DLA CLIFFE DEKKER HOFMEYR

6 FEBRUARY 2012

DATA PROTECTION AND PRIVACY ALERT

INTERNATIONAL CO-OPERATION TO PROTECT PERSONAL DATA

Europe is moving forward with efforts to make the protection of personal information easier, quicker and less costly.

On 25 January 2012, the European Commission (the Commission) released its proposal to reform the European Union's data protection framework for its 27 member states and 500 million individuals. The proposed framework, which provides for international co-operation between the Commission and non-European countries (such as South Africa) to achieve consistency in the protection of data and easing the flow of personal data across borders and which the Commission estimates will save businesses up to €2,3 billion a year, is subject to review by the European Parliament and member states (through the Council of Ministers) before being implemented.

The need for an international focus on data protection has arisen from a number of developments, including cloud computing that allows data to be processed in the East, stored in the USA and accessed from Europe, often resulting in the routine transfer of data between countries located inside and outside of the European Union. This places a threat on the security of data, particularly as not all countries provide the same level of data protection.

South Africa is still in the process of adopting legislation to protect personal data. The Protection of Personal Information Bill is in its fifth draft having last been debated by the Committee of Parliament on 10 October 2011. Considering the ever increasing volume of data being processed and transferred at the click of a button, it would make sense for the drafters of the South African legislation to consider the latest developments in Europe.

continued

IN THIS ISSUE

Multinational companies doing business in and from South Africa are dependent on binding corporate rules regulating the transfer of data to and from Europe, which requires that the rules must be verified by at least three data protection authorities in advance. The proposed framework will eliminate this red tape as the rules will only be required to be approved by a single data protection authority in Europe. The approval in Europe will also apply in South Africa.

Faan Coetzee

CHANGES TO EU PRIVACY LAWS

New draft Regulations (to the current EU Data Privacy Protection Directive) that seek to set out a revolutionary legal framework in efforts to enhance the protection of personal data in the European Union (EU), have been published for comment by the European Commission.

These Regulations impose more stringent obligations on data controllers and enhance the rights of data subjects by allowing for greater transparency as to how, where and by whom personal data is used and stored and introduce various new provisions, including in respect of breach notification mandates, increased enforcement measures and penalties, rules relating to explicit opt-in rights for data subjects in respect of direct marketing and behavioural advertising, data protection officer requirements in some instances and data protection impact assessments. In addition, the Regulations also propose revised provisions in respect of the cross border transfer of personal information outside of the EU.

Although South African legislators have to a certain extent already contemplated and addressed a number of these issues in the Protection of Personal Information Bill (PPI Bill), the Regulations should be considered in order for South Africa's data protection laws to be aligned to international trends shaping data privacy. In particular, consideration will need to be given to the critical nuances introduced by the Regulations, such as the inclusion of online identifiers (including IP addresses or cookie identifiers) in the definition of a 'data subject' and the introduction of the concept of data portability (which entitles a data subject a new right to obtain a copy of its data in a "structured format which is commonly used" and the right to transfer data from one automated processing system, such as a social network, to another without any intervention by the data controller) which extend the scope of data privacy protections.

The Regulations, once approved, will apply to any data subject in the EU irrespective of where the data controller or its equipment is located. Notwithstanding the enactment of the PPI Bill, if any person in South Africa processes the personal information of a data subject located in the EU, it will be subject to the Regulations and will be required to designate an EU representative to act as a controller and be answerable to the EU data protection authority on its behalf.

Simone Gill, Tayyibah Suliman and Genevieve Mojapelo

DIRECT MARKETING IN THE CONTEXT OF PRIVACY REGULATION

The ever growing volume of consumer complaints relating to unsolicited and unwanted commercial messages seems to be having a legislative effect, as the issue of privacy and the right to reject and not receive unsolicited commercial messages is a theme in existing pieces of legislation and in the draft Protection of Personal Information (PPI) law.

The Electronic Communications and Transactions Act, 2002 (the ECT Act) was groundbreaking in that, for the first time, the legislature addressed the issue of spam, or unwanted unsolicited commercial electronic communications.

The ECT Act prescribes that in the case of electronic unsolicited messages, such as spam emails and SMS's, the sender must include in the message an option for the consumer to cancel their subscription to the mailing list, ie to opt out. In addition, the ECT Act provides that if the consumer requests it, the parties sending the message must disclose the source from which that person obtained the consumer's personal information. Failure to comply with these provisions actually constitutes a criminal offence. Yet, from the advent of the ECT Act to the coming into effect of the Consumer Protection Act, 2008 (the CPA) nearly a decade later, it seems as though few, if any, marketers even knew of the provisions of the ECT Act, and even fewer complied with them. There is certainly no readily traceable record of successful prosecutions of errant marketers under this provision.

The fanfare that accompanied the enactment of the CPA drew attention to its provisions. Since the CPA took effect on 1 April 2011, there has been a noticeable attempt at compliance by advertisers with its privacy provisions. The CPA provides every consumer the right not only to ask direct marketers to desist from engaging in any direct marketing practice (whether electronic or otherwise), but also to pre-emptively block any such communications (other than personal approaches).

The CPA, read with its regulations, goes much further. It is intent on creating a national registry of pre-emptive blocks and creating a regulatory regimen in terms of which a direct marketer simply will not be able to send direct marketing communications to a consumer unless they have, post 1 April 2011, first obtained the consumer's consent to do so (which only applies to existing customers and is subject always to the right of the consumer to opt out at a later stage). Alternatively, the direct marketer must have first checked with the National Registry that the consumer has not, in fact, registered a pre-emptive block against the particular mode and type of direct marketing, or the direct marketer itself.

The PPI Bill also seeks to regulate the issue of direct marketing and unsolicited communications. In this case, the Bill refers specifically to electronic communications and so there is only a degree of overlap with the provisions of the CPA, but not a complete concurrence. The draft Bill does contemplate that the provisions of the ECT Act described above will be repealed and replaced under the Bill. What the Bill provides is that it will simply be illegal for a direct marketer to seek to engage in direct electronic marketing (which includes by automated calling machine, fax, SMS or email) unless the data subject has given prior consent to the activity and/or the data subject is an existing customer of the marketer.

In this case, the term "existing customer" is defined and the Bill makes it clear that one can market directly to an existing customer if the contact details of that customer have been obtained in the context of a sale of a product or service for the purpose of marketing similar products or services (ie the details were not taken for some other purpose and the direct marketing function was not disclosed). The customer must also be given a reasonable opportunity to object, free of charge, to such use of their electronic details at the time when the information was collected and afterwards, in each and every electronic communication sent to the data subject for the purposes of marketing.

It is also made clear that every direct marketing message must contain details of the identity of the sender or the party on whose behalf it is sent, and the mode by which the recipient can send a request asking that such communication cease.

The legal landscape for direct marketing, while being consistent with provisions that have already been in place under the ECT Act for some period of time, looks set to become more rigorous in the sense that there is every indication from policy makers and government that compliance with the CPA and the PPI Bill, when it is eventually enacted, will be far more vigorously enforced. At the same time, the advent of an era of consumer protection under the CPA has created unprecedented levels of awareness on the part of consumers of their rights in law and it is to be expected that consumer activism on its own will account for a considerable lessening of direct marketing activities overall, as consumers find their voice to request that such activities cease.

Nick Altini

EMAIL ARCHIVING AND THE LAW

The use of email for business purposes has already, to a large degree, replaced many of the more conventional methods of communication, resulting in organisations being faced with the sometimes onerous task of implementing and maintaining effective systems and processes to maintain control over essential business communications. In addition to general information retention provisions found in various pieces of legislation that will in most instances also apply to information obtained electronically, the Electronic Communications and Transactions Act, 2002 (ECT Act) contains specific provisions detailing how electronic communications are to be stored and the manner in which to prove the integrity of those communications.

The ECT Act legitimises electronic communications by:

- Providing that electronic communications be treated in the same way as more traditional forms of communication.
- Prescribing that information is not without legal force and effect merely because it is in electronic form, while recognising that electronic communications may be easily manipulated and accordingly, that the integrity of the document is only legally viable if the information has remained unaltered.

The ECT Act, supported by various judicial decisions, has made it clear that evidence is not inadmissible simply because it is in electronic form. However, the integrity of the electronic evidence is vital. The ECT Act provides that electronic evidence must be given "due evidential weight", which will depend on a number of factors, including the reliability of the manner in which the electronic evidence was generated, stored or communicated and the manner in which the originator was identified.

In order for electronic communications to be treated equally to paper based counterparts, organisations are to ensure that they implement and maintain good email and document management systems. This is necessary to ensure that the handling of electronic information complies with the specific requirements set out in the ECT Act for the storage of electronic communication. Implementing these systems will require appropriate policies, email disclaimers and the use of robust technology, keeping in mind that the integrity of an email must be maintained for its entire life span, from capturing and retrieval to deletion.

The storage and security of personal information will be largely impacted by the Protection of Personal Information Bill (the Bill), once enacted.

The Bill aims to promote and enforce the constitutional right to privacy, by safeguarding personal information. It imposes stringent obligations on persons holding and processing personal information and also imposes system security requirements.

Although it is not yet clear what will be considered appropriate and reasonable under the Bill, organisations must ensure that stringent security requirements, including access controls, user identification and comprehensive indemnity provisions, are in place to safeguard the security of personal information.

Simone Gill and Victor Omoighe

DLA CLIFFE DEKKER HOFMEYR

CONTACT US

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

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

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

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

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

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

Brigit Rubinstein
Director
Dispute Resolution: Litigation, Arbitration and Mediation
T + 27 (0)21 481 6308
E brigit.rubinstein@dlacdh.com

Simone Gill
Director
T + 27 (0)11 562 1249
E simone.gill@dlacdh.com

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

CAPE TOWN

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

5th floor Protea Place Protea Road Claremont 7708, PO Box 23110 Claremont 7735 South Africa
Dx 5 Cape Town
T + 27 (0)21 683 2621 **F** +27 (0)21 671 9740 **E** ctn@dlacdh.com

www.cliffedekkerhofmeyr.com

EVERYTHING MATTERS