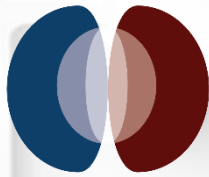




Comments concerning the Data Protection Regulations (KE)



ONG'ANYA OMBO
ADVOCATES

INTRODUCTION

We refer to the call for comments concerning the draft Data Protection (General) Regulations, Data Protection (Registration of Data Controllers and Data Processors) Regulations, and Data Protection (Compliance and Enforcement) Regulations, 2021.

We have invaluable knowledge and experience on data and privacy Law considering our successful track record in advising foreign undertakings on application and navigation on matters data laws including but not limited to African Union Convention on Cyber Security and Personal Data Protection; Budapest Convention on Cybersecurity; Data Protection Act (KE); Data Protection Act (UK); General Data Protection Regulation; Privacy Shield; and California Consumer Privacy Act.

DATA & PRIVACY LAWS

LEARNING FROM HISTORY

We initiate our comments by requesting the Commissioner, with other relevant Government Agencies and Branches, to consider reviewing the approach of the Official Secrets Act on the access of data by learning from Huawei's Case. The People's Republic of China requires that every private company have a Government representative, particularly appointed by the Communist Party of China (CPC), who takes an active role in the private company's Board. In the long run, the practice is one reason why western countries are concerned about the autonomy between the Chinese government and private companies registered in China. In the Republic of Kenya, if a Kenyan citizen gets the opportunity to initiate some of the significant-tech or innovation projects that will span across the globe, it will be near impossible to be entertained by other countries if it is clear that their respective data is easily accessible by a foreign government (herein: Kenya) based on the strict terms of Statute Law Miscellaneous (Amendments) Act 20 of 2020.

While we understand the Government's interests, the same needs to be presented cordially and considering the other stakeholders.

DATA PROTECTION REGULATION, 2021

Reg. 4 (2): The reading of s 32 Data Protection Act (DPA) and Reg. 4 (2) Data Protection (General) Regulations (DPGR) creates a vague approach of Consent and Processing of the Subject's data.

The application of s 32 (3) of the DPA needs to be expanded through the DPGR to resolve an apparent vagueness in the primary legislation considering it is yet to fully come into effect or complied with by data controllers or processors. The withdrawal of consent by a Subject can refer to all data (currently or previously collected). However, the DPA only focuses on the current request for consent. Considering most undertakings have a high disregard of data and privacy laws, it is essential to lockout rogue data collectors' chances of retaining the unlawfully collected information based on new consent.

Reg. 4 (4) provides that the consent can be issued orally. It is evident that circumstances requiring oral consent are foreseeable and will result in abuse of the model of issuance of consent by a Data Subject. In this instance, a data subject, collectors, or processors are likely to benefit and suffer in the following ways:

1. A Data Subject may state that no consent was issued since the Data Controller/Processor must establish that consent was given. It will likely be penalised for not being able to establish oral consent.
2. Data Subject's data may be collected unlawfully, and the Data Controller/Processor may rely on oral consent.

Reg. 5 (1): We propose the replacement of the conjunction "and" with a disjunction "or" that is between Reg. 5 (1) (d) and (e). Our reason is based on the fact that each of those ways of collecting data can occur separately and not necessarily in conjunction. Data Collectors or Processors are likely to breach the law by using one style of data collection unlawfully and claim that since it was not in conjunction with the remaining four styles, there is no breach of law.

Reg. 5 (3): The regulations approach on connected "new purpose" ignores the possibility of a continuum. It is prudent that Data Processors and Collectors issue a notice to seek consent as the "new purpose" is entirely new from the initial contract between the Data Controller or Processor.

Reg. 6 (3): To restore the meaning of Reg. 6 (3) (d), it requires revision from "(d) notify any relevant third party where personal data subject to such restriction may have been shared." to "(d) notify any relevant third party where personal data, subject to such restriction, may have been shared."

Reg. 6 (4): Considering that "may" means discretionary while "shall" or "will" means mandatory, the use of "may" in Reg. 6 (4) indicates that a Data Processor or Controller has the discretion to apply any of the restriction measures – or even disregard the application of any.

As a result, Data Processors or Controllers have the liberty to disregard the restriction – whether legitimately or illegitimately.

