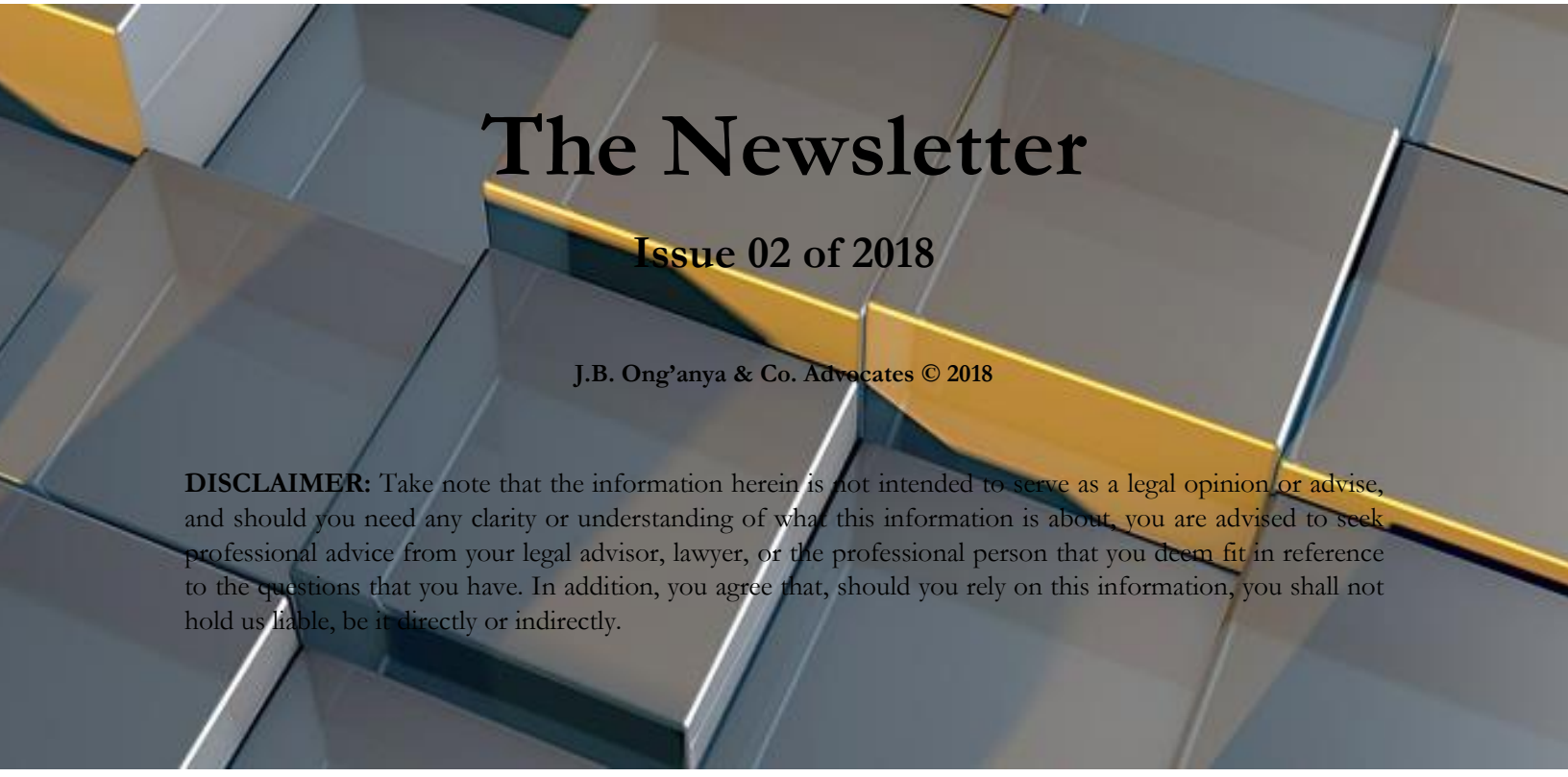
J.B. Ong'anya & Co.
Advocates



The Newsletter

Issue 02 of 2018

Introduction

The European Union (the "EU") enhanced its Data Laws when it passed the General Data Procedure Rules (the "GDPR") on May 25, 2016. The GDPR came into effect on May 25, 2018, thus, there was a transition period of two years.

Other than the GDPR addressing the loopholes that existed. The GDPR is in place to address current and future activities that fall under Data Protection.

The GDPR addresses the collecting, recording, organising, storing, using, disclosing, and disseminating of Data.

Why is GDPR Relevant to Kenya or African based entities?

Unlike before, the GDPR applies to all entities that have presence in the EU, and that does not matter whether it is accessed in one EU State or by a handful people in the EU or one EU State.

Therefore, if any entity that is outside the EU has presence in the EU and collects whatsoever form of Data from the members of the EU, then it is prudent that the company should set measures that are in line with the GDPR.

