**CISPE – Q&A Media Briefing, 27 September 2016**

## CISPE ASSOCIATION, GOALS AND PARTICIPATION

### 1 What does CISPE stand for?

CISPE stands for "Cloud Infrastructure Services Providers in Europe". CISPE is a coalition of companies with a primary focus on the provision of cloud computing infrastructure for customers in Europe. Its main goals are:

- *First*, Contributing to the European public policy debate around cloud computing and the Digital Single Market from the perspective of providers of IT infrastructure services otherwise called "Infrastructure as a Service" (IaaS),
- *Second*, Promoting the benefits and value of IaaS within Europe,
- *Third,* Developing and managing the CISPE data protection Code of Conduct for cloud infrastructure providers.

### 2 Who are the members of CISPE?

CISPE is open to companies from all over the world, however, the majority of CISPE companies have their global headquarters in Europe and are small or MidCap enterprises. At present, members come from various European countries including Bulgaria, France, Germany, Spain, Finland, Italy, The Netherlands, Norway, Poland, Switzerland and The United Kingdom and operate in more than 15 countries. They represents major players in the cloud infrastructure services sector. The following cloud computing infrastructure service providers endorse the CISPE code of conduct: Arsys, Art of Automation, Aruba, BIT, Daticum, Dominion, Fasthosts, FjordIT, Gigas, Hetzner Online, Home, Host Europe Group, IDS, Ikoula, LeaseWeb, Lomaco, Outscale, OVH, Seeweb, Solidhost, UpCloud, VTX, XXL Webhosting, 1&1 Internet.

CISPE membership is expected to grow beyond the initial founding members as interested companies declare their infrastructure services to be in compliance with the CISPE Code of Conduct. The Code of Conduct requires the adhering cloud infrastructure services providers to offer their customers the ability to exclusively process and store data within the EU/EEA territories, giving confidence to the industry and consumers.

### 3 How will CISPE encourage innovation in Europe?

CISPE is the only association in Brussels focused on cloud infrastructure services and governed by a majority of European SMEs and Midcap companies globally headquartered in Europe. CISPE's goals are to contribute to the European public policy debate and ensure a better knowledge of the European cloud infrastructure industry. CISPE offers a unique perspective on how to promote ubiquitous cloud computing infrastructure deployment that is key to the success of Europe's Digital Single Market. By ensuring a better representation of CISPE's members' interests and agreeing on common views, notably in the field of data protection, it will enable European businesses and public institutions to progress further in the cloud infrastructure market and focus on innovation.

### 4. How can CISPE contribute to develop a dynamic European single cloud market?

Several EU policy initiatives and legislations, notably on cybersecurity, privacy, public procurement, data flow and telecommunications are affecting the cloud service sector and its customers. We support the right kind of standards and regulations that will remove barriers to the Digital Single Market, not the ones that create further fragmentation and legal uncertainty that could hinder innovation and prevent businesses in Europe from growing.
To encourage the development of the cloud market in Europe, it is of the utmost importance that the voice of the cloud infrastructure providers be heard and that their challenges and opportunities be known. This will ensure the best possible environment for the growth and the creation of new services across the EU.

### 5. What is the membership criteria to adhere to CISPE?

CISPE membership is open to all cloud infrastructure providers, whatever their size, who give their customers the assurance that their services do not process their personal data, for their own benefit or for the resale to third parties, such as for the mining of personal data, profiling of data subjects, marketing or similar actions. In addition,

CISPE members must offer their customers the ability to exclusively process and store data within the EU or EEA territories. This gives customers the assurance that their data remains in their control and ownership.

### 6. Which companies can join CISPE?

Any company that provides cloud infrastructure services complying with the CISPE Code of conduct – and that clearly and unambiguously identifies such services using the corresponding CISPE trustmarks – may participate in and benefit from joining CISPE. In addition, companies that wish to participate in CISPE's board activities must have the provision of cloud infrastructure services in Europe as part of their core business.

### 7. What are CISPE's main policies of interest?

We have observed there is a widespread misunderstanding about the nature of "infrastructure" services (IaaS) and the different cloud deployment models (IaaS, PaaS, and SaaS). We are concerned that this may fuel a "one size fits all" approach for public policies that are out of touch with technological reality. Our industry is looking forward to the opportunity to address this gap in collaboration with the European Commission and other policy makers across Europe. This is important to understand cloud infrastructure correctly, given its huge potential to help reach the Digital Single Market objectives.

CISPE will contribute to the policy debate in fields that relates to the interest of its members, such as data protection, data flow, and network information security. As for the recently announced European Cloud Initiative, CISPE is looking forward to working together with the various stakeholders to build the best initiative for growth, employment and data protection in Europe.

### 8. What are CISPE's recommendations in order to create a cloud infrastructure single market?

1. Propose and develop "cloud first" public procurement policy initiatives that will drive the growth of the single cloud infrastructure market in Europe and underpin the Digital Single Market growth goals.
2. Promote coherent EU-wide security requirements and technical standards across Member States - including for critical infrastructure operators – to avoid the fragmentation of the EU single cloud infrastructure market due to contradictory national requirements.
3. Support comprehensive cloud requirements in the EU Data Protection Regulation, including a privacy Code of Conduct for Infrastructure providers that helps create a high level of harmonized data protection taking into account the particular features of IaaS cloud computing and that can enable EU businesses to fully and trustfully leverage the benefits of the cloud computing infrastructure.
4. Keep the EU cloud infrastructure market open and competitive (free from "lock-in") so that cloud users are able to make informed choices about how their data are processed and stored, and that companies implementing the required standards are not compelled to use specific equipment or limited in their ability to offer their services across the entire EU internal market.
5. Ensure that the EU legal framework, including new copyright rules, takes account of the particular features of IaaS cloud computing.

