September 12, 2018

Review Of The Data Protection Bill 2018

Introduction

On 3rd July 2018, the Data Protection Bill **(the "Bill")** was introduced to establish a comprehensive data protection regime in Kenya. The principal object of the Bill is to protect personal data collected, used or stored by both private and public entities. The Bill recognizes that data protection forms part and parcel of the expectation of the right to privacy. It provides for the legal framework for protection of a person's privacy in instances where **personal information** is collected, stored, used or processed by another person.

Once enacted, the Bill will give effect to **Article 31(c)** and **Article 31(d) of the Constitution of Kenya 2010**, which guarantees the right of every person not to have "information relating to their family or private affairs unnecessarily required or revealed" and the right not to have "the privacy of their communications infringed". In keeping with Article 24 (1) of the Constitution, the Bill provides that the right to privacy will be limited for the following purposes: protection of national security and public interest, prosecution of a crime, protection of the rights of others and for compliance with an obligation imposed by law.

Apart from the Constitution, the current laws regulating the collection and use of personal data in Kenya include; the **Access to Information Act (No. 31 of 2016),** the **Kenya Information and Communications Act (No. 2 of 1998)** and the **Consumer Protection Act (No. 46 of 2012).**

The Bill follows the path taken by the European Union in enacting the **General Data Protection Regulation ("the GDPR")** in May 2018 and makes Kenya the second country in East Africa after Rwanda to have a legislation dedicated to data protection. The GDPR has been hailed as the first step in checking the excesses of powerful technology firms that collect vast amounts of personal data from their users for commercial or competitive advantage.

Kenyan firms that transact business with any of the 28-member EU bloc countries will be expected to adapt to the new legislation. Any company that processes the data of an EU member state citizen or temporary resident, has employees based in an EU member state, offers goods or services in an EU member state or has a partnership with an EU business falls under the law.

Definitions

"Personal data" is defined in the Bill to mean information about a person relating to the race, gender, sex, pregnancy, marital status, national ethnic or

social origin among others. It may also mean information relating to the educational, medical, criminal or employment history or information relating to financial transactions in which the person has been involved in. It may also include contact details/telephone numbers of the person or his/her opinions about another person and any information given in support or in relation to a grant or award.

An ***"Agency"*** means a person who collects or processes personal data; and in our circumstances, includes law firms or lawyers.

A ***"Data Subject"*** is defined in the Bill to mean a person from whom personal data is obtained.

"Processing" means collection, organization, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or any other means, alignment, combination, blocking, deletion or destruction of information or data.

Application of the Bill

The Bill applies to any person who collects or processes personal data. This includes public and private entities with an exception of public bodies processing personal data which involves national security or used for the prevention and combating of money laundering activities will be exempted from the Bill.

The Principles guiding data protection

The Bill sets out the following data protection policies:

Information shall be collected, processed, stored or dealt with in any other manner if it is necessary for or directly related to a lawful, explicitly defined purpose and shall not intrude on the privacy of the data subject;

Information shall be collected directly from and with the consent of the data subject;

Where information relating to the data subject is held by a third party, the information may only be released to another person or put to a different use with the consent of the data subject;

The data subject shall be informed of the purpose to which information shall be put and the intended recipients of that information at the time of collection;

Information shall not be kept for a longer period than is necessary for achieving the purpose for which it was collected;

Information shall not be distributed in a manner that is incompatible with the purpose for which it was collected with the consent of the person and subject to any notification that would attract objection;

Reasonable steps shall be taken to ensure that the information processed is accurate, up-to date and complete;

Appropriate technical organizational measures shall be taken to safeguard the data subject against the risk of loss, damage, destruction of or unauthorized access to personal information; and

Data subjects have a right of access to their personal information and a right to demand correction if such information is inaccurate.

The rights of data subjects

The Bill provides for the rights of data subjects in relation to their personal information. These include;

Right to be informed by the agency of the use to which the data is to be put;

Right to access their data which is in possession of an agency;

Right to object to the collection or processing of all or part of data by an agency;

Right to correction of false or misleading data;

Right to deletion of misleading, false or data which has been objected to;

Right to information relating to the person processing the data and any other person to whom the data is to be transmitted;

Right to know the place and origin of the data; and

Right to an explanation in respect of the processing of data and the outcome of such processing.

