Data Protection In Marketing

By Mududa Tollo

“Personal Data, the new oil, is a strategic asset but there must be ethical boundaries in its processing for marketing purposes. A marketer’s primary concern in data protection is how to mitigate consumer privacy expectations whilst exhaustively exploring and utilizing data available for best marketing strategies.

Abstract

A marketer's primary concern in data protection is how to mitigate consumer privacy expectations whilst exhaustively exploring and utilizing data available for best marketing strategies.

The goal of marketing and using data is to make informed decisions, optimize marketing strategies, and create more relevant and valuable interactions with consumers. Data is a valuable tool for achieving these objectives, as it provides the insights and metrics needed to measure, adapt, and improve marketing initiatives.

Genesis

Data Protection law in Kenya is cemented in the supreme law of the land which is the Constitution. The Constitution was promulgated on 27 August, 2010 and its Article 31 guarantees every person's right to privacy.

This provision stipulates that every person has the right not to have their person, home or property searched, their possessions seized, information relating to their family or private affairs unnecessarily required or revealed or the privacy of their communication infringed.

The Data Protection Act No. 24 of 2019 (hereinafter referred to as "the Act") was enacted on 25 November, 2019 pursuant to the aforementioned Article 31 of the Constitution.

The Act at Section 5 established the Office of the Data Protection Commissioner and the Data Protection Commissioner as its head and accounting officer. She oversees enforcement of the Act and maintains a register of data controllers and processors and is mandated to promote self-regulation among data controllers and processors.

Nexus between marketing and data protection

In examining data protection in marketing, it is vital to define what personal data means and differentiate between data privacy and data protection.

Personal Data is simply any information relating to an identified person or identifiable natural person.

Sensitive personal data is any information on a data subject's race, health status, ethnic social origin, genetic data, biometric data, sex or sexual orientation of the consumer, spouse or spouses, marital status, a person's children or parents or any family data.

Data privacy concerns who has access to that data but data protection lays emphasis on the tools, policies and mechanisms employed to restrict access to data.

The Act does not expressly refer to marketers just as it does not expressly refer to other professionals but the Third Schedule of the Data Protection (General) Regulations, 2021 which was gazetted on 14 January, 2022 lists businesses that are wholly or mainly in direct marketing as amongst those that shall mandatorily register as data controllers and processors.

Data Controller and Data Processor

A data controller is defined as a natural or legal person, public authority or entity which alone or jointly with others determines the purpose and means of processing of personal data while a data processor is a natural or legal person, public authority or entity which processes personal information for a data controller.

Data Subject

A data subject is an identified natural person whose data is the subject of personal data.

This definition of data controllers and data processors gives the Data Protection Commissioner a wide latitude in application and enforcement of the Act.

We will for purposes of this article presume marketers to be data controllers and processors and consumers the data subjects.

Moreover, Paragraph 14 of the Data Protection (General Regulations), 2021 defines what constitutes commercial use of data in direct marketing. It is where data or personal information is used to advance economic interests by sending a catalogue through any medium addressed to a data subject, displaying an advertisement on an online media site where a data subject is logged on using their personal information, and advertisement in the form of sending electronic messages to data subjects using their personal information.

It further states that marketing is not direct where personal information is not used to identify recipients.

Implications of data protection

Personal Data, the new oil, is a strategic asset but there must be ethical boundaries in its processing for marketing purposes. There must be interest in this subject by marketers for the following reasons:

(a). The law requires a marketer to practice within the confines of the Data Protection Act No. 24 of 2019. A statutory breach may culminate in the imposition of an administrative fine not exceeding five million shillings or to imprisonment for a term of not more than two years or both.

A data controller or processor who uses personal information for commercial purposes without the consent of a data subject may upon conviction be fined a sum not exceeding twenty thousand shillings and to imprisonment for a term not exceeding six months or to both as stipulated in the Data Protection (General Regulations), 2021.

(b). Respecting privacy can enhance consumers' trust in marketers and their products which may lead to a more accurate feedback.

(c). Better data quality that is accurate and up-to-date.

(d). Adhering to data protection laws and principles can improve a company's data management model.

(e). It can save the company's time and costs that may be expended in man hours needlessly incurred in the defense to complaints lodged with the data protection commissioner by data subjects.

