Knowledge Exchange

OALP Client Update

Olaniwun Ajayi LP

Data Protection - Lessons from the Safe Harbour Ruling

November, 2015

Introduction

On 6 October 2015, the European Court of Justice (**ECJ**) delivered a ruling in relation to the US-EU Safe Harbour Framework (European Commission's trans-Atlantic data protection agreement of 2000), an agreement between the United States Department of Commerce and the European Union (the **Agreement**) which allowed US companies to self-certify (give the assurance without the need to expressly seek consent) that they would protect the data of EU citizens when it is transferred from the EU to the US. The ECJ ruling however invalidated the self-certify mechanism, thereby effectively nullifying the Agreement.

Background

Up until 2000 when the Agreement came into force, the personal data of EU citizens could not be transferred to the US without the prior consent of data owners, due to the stringent EU directive on data protection. The Agreement was therefore a policy compromise in response to the EU directive which differed from the more lenient data protection policies in the US. US Companies that wanted to take benefit of the Agreement were required to annually self-certify that they would comply with the principles which underpin the Agreement thereby removing the need for US companies to enter into bilateral agreements seeking the consent of data owners to the transfer of their data to the US.

In an aftermath case following the 'Snowden revelations', the ECJ in its ruling held that the protection of personal data transferred from the EU to the US cannot be guaranteed as US policy considerations such as national security and public interest superseded the Agreement and in these circumstances, personal data could be disclosed without the consent of the data owners. The Agreement was thus invalidated.

Now that the ECJ ruling has been delivered, American companies such as Facebook and Google seeking to transfer personal data from the EU to the US, cannot rely on self-certification and must revert to the position pre-2000 by generating contract clauses and data protection policies seeking the consent of data owners in order to expressly guarantee an adequate level of protection in line with EU laws.

For further information, please contact Intellectual Properties Practice:
IP@olaniwunajayi.net, Olaniwun Ajayi LP
The Adunola, Plot L2, Banana Island, Ikoyi, Lagos.
+234 1 270 2551

This publication is provided to highlight issues and for general information purposes only, and does not constitute legal advice. Whilst reasonable steps were taken to ensure the accuracy of information contained in this publication, Olaniwun Ajayi LP accepts no responsibility for any loss or damage that may arise from reliance on information contained in this publication. Should you have any questions on issues reported here or on other areas of law, please contact the editors or any counsel in the firm

Implications for Nigeria-Cloud Storage

Storage of data on 'the cloud' is increasingly becoming, for various reasons, the preferred method of storing both corporate data and client data. Data storage on the cloud raises data protection concerns and calls to question the choice of jurisdiction of storage, and the adequacy of the data protection legal framework in the jurisdiction of storage.

Nigerian corporates whose choice of jurisdiction of storage is the EU, for example, or whose professional advisers select the EU as their jurisdiction for data storage, now have increased comfort regarding the level of data protection given to such data in the wake of the ECJ ruling. Where the choice of storage is the USA or Nigeria, the guarantee for protection of data remains minimal. Whilst Section 37 of the Constitution grants every Nigerian citizen the right of privacy, Nigeria does not currently have dedicated data protection legislation thus exposing Nigerian citizens to the risk of their personal data being transferred from Nigeria and used without their consent. Related to the matter of protection of client or customer data is the pertinent question of consent to storage of client or customer data and intellectual property, in a jurisdiction other than that in which the firm or company servicing the client/customer resides.

Another possible risk of the exposure of personal data is the use of private email accounts for official/work related emails. Unlike official email accounts which are usually accompanied with a layer of security systems which guarantee a certain level of security of any information which passes through a company's email server, and whose server storage location is ascertainable, the level of security provided by private email service providers cannot be guaranteed, particularly where the locations of the providers cannot be ascertained beforehand.

Conclusion

Whilst the lacuna in Nigerian law remains, Nigerian citizens are particularly vulnerable to the risk of their data being exploited or exposed. The alternative locations of storage notably the EU are not however devoid of limitations. Consequently, corporates are required to, to some extent, self-regulate themselves and should ensure that they have in place, a robust corporate data protection and intellectual property protection policy which provides sufficient protection for personal and client data and ensures that personal information is not transferred without the free and informed consent of the owner. They should also be mindful of their choice of server location, choosing as far as possible, for cloud storage, a jurisdiction which has a robust data protection legal framework.

For further information please contact our Intellectual Property Practice at:

IP@olaniwunajayi.net

Olaniwun Ajayi LP
The Adunola,
Plot L2, 401 Close
Banana Island,
Ikoyi, Lagos.
+234 1 270 2551

This publication is provided to highlight issues and for general information purposes only, and does not constitute legal advice. Whilst reasonable steps were taken to ensure the accuracy of information contained in this publication, Olaniwun Ajayi LP accepts no responsibility for any loss or damage that may arise from reliance on information contained in this publication. Should you have any questions on issues reported here or on other areas of law, please contact the editors or any counsel in the firm