citynetwork

REGULATORY ASPECTS TO CONSIDER WHEN COMPARING CLOUD PROVIDERS

COMPARING APPLES WITH APPLES

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 service level agreements (SLAs).

Organizations that operate in certain fields or store sensitive information on behalf of their clients are almost always subject to more stringent regulatory demands. Companies in the banking and finance, healthcare and government sectors also have specific rules and regulations that apply to them and their affiliates, sub-contractors and service providers. For these organizations, General Terms and Conditions are not sufficient to meet the requirements relating to how information, by law, can be processed and stored. 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 comply with such a request, one way or another. One of the most important aspects for you, the customer, is the price. As your demands increase, so does the price. The challenge is to identify the appropriate level for your organization while always ensuring compliance with laws and regulations.

In conclusion, when comparing cloud providers, you need to ensure that potential providers are evaluated on the same basis with respect to technical, legal, compliance, SLA and price aspects.

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 vary from country to country or continent to continent, and sometimes are in direct conflict with one another.[1]

[1] EDPB rules on the CLOUD Act: restrictive position on the legitimacy of data transfers to US investigating authorities
https://www.cms-lawnow.com/ealerts/2019/07/edpb-rules-on-the-cloud-act-restrictive-position-on-the-legitimacy-of-data-transfers

GENERAL POINTS ABOUT DATA STORAGE AND DATA TRANSFERS FROM AN EU AND GDPR PERSPECTIVE

- ***Where* data is geographically stored is not as important as *who* can access it.**
- **International administrative access to data stored in, for instance, Sweden is considered an international data transfer[2].**
- **The legal entity of the provider will determine which country's rules and which laws the provider is subject to.**
- **EU companies have no choice but to follow EU regulations and the General Data Protection Regulation (GDPR).**
- **US providers must follow US laws, including the CLOUD Act, even if they have offices and data centers in Europe[3].**

PENALTIES

The penalties for compromising or breaching the personal data of employees, customers or both are quite severe under the new EU GDPR. As described in Article 49 of GDPR[3], the penalties are as follows:

- **Minor breach: 2% of annual revenue or €10 million (whichever is higher)**
- **Major breach: 4% of annual revenue or €20 million (whichever is higher)**

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

[2] Art. 49 GDPR. Derogations for specific situations - https://gdpr-info.eu/art-49-gdpr/
[3] GDPR fines & penalties - https://www.gdpreu.org/compliance/fines-and-penalties/

QUESTIONS TO ASK WHEN EVALUATING A CLOUD PROVIDER AND DRAFTING A CONTRACT

Are you allowed to visit their 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 for an audit to be conducted to 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. For instance, if you are storing data that is classified at a certain level by one nation, it may be exposed to additional risks if the cloud provider engages administrators in a competing nation. Data sovereignty rules also apply to the location of administrators.

FINAL WORDS OF ADVICE

We might live to see the day when data breaches are a thing of the past, although this is highly unlikely. Given that human error, a rogue employee or the potential butterfly effect of insignificant mistakes could spell catastrophe, the only real question is to what degree we can prepare and protect ourselves against the inevitable. In the information age we are living in, the answer is to be one step ahead of your competitors by constantly improving your awareness of potential risks and subsequently mitigating them.

- **Ensure that the data protection chain is never broken.**

- **Assess and contractually sign off on your data relationship with anyone who has direct or indirect access to the data for which your organization is responsible.**

- **Your organization's ability to take legal action against a subcontractor will never remove the stains on your reputation in the event of an incident.**

ABOUT CITY NETWORK

City Network is a leading provider of IT infrastructure services.

The company provides public, private and hybrid cloud solutions based on OpenStack from more than 20 data centers around the world. Through its industry-specific IaaS City Cloud, City Network can ensure that customers comply with demands originating from specific laws and regulations concerning auditing, reputability, data handling and data security, such as the Basel and Solvency directives and GDPR. City Network is certified according to ISO 9001, 14001, 22301, 27001, 27010, 27013, 27017 and 27018. The company is also compliant with PCI-CPP C5, SOC 2, PCI-DSS and HIPAA, internationally recognized standards for quality, sustainability and information security.

SALES@CITYNETWORK.EU WWW.CITYNETWORK.EU

WWW.FACEBOOK.COM/CITYNETWORK

WWW.TWITTER.COM/CITYNETWORK

WWW.YOUTUBE.COM/CITYNETWORKHOSTING

citynetwork