(f). Consumers want their privacy respected. In the year 2015 research conducted by EMC2 Corporation in fifteen countries found that 87 per cent of respondents supported data protection legislation to prohibit trading of their data without consent. The Constitution of the Republic of Kenya which is the anchor of data protection was approved by 67% of Kenyans in the referendum before its promulgation on 27 August, 2010 as aforementioned.

(g). Less risks of data breaches and cyberattacks.

(h). Minimizes potential harm or distress to consumers. This ought to be a marketer's first reason for compliance with consumer privacy expectations.

Consumer expectation

In aspiring to acquire the capacity to protect privacy rights a marketer has to first identify privacy expectations of a consumer in any given circumstance and interpret applicable laws or principles.

Prediction of all possible infringement matrices is not viable but a marketer can foresee actions or omissions that have formed notoriety in daily function with the objective of introspectively weighing as to whether an action or omission may be acceptable to consumers.

Instances of routine daily privacy intrusion include receipt of unsolicited electronic mail and telephone calls and unauthorized use of photographic images for commercial gain.

Predictive analytics and data mining are less visible but possibly have a greater negative impact on an individual's health as tools of commercial manipulation.

Online marketing has gained considerable traction as a major part of direct marketing. Assessment of probable intrusion or illicit marketing is both factual and legal and can be properly made with appropriate training.

The level of privacy expectation is dependent on various factors which includes cultural background.

It can be argued in given circumstances that privacy expectation by a consumer can range from expecting her banker not to introduce a new product in a telephone call whose purpose was to address an administrative issue on the status of her bank account.

It can be surmised that a consumer's least privacy expectation is in the law as the two are intertwined.

How marketers can address consumer privacy rights

Paragraph 15 of the Data Protection (General Regulations), 2021 permits commercial use of personal data for direct marketing, but not sensitive personal data. Direct marketing is allowed where:

◊ The data has been collected from the consumer.

◊ The consumer is notified that the collected data will be used for direct marketing.

◊ The consumer has consented for the use of her personal data for direct marketing.

◊ There is a simplified opt-out mechanism provided by the marketer for the consumer to request to not receive direct marketing communications.

◊ The consumer has not made an opt out request.

A marketer is obligated under the aforesaid regulation to develop a function in transmitted messages to the consumer in direct marketing enabling her to request for the restriction of the messages without incurring charges.

When initiating communication in direct marketing to a consumer a marketer ought to disclose its identity and a valid address to which the consumer can send a request to have the communication ceased.

Transmission of communication in direct marketing is not permitted if the marketer has initiated an automated calling system without human intervention.

Opt out requirements

Paragraph 17 of the regulations require the consumer be given the ability to opt out from future direct messages by simply responding to a direct marketing message with a single word instruction. A marketer must provide a link prominently located in the email to take the consumer when she wishes to subscription control centre. Consumers must also be verbally informed that they can opt out from future calls and marketers should list instructions guiding consumers on how to opt out.

Similarly, the Kenya Information and Communications Act (Consumer Protection) Regulations at Regulation 17 prohibits unsolicited communications. All communications in direct marketing presuppose consent. Use of automated calling systems without human intervention, facsimile or electronic mail for direct marketing without the consent of the subscriber constitutes an offence.

The same provision states that electronic mails cannot be sent without disclosure of the identity of the sender or on whose behalf the communication has been made. The recipient must have been given in the communication from the sender an address to which she may request that the communication should cease.

The consumer or subscriber must also be given the opportunity to object without any financial charge and in a simple manner to the use of her data at the point of collection of the data or on the occasion of each message where there was no initial objection.

The opt-in principle must be adopted in all automated direct-marketing schemes. Subscribers must be rendered the opportunity to accept or reject inclusion in a marketer's mailing list.

Retention of personal data

Upon collection of personal data, a marketer should prepare a data retention schedule with appropriate time limits for periodic review that considers storage needs for a time that is not longer than what is necessary as determined by the purpose of collection after which the data must be erased and deleted even for anonymized and pseudonymized data.

The aim for the review is to assess whether the retained data is accurate, identify appropriate security measures and plan for the procedure to be followed when the retention period lapses.

