MARKET PERSPECTIVE

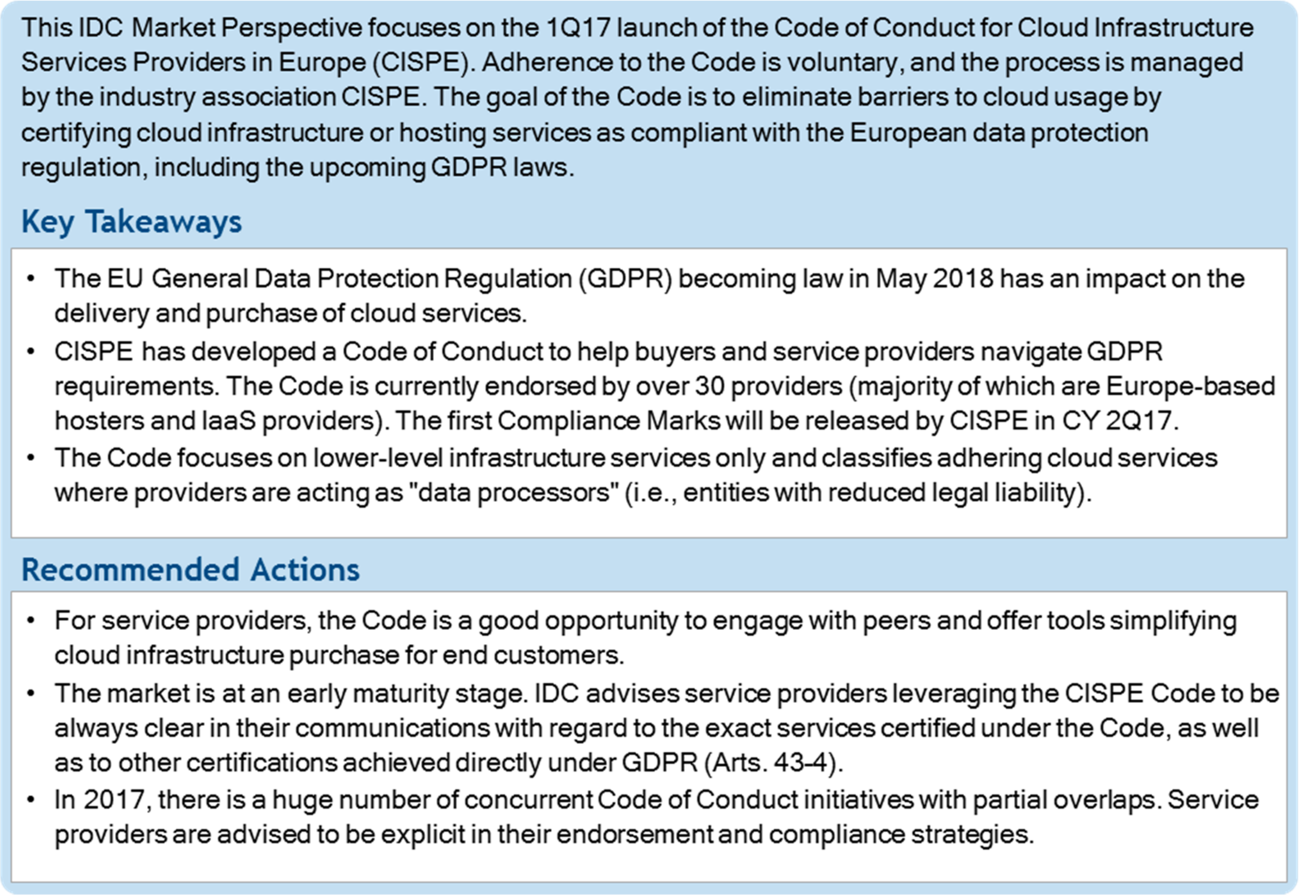
Implications of the Code of Conduct for Cloud Infrastructure Service Providers in Europe

Giorgio Nebuloni

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: Implications of the Code of Conduct for Cloud Infrastructure Service Providers in Europe



This IDC Market Perspective focuses on the 1Q17 launch of the Code of Conduct for Cloud Infrastructure Services Providers in Europe (CISPE). Adherence to the Code is voluntary, and the process is managed by the industry association CISPE. The goal of the Code is to eliminate barriers to cloud usage by certifying cloud infrastructure or hosting services as compliant with the European data protection regulation, including the upcoming GDPR laws.

Key Takeaways

- The EU General Data Protection Regulation (GDPR) becoming law in May 2018 has an impact on the delivery and purchase of cloud services.
- CISPE has developed a Code of Conduct to help buyers and service providers navigate GDPR requirements. The Code is currently endorsed by over 30 providers (majority of which are Europe-based hosters and IaaS providers). The first Compliance Marks will be released by CISPE in CY 2Q17.
- The Code focuses on lower-level infrastructure services only and classifies adhering cloud services where providers are acting as "data processors" (i.e., entities with reduced legal liability).