Duties of companies and other agencies

The Bill sets out various duties of companies and other agencies collecting or processing personal data. These include, the duty to;

Notify the data subjects of the fact that their information is being collected and the purpose for which the data is being collected, the contact details of the company and intended recipient of the information, the consequences of failure to provide the required information and their right of access to and correction of the data collected.

Not to profile data subjects based on the information collected or processed unless the information was collected for purposes of maintaining law and order by any public body.

Adopt the necessary measures to ensure protection and security of personal data i.e. by identifying foreseeable internal and external risks and establishing, maintaining and updating appropriate safeguards against identified risks.

Observe generally acceptable security practices and procedures including specific industry or professional rules and regulations.

Notify the data subject and the Kenya National Commission on Human Rights of any security compromises i.e. where personal data has been accessed or processed by unauthorized persons.

Take the necessary steps to restore the integrity of their information system where personal data has been compromised.

Correct, delete or destroy false or misleading data upon request (in writing) by the data subject. The company must consider the request and inform the data subject of the decision within seven days of receipt of the request.

Not to use personal data for commercial purposes without the consent of the data subject or unless authorized by law.

However, there are circumstances under the Bill where companies and other agencies will not be required to obtain the consent of the data subject when retrieving or processing data. These include; where the information is publicly available, where the user has authorized the collection of the data from a third party or where non-compliance does not prejudice the interests of the user or where the information being collected is meant to help detect or prevent a crime or threatens national security.

Transfer of personal data

The Bill prohibits transfer of personal data of a data subject to other jurisdictions unless: the transferee is subject to a law or agreement relating to protection of personal data (such as the GDPR), the data subject consents to the transfer, the transfer is necessary for the performance of a contract between the agency and the transferee, and the transfer is for the benefit of the data subject. The criteria must be met for the transfer to be valid.

Processing of special personal information

The Bill prohibits processing of special personal information and data relating to minors. ***Special personal information*** includes information

relating to the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health, biometric information of a data subject or relating to the alleged commission of an offence or any proceedings in respect of any offence allegedly committed by a data subject.

Such information may only be processed in the following circumstances:

With the consent of the data subject, parent or guardian

Where it is required under national or international law or for the purpose of statistical or research purposes or when it is publicly available.

For information relating to the religious or philosophical beliefs, the agency is a spiritual or religious organization and the data subject is an employee/member of the organization who has consented to the processing of the data.

For information relating to a data subject's race or ethnic origin, data processing it is essential to the identification of the data subject and is not aimed at discriminating the data subject unfairly.

For information relating to trade union memberships, the agency is a trade union to which the data subject belongs and the processing

For information relating to health, the agency is a medical or social service institution, insurance company or a medical scheme, a school, a public or private body acting under a lawful duty to manage the welfare of the data subject or an administrative body, pension fund or employer processing data for purposes of implementation of the law relating to the health of the data subject.

For information relating to political persuasion, the agency is a political party formed under the Political Parties Act or a public body whose functions are political in nature and the data subject is a member of the agency and the information is necessary to the formation or carrying out of the agency's activities.

Enforcement of the Bill

Under **Part IV of the Bill,** the Kenya National Commission on Human Rights (established under **Clause 3** of the Kenya National Commission on Human Rights Act) will be the institution responsible for oversight and implementation of the Bill, including investigating reports on the observance of the right to privacy and providing a framework or mechanism for the effective management of conflicts and the resolution of disputes.

All complaints under the Bill shall be lodged with the Secretary to the Commission in writing or orally. Where upon investigations the Commission is satisfied that a person has or may contravene any of the provisions of the Bill (if enacted), the Commission may issue a notice to that person requiring them to refrain from such contravention i.e. requiring the person to rectify, block, erase or destroy any inaccurate data.

Offences and penalties

The Bill creates the following offences and penalties;

Interference with personal data of a data subject or infringement on the right to privacy which will attract a fine not exceeding Kshs. 500,000 or to imprisonment for a term not exceeding 2 years or to both.

