MARKET PERSPECTIVE

Implications of the EU Cloud Code of Conduct on European Cloud Infrastructure

Michael Ceroici
Duncan Brown
Giorgio Nebuloni

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: Implications of the EU Cloud Code of Conduct on European Cloud Infrastructure

This IDC Market Perspective focuses on the 1Q17 launch of the EU Cloud Code of Conduct (CoC). The goal of the CoC is to make cloud adoption in Europe more secure and transparent, particularly in light of the forthcoming General Data Protection Regulation (GDPR) in 2018.

Key Takeaways

- The CoC was officially announced in early 2017, with IBM, Salesforce, Oracle, SAP, and Alibaba Cloud as founding members.
- While adherence to the CoC is voluntary, it may spur a "race to the top" for data protection services among European cloud service providers.
- The CoC may help provide assurance to European firms that their cloud suppliers understand liability obligations and accept their share of said liability.

Recommended Actions

- With competing voluntary data protection regulations covering more narrow scopes than the CoC, adopters should use this fact as an opportunity to attract a wider customer base.
- Adherers to the CoC can use it as a messaging tool to educate customers on the importance and necessity of choosing cloud providers with the utmost data protection precautions in place.
- Service providers should monitor the availability of third-party CoC assessors as opposed to only relying on self-assessment.

Source: IDC, 2017

July 2017, IDC #EMEA42886117

NEW MARKET DEVELOPMENTS AND DYNAMICS

With GDPR regulations coming into force in 2018, there is a general realization that many European firms are ill-equipped to ensure they have the right security infrastructure in place to comply with the regulations. Some cloud service providers were early to recognize the impact of GDPR, especially as a distrust of cloud security prevalent in Europe — an issue that cloud service providers needed to address.

In response to these needs, the Cloud Select Industry Group (CSIG) began to develop the EU Cloud Code of Conduct (CoC) to establish a set of data protection requirements for service providers (SPs) and support transparent implementation and development of the CoC. The CoC was developed specifically in anticipation of incoming GDPR regulations and industry best practices. Work on the CoC was started in 2012 and officially launched in February 2017, following cooperation between cloud service providers and the European Commission. A key aspect of the CoC is it covers all aspects of cloud services, including infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). In contrast, the Cloud Infrastructure Services Providers in Europe (CISPE) — an alternative cloud coalition — focuses only on business-to-business (B2B) cloud infrastructure services.

SCOPE EUROPE was established as an independent organization whose responsibility is to oversee the CoC's development and governance rules. It will oversee SP applications to ensure they are compliant with the requirements detailed in the CoC. Approval of the CoC by the European Data Protection Board is anticipated in 2018 once GDPR takes effect.

The CoC will contribute to creating a more transparent and definitive guideline for cloud SPs to adhere to, and ensure that cloud users can be confident they are receiving the highest-grade cloud security with their choice of provider. In a post-GDPR environment where personal data security is paramount, having this assurance can help firms better manage their cloud supply chains.

This report will center on the EU Cloud CoC, SCOPE EUROPE, and the cloud regulations inherent in the CoC and GDPR itself. Discussions around CISPE can be found in *Implications of the Code of Conduct for Cloud Infrastructure Service Providers in Europe* (IDC #EMEA42512717, May 2017).

The EU Cloud Code of Conduct

According to SCOPE, the goals of the EU Cloud CoC are:

- To make it easier and more transparent for cloud customers to decide which cloud solutions are the right fit for their needs by providing confidence that member SPs handle personal data with a level of protection that is compliant with GDPR regulations
- To strengthen the confidence in cloud computing by overcoming trust issues between cloud providers and users
- To create a future European benchmark for secure cloud provisioning in the face of incoming GDPR regulations

These goals will be achieved by enacting several stringent rules around cloud provisioning. Implementers of the CoC have placed a strong emphasis on the fact that the requirements are rigorous and no exemptions are permitted for any members. Because the CoC is not enacted by a public agency, however, the rules are not enforceable but serve as a strict guide for compliance of member SPs.

Through the CoC, SPs must ensure that all personal data is processed in consideration of GDPR and any national data protection derogations. The CoC includes sets of terminologies, structure,

and SP security obligations to remove as many uncertainties as possible for both SPs and interested buyers.

An inherent benefit cited by SCOPE is that the CoC is broad enough to encompass all forms of cloud provisioning, whether IaaS, PaaS, or SaaS. At a time when data protection regulations are in rapid flux and competing sets of regulations are vying for the broadest acceptance, this can be considered a significant advantage for the CoC.

In summary, IDC believes the CoC will serve to:

- Act as both a benchmarking and educational agent for evolving European data protection regulations. Many small to medium-sized enterprises are unaware of or unprepared for GDPR data protection reforms, and as such adopting an SP that complies with the CoC can be a way to ensure data protection meets GDPR minimum.
- Create a "race to the top" in SP data protection efforts. More SPs will feel the pressure to up their compliance with data protection regulations to keep pace with competing providers.
- Help derisk European cloud propositions, especially by U.S.-based SPs by creating a firm set of requirements at which they can aim (rather than second-guess at GDPR nuances).

Adherence Process

Founding members of the CoC include large SPs such as Salesforce, Alibaba Cloud, IBM, Oracle, and SAP. They play a part in the development of the CoC's regulations to improve transparency around data protection issues and how these are being addressed by European cloud providers. Increasing SP participation in CoC adherence may broaden stringent cloud security requirements, particularly for other future regulatory bodies.

