

# DATA PROTECTION AND PRIVACY ALERT

9 October 2013

## SECURITY OF PERSONAL INFORMATION – COMPLIANCE UNDER THE PROTECTION OF PERSONAL INFORMATION BILL

With the recent approval and passing of the Protection of Personal Information Bill (Bill) by the National Assembly and its impending enactment upon signature by the President, private and public entities will have to consider and implement processes and procedures to ensure compliance with the far reaching obligations imposed by the Bill.

The Bill, when promulgated into law, will safeguard personal information, which includes, *inter alia*, information relating to the education, medical, financial, criminal or employment history of the person; any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; and the name of the person, if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

One of the conditions imposed by the Bill on persons processing (defined widely under the Bill to include the collection, receipt, recordal, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use of personal information) personal information is for such persons to ensure that the confidentiality and integrity of such information is maintained by taking appropriate, reasonable technical and organisational measures to prevent the loss of, damage to, unauthorised destruction of and the unlawful access to or processing of personal information.

This condition is critical in an age where electronic transactions have become the norm. One example is the world of online shopping which is ever increasing due to the ease with which consumers can conclude transactions and arrange for delivery of goods at the click of a button. Online transactions, by their nature, necessitate the submission and processing of large volumes of consumer data. The need to ensure that the security and integrity of such data (to the extent that it constitutes personal information) is maintained is paramount under the Bill.

*continued*

Internationally, it seems that many organisations are heeding the call for better protection and security of consumers' personal information. By way of an example, according to recent media reports, Visa, MasterCard and American Express, have announced their proposal to offer a standard to meet consumer demand for protection of personal data and also to enhance security of digital payments and simplify the consumer experience of online shopping. The new standard involves the use of digital payment tokens which will replace the card account numbers in online transactions. Device, transaction, merchant and category restricted tokens which will be used to process, authorise, clear and settle transactions (in the same way as is currently done with traditional card payments) will be generated and provided to merchants, issuers or consumers via digital wallets.

The use of these tokens will see the addition of new data fields which will require richer information about the transactions which could assist with improving fraud and the consumer's security with regards to their personal information with the tokens being limited for use only in specific environments. According to media reports, the proposed token framework is still to be presented to other card associations as well as to industry bodies.

The steps taken by global organisations in increasing data security is indicative of the emphasis being placed on this issue globally. Local entities will have to review and consider their current technological security measures so as to ensure compliance with all the requirements under the Bill, including those relating to security of personal information.

Although the Bill makes provision for a transitional compliance period of one year, the obligations imposed are extensive and steps should be taken to ensure compliance sooner rather than later.

*Simone Gill, Mukelo Ngobese and Nomsa Msibi*

# CONTACT US

For more information about our Data Protection and Privacy Services and the Protection of Personal Information Bill, please contact:



**Nick Altini**  
National Practice Head  
Director  
Competition  
T +27 (0)11 562 1079  
E [nick.altini@dlaadh.com](mailto:nick.altini@dlaadh.com)



**Aadil Patel**  
National Practice Head  
Director  
Employment  
T +27 (0)11 562 1107  
E [aadil.patel@dlaadh.com](mailto:aadil.patel@dlaadh.com)



**Preeta Bhagattjee**  
National Practice Head  
Director  
Technology, Media and  
Telecommunications  
T +27 (0)11 562 1038  
E [preeta.bhagattjee@dlaadh.com](mailto:preeta.bhagattjee@dlaadh.com)



**Brigit Rubinstein**  
Director  
Dispute Resolution  
T +27 (0)21 481 6308  
E [brigit.rubinstein@dlaadh.com](mailto:brigit.rubinstein@dlaadh.com)



**Gillian Lumb**  
Cape Town Regional Practice Head  
Director  
Employment  
T +27 (0)21 481 6315  
E [gillian.lumb@dlaadh.com](mailto:gillian.lumb@dlaadh.com)



**Faan Coetzee**  
Consultant  
Employment  
T +27 (0)11 562 1600  
E [faan.coetzee@dlaadh.com](mailto:faan.coetzee@dlaadh.com)



**Simone Gill**  
Director  
Technology, Media and  
Telecommunications  
T +27 (0)11 562 1249  
E [simone.gill@dlaadh.com](mailto:simone.gill@dlaadh.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**

### **JOHANNESBURG**

1 Protea Place Sandton Johannesburg 2196, Private Bag X40 Benmore 2010 South Africa  
Dx 154 Randburg and Dx 42 Johannesburg

**T** +27 (0)11 562 1000 **F** +27 (0)11 562 1111 **E** [jhb@dlacdh.com](mailto:jhb@dlacdh.com)

### **CAPETOWN**

11 Buitengracht Street Cape Town 8001, PO Box 695 Cape Town 8000 South Africa  
Dx 5 Cape Town

**T** +27 (0)21 481 6300 **F** +27 (0)21 481 6388 **E** [ctn@dlacdh.com](mailto:ctn@dlacdh.com)