Cloud infrastructure providers unveil ground-breaking data protection Code of Conduct

Summary
Cloud Infrastructure Services Providers in Europe (CISPE), a newly formed coalition of more than 20 cloud infrastructure providers operating in Europe, announces the launch of the **first-ever data protection code of conduct** requiring cloud infrastructure services providers to offer their customers[1] the ability to exclusively process and store data within the EU/EEA territories.

Under the CISPE Code of Conduct, cloud infrastructure providers cannot data mine or profile customers' personal data for marketing, advertising or similar activities, for their own purposes or for the resale to third parties. The CISPE Code precedes the application of the new European Union (EU) General Data Protection Regulation (GDPR). It aligns with the requirements set out in this new regulation aiming mainly at giving citizens back the control of their personal data, and simplifying the regulatory environment for international business by unifying the regulation within the EU. CISPE brings together bigger and smaller leading cloud infrastructure service providers headquartered or operating across more than 15 countries.

Story
Today the members of CISPE, a coalition of companies committed to the provision of cloud computing infrastructure in Europe, announce their establishment and commitment to embrace a data protection Code of Conduct. The CISPE Code of Conduct makes it simpler for customers to assess whether Cloud Infrastructure Services are suitable for the processing of personal data that they wish to perform, and those that are suitable are identified by a clear Trust Mark. This Trust Mark can be used by cloud infrastructure providers to show customers they are compliant, and compliant organisations will also be listed on the CISPE website.

Under the CISPE Code of conduct, cloud customers will receive the assurance that providers of cloud infrastructure 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.
"*This is the first industry-wide Code of Conduct to do so. It gives customers the assurance that their data always remains in their control and in their ownership*," Alban Schmutz, VP OVH and Chairman of CISPE.

In addition, providers certified with the CISPE Code of Conduct must offer their customers the ability to exclusively process and store data within the EU or EEA territories. This means customers from industry or software vendors procuring such cloud infrastructure services can control where their data is processed and stored physically, while knowing that their provider will not re-use or resell their data.

MEP Eva Paunova, Member of the Committee on the Internal Market and Consumer Protection, said, on hearing today's news, *"The demand for strong cloud infrastructure, where customers are assured that their data is well-protected, is increasing. We as policy-makers can draft a perfect piece of legislation on paper, but what is key is to know what is feasible and what can work on the ground. To that end, I welcome the CISPE Code of Conduct and how it helps European cloud customers to understand that their content is receiving a high standard of data protection. "*

The new CISPE Code of Conduct gives customers of cloud infrastructure services an important compliance tool that helps them in identifying infrastructure service providers that give them the ability to build services and applications that comply with existing EU Data Protection regulations by keeping content within the EU or EEA. The CISPE code, and Trust Mark awarded to those cloud providers that are in compliance, also demonstrates a cloud infrastructure service providers' commitment to maintaining the highest levels of data protection and adherence to practices that are fully aligned with the principals of the European Union.

[1] Software vendors, System Integrators, Manufacturing and Services Industries, Administrations, NGOs, etc.

"The CISPE Code of Conduct show that the European cloud computing industry is capable to provide secure and compliant services for all personal and technical data in Europe and improve trust in digital services," Axelle Lemaire, French Minister for Digital Affairs and Innovation.

The CISPE Code precedes the entry into force of the new, and more stringent, EU General Data Protection Regulation in May 2018 and builds on internationally recognised security standards that enhance data security processing for all cloud customers and for their users. The new code of conduct has been constructed in such a way that it will be aligned with the GDPR when it comes into force. The launch of CISPE Code of Conduct was made today at a round table conference held in Brussels with the attendance of industry key players, SMEs and policy makers and hosted by MEP Eva Paunova, Member of the Committee on the Internal Market and Consumer Protection.

Background information

About CISPE - CISPE is a coalition of technology companies focused on the provision of cloud computing infrastructure services across Europe. Headquartered in 11 European countries (Bulgaria, France, Germany, Spain, Finland, Italy, The Netherlands, Norway, Poland, Switzerland and The United Kingdom) and operating in more than 15, 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 is governed by a majority of (a) organisations with their global headquarters in the EU/EEA with representation from at least three different Member States, and (b) a majority of small/midcaps (<€1 billion yearly turnover). Participation in CISPE is open to any infrastructure cloud provider whose services meet the privacy and data processing security requirements of the CISPE Code. CISPE will ensure that cloud infrastructure providers, particularly SMEs, are at the heart of the European public policy debate on cloud computing. CISPE members share the European Commission's commitment to improving access to digital goods and services and creating an environment where digital services can thrive.

How to participate and benefit from the CISPE Code of Conduct? Find more information on the association, the CISPE Code of Conduct and register interest: WWW.CISPE.NET

About cloud infrastructure[2] - Cloud Infrastructure as a Service (or "IaaS") is at the heart of Europe's digital agenda and of the new economy. Cloud infrastructure enables innovators to rapidly deploy global solutions without the need for either capital expenditure or time-consuming deployments of private infrastructure. Infrastructure suppliers have the specificity to own storage and computing infrastructure to provide them to their customers, without having access to the data that will be stored or processed. Infrastructure providers provide their customers the ability to get very high technical and financial flexibility. They are the suppliers on which other Cloud computing actors are building their own services to their customers. Cloud computing infrastructure deployment is key to the success of Europe's Digital Single Market as it enables businesses and administrations to focus on innovation and high-quality products and services.

For more information please contact:
VIRGINIE LOUIS, Head of Media Relations, ICF MOSTRA | direct +32 (0)2 333 59 15 | mobile +32 471 13 97 64 | virginie.louis@mostra.com

[2] ***IaaS*** *or Cloud Infrastructure as a Service: a provider leases a technological infrastructure, i.e. virtual remote servers the end-user can rely upon in accordance with mechanisms and arrangements such as to make it simple, effective as well as beneficial to replace the corporate IT systems at the company's premises and/or use the leased infrastructure alongside the corporate systems. Such providers are usually specialised market players and can rely actually on a physical, complex infrastructure that often spans over several geographic areas*