Resolution
on Cloud Computing

Punta del Este / Canelones, Uruguay - 26 October 2012

Cloud Computing (CC) is attracting increasing interest due to promises of greater economic efficiency, lower environmental impact, simpler operation, increased user-friendliness and a number of other benefits. However, the evolution of CC raises a number of important issues relating to, for example, the fact that the technology is still developing, data processing has become global, and lack of transparency is making it more difficult to enforce privacy and data protection rules. These issues may magnify certain risks inherent in data processing, such as breaches of information security, violation of laws and principles for privacy and data protection, and misuse of data stored in the cloud.

Members of the International Conference and other stakeholders, including, for example, the International Working Group on Data Protection in Telecommunications (IWGDPT, a.k.a. "Berlin Group")[1], have begun to consider data protection and privacy issues relating to CC.

Without endorsing any particular group's analysis, the International Conference welcomes such efforts. Therefore, to further encourage such efforts and to help reduce risks associated with the use of cloud computing services and to promote accountability and proper governance,

the 34th International Conference of Data Protection and Privacy Commissioners recommends that:

- Cloud computing should not lead to a lowering of privacy and data protection standards as compared with other forms of data processing;

- Data controllers carry out the necessary privacy impact and risk assessments (if necessary, by using trusted third parties) prior to embarking on CC projects;

- Cloud service providers ensure that they provide appropriate transparency, security, accountability and trust in CC solutions in particular regarding information on data breaches and contractual clauses that promote, where appropriate, data portability and data control by cloud users; cloud service providers, when they are acting as data controllers, make available to users, where appropriate, relevant

---

[1] See, e.g., the Group's Working paper "Cloud Computing - Privacy and data protection issues (Sopot Memorandum)", Sopot (Poland), 23./24. April 2012; http://www.datenschutz-berlin.de/attachments/875/Sopot_Memorandum.12.6.12.pdf

information about potential privacy impacts and risks related to the use of their services.

- Further efforts be put into research, third party certification, standardisation, privacy by design technologies and other related schemes in order to achieve a desired level of trust in CC; to build privacy thoroughly and effectively into cloud computing adequate measures should be embedded into the architecture of IT systems and business processes at an early stage (privacy by design);

- Legislators assess the adequacy and interoperability of existing legal frameworks to facilitate cross-border transfer of data and consider additional necessary privacy safeguards in the era of CC, and

- Privacy and Data Protection Authorities continue to provide information to data controllers, cloud service providers and legislators on questions relating to privacy and data protection issues.

All stakeholders - providers and customers of CC as well as regulators - should cooperate in order to ensure a high level of privacy and data protection and IT security.