Recommended Actions

- For service providers, the Code is a good opportunity to engage with peers and offer tools simplifying cloud infrastructure purchase for end customers.
- The market is at an early maturity stage. IDC advises service providers leveraging the CISPE Code to be always clear in their communications with regard to the exact services certified under the Code, as well as to other certifications achieved directly under GDPR (Arts. 43-4).
- In 2017, there is a huge number of concurrent Code of Conduct initiatives with partial overlaps. Service providers are advised to be explicit in their endorsement and compliance strategies.

Source: IDC, 2017

NEW MARKET DEVELOPMENTS AND DYNAMICS

In June 2016, after more than two years of discussions, high-level guidelines for data protection were released by the European Commission and the assembly of industry players called Cloud Select Industry Group (C-SIG). Those guidelines were released under the name EU Code of Conduct (CoC) for cloud service providers. However, those directives are targeted broadly at business-to-business (B2B) cloud services, without distinctions between the type of cloud service delivered. The devil, however, is in the details and important fine lines need to be drawn to operationalize the General Data Protection and Regulation (GDPR) in the infrastructure-as-a-service (IaaS) space.

CISPE, a coalition of cloud infrastructure service providers with European operations, was originated in the first EU CoC discussion groups, and then spun off as a separate initiative with the goal of representing more extensively both IaaS providers and midsize cloud service players. CISPE focuses on the B2B cloud infrastructure services only, as opposed to the broader EU CoC initiative that covers all types of cloud services. In June 2016, CISPE presented the first version of its own suggested guidelines to the European Commission and C-SIG.

In this report, we will limit the discussion and reporting on CISPE and the initiatives it is implementing in the infrastructure space. In parallel to CISPE, on February 15, 2017, the EU CoC was handed over from the C-SIG to SCOPE Europe, a subsidiary of the think-tank Selbstregulierung Informationswirtschaft e.V. (SRIW), with the goal of incorporating GDPR regulatory guidelines. We will do the analyses of SCOPE Europe and the EU CoC in the other reports.

CISPE's Data Protection Code of Conduct

On September 27, 2016, CISPE unveiled publicly in front of the European Parliament and European Commission the first full iteration of the CISPE Data Protection Code of Conduct (hereafter "Code"). After the initial review, the Code was signed off by CISPE on January 27, 2017.

According to CISPE, the ultimate goals of the Code are:

- To eliminate barriers to cloud usage by making it easier for an end buyer to know if a certain cloud infrastructure or hosting service is compliant with the European data protection regulation
- To help cloud customers in the EU assess if a particular IaaS service provides appropriate safeguards for the data processing that end customers wish to perform, ahead of the entry into force of the upcoming GDPR law

The goal will ultimately be achieved by the granting of CISPE Compliance Marks to cloud infrastructure or hosting services that comply with the Code and having the Code recognized by European authorities.

Adherence to the Code is voluntary, and CISPE is not a public authority. According to the materials published, the Code is focused exclusively on IaaS providers, described as suppliers of "virtualized hardware or computing infrastructure," without visibility or control on the type of personal data stored in their servers. The Code explicitly excludes providers of software as a service (SaaS) who, according to CISPE, have a high level of control on the type of personal data they require the end customer to provide in their applications. CISPE has indicated it is evaluating potential expansion to the coverage of its Code to other cloud fields, once the IaaS space has been satisfactorily addressed.

As of May 2017, the Code and Compliance Marks hold no legal value as they are awarded by an industry association without legal powers. However, CISPE has started the process of submitting its Code to the European authorities under Article 27 of the Directive 95/46 and Article 40 of the GDPR. If and when the European authorities recognize that, buyers could refer to the Code adherence as a way to prove GDPR compliance, and even to mitigate penalties in case of a breach. IDC believes recognition by the European Data Protection Board and European Commission won't happen until mid-2018 at the earliest. In order for that to happen, not only the CISPE's code but also its governance and monitoring body must fulfill the requests of European authorities.

The key requirements for cloud infrastructure service providers (CISPs) advancing adherence to the code for one of their services are:

- Compliance of the service with the Code requirements
- Compliance of the service with the European Data Protection Directive and upcoming compliance with EU GDPR enforced in May 2018
- Ability for the end customer to store and process all data sets within the European Economic Area (EEA)

From the initial description of IaaS providers onward, the whole Code is set to cover activities of the adhering CISPs as "data processors," not "data controllers." In legal terms, data controllers are entities determining the purpose for which and the manner in which personal data is processed – as opposed to data processors, who process and potentially store the data on behalf of the data controller. Most of the responsibility for personal data falls on data controllers, who typically are the end customers. CISPs are typically listed as data processors, and CISPE sees itself acting to squarely position IaaS providers as such. Thus, the Code explicitly does not cover the areas where the CISP is acting as a data controller (e.g., in personal data of the enterprise customer signing up for the cloud service).