Obstructing the Commission or any other person from the performance of their functions without reasonable cause, knowingly giving false or misleading information to the Commission or any other person, failure to comply with any notice issued under the Bill. This will attract a fine not exceeding Kshs. 100,000 or to imprisonment for a term not exceeding 2 years or to both.

Processing of data in any other manner contrary to the provisions of the Bill which will attract a fine not exceeding Kshs. 500,000 or to imprisonment for a term not exceeding 5 years or to both.

The offences and penalties apply to body corporates and any officers responsible for the commission of the offences. Any person who discloses data or publishes disclosed data in good faith pursuant to the provisions of the Bill will be exempt from any civil or criminal liability.

Conclusion

At a time when user information is increasingly at risk from hackers, the Bill will hold entities and persons responsible for data breaches. The recent Facebook data breach that affected 87 million users is a good example of how important it is to protect user information and the implications such data breaches can have on a business.

The Bill will complement the Computer Misuse and Cybercrime Act which protects Kenyans against cyber infiltration, interference, and unauthorized access. This law provides for a fine of up to Kshs.20 million or a ten-year jail term in an effort to curb cyber-criminal activities.

Entities that use of data to operate or enhance their business operaton will need to take stock of this legislation and implement data management systems.

Recommendations

Entities need to invest in awareness and training, continuous monitoring and log analysis, continuous risk assessment, vulnerability and patch management, and independent reviews.

Most importantly, these regulations demand sweeping changes in how organizations must now obtain consents from clients to use their information.

The GDPR demands that such consents must be clear and distinguishable from other matters and be provided in a clear and easily accessible form,

using clear and plain language. It must be as easy to withdraw consent as it is to give consent.

There are five best practices that GDPR will expect organizations to adhere to:

Entities must not re-use or disclose personal information for purposes that do not link back to its original intended purpose. Organizations are required to be transparent with individuals about how their data will be used, under a lawful basis;

Entities will be required to take steps to ensure that personal information is kept secure and backed up through organizational and technical security measures;

Data must only be kept for as long as it is needed – restricting the storage of personal information;

Personal data will need to be accurate. In cases where it is not, corrections must be made. Individuals will have the right to update any of their personal information that is incorrect; and

The collection and storage of any data must be kept minimal; collecting only what is adequate and relevant for the intended purpose.

The GDPR also has a starter guide that includes advice on steps to be taken, such as making senior business leaders aware of the regulation, determining which information is held, updating procedures around subject access requests, and what should happen in the event of a data breach. **[A summary is attached to this document]**

Without a general data protection framework, it is up to entities that collect personal data to employ internal strategies to protect data. Failure to properly collect and use data will expose the entity to risks such as identity theft, misuse of personal information, unauthorized distribution or sale of data, financial loss and erosion of privacy. The data may therefore be

repurposed and used for purposes other than what it was collected for, attracting penalties to be imposed under the Act.n.

To achieve a people centered digital economy, it is important for this e Bill is enacted into law so as to ensure that personal data is protected and s to affords the highest protection of privacy for Kenyans.

Return

LATEST NEWS & UPDATES

Impact of Covid-19 on Court Processes

Measures taken BY CBK to mitigate effects of COVID – 19

Mombasa Court Orders Stay of County Rates Increases

MORE UPDATES

WHO ARE WE?

Daly & Inamdar Advocates is a leading Kenyan law firm and a member of the Nextlaw Referral Network and Mackrell International, Top Tier Global Leading Law Firm Networks as ranked by Chambers Global

MORE ABOUT US

AWARDS AND ASSOCIATIONS

FOLLOW US

ADDRESS & CONTACTS

Nairobi Head Office

ABC Towers, ABC Place, 6th Floor

Waiyaki Way

P.O. Box 40034

Nairobi-00100

Tel: (+254) 20 – 4297000 or 0711064000

Fax: (+254) 20 – 4448907

Mobile: (+254) 722/734 – 310304

Mombasa Office

Sea View Plaza, 1st Floor

Mama Ngina Drive

P.O. Box 80483

Mombasa–80100

Tel: + 254 (0) 716 430 651, 734 606 070 202 443 829

DROP US A LINE