Data Protection Policy

Marketers must develop and publish a data protection policy that details data handling procedures.

The policy should contain data handling procedures including complaints mechanism, identify the nature of data collected, state how a consumer can access her personal data and provide requirements where data is to be transferred outside the country, to third parties or other data controllers and processors, and specify such recipients. If the above is adhered to then the direct marketing is considered licit.

Unacceptable, illicit, privacy-intrusive, manipulative marketing is what consumers need to be protected from by marketers in online and offline business practices. Manipulative marketing is one that targets and exploits an individual's cognitive, emotional and decision-making vulnerabilities and is hidden or not transparent. Exploitation may be based on personal characteristics of consumers,

Safarilink

Fly Safarilink and Get

5% Discount to MOMBASA

Book online at www.flysafarilink.com

Promo Code: **MA**

Terms and Conditions Apply

Safarilink operates daily flights to Amboseli, Chyulu Hills, Diani, Kisumu, Kisumu, Kilimanjaro, Lamu, Loisaba, Lewa Downs, Maasai Mara, Migori, Mombasa, Malindi, Naivasha, Nanyuki, Samburu, Tsavo West and Zanzibar.

020 6690 000 | 0730 888 000

www.flysafarilink.com

power characteristics of marketers or vulnerability indicators.

Personal characteristics may go as far as exploiting someone's mental illness or age. The consumer in this instance is unable to protect herself from online messages nor realize the implication of this form of marketing which consists of aggressive communication, undue influence, deception that is fostered by predictive analytics and machine learning. A marketer's role in manipulative marketing may be intentional or unintentional but remain accountable in both occurrences.

Profiling and predictions can tell a person's location, movement, behavior, interests across different websites and devices all these made conceivable by use of advanced technology.

Automated processing including profiling can cause significant effects on a consumer such as affecting the circumstances, behavior or choices of the consumer; have a prolonged or permanent impact on the consumer or cause the exclusion or discrimination of individuals. This removes freedom of choice.

When initiating communication in direct marketing to a consumer a marketer ought to disclose its identity and a valid address to which the consumer can send a request to have the communication ceased. Transmission of communication in direct marketing is not permitted if the marketer has initiated an automated calling system without human intervention.

The elderly, children and those suffering from mental illness may not withstand illicit marketing which unpleasantly relies on processing of sensitive personal data. Profiling of a child is prohibited.

A marketer's risk of infringing consumer privacy rights starts at the point of processing personal data. Marketing is at a high risk of infringing fundamental rights and freedoms of consumers when:

» Automated profiling analyses personality and causes significant effects on individuals.

» In large scale data processing of personal data.

» Systematic monitoring of a public accessible area.

Personal data and even non-personal data when processed without transparency with use of advanced analytical tools and target practices ultimately leads to predictive profiling, systemic monitoring of data subjects and target vulnerable groups.

A consumer's least privacy expectation is certainly in the law and marketers can mitigate illicit marketing by:

(i). Complying with provisions of the Data Protection Act No. 24 of 2019.

(ii). Investing in consumer knowledge for a more defined privacy expectation tailored to the marketer's product which would lower the consumer privacy expectation and make it less demanding to fulfill for a marketer.

Principles of Data Protection

The Act provides that the Data Commissioner may carry out periodical audits of the processes and systems of a data controller and data processor to ensure compliance with the Act.

Marketers are expected to formulate appropriate organizational measures where the transmission of data is over an information and communication network. The technological development available, cost of implementing the security measures, nature of the data processed and the special risks accompanying the process are factors to be considered in developing an organizational measure.

Data must be collected and processed with the legal obligation of the marketer in mind. We should mention some of the principles listed at Section 25 of the Data Protection Act that guide marketers when processing personal data.

(1). Lawfulness, fairness and transparency in processing data.

Consent is the most common element of a legal basis for processing data. It must be freely given, not conditional and unambiguous. An avenue that offers real choice to the consumer must be exercised and the consumer informed of her rights before giving consent.

Where the consumer is a child, the child's guardian or parent must give the consent. A mechanism should be installed for age verification and consent before processing personal data. If consent is not asked the marketing is deemed illicit and privacy-intrusive.