IDC believes there are two main reasons behind the focus on the data processor role:

- Clarifying where the responsibility lies between the IaaS user (enterprise, public body, or ISV) and IaaS provider or CISP, especially when it comes to security tools and processes.
- Safeguarding IaaS providers, especially small ones, from potential loopholes in the upcoming GDPR regulation that could have legal consequences for them. As an example, GDPR currently envisions a potential for joint liability for both ISV and CISP in case of a breach in a SaaS application running on top of an IaaS platform. By clarifying the responsibility areas for the CISP, the Code should guide toward correct responsibility assignment.

In summary, IDC maintains that the Code is both:

- An explanation of what GDPR articles mean in terms of specific requirements for CISPs. In some cases, it fine-tunes the GDPR guidelines (e.g., suggesting to obviate the need of an onsite auditing of the CISP datacenter by the end customer through use of audit reports provided by the CISP).
- A complement to GDPR in adjacent areas, including the CISP commitment to not reuse customer data as well as a more detailed granularity on the responsibilities of CISP and end customers in matters of compliance.

Adherence Process

The Code is currently endorsed by the following providers: Amazon Web Services, Arsys, Art of Automation, Aruba, BIT, Dada, Daticum, Dominion, Enter, Fasthosts, FjordIT, Gigas, Hetzner Online, Home, Host Europe Group (part of GoDaddy EMEA), IDS, Ikoula, LeaseWeb, Lomaco, Netalia, Netcetera, Outscale, OVH, Seeweb, Serverplan, Solidhost, UpCloud, VTX, XXL

Webhosting, and 1&1 Internet. The majority of the endorsers are companies with a strong dedicated or web hosting background and European headquarters.

IDC believes there are three steps necessary from one or more CISPE service providers before the Code becomes relevant and useful to an end buyer:

- Declaration of compliance by a service provider for a specific service
- Confirmation of adherence to the Code of a specific service by certification of a third party or self-assessment by the CISP submitting adherence
- Granting of a Compliance Mark, specifying how adherence was achieved

On February 14, 2017, CISPE announced that 14 service providers have declared compliance (step 1) for a total of 35 cloud infrastructure services to the CISPE Data Protection Code of Conduct. It is important to note that single cloud services, not providers as such, can declare and be tested for compliance. Only base infrastructure or hosting services can be submitted, as both platform-as-a-service or PaaS (database as a service and other middleware services) and SaaS services are excluded by CISPE due to their opening up of the data controller issue.

The second step – confirmation of adherence of a service to the Code – can be achieved by a CISP in two ways:

- Presenting a third-party auditor report to CISPE, certifying Code compliance for the service in question.
- Presenting a Declaration of Adherence to CISPE where the CISP declares compliance for the service in question to the Code by self-assessment (i.e., self-auditing). CISPE can then execute stress-tests of the self-assessment.

CISPE allows self-assessment for the next 12 months in order to accelerate onboarding for smaller providers that cannot yet invest in an external auditor. Come May 2018, GDPR will be enforced, so all CISP requiring adherence will need to have GDPR compliance tested by an auditor. At that point, the self-assessment option will be retired.

For the third step, CISPE says that, when completed and certified by the CISPE Executive Board, both procedures will result in:

- Publicly referenceable Compliance Marks of a similar look and feel, but distinct wording stating whether there was an external audit or not
- Visible incorporation of the Compliance Mark in the CISPE Public Register of adhering services

Self-assessment Compliance Marks are valid only for one year and will require external auditing to be renewed in 2018. IDC understands that the first wave of confirmation of adherence is currently ongoing and the first Compliance Marks should be released in CY 2Q17.

CISPE Structure

CISPE is registered in the EU Transparency Registry and incorporated as a non-profit association. The organization is structured around:

- A General Assembly including all companies that pay the association fee. Each company holds one vote regardless of size or association fee. Votes are used to elect an Executive Board and propose changes to the Code.
- An Executive Board (EB) with a maximum of 10 representatives, elected by the General Assembly.

- A Complaints Committee, appointed by the EB, deciding on potential breaches to the Code.
- A Secretariat, appointed by the EB, reviewing and operating the Adherence Process.
- A Code of Conduct Task Force (CCTF) involving each organization with at least one service declared under the Code. CCTF is tasked with evolving and updating the Code itself.

Although open to all IaaS industry players, the organization aims to represent small to midsize CISPs and European players. The governance documents state that over 50% of the CISPE Executive Board members must have yearly revenue below $1 billion. Also, as a parallel requirement, over 50% of the board members must have their global headquarters in a European state. The Executive Board must also at all times include at least three companies with headquarters in three different member states in Europe.

