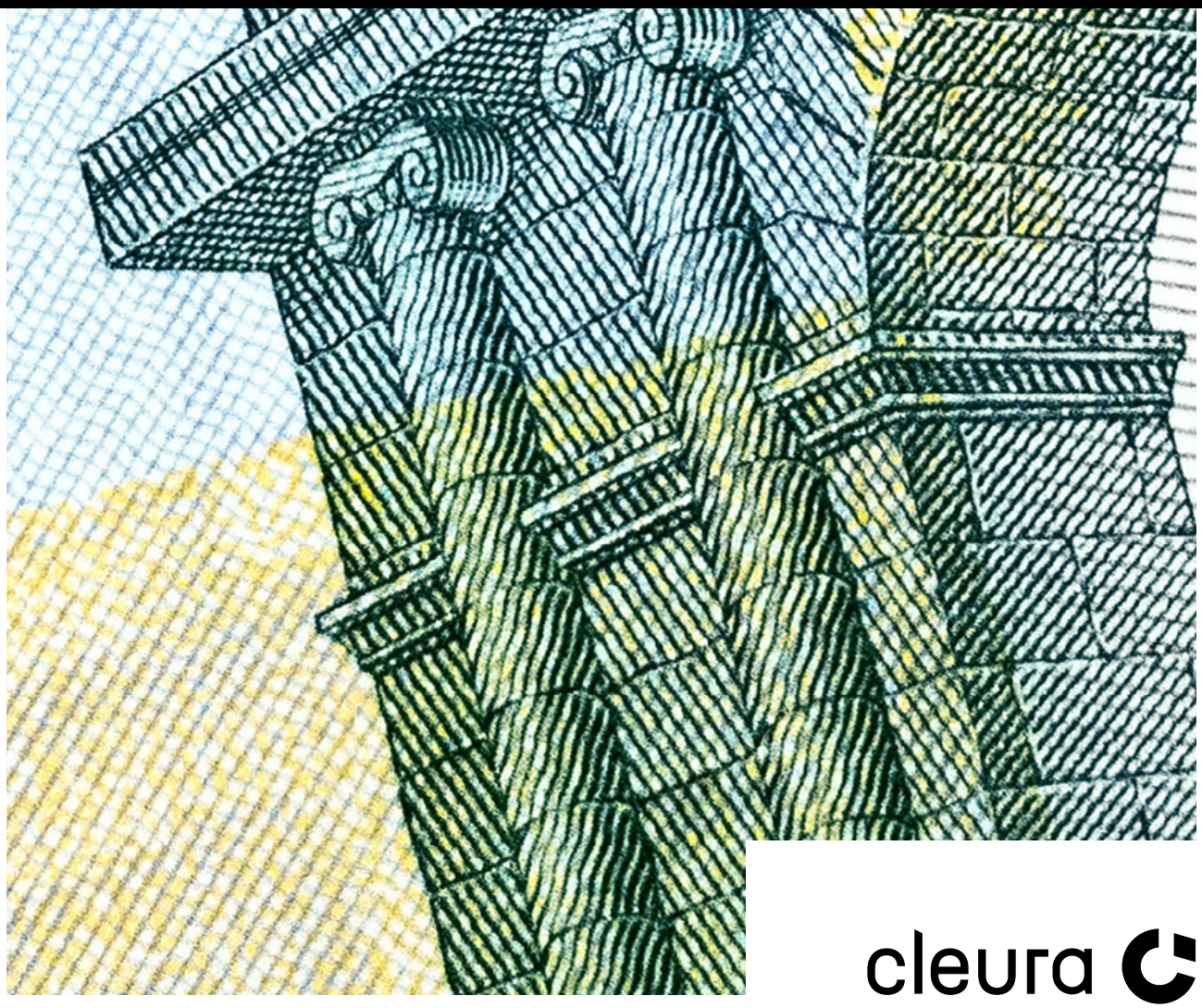
WHITEPAPER

Regulatory aspects to consider when comparing cloud providers



cleura

Introduction

Cloud services for digital infrastructure are at the very heart of the digital transformation. As with other critical public infrastructure, cloud services are subject to a variety of legal frameworks. The use of cloud services often involves compliance with laws and regulations from several countries, and this is when things can become complicated. This white-paper aims to help highlight the issues and processes that cloud services purchasers should consider in order to ensure adequate regulatory compliance.

Comparing apples with apples

When comparing different cloud providers, be careful to evaluate the same qualifications of potential providers in terms of technical, legal and compliance aspects as well as service level agreements (SLAs) and price.

A "Standard Contract," also defined as "General Terms and Conditions" in a public cloud, is the simplest form of agreement between a user and a cloud provider. The General Terms and Conditions state the fundamental purposes and expectations of the service and define the relationship between the end user and the provider.

The General Terms and Conditions relate to the public price list available from the public cloud provider. This is the most basic form of contract, outlining a standard level of compliance, liabilities and SLAs.

Organizations that store particularly sensitive and restricted information are almost always subject to more stringent regulatory demands than those offered in the General Terms and Conditions. The General Terms and Conditions are as the name itself suggests, general, and do not as a rule comply with the protection level or the rules that companies in banking and finance, healthcare and government and other public sectors apply to themselves and their affiliates, sub-contractors and service providers. These types of organizations require a direct contract with the cloud provider, stipulating more rigorous demands in regard to compliance, SLAs and the ability to perform on-premises audits on an annual basis.

Almost all public cloud providers can draw up a direct contract to meet such requirements, one way or another. One of the most important aspects for you, the customer, is to be aware of the price. As your demands increase, so does the price. The challenge is to identify the appropriate level for your organization while ensuring compliance with laws and regulations.

Risk assessment

All stakeholders involved in the service delivery chain must make their own risk assessment based on the customer/business demands placed on security, compliance and liability claims in conjunction with the relevant service.

A risk assessment should cover:

- Data storage locations
- Data transfer points
- Administrator access
- Conflicting data laws in different countries or regions
- Legal entity of the cloud provider
- Country of legal settlement
- Sub-contractors and affiliates

How to make sense of international data laws

A number of data protection laws and regulations are currently in force across the globe that affect an organization's ability to utilize international cloud services and IT services in general. One of the issues lies in the fact that cloud service providers – and users alike – want data to be available from any corner of the world at any time. At the same time, these services are being provided in a world where data transfer and data protection laws still vary considerably from country to country or continent to continent, and sometimes are in direct conflict with one another.

One simple starting point is that data legislation in the cloud service provider's country of domicile applies. For example, a US cloud service provider with data centers in Sweden is subject to US data protection law as the owner is not domiciled in Europe.

General points about data storage and data transfers from an EU and GDPR perspective

- Where data is geographically stored is important, but who can access the data is equally important. The US Foreign Intelligence Surveillance Act (FISA 702) regulates the collection of data for purposes related to national security. A number of judicial bodies have found FISA 702 to be extraterritorial. This means that even if data is stored in Sweden at a Swedish company, if this company is owned by a US company then FISA 702 should be considered.
- International administrative access to data stored, for example, in Sweden is treated as an international data transfer.
- The provider's legal domicile may be problematic, if the country's laws are in direct conflict with laws in the EU. A company with legal domicile in the EU has no choice but to comply with EU rules and the General Data Protection Regulation (GDPR).
- US providers must also comply with EU rules in order to provide services in Europe, but must also consider US law. This includes laws that are in direct conflict with GDPR.

Penalties

The penalties for compromising or breaching the personal data of employees or customers are quite severe under GDPR. As described in the legislative text, the penalties are as follows:

Minor breach: 2% of annual revenue or EUR 10 million (whichever is higher)

Major breach: 4% of annual revenue or EUR 20 million (whichever is higher)

The penalties are imposed per case and include both affiliates and subsidiaries to the parent company. Examples of enforcement can be found at www.enforcementtracker.com.

In addition to penalties, the credibility of operations is naturally at risk toward employees, customers and other interested parties, which may result in even greater financial damage.

Questions to ask when evaluating a cloud provider and drafting a contract

Are you allowed to visit the cloud provider's sites and perform your own audits?

Due to potential differences in Statement of Applicability (SOA) for ISO 27001 between you and your supplier, it is necessary to validate that the information security chain remains intact. In short, your organization bears full responsibility for assessing risks related to the cloud provider. In turn, this requires the establishment of a direct agreement to allow for such audits, which is the case for all cloud providers.

Is the entire chain of administrators covered by confidentiality agreements and have appropriate background and screening checks been conducted and passed?

Every nation has a set of requirements to which every individual who has access to classified data is subject. As a data processing organization, it is your responsibility to ensure your cloud providers comply with these requirements. Agreements must allow for checks to be performed of all relevant staff of the cloud provider, or that you can verify that the cloud provider has performed the checks and controls This must be done for each individual and cannot be covered in a general agreement.

Have you verified appropriate risk assessment of your cloud provider's suppliers?

You are required to verify and evaluate any contracts your cloud provider has with its suppliers that are relevant for the security and confidentiality of your data. The agreement should contain provisions allowing for the audit of relevant suppliers of your cloud provider.

Where are the administrators with access to the data located?

The assessment of risk should not be based solely on where your data is being stored physically, but also on who has access to the data and from where. If you are storing data that is classified by one nation, it may be exposed to additional risks if the cloud provider engages administrators located in another nation. Data sovereignty rules also apply to the location of administrators.

About Cleura

Cleura is a leading global supplier of IT infrastructure cloud services based on OpenStack. The company delivers public, compliant and private clouds.

Cleura is certified according to ISO 9001, 14001, 27001, 27010, 27013, 27017 and 27018 – internationally recognized standards for quality, sustainability and information security. Its services are available from more than 20 data centers around the world. With its compliant cloud, City Network ensures that customers adhere to demands originating from specific laws and regulations concerning auditing, reputability, data handling and data security, such as Basel, Solvency and GDPR.
Cleura is a part of Iver.

20220520

sales@cleura.com / cleura.com

cleura