Online behavioral marketing is based on automated profiling, this can only be cured by an explicit consent.

Consumers must be informed of the use to which their personal data will be put, have the right to access their personal data that is in the possession of the marketer, object to the processing of all or part of their personal data or have the data collected directly

from the consumer unless authorized to do so or where she has intentionally made the personal data public.

Consumers should be informed whether their data will be shared with third parties and of their right to withdraw consent. Marketers must respond to any consumer rights requests.

Data processing must be lawful, for instance, it cannot be based on sensitive personal data. As aforementioned sensitive personal data is any information on a data subject's race, health status, ethnic social origin, genetic data, biometric data, sex or sexual orientation of the consumer, spouse or spouses, marital status, a person's children or parents or any family data.

Section 45 permits processing of sensitive personal data in limited circumstances if the consumer permits it or is done in the course of legitimate activities by a foundation or a not-for-profit organization, religious or trade union or in the defense of a legal claim.

Data on health may only be processed by a health care provider or under professional secrecy.

The fairness principle aims at preventing an unfair imbalance in the relationship between a marketer and consumer. Power imbalance can be a situation that affords a consumer a higher risk of suffering from adverse effects while the marketer has the informational dominance or institutional hierarchy.

(2). Personal data must be collected for specific and legitimate purposes only.

The data requested should be sufficient to fulfill the purpose and not excessive. A rational link between the data and objective ought to be established.

(3). Explanation required from the marketer to the consumer where information requested concerns family or private affairs.

The Act provides that data subjects must be given reasons as to why their private affairs need to be disclosed by them before collection of such data by a marketer and request for the consumer's consent for the collection.

(4). To keep accurate and up-to-date data

A marketer has the duty to notify consumers that they have the right to correct any information stored by the marketer that is misleading or false and request for deletion.

(5). To keep personal data in a form which identifies the consumer for no longer than is necessary and only for the purpose for which it was collected.

(6). To not transfer data without proof of adequate safeguards or consent from the data subject.

Anonymization of data is one of the ways that data can be kept in an appropriate form especially where it is foreseen that the marketer intends to keep the data for a long time as authorized by a consumer. Anonymization is the removal of personal identifiers from personal data so that the consumer's information is no longer identifiable. Section 37(2) of the Act provides that where the personal data collected is for commercial purposes it shall where possible anonymize the data so as to no longer have the data identifiable.

Encryption may also be used in keeping personal data in an appropriate form that fits the use. It is the process of converting the content of any readable data using technical means into coded form.

Pseudonymization is where personal data is processed in such a manner that it can no longer be attributed to a specific data without the use of additional information and such additional information is kept separately and is subject to technical and organizational measures.

> **"In aspiring to acquire the capacity to protect privacy rights a marketer has to first identify privacy expectations of a consumer in any given circumstance and interpret applicable laws or principles. It can be surmised that a consumer's least privacy expectation is in the law as the two are intertwined.**

Data Protection Impact Assessment

Marketers are obligated to assess any intended processing of data with the aim of establishing whether the risk involved in the exercise might compromise consumers' rights to privacy. The nature, magnitude and purpose of an intended operation should inform a marketer whether an impact assessment is necessary.

By law as stated at Section 31 of the Act, the data protection impact assessment involves a systematic description of the intended processing operation, the necessity and proportionality, the risks attached to the process and the security measures and mechanisms proposed to mitigate identified risks.

If the assessment report discloses a high risk to consumers' rights and freedoms the marketer is obligated to consult the Data Commissioner or simply stop the processing if there are no available specific mitigation measures. The Data Commissioner must receive the data impact assessment report within sixty days prior to processing of data by the marketer.

In essence, what should a marketer do to comply with consumer privacy expectation and data protection laws?

(a). Minimize processing of personal data and pseudonymize where and as soon as possible.

(b). Be transparent in the processing of personal data.

(c). Formulate and implement policies, structures, processes and measures both technical and organizational that include staff training that adhere to data protection principles and achieve reasonable and acceptable security features but tailor them to your circumstances, gradually.

Ray Mududa Tollo is the Managing Partner at Omulele & Tollo Advocates. You can commune with him on this or related matters via mail at: Tollo@ot-advocates.com.