The three key objectives and requirements for SPs set out by the CoC are the following:

- The need to implement appropriate measures to ensure the security, integrity, confidentiality, and availability of customer data being processed
- A requirement to achieve security objectives set out for access controls, encryption, physical infrastructure security, management direction, human resources, asset management, and communications security
- An obligation to supply customers with details on the appropriate technical, physical, and organizational measures the SP has taken, as well as to promptly notify the customer in the event of any changes which would reduce the level of security

An important note is that adherents to the CoC are also mandated to nominate a data protection officer (DPO), who must be available for contact by the customer during the duration of SP compliance with the CoC's conditions. The DPO role is not mandatory under GDPR, but is considered best practice, and so the inclusion of it with the CoC establishes a high bar for SPs to reach. Including a mandatory DPO appointment in the CoC will further push this role as a mainstream requirement, rather than an option in data protection planning.

The CoC also sets out stringent requirements when involving third parties in the handling of customer data. Key requirements for SPs in the CoC include the need to:

- Maintain an updated list of entities engaged by the SP when handling customer data, including legal entities responsible and exact physical locations
- Ensure that third parties engaged by the SP have at least equivalent levels of protection regarding customer data

- Demonstrate through appropriate documentary evidence that the SP has taken appropriate measures to obtain the guided levels of protection
- Provide more detailed information regarding processing locations to customers upon request, with the caveat that this information be considered confidential by the customer

To make the adoption process easier for SPs, the CoC includes a checklist for a variety of security objectives that need to be met to obtain and maintain the necessary levels of data protection. Compliance monitoring can be done through self-evaluation or by certified third parties.

SPs that comply with the CoC can display an EU Cloud CoC mark on their website or public engagement material, thereby letting buyers know which providers they can count on for stringent cloud security adherence. While the design of the CoC is targeted at firms processing customers' private data, its design is such that firms processing their own data or in conjunction with a third party can also choose to become CoC adherents.

Potential and Challenges

With the announcement of the CoC, there remain important tasks for the members to tackle to ensure the procedures are well-tested.

Self-assessment may be a concern for cloud customers considering certified CoC SPs. While an individual assessment system may serve as an easy way to attract cloud providers, it can also leave open the chance for SPs to take a relaxed approach to assessment to obtain certification. In addition, at the outset there may be no certified third parties able to assess the SPs, leaving – at least early – self-assessment as the only option. There is an opportunity for SCOPE to take a more active role in self-assessments, perhaps a form of final due diligence, to ensure that the security standard of members and the reputation of the CoC are not diminished by poor performers over time.

In addition, there remains the task of attracting new members to the CoC, establishing collaboration with other cloud certification schemes (such as Trusted Cloud Germany, BSI C5), and receiving endorsement from official EU bodies such as the European Data Protection Board and individual national regulatory authorities. The latter will be particularly important after the induction of GDPR in May 2018. The long-term convergence of cloud data protection standards remains to be seen, with the already existing CISPE as a competitor in B2B cloud infrastructure services, the Cloud Security Alliance code in preparation, and other national initiatives already in play. The broad inclusion of cloud services in the CoC should be emphasized as an advantage over alternative voluntary regulations.

ADVICE FOR THE EUROPEAN SERVICE PROVIDER

IDC believes that the EU CoC can serve as a useful tool for European enterprises and public institutions considering a move to cloud technology securely. The early stage of cloud data protection certifications means that the broad scope of the CoC puts it in a good position for attracting interested SPs.

The CoC and similar codes may help spur more action and education for buyers in the European space. Data protection can often be a complex issue, with various stakeholders involved, rapidly evolving regulatory requirements, and different vertical use cases. Having SPs adhere to strict conducts will inspire more confidence among European businesses and institutions to trust their data with a cloud provider. That confidence may push reluctant businesses to choose those certified SPs over competitors, in a market where data security will only increase in importance.

IDC recommends service providers to look at the different cloud data protection conducts on the market and evaluate which would best suit their business case. While some may become more influential or widespread than others, gaining certification with a body such as the EU Cloud Code of Conduct may go a long way to ensure that they meet or exceed the security requirements of GDPR. In addition, the constant dialogue mandated to adherents of the CoC means that SPs and customers remain involved and up-to-date on industry developments, internal security needs and changes, and more trusted relationships around the protection of personal data in the cloud.

LEARN MORE

Related Research

- *The Impact of GDPR on Cloud Services Providers – Part 1: General Considerations for Contracts and Liability* (IDC #EMEA42627817, June 2017)
- *The Impact of GDPR on Cloud Service Providers – Part 2: Security, Data Transfer, and Other Considerations* (IDC #EMEA42627917, June 2017)
- *Implications of the Code of Conduct for Cloud Infrastructure Service Providers in Europe* (IDC #EMEA42512717, May 2017)
- *Western Europe Public Cloud Security Forecast, 2016-2020* (IDC #EMEA42179116, February 2017)
- *IDC FutureScape: Worldwide Cloud 2017 Predictions – European Implications* (IDC #EMEA42241617, January 2017)

Synopsis

This IDC Market Perspective focuses on the 1Q17 launch of the EU Cloud Code of Conduct. The goal of the CoC is to make cloud adoption in Europe more secure and transparent, particularly in light of the forthcoming General Data Protection Regulation (GDPR) in 2018. This report includes a preliminary summary of the CoC's development, adherence processes, as well as opportunities and challenges for European cloud service providers.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC Central Europe GmbH

IDC Central Europe GmbH - Deutschland & Schweiz
Hanauer Landstraße 182 D
60314 Frankfurt am Main, Deutschland
+49 (0)69 90502-0
Twitter: https://twitter.com/idc_deutschland
www.idc.de