## CODE OF CONDUCT

### 9. Is CISPE Code of Conduct publicly available and where can I find it?

Yes. The code of conduct can be downloaded at no cost from our website: www.cispe.cloud/code

### 10. What are the characteristics of the Code of Conduct?

Under the CISPE Code of Conduct, cloud service providers confirm that they:

- Offer the choice to customers to store and process exclusively in the EEA territory;
- Are committed not to re-use their customers' personal data for their own purposes or for third parties, such as for mining of personal data, profiling of data subjects, marketing or advertising actions.

**11. What assurances do customers get from knowing their IaaS provider is compliant with the CISPE code of conduct?**

Until the application of the GDPR in 2018, providers can either self-certify that their services are in compliance with the CISPE code or request a third-party (e.g. auditing companies) to assess if their services indeed comply with the Code. After the application of the GDPR only certified bodies, that is organisations recognised by the competent data protection authorities, can certify that services declared under the Code are indeed compliant with such Code. In both instances, failure to comply with the Code could trigger the same sanctions and penalties for non-compliant cloud infrastructure service providers.

**12. What is the regulatory value of the CISPE Code?**

As of today, Codes of Conduct do not need to be validated by regulators: they are trustfully applied, or not. The European Data protection Authorities, in particular the Article 29 Working Party that currently brings together all national data protection agencies in Europe, may review and issues an opinion (favourable or not) to any given Code of Conduct. The CISPE Code fo Conduct will be submitted to the review of the Article 29 Working Party in due time.

**13. How do Cloud infrastructure Services Providers declare that they comply with the CISPE Code?**

Companies that wish to declare the compliance of their cloud infrastructure services with the CISPE Code of Conduct should register their interest through the CISPE website on: WWW.CISPE.NET

**14. How do customers know that a given cloud infrastructure service provider complies with the Code?**

Cloud customers that wish to know if the infrastructure services they procure are in conformity with the CISPE Code of Conduct should consult: WWW.CISPE.NET

**15. Is the CISPE Code relevant for customers outside of Europe?**

Yes. Particularly if such customer wishes to host or process their data in Europe and when they are looking for providers that commit not not re-use or monetise such customer data.

**16. Can non-European cloud providers sign up to the CISPE code?**

Yes, provided that these companies declare that at least one of their cloud infrastructure service meets the requirements set forth under the CISPE Code of Conduct.

**17. Is this the first Code of Conduct of this type? Are there other similar codes in existence or anticipated?**

To our knowledge this is the first-ever code for cloud computing infrastructure services. We expect more sector specific codes of conducts to see the light of day in anticipation of the application of the new European rules on data protection in 2018.

BACKGROUND

**18. What is the difference between infrastructure providers and other cloud providers?**

Cloud infrastructure computing services" (IaaS), means the on-demand delivery of IT resources via the Internet with pay-as-you-go pricing. Instead of buying, owning and maintaining their own datacenters and servers, our customers only pay for the quantity of the compute power, storage, databases, and other services that they use.

Cloud Infrastructure Service Providers ("CISPs") manage and maintain the technology infrastructure of their customers in a secure environment where they can access resources via the Internet to develop and run their own applications and manage their own content and end users.

Many of the examples of internet-based services illustrating the EU Commission definition of online platforms, such as NETFLIX, AIRBNB and YELP, are enabled through our cloud infrastructure services.

Contrary to other types of cloud providers such as those provisioning Software as a Services ('SaaS') that have contractual relations with their end users and may enable interactions between two or more distinct but interdependent groups of users, CISPs have a relation with a single user: their customer.

CISPs do not process or resell their customers or end-users' personal data for their own purposes, such as for mining of personal data, profiling of data subjects, marketing or advertising actions for our own benefit or for third parties. CISPs do not typically have technical access, use or control over their customer or end users' applications, content or personal data (particularly when such data is encrypted either by the customer or by its end-users) for any purpose other than legally required and for maintaining their services and providing such services to the customer and their end-users or clientele.

**19. What is so specific in the IaaS perspective?**

Contrary to other types of cloud providers such as those provisioning Software as a Services ('SaaS') that have contractual relations with their end users and may enable interactions between two or more distinct but interdependent groups of users, CISPs have a relation with a single user: their customer.

CISPs do not process or resell their customers or end-users' personal data for their own purposes, such as for mining of personal data, profiling of data subjects, marketing or advertising actions for our own benefit or for third parties. CISPs do not typically have technical access, use or control over their customer or end users' applications, content or personal data (particularly when such data is encrypted either by the customer or by its end-users) for any purpose other than legally required and for maintaining their services and providing such services to the customer and their end-users or clientele. The IaaS is the data Processor whose mission is defined by the Controller. The Controller and the Processor are facing very different challenges and obligations when it comes to data protection.

**20. Definitions**

Cloud infrastructure computing services" (IaaS), means the on-demand delivery of IT resources via the Internet with pay-as-you-go pricing. Instead of buying, owning and maintaining their own datacenters and servers, our customers only pay for the quantity of the compute power, storage, databases, and other services that they use, much as they do for utility services such as water and electricity which they can pay for by usage.

Cloud Infrastructure Service Providers ("CISPs") manage and maintain the technology infrastructure of their customers in a secure environment where they can access resources via the Internet to develop and run their own applications and manage their own content and end users. Capacity can grow or shrink instantly and customers only pay for what they use. Many of the examples of internet-based services illustrating the EU Commission definition of online platforms, such as NETFLIX, AIRBNB and YELP, are enabled through our cloud infrastructure services.

**For more information please contact Virginie Louis, Head of Media Relations, ICF MOSTRA, e-mail: virginie.louis@mostra.com, mobile +32 471 13 97 64**