



DATA PROTECTION AND PRIVACY ALERT

A PRIVATE AFFAIR IN THE CLOUD

The evolution of cloud computing introduces a number of complexities for the application of contemporary data privacy and protection laws in the cloud-based environment. The flexibility of cloud-based services allows for these services to be provided to numerous data subjects across various jurisdictions by any number of service providers located across the world.

On 24 April 2012, the International Working Group on Data Protection in Telecommunications published its *Working Paper on Cloud Computing – Privacy and Data Issues*, which is intended to implement data protection standards within the cloud. Although the guidelines detailed in the Working Paper are not mandatory, it appears that the intended approach to data protection in the cloud is one of uniformity, with a view to ultimately developing best practice based processing of personal information.

The recommendations under the Working Paper highlight some of the risks and complexities associated with cloud computing. The overreaching nature of the Working Paper will serve to ensure that there is no lowering of general data protection standards for processing personal data in the cloud. The Working Paper specifically advocates the following general recommendations:

- Carrying out privacy impact and risk assessments prior to embarking on cloud computing projects.
- Development of practices by cloud service providers to ensure greater transparency, security and accountability regarding information on potential data breaches; and also more balanced contractual clauses to promote data portability and data control by cloud users.

- Research, third party certification, standardisation, privacy by design technologies and other related schemes in order to achieve a desired level of trust in cloud computing.
- Legislative reassessment of the adequacy of existing legal frameworks allowing cross border transfer of personal information and consideration of additional privacy safeguards.
- Accounting for independent audit trails with regards to the location of the personal information.
- Continuity in the provision of information by data controllers to privacy and data protection authorities.

These recommendations are aligned to the general principles set out in the European Union and Safe Harbor data privacy frameworks.

The Working Paper also provides more specific recommendations, on 'best practice', 'controllers', 'cloud service providers' and 'auditing'. These specific recommendations contemplate the implementation of technical measures that can be used to determine the exact physical location where personal information is held and stored, with an audit trail specifying any copying and/or deletion of personal information. In addition, the Working Paper includes a suggestion for encryption of all personal information (both at rest and in transit) and also recommends the conclusion of agreements between data controllers and cloud service providers to expressly designate and limit the physical locations where personal information will be processed. The Working Paper specifically provides that the cloud service provider should not be entitled to use personal information in the cloud for its own purposes.

continued

It is likely that significant steps will need to be taken by cloud service providers in order to comply with the recommendations under the Working Paper and/or applicable data protection laws, which may potentially require substantial financial resources, including for procuring and implementing the appropriate technology required to give effect to the recommendations and/or laws.

In the South African context, the principles under the current draft of the Protection of Personal Information Bill (PPI) (in particular, the provisions which relate to the conditions for lawful processing of personal information and transborder

information flows) can be aligned to the recommendations under the Working Paper. The real test for cloud service providers and their customers will however be in the practical implementation of the principles under PPI. Many of the recommendations under the Working Paper will serve to provide guidance in this respect, particularly in the measures which need to be implemented to maintain a level of transparency in the supply chain of personal information in the cloud.

Tayyibah Suliman and Mukelo Ngobese

CONTACT US

For more information about our Data Protection and Privacy services, please contact:



Nick Altini
Director
National Practice Head
Competition
T + 27 (0)11 562 1079
E nick.altini@dcladh.com



Aadil Patel
Director
National Practice Head
Employment
T + 27 (0)11 562 1107
E aadil.patel@dcladh.com



Preeta Bhagattjee
Director
National Practice Head
Technology, Media and
Telecommunications
T + 27 (0)11 562 1038
E preeta.bhagattjee@dcladh.com



Brigit Rubinstein
Director
Dispute Resolution
T + 27 (0)21 481 6308
E brigit.rubinstein@dcladh.com



Simone Gill
Director
Technology, Media and
Telecommunications
T + 27 (0)11 562 1249
E simone.gill@dcladh.com



Faan Coetzee
Consultant
Employment
T + 27 (0)11 562 1600
E faan.coetzee@dcladh.com



Gillian Lumb
Director
Regional Practice Head
Employment
T + 27 (0)21 481 6315
E gillian.lumb@dcladh.com

This information is published for general information purposes and is not intended to constitute legal advice. Specialist legal advice should always be sought in relation to any particular situation. Cliffe Dekker Hofmeyr will accept no responsibility for any actions taken or not taken on the basis of this publication.

BBBEE STATUS: LEVEL THREE CONTRIBUTOR

©2012