Reg. 7 (7): Reg. 7 (5) needs revision considering it does not make sense why the person (Data Subject) who wants to object to the processing of his/her data has to demonstrate that there are ***compelling legitimate grounds for the processing, which override the interests, rights, and freedoms of the individual; or (b) the processing is for the establishment, exercise or defence of a legal claim.***

Reg. 8 (4): The Commissioner may consider revising the drafting of the regulations barring an owner of the data from requesting their data considering that while some of the grounds are close to being reasonable, most are one-sided – and more Data Processor or Collector centred.

There is a high chance that less than 10% of Data Controllers or Processors will comply with the data access request.

Part III concerns the possible interaction between the DPA, DPGR, and Computer Misuse and Cybercrimes Act (CMCA). The opt-out options are mostly automated; therefore, considering that CMCA also addresses the infrastructural systems (hardware and software); how will the Commissioner ensure that Data Processors and Collectors have infrastructures that are first (a) safe to keep the data collected or being processed and (b) opt-outs are respected.

We have encountered many scenarios whereby Data Processors or Collectors send marketing data even after unsubscribing (whether one subscribed or not).

Therefore, there is a need to adopt an enthusiastic approach to the opt-out modalities since it is more than what is provided on paper in black and white and Data Processors or Collectors indicating "**to opt-out do this...**", "**to unsubscribe...**" or "**select your preferred...**" but more of functional infrastructural systems.

Reg. 18 (1): There is a need to have data classified in various categories to allow the Data Subject and Data Processor or Collector to refrain from a conflict. For instance, some laws require storage of certain type of data to a maximum of six years. In that regard, the type of data ought to be relevant to the need to store such information and no other unrelated data.

Reg. 19: In the real and practical world, the concept of data anonymity or pseudonymity is a fallacy. However, for purposes of legitimate interests and in line with CMCA, it is essential to note that anonymised and pseudonymised data still has direct links to the Data Subject. Therefore, when a publisher accesses advertising companies' advertising portal, pick consumer-focused tags under interests, demographics, among others, to target specific users. These data trigger advertisements to reach the owner of the anonymous or pseudonymous data.

Therefore, is this provision a mere paperwork, or are models used to ensure that it is used. For instance, anonymous or pseudonymous data for purposes of analytical presentation is reasonable but not on matters marketing.


Reg. 20: Sharing of personal data occurs in various instances, for instance, associated companies (meaning of associated: Companies Act, 2015), interoperable systems (change of servers, data centres, cloud solutions, among others), mergers & acquisitions, among others.

In reference to Reg. 20 (6), the term "organizational structures" is broad considering what amounts to "corporate structures" or "associated companies." Transfer of data or the possibility of transfer of data must be disclosed at the earliest time possible and, if it arises at a later date, new consent must be requested.

Company A, dealing in asset management services, needs permission to send a Data Subject's data to Company B, dealing in insurance services – regardless of the two companies being owned by the same person or individual.

Further, in reference to CMCA, the Commissioner needs to consider the concept of authorised personnel handling of data in unauthorised manner. The DPA and CMCA need to be realigned to avoid conflict during the application on unlawful sharing of personal data.

Reg. 28 & 29: It is a fact that the development of law may lead to borrowing a leaf from other jurisdictions. However, countries tend to have other influential nonmarket factors that need to be considered in that process. The regulations were not localised to consider the possibility that some individuals lack the chance to be given the notice and, if notice is through email or electronic gadgets, most users do not have the essential devices to allow them to read the policies or notices.



It is a fact that in most instances, Data Subjects do not read these policies. However, this culture should not be used to deny the Data Subject a chance to receive the notice (**digital**: directions or links – considering that most companies know the type of gadget being used to reach out to them; and **physical**: there needs to be directions on where the Data Subject can access, read and even retain a copy of the policies). A good example is the gambling industry; a Data Subject is hardly aware of these notices and how maliciously the same may be applied.

In consideration of the CMCA and DPA:

Recently, the United Kingdom considered that a company's software glitch could not be a ground to deny payment to the winner in gambling activities. However, many Data Subjects win in Kenya, and the companies claim software glitches, resulting in denying them the winnings. Thereafter, the companies (Data Collectors and Processors) process these people's data for marketing purposes and deny them access to the platform – based on the policies and continue to market their services to those people.

Reg. 31, 32, 33, & 34: The Commissioner will need to conduct several events to educate most businesses on the need to consider upgrading their respective systems (hardware and software) to enhance integrity, confidentiality, and availability. Most private entities, including Government Agencies, have shown a low level of concerns about this Regulation's principles.

DATA PROTECTION (REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS) REGULATION, 2021

Reg. 4 (b): Issues about employees and data under Regulations and the DPA indicate a high level of confusion or disregard for employees and data. The s 72 of the DPA fails to acknowledge that even an authorised employee is likely to access unauthorised (an independent offence) and uses the unauthorised accessed data (a separate offence).

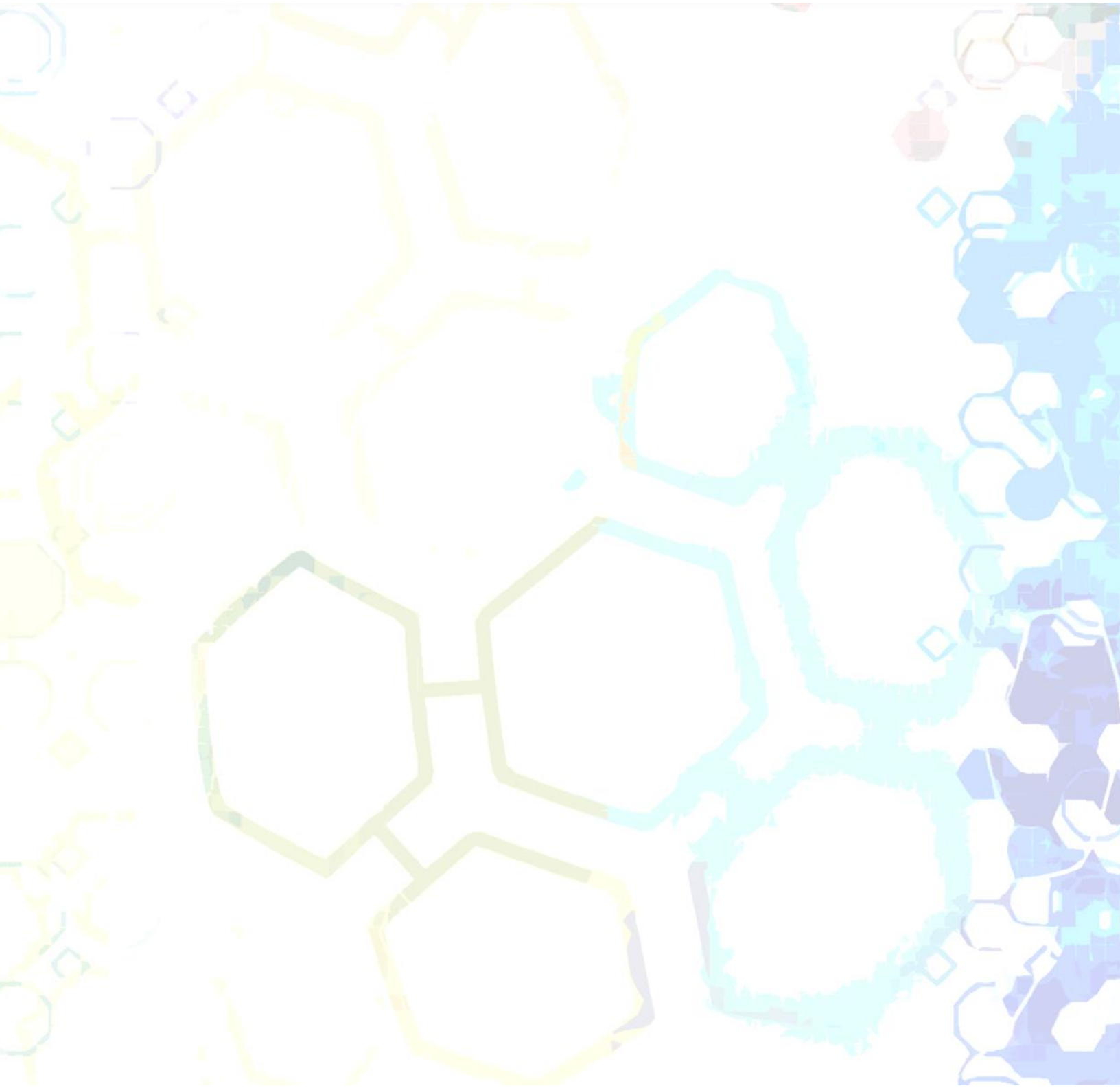
In the draft Data Protection (Registration of Data Controllers and Data Processors) Regulations under Reg. 4 (b), the Reg. disregards the classification of employees as individuals who need protection on what data the employer may collect and process, and how employees can play a major role in protecting or violating the data.

Reg. 7 & 11: We note that Reg. 11, referred to as under Reg. 7, takes a stringent position about compliance during the registration and verification of Data Controllers or Processors, which is commendable. However, the provision seems to disregard the provisions of Article 47 of the Constitution and the Fair Administrative Action Act of the laws of Kenya.

Reg. 12: There is a need to define the phrase "wholly or mainly in marketing" as Reg. 8 references the Third Schedule. There are marketing companies that only focus on providing marketing solutions without necessarily collecting or processing data – the only available data these marketing entities have access to is already collected, processed, and presented as analytics without disclosing any personal data; therefore, it is essential

to provide a definitive approach on how such marketing companies will be affected by the mandatory registration.

Reg. 15 (2): Revise “Fair Administration Act, 2015” to “Fair Administrative Action Act, 2015.”



DATA PROTECTION (COMPLIANCE AND ENFORCEMENT) REGULATIONS, 2021

Reg. 4 (4): The Regulation needs to have specific timelines that the Commissioner's Office will provide a placeholder.

Reg. 6: The Commissioner's Office needs to secure knowledgeable and talented individuals who genuinely understand Data and Privacy Law, capable of deciphering facts (intricate) and law, and apply the law with the required skill.

We have previously interacted with certain two Government Agencies that failed to understand minor issues within their scope of duties.

Reg. 7 & 8: There is a high chance that most data subjects will be negatively affected by these regulations considering the data subject may give up on a case due to frustrations.

Does the idea of settlement consider the infrastructural adjustments that the offending entity must effect or merely taking a specific action as per the complaint by the Data Subject?

Our understanding is that there is a likelihood that the infrastructure of the Data Processor or Controller will require to effect certain adjustments within their respective infrastructure.

Reg. 13: The Regulation is silent on the appeal options for the parties save for the Reg. 18 that provides appellate rights to the Data Processor or Controller as compared to the Data Subjects who are likely to find some decisions of the Commission to be unjustifiable; hence, the need to appeal.

Considering Reg. 18 only accords the Data Controller and Processor right to appeal and fails to offer the same opportunity to the Data Subject, then the law is unfairly discriminatory towards the people that the Data Protection Act, 2019 meant to protect.

NEXT STEPS?

Learn from history.

Localise the legislation.

We hold the opinion that there is a need to have laws and regulations concerning data and privacy. However, considering that the Republic of Kenya is coming late into the event, it is not that highly disadvantaged in learning from other countries worldwide. It is essential that since there are experts on both legal and information technology fronts, and the Government can compensate for their respective services. The Commissioner should align ideas, intended written practices with current and future practical circumstances.

Legislation touching on technology and innovation must consider a past, present, future, and, importantly, practical approach. Also, while taking all those angles, it is essential to appreciate the locality where the intended laws will be applied, which is generally known as localisation of laws.

We encourage the Commissioner to look into how various Government agencies across the world were able to develop local but internationally respected regulations by working hand in hand with persons who had the practical knowledge of the various aspects touching on a specific sector.

General Inquiries:

hello@onganyaombo.com

Strategic Litigation Services:

jb@onganyaombo.com

Strategic Corporate & Crossborder Practice:

om@onganyaombo.com

General Service Category:

1. Strategic Litigation.
2. Alternative Dispute Resolution.
3. Property and Banking Law.
4. Policy Monitoring & Legal Audit.
5. Corporate and Commercial Law.
6. Strategic Legal Consultancy.

Contact:

Ong'anya Ombo Advocates LLP,
4th Floor, Windsor House,
University Way,
P.O. Box 15598 – 00400,
Nairobi, KE.

m: +254 703 672 515

e: hello@onganyaombo.com

w: www.onganyaombo.com