How does one establish presence?

The GDPR is influenced by two significant cases that were decided by the Court of Justice of the European Union (the "CJEU"). In C-131/12 (the "Google Case") and C-230/14 (the "Weltimmo Case") the concept of establishment of presence was addressed in broad terms whereby in the Google Case it addressed the physical establishment while in the Weltimmo Case it addressed the virtual establishment.

Therefore, if one has a company or its subsidiary in the EU, the entity needs to comply with the GDPR, while if its online presence penetrates to EU Citizens, the operations of the website, inclusive of the company owning it, must comply with the GDPR.

Classification of Data?

The GDPR classifies Data into two general categories that ought to be observed by entities that collect or process such data from the EU Citizens. Under the GDPR, there are two classes of Personal Data: Identifier Personal Data, and Sensitive Personal Data. The information in those groups are treated with different magnitude, based on the GDPR.

Does this obligation end with the entity having presence in the EU?

The entity having presence in the EU will need to vet its vendors or service providers if they are compliant with the GDPR. For instance, if a Kenyan company collects data from France but the Data is stored in a separate entity established in South Africa, it will be important for the Kenyan entity to make sure that the Data handlers are compliant with the GDPR.

Who is a Data Processing Officer (the "DPO")?

Depending on the operations of the entity, it might be imperative that the entity appoints someone in the EU as its DPO who will be in charge of effecting the purpose of the GDPR.

Are there penalties for Non-Compliance?

The GDPR provides for penalties for non-compliance with the GDPR. These penalties fall under Criminal and Civil category, and in certain instances will take effect as violation of Human Rights.

J.B. Ong'anya & Co. Advocates

KENYA: Offences under the Computer Misuse and Cybercrimes Act, 2018

Offences	The law	Comments
Unauthorised access	Occurs when a person knows they do not have the authority to access certain information but makes effort to access the information.	The important question is whether the person accessing the information does have the authority to do so.
Access with intent to commit further offence	Occurs when one unlawfully or lawfully gains access and commits an offense or facilitates commission of an offence.	The provision is interlinked with the one for "Unauthorised Access". Whereby one gains access and commits an offence. However, the provision also provides that one can commit an offense even if access to the system was secure/authorised.
Unauthorised interference	Takes place when a person's action is intentional and without authorization, not to mention it leads to a certain interference.	The provision provides that **Unauthorised Interference** can only take place on condition that there exists "**intention**" and "**lack of authority**".
Unauthorised interception	Takes place when a person's action is intentional and without authorization, which leads to intercepting or causes interception whether directly or indirectly and leads to transmission of data.	The provisions adopt the conjunctive word "and". Therefore, there is need of **intention** and **lack of authority**. In addition, there is a loophole on what happens if there is no transmission of data.
Illegal Devices and Access Codes	It is an offence for one to provide or receive any device or access codes that can lead to any of the offenses mentioned in Part II of the Act (the offenses highlighted in the newsletter).	The act of providing or receiving the device or access codes ought to be from a point of being aware that the device or access codes are for purposes of committing a certain offense.
Unauthorised Disclosure of Password or Access Codes	A person who knowingly and without authority discloses password or access codes will be held liable.	There must be an aspect of knowledge and lack of authority.
Cyber espionage	Occurs when a person unlawfully and intentionally performs, authorizes or allows one to perform any of the offenses for purposes of gaining access, and intercept data. Anyone who uses National critical information for the benefit of another State against Kenya will be held liable.	Also, in this case, the person ought to have acted unlawfully and intentionally.

False publication	The intentional act of publishing false, misleading or fictitious information with the intent of it being acted upon as authentic, will lead to an offence.	The two important factors are "**intention to publish the information**" and having the "**intent that it should be believed to be true**".
Publication of False Information	It only occurs when false information is published in print, broadcast, data or over computer system with the main aim of causing panic, chaos or violence among citizens of Kenya or likely to lead to discrediting a person's reputation.	One has to **knowingly** publish false information, and there must be the **aim** to discredit a person's reputation, cause panic, chaos or violence.
Child pornography	Publishing, Producing, or Possessing child pornography is an offense. It does not matter whether the information is in audio, or visual format.	The provision uses a disjunctive, therefore, any of the three applies separately, but can also be applied conjunctively. There are certain statutory defences, for instance, holding them in good faith for scientific research, medical or law enforcement.
Computer forgery	A person who deletes or distorts computer data with the view of presenting alternative data as authentic will be deemed to have committed an offence under the Act.	It does not matter whether a person has been given such authority as long as the act is intentional and meant to present inauthentic computer data as authentic.
Computer fraud	Occurs when a person with fraudulent or dishonest intent unlawfully gains, causes unlawful loss, or attains an economic benefit through the other offenses mentioned, the person will be held liable.	The offenses are restricted to what the Act is providing, and it is also important that there is an element of fraud or dishonesty that is coupled with intent.
Cyber harassment	It takes place when an individual or as a group of persons do communicate (directly/indirectly), willfully, to a person they know in a manner that will cause fear towards a person. In addition, it is important that the person knows or ought to know that their conduct will cause such fear.	The communication ought to be **willfully**. Also, the Act provides a leeway for a person to justify whether they knew their conduct could result towards a certain outcome, in this case cyber harassment.
Cybersquatting	This occurs when one intentionally uses a name, business name, trademarks, domain name among similar information and use them as their own without seeking permission	There is an element of **intention** that has to be established. Such issues have been highly referred to as Domain Disputes, and have been heavily addressed through the

