8 FEBRUARY 2016

DATA PROTECTION AND PRIVACY ALERT

IN THIS **ISSUE**

THE SINKING SHIP OF TRANSATLANTIC DATA TRANSFERS

International trade and modern day communication necessitates cross-border flows of personal information around the world. Social networks are but just one medium for the international transfer of personal information. One of the objectives of the Protection of Personal Information Act, No 4 of 2013 (POPI) is to regulate flows of personal information across the borders of South Africa, and protect the interests of free flows of information internationally.

CDH
CLIFFE DEKKER HOFMEYR

THE SINKING SHIP OF TRANSATLANTIC DATA TRANSFERS

POPI establishes the office of the Information Regulator which is tasked with assessing the adequacy of foreign data protection regimes where personal information and particularly special personal information is transferred and processed in a country abroad.

International trade and modern day communication necessitates cross-border flows of personal information around the world. Social networks are but just one medium for the international transfer of personal information. One of the objectives of the Protection of Personal Information Act, No 4 of 2013 (POPI) is to regulate flows of personal information across the borders of South Africa, and protect the interests of free flows of information internationally.

The Safe Harbour Decision was conveyed in light of Article 25(6) of Directive 95/46/EC (the Privacy Directive), which states that a third country ensures an adequate level of protection in light of all the circumstances surrounding a data transfer operation or set of data transfer operations, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations by the Commission, for the protection of the private lives and basic freedoms and rights of individuals.

POPI establishes the office of the Information Regulator which is tasked with assessing the adequacy of foreign data protection regimes where personal information and particularly special personal information is transferred and processed in a country abroad.

During July 2000, the United States (US) Department of Commerce issued the 'Safe Harbour Privacy Principles', with the hope of fostering and promoting the development of transatlantic international trade. The main aim of the Safe Harbour Principles was to provide a practical platform which would facilitate transatlantic data flows and thus trade between the US and the European Union (EU). Essentially, Safe Harbour certification created the presumption of 'adequacy' solely for US entities receiving personal data from the EU. In order for an entity to achieve Safe Harbour 'self-certification', a US based entity would simply have to submit a letter containing its contact details, a description of the activities of the organisation in relation to the personal information it received and a description of the organisation's privacy policy relating to the manner in which they processed personal information. The letter would need to be signed by a corporate officer on behalf of the organisation and sent to the US Department of Commerce which would maintain a list of certified entities.

Decision 2000/520 (Safe Harbour Decision) of the EU Commission (Commission) recognised the adequate level of data protection for personal data transferred from the EU to the US. The Safe Harbour Decision was conveyed in light of Article 25(6) of Directive 95/46/EC (the Privacy Directive), which states that a third country ensures an adequate level of protection in light of all the circumstances surrounding a data transfer operation or set of data transfer operations, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations by the Commission, for the protection of the private lives and basic freedoms and rights of individuals. The Safe Harbour Decision was a beacon of global trade but its validity has recently been struck down after scrutiny by Europe's highest court in the case of *Maxmillian Schrems v Data Protection Commissioner and Digital Rights Ireland Ltd* (C-362/14).

Mr Schrems, an Austrian national, was a user of the social network Facebook since 2008. Any person wishing to sign up with Facebook in the EU would conclude a contract with the relevant subsidiary (in Mr Schrems's case, Facebook Ireland) of the US based Facebook Inc. Naturally, some or all of Mr Schrems and any other Facebook user's personal data would

CDH
CLIFFE DEKKER HOFMEYR

THE SINKING SHIP OF TRANSATLANTIC DATA TRANSFERS

CONTINUED

In June 2013, Mr Schrems lodged a complaint with the Data Protection Commissioner (Commissioner) asking that the Commissioner exercise its statutory powers by prohibiting Facebook Ireland from transferring his personal data to the US.

be transferred to Facebook Inc's servers located in the US where such data is processed. In June 2013, Mr Schrems lodged a complaint with the Data Protection Commissioner (Commissioner) asking that the Commissioner exercise its statutory powers by prohibiting Facebook Ireland from transferring his personal data to the US. At the heart of Mr Schrems's complaint was the contention that US law and practice did not ensure adequate protection of his personal data held in US territory against surveillance by the US public authorities. The complaint was couched in light of the revelations made by Edward Snowden concerning activities of the US intelligence services and in particular the National Security Agency (NSA). The Commissioner was of the view that it was not required to investigate the complaint because Mr Schrems failed to prove that the NSA had accessed his personal data and further, because the transfer of data had to be considered in light of the Safe Harbour Decision which found the US level of data protection to be adequate. Mr Schrems then brought an action to the High Court of Ireland who found that the mass and undifferentiated accessing of personal data is clearly contrary to the principle of proportionality and fundamental right to privacy entrenched in the Irish Constitution. The High Court went on to observe that the action brought by Mr Shrems challenged, although not explicitly, the legality of the Safe Harbour Decision and the regime operating under it. Accordingly, the High Court referred the following questions to the Court of Justice for the European Union (CJEU): Whether a data protection office bearer in the position of the Commissioner is bound by community rulings such as the Safe Harbour Decision? Alternatively, can the office bearer conduct his/her own investigation of the matter in light of the relevant factual developments?

The CJEU noted that the Privacy Directive requires EU member states to set up national supervisory authorities responsible for monitoring, with complete independence, compliance with EU rules regarding cross-border transfers of personal data. It went on to note that the national supervisory authorities are required to ensure a balance between the observance of the fundamental right to privacy on the one hand and the interests of requiring free movement of personal data on the other. To this end, national supervisory authorities have broad investigative powers, but are limited to personal data processed within their own countries. However, the CJEU went onto note that where an EU member state transferred data to a third country (as was the case for Mr Schrems) this certainly fell within the ambit of the Commissioner's powers. In finding that the Commissioner indeed had a duty to monitor the level of adequacy of the US's data protection laws and practice, the CJEU held that the Safe Harbour Decision did not have the effect of preventing the Commissioner from investigating Mr Schrem's complaint.

CDH
CLIFFE DEKKER HOFMEYR

THE SINKING SHIP OF TRANSATLANTIC DATA TRANSFERS

CONTINUED

Mass surveillance under the guise of national security could also be a cause for concern for South Africans with intrusive legislation such as the Protection of State Information Bill and the Cybercrimes and Cybersecurity Bill on the table.

The CJEU then went on to consider the validity of the Safe Harbour Decision and fundamentally, the validity of the long standing Safe Harbour regime which had underpinned transatlantic data flows for more than a decade. In underlining the wording of Article 25(6) of the Privacy Directive, which states that a third party 'ensures' an adequate level of protection by reason of its domestic law or international commitments and that such must be assessed for the protection of the private lives and basic freedoms and rights of individuals, the CJEU emphasized the high level of protection required by countries to which personal data travels from the EU. Touching on the requirement of 'adequacy' (which is not defined in the Privacy Directive) the CJEU drew attention to the fact that the term 'adequate' meant that a third country recipient did not need a system with as stringent data protection laws as the EU. Furthermore, the CJEU highlighted that Article 25(2) of the Privacy Directive requires an assessment of the receiving country's data protection laws and practice in light of 'all surrounding circumstances'. It held that the reliability of an 'adequate system' is:

> "founded essentially on the establishment of effective detection and supervision mechanisms enabling any infringements of the rules ensuring the protection of fundamental rights, in particular the right to respect for private life and the right to protection of personal data, to be identified and punished in practice." (at paragraph 81)

The CJEU noted the weaknesses in the US data protection system exposed by the Snowden leaks and that many US entities were not complying with the Safe Harbour Principles in practice. This drew the CJEU to the conclusion that the Commissioner was obliged to investigate Mr Schrems's complaint with due diligence and furthermore, that the Safe Harbour Decision is now invalid.

US and EU officials are currently in discussions over a new framework for transatlantic data flows which meet the requirements of the adequacy determination.

With South African data protection law still in its infancy and the duties of the Information Regulator's office defined in POPI still confined largely to paper, it will be interesting to see how the South African law is applied and how the office of the Information Regulator manages cross-border flows of personal information. Although POPI has been signed into law by the President, a number of its provisions are yet to come into full force and effect. Mass surveillance under the guise of national security could also be a cause for concern for South Africans with intrusive legislation such as the Protection of State Information Bill and the Cybercrimes and Cybersecurity Bill on the table. When one considers the number of entities and the vast quantity of personal data exchanged through business conducted on the basis of Safe Harbour Decision, the importance of protecting individual privacy rights in the digital age cannot be understated.

Bilal Bokhari and Simone Gill

CDH
CLIFFE DEKKER HOFMEYR

OUR TEAM

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

Preeta Bhagattjee
National Practice Head
Director
T +27 (0)11 562 1038
E preeta.bhagattjee@cdhlegal.com

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

Christoff Pienaar
Director
T +27 (0)21 481 6350
E christoff.pienaar@cdhlegal.com

Fatima Ameer-Mia
Senior Associate
T +27 (0)21 481 6374
E fatima.ameermia@cdhlegal.com

Tayyibah Suliman
Senior Associate
T +27 (0)11 562 1248
E tayyibah.suliman@cdhlegal.com

Mariska van Zweel
Senior Associate
T +27 (0)21 481 6345
E mariska.vanzweel@cdhlegal.com

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@cdhlegal.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@cdhlegal.com

CDH
CLIFFE DEKKER HOFMEYR