KTA ADVOCATES

INNOVATE.
GROW.
DISCOVER.

# KTA
# DATA PRIVACY ALERT

By Kenneth Muhangi

CAMANI IP NETWORK

ktaadvocates.com

KTA ADVOCATES

# Cross Border Transfer of Data in Uganda & Schrems II

In the Fourth Industrial Revolution (4IR), it would be wholly impractical for any organization, irrespective of sector, to do business, let alone cross border business, without the ability to transfer data. In Uganda, transfer of data across borders is in most instances a necessity owed to the relatively limited infrastructure required to store or process data.

Such transfer is regulated by section 19 of Uganda's Data Protection & Privacy Act (DPPA) that provides that where a data processor based in Uganda processes or stores personal data outside Uganda, the processing shall only be lawful with consent of the data subject; further that the processor shall ensure that the receiving country has an equivalent level of protection to that in Uganda.

Section 19 is analogous to Article 46 of the General Data Protection Regulation (GDPR) that offers wider considerations when dealing with cross border transfer of data. The GDPR has congealed the importance of observance of best practice when dealing with cross border transfer of data. Article 3 in particular, extends the scope of the GDPR to cover data processed outside the EU, as long as the data relates to a data subject who is a citizen of any of the EU countries.

Article 46, provides that any transfer of personal data to a third country can only take place if certain conditions are met by the data exporter and the data importer. For an entity to lawfully transfer or process personal data outside of the EU, that entity must identify a valid transfer mechanism to legally transfer that personal data.

Consequently, entities domiciled or operating in Europe and which carry out business whether directly or indirectly with markets out of Europe (such as the United States or Uganda) must ensure that the receiving country is possessed of adequate data protection laws that will protect EU citizens. In the absence of adequate regulation, the General Data Protection Regulation (GDPR) allows a data controller

to transfer/process personal data outside the EEA using appropriate safeguards  such as EU adopted or approved standard contractual clauses (SCC's), Codes of Conduct and/or Binding Corporate Rules. In addition, the company in question must ensure that data subjects have enforceable rights and effective legal remedies in the third country.

[1] *In 2019, Uganda passed into law its Data Protection and Privacy Act, mirrored against the GDPR*

Key under such SCC's is consent and right to be forgotten, which was first introduced by the European Court of Justice (ECJ) in a case involving Google Spain , where the ECJ affirmed that data subjects have a "right to be forgotten" and held that Google must delete "inadequate, irrelevant or no longer relevant" data from its results when a member of the public requests it.

The European Commission also has the power under Article 45, to review a third country's legal system, domestic law and international commitments to determine whether it ensures an adequate level of protection for personal data. On 12th July 2016, the EU did utilize such power in (EU) 2016/1250 and ruled that the US had adequate protection to enable data transfers under EU law pursuant to the EU/US Privacy Shield Framework. The EU/US Privacy Shield provided guidance on the secure sharing/transfer of personal data between the EU and US and was revered as a valid mechanism to aid companies comply with EU data protection requirements.

# Schrems II, Surveilance and Standard contractual clauses (sccs)

On 16 July 2020, the Court of Justice of the European Union (CJEU) in C-311/18 (Schrems II) invalidated the Safe Harbor/Privacy shield framework between the European Union (EU) and the United States (US). Consequently, any transatlantic data transfers to the US from the European Economic Area (EEA) and relying on the Privacy Shield are now illegal.

On invalidating the shield framework, the CJEU held that US surveillance laws were incongruent with Article 45(1) of the GDPR, read in light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union (CFREU) .

On interpreting whether the EU Commission in its earlier decision had succinctly addressed the issue of the US having an adequate level of protection, the CJEU held that in Implementing Decision (EU) 2016/1250, the Commission failed to consider Article 7 on respect for private and family life, Article 8 on protection of personal data and Article 47 on the right to an effective remedy and to a fair trial of the CFREU. The provisions would in essence act as a sort of SI indicator for what amounts to an adequate level of protection in a third country.

[2] *https://gdpr-info.eu/art-46-gdpr/*
[3] *https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62012CJ0131*
[4] *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG*
[5] *https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf*
[6] *https://www.privacyshield.gov/Program-Overview*

The decision reinforces/supplements decisions from other jurisdictions that have underpinned the importance of data and privacy as human rights. In 2017, the Supreme Court of India in Justice K.S. Puttaswamy (Retd.) & Anor. v Union of India & Ors, WP (Civil) 492 of 2012, declared that privacy is a fundamental right protected under the country's constitution for each of its over 1.3 billion citizens.

Using the same stare-decisis, and In light of the court’s concerns around the US surveillance activities and lack of redress mechanisms for data subjects, it is likely that the CJEU would reach the same conclusion for Uganda whose surveillance laws such as the Regulation of Interception Act (RICA) do not surmise the safeguards envisioned by the DPPA and the GDPR.

# Standard Contractual Clauses (SCCs)

The CJEU in its decision did not invalidate SCCs and BCRs but emphasized that even when using such standard contractual clauses, organizations must assess the level of personal data protection offered in the US, taking into account the circumstances of each particular transfer and any supplementary protection measures they take themselves.

In particular, section 128 of the CJEU judgment states that;

"Article 46(1) of the GDPR provides that, in the absence of an adequacy decision, a controller or processor may transfer personal data to a third country only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. According to Article 46(2)(c) of the GDPR, those safeguards may be provided by standard data protection clauses drawn up by the Commission."

Further, according to sections 131 and 132 of the CJEU ruling, it is incumbent upon the controller or processor established in the European Union to provide adequate safeguards in the form of SCCs which may be adopted and/or supplemented by the Commission.
Uganda's DPPA does not specifically provide for SCCs but under section 7 (2) (C) personal data may be collected and/or processed in furtherance of a contract to which the data subject is party and under 17 (2) (e) of the DPPA, 2019 a person who processes personal data shall take into account the contractual rights and obligations between the data subject and processor.

[7] *Section 198 of the C-311/18 judgment*
[8] *C-311/18 judgment*

We may discern therefore that Data controllers and processors (recipients) in utilizing SCC's are advised to;

1. Mutually undertake to ensure that the processing and transfer of data pursuant to SCCs, has been and will continue to be carried out in accordance with 'the applicable data protection law', and with due consideration to the fundamental rights and freedoms of individuals, and in particular, their right to privacy.

2.The recipient of data is required to notify within reasonable time, the controller ofany inability to comply with its obligations under the contract concluded.

3. Suspend the transfer of data and/or to terminate the contract where the recipient is not, or is no longer, able to comply with the standard data protection clauses. Unless the controller does so, it will be in breach of its obligations the appropriate law .

4. Ensure that the controller and recipient of personal data satisfy themselves that the legislation of the third country of destination enables the recipient to comply with the standard data protection clauses. Conversely, compliance with an obligation prescribed by the law of the third country of destination which goes beyond what is necessary for those purposes must be treated as a breach of those clauses.

5. The data controller and the recipient of personal data are required to verify, prior to any transfer, whether the level of protection required by the appropriate law of the sending country, is respected in the third country concerned. The recipient is, where appropriate, under an obligation, to inform the controller of any inability to comply with those clauses, the latter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract .

[9] *Section 128, Case 311/18*
[10] *Section 138 Case 311/18*

6. Pursuant to 5 above, If the recipient of personal data to a third country has notified the controller, that the legislation of the third country concerned does not allow him or her to comply with the standard data protection clauses, it follows that data that has already been transferred to that third country and the copies thereof must be returned or destroyed in their entirety .

7. A controller is obligated to, where special categories of data could be transferred to a third country not providing adequate protection, to inform the data subject before, or as soon as possible after, the transfer.

8. Should the data subject object to any transfer pursuant to standard data protection clauses, the controller is obligated to notify the competent supervisory authority of any such objection.

[11] *Section 139 Case 311/18*
[12] *Section 140 Case 311/18*
[13] *Section 141 Case 311/18 incorporating advice from the Advocate General*
[14] *Section 142 Case 311/18*
[15] *Section 143 Case 311/18*
[16] *Section 144 Case 311/18*

# Conclusion

The CJEU judgment inter-alia re-emphasizes the power/importance of data oversight authorities and the effect a single decision can have on entire industries that depend on cross border transfer of data. This is the second time the CJEU has negated a data transfer framework with the US and in both instances citing trepidations over the US's surveillance activities and lack of an adequate level of protection for personal data. Uganda's own DPA should take cognizance of such decisions and work towards bringing her laws in line with international best practice.

***Kenneth Muhangi*** *is a Lecturer of IP and ICT Law, Managing Partner at KTA Advocates (Technology, Media, Telecommunications & Intellectual Property), represents Uganda at the 4IR Portfolio Communities of the Centre for Fourth Industrial Revolution of the World Economic Forum, External advisor to the Ministry of ICT on innovation and ICT policy development and is a consultant with the World Bank.*

# TMT & IP Team

KTA ADVOCATES

# Team

**Kenneth Muhangi**
Managing Partner

**Dorothy N Nankunda**
Senior Associate

**Hilary Ahimbisiwe**
Junior Associate

**Bonita Mulelengi**
Senior Associate

**Margaret Nyakusemera Kabanyoro**
Junior Associate

**Judith Kagere**
Junior Associate

KTA ADVOCATES

**Shamila Nakanwagi**
Junior Associate

KTA
ADVOCATES

## Contact Us

Floor 3, Plot 4 Hannington Road
Kampala, Uganda,P.O. Box 37366,

+256 414 530 114 / +256 414 531 078

partners@ktaadvocates.com