracing cloud-based services in an ongoing drive to cut costs and alleviate the complexity of onsite IT management. Cloud computing is rapidly becoming the dominant new paradigm for enterprise IT, with cloud-based technologies offering companies the opportunity to drive the growth and innovation they require to compete. Such digital transformation understandably raises questions about data security, privacy, service reliability and legal and regulatory compliance.

For in-house legal and compliance staff, it may not always be clear exactly how cloud services differ from more traditional outsourcing models, nor how they should evaluate the benefits and risk involved. The goal of this paper is to help you consider some of the fundamental questions that are raised by the shift to cloud computing.

## 1. What data is involved?

It’s critical that every customer considering moving their data to the cloud maps out exactly what types of data their organisation uses and creates.  Certain data may be particularly confidential or sensitive. Different industries will categorise and value types of data in different ways, but all customers certainly must determine whether the data is personal data or is not.

GDPR widely interprets the term personal data and sanctions for abuse are high so it’s wise to consider this initial issue very carefully. Whether the data is personal or not, you will still want to consider the importance of confidentiality over the data.

**Learn more about how Microsoft can help you comply with GDPR:**

**GDPR Compliance**

## 2. How and where will your data be stored and managed?

Certain laws and regulations will require, at a minimum, that you have transparency on how and where specified data is transferred, stored and processed. As such, you should require that your cloud provider be clear about where their data is stored, where it is backed-up, and from where it is accessible. Hyper-scale cloud storage is complex and service providers will sometimes make territorial decisions about their data centers and data storage architecture.

Similarly, it is important to understand how your cloud provider may use your data. Will it be mined for advertiser-supported services? Do you know what sub processors may be used? Do you know how your cloud provider will respond to third party requests for your data? Simply knowing your data is “in the cloud” is not going to be an adequate answer to your board or any regulator concerned with understanding how and where your data is stored.

**Learn more about Microsoft's approach to managing your data:**

**Data Management**

## 3. What laws and regulations apply?

In addition to the general laws of data protection that affect everyone storing personal data, your sector may have specific regulations relating to how you must treat data stored in the cloud. It's increasingly rare for governments or regulators to wholesale block or ban the use of cloud services in their region, but it is not unusual for regulators to have particular rules or considerations when data is stored and processed in the cloud.

The Financial Services regulations are probably the most comprehensive across all of the sectors in providing special rules of how the cloud should be utilized by financial services firms. In contrast, the retail sector has few, if any, industry laws that apply specifically to their cloud activities.

You will know if you are already regulated on a sector-basis and will need to determine what conditions, if any at all, might apply to your cloud engagement. Such conditions may involve a requirement to seek prior approval or notification from your regulator. Often your regulator will provide its views on cloud adoption and you should obviously avail yourself of those published views.

**Learn more about industry-specific regulations across Europe:**

**Legal & Compliance Site**

## 4. What general or industry-specific standards or certifications apply?

Whether regulated or not, you will be aware of and might currently comply with certain industry standards. These might be in Codes of Conduct signed-up-to as part of an industry body; they might be related to say, using credit cards, or they might be more national and international standards such as ISO or BSI standards.  The right cloud technology can help you with tools to comply with such standards and certifications, such as Microsoft's Compliance Manager.

Additionally you will look for your cloud provider to build their technology in a manner which aligns to the standards and certifications applicable to you and your industry and will actually help you to run your organization in a compliant manner. Cloud providers should be looking to offer a rich set of compliance offerings to help you meet these needs.

**Learn more about Microsoft's compliance offerings:**

**Compliance Offerings**

## 5. What about the cloud services contract?

As with any technology outsourcing arrangements, you will look for certain terms to be reflected in the contract with your cloud services provider. Some of these will be required for you to meet key legal and regulatory requirements, for example, the privacy and data protection terms must reflect the requirements of GDPR. Additionally, you may seek terms mandated by your industry's applicable regulation or standards.

Outside of such required terms, the cloud contract is like any other important contract with a supplier and you should take care to ensure that key provisions are appropriately covered. Service Levels; data management; liability; termination and data portability are all examples of provisions that should be covered to your satisfaction while recognising that the standard nature of cloud services can require a uniform contractual approach from cloud providers on many of these topics.

**See the key contractual provisions for Microsoft's enterprise cloud services:**

**Online Services Terms**