Companies associating into CISPE must declare at least one service under the Code within six months. On the other hand, CISP players can declare and receive Compliance Marks for their services even if they are not assembly members of CISPE. According to CISPE, Service Declarations and the use of the relevant Trust Mark are subject to the following handling fee: €990 for the declaration of one service or €2,990 for the declaration of three or more services.

Potential and Challenges

IDC believes CISPE has an incredible potential in terms of influencing the discussion around cloud infrastructure in Europe and easing the buying pain for end customers. IDC views positively in particular the efforts put into defining how and where responsibility is handed over between providers and end users in the topic of network security policies (Section 5. Transparency).

However, there are a few challenges for CISPE to overcome in the next six months:

- **Gray areas.** The Code excludes PaaS (e.g., middleware-as-a-service, or database-as-a-service offerings) from being certified with Compliance Marks, on the grounds that the CISP's role is less clear and subject to become a "data controller." IDC believes cloud infrastructure is increasingly hooking into higher-level services to support IoT or cognitive workloads, so in a few years' time, "pure infrastructure" will cease to exist. Developing a good compliance process for those gray areas would give CISPE an immense credibility in the enterprise customer community. IDC recommends CISPE to assess viability of doing so, perhaps in the frame of the initial work it is initiating on sector-specific extensions.
- **Self-assessment.** This is a good pragmatic step to expand participation, yet it also opens the risk of subpar services sporting a Compliance Mark, damaging CISPE's reputation. Having a tighter and more structured process for CISPE to verify self-assessed declarations could minimize that risk.
- **Branding.** The continued existence and partial overlap of a parallel Code of Conduct (the EU CoC) and the presence of other Code of Conducts and guidance to data privacy regulation (e.g., Germany's C5, the CSA's initiatives, and more) are likely to create confusion among the end customers and in the SP community. Some SPs might sign up for one of the Codes but not for the other. Branding for the CISPE Code (and other codes) should be refined to increase clarity.

ADVICE FOR THE EUROPEAN SERVICE PROVIDER

IDC believes the Code can be a very useful tool for European enterprises, governments, and small business buyers. The usage of clear Compliance Marks should simplify the selection process, and the joint work of a broad ecosystem of global and local providers will reduce barriers to entry in procurement of IaaS services. This does not mean that IT buyers should become complacent toward the compliance status of their providers.

Enterprise buyers should note that:

- Single services, not providers, are certified by the Code, so it is possible the cloud service you want is not in there even if your provider is (for another service).
- The Compliance Marks have no legal value as of May 2017 and do not replace contracts or specific agreements between the buyer and supplier, nor do they replace taking action internally to comply with the GDPR. CISPE is working toward having official EU authorities recognize the Code, but that process won't bear fruit until 2018 at the earliest.

IDC advises end buyers to start asking their CISPs about their stance on the CISPE Code. CIOs should also create a task force including a member of the CISO staff, a member of legal/compliance and risk teams, and a member of the cloud or infrastructure administrators to look into the Code and report back to the broader IT department by September 2017. In particular, the "Section 5. Transparency" is worth a read.

From a service provider standpoint, the Code is a good opportunity to engage with peers in an open forum. Association costs are low for smaller providers and the benefits of engagement outweigh costs or disadvantages. Beyond and above the Code itself, CISPE has ongoing efforts interacting with the European Commission and influencing the still-fluid regulatory frame for Data Protection. IDC believes that being represented in those discussions is invaluable for providers of all sizes.

On the other hand, IDC advises service providers to be always clear in their communications as regards:

- The multiple industry efforts ongoing around different Code of Conducts
- The exact services certified under one or more Code of Conducts
- The certifications achieved directly under GDPR (Arts. 43-4)

The understanding of data protection and compliance topics remains low in several buyer segments. Complicating it further with unclear statements might slow purchasing instead of accelerating it.

LEARN MORE

Related Research

- *Western Europe Public Cloud Security Forecast, 2016-2020* (IDC #EMEA42179116, February 2017)
- *Rule 41 Adds Potential Complications to GDPR and Privacy Shield – But Don't Panic* (IDC #lcEMEA42209417, January 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 Code of Conduct for Cloud Infrastructure Service Providers in Europe (CISPE), providing essential information on the items included and the ecosystem support. It also includes a preliminary assessment of the implications of such an initiative for both end customers purchasing cloud infrastructure services and service providers active in Europe.

"The CISPE Code of Conduct can be a very useful tool for European IT buyers. Clear Compliance Marks should simplify the selection process, but buyers should continue questioning and reading fine prints of their cloud infrastructure contracts," said Giorgio Nebuloni, research director, IDC European Infrastructure.

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