	– usually through registering a domain name similar to the name, trademark or confusingly similar to the name or trademark, not to mention using it in bad faith.	Uniform Domain Name Dispute Resolution (UDRP) which is as per the Internet Corporation for Assigned Names and Numbers (ICANN).
Identity Theft and Impersonation	When one fraudulently or dishonestly utilizes identification details of a person.	There must be an element of fraud or dishonesty.
Phishing	It occurs when a person sets up and operates a system with the intention to make its users or recipients of certain messages to reveal their identifiers for the system operators to effect their unlawful course or gain unauthorized access.	The key issues are intention to induce, use the personal identifiers for unlawful use or gain unauthorized access.
Interception of electronic messages or money transfer	Takes place when one taps into an electronic messages or money transfer and unlawfully destroys or aborts such processes or systems.	The key word is unlawfully destroying or aborting the process or system.
Willful misdirection of messages	Occurs when one willfully sends a message to a wrong person.	The main areas of focus are **"willful"** and **"wrong person"**.
Cyberterrorism	Takes place when a person accesses or enables one to access a computer for purposes of carrying out a terror attack.	It is a strict liability provision. The lack of intent does not matter.
Inducement to deliver electronic message	When a person persuades anyone in charge of electronic devices to deliver any electronic message not meant for him.	The key words are: persuade, in charge of electronic devices, and delivery of messages not meant for that person.
Intentionally withholding message delivered erroneously	If a person, intentionally hides or detains any electronic mail, message, electronic payment, credit and debit card that was found by that person or delivered by mistake.	One must **intentionally hide or detain** and must be the person who **found it** or was **delivered** to the person.
Unlawful destruction of electronic messages	When one unlawfully destroys or aborts any electronic mail or processes through which money or information is conveyed.	The act is basically unlawfully. What is unlawful is as per the Act or basically any other law concerning computers.
Wrongful distribution of obscene or intimate images	Occurs when a person transfers, publishes, or disseminates, including presenting it in digital format for	The Act makes the objective of the provision quite wide as it uses the term "**including"**.

	distribution or downloading of the images.	
Fraudulent use of electronic data	It involves deletion or distortion of information; misrepresentation; intend to defraud, franks electronic message, instructions, etc.; manipulation of a computer, among others.	It is a combination of other factors already addressed by the Act.
Issuance of false e-instructions	Any individual who uses a computer or an electronic device for financial transactions, and issuance of electronic transaction will be held liable if the individual issues false e-instructions.	It is a strict liability provision.
Reporting of cyber threat	A person operating a computer system is required to report any case of cyber-attacks of whatsoever nature.	Creates an obligation for the Chief Technology Officers (CTOs) among other persons holding similar positions to always report cases of cyberattacks.
Employee responsibility to relinquish access codes	Based on the employer-employee contract separation clause, the employee is expected to give up their rights to computer networks or systems. Nevertheless, the provisions of the Act will supersede.	The process is guided by the law save where a contract provides otherwise.
Aiding or abetting in the commission of an offence	Occurs when a person knowingly and willfully assists commission of any offenses in the Act.	The key element is **"knowingly"** and **"willfully".**
Offences by a body corporate	Any offense, under the Act, committed by a corporate will be pinged on the respective office holders unless they prove that they exercised caution to prevent such an offense from taking place.	It provides room for the employees to act as per the law and not hide behind the corporate veil/ personality – to a certain degree.
Offences committed through use of computer systems	When a person commits an offense under a different law but with the use of a computer, the person will also be punished through this Act separately.	This is not an alternative but concurrent punishment to that provided by another law.

THE TEAM

J.B. Ong'anya, Litigation Advocate.

Sophia Khalid, Solicitor (the U.K.) – Strategic Legal Consultant.

Ombo Malumbe, Strategic Legal Consultant.

J.B. Ong'anya & Co. Advocates
Windsor House, 4th Floor,
Muindi Mbingu Street/ University Way
P.O. Box 15598 – 00400
Nairobi

m: (+254) 0724 026